Quantum complexity, simulation, and random access memory

A Dissertation
submitted to the Faculty of the
Graduate School of Arts and Sciences
of Georgetown University
in partial fulfillment of the requirements for the
degree of
Doctor of Philosophy
in Computer Science

By

Shuchen Zhu, M.S.

Washington, DC
March 13, 2024
Quantum complexity, simulation, and random access memory

Shuchen Zhu, M.S.

Dissertation Advisor: Justin Thaler, Ph.D.

Abstract

Quantum computers can potentially transform the landscape of computing by harnessing the distinct properties of quantum mechanics. In this dissertation, we deepen our understanding of quantum computing, exploring its capabilities, algorithmic design, and hardware architecture. Specifically, we

• show an improved quantum query complexity lower bound for \( k \)-distinctness function;

• give a better analysis of the error bound of the product formula which is used in digital quantum simulation;

• demonstrate two discretization schemes to simulate lattice quantum chromodynamics on quantum computers;

• show a quantum algorithm computing the ground state energy of physical systems with low-depth circuits;

• develop a quantum lookup table architecture that unifies all previous quantum RAM models.

Index words: quantum computing, quantum simulation, quantum query complexity, ground state estimation, QRAM, quantum data lookup, Trotter error, product formula
I owe an immense debt of gratitude to my thesis advisor, Justin Thaler, who welcomed me into the world of theoretical computer science five years ago, at a time when I had virtually no experience. Justin generously shared his ideas and insights, all while allowing me the ultimate freedom to pursue the directions that captivated me the most. Over the years, Justin has remained supportive, attentively listening to every project I’ve been involved in various stages of my research endeavors. He showed me the essence of being an encouraging collaborator, I can barely remember a meeting that didn’t conclude with his uplifting and motivating words. I greatly enjoy our discussions within academia, as well as our broader conversations encompassing various aspects of life. A single paragraph is far from expressing the full extent of my gratitude.

I would like to thank Jeremy Fineman, Sasha Golovnev, and Calvin Newport for serving as members of my dissertation committee. I consider myself exceptionally fortunate to have had the chance to take Jeremy’s algorithm and Calvin’s theory of computation courses, which played a significant role in nurturing my passion for the field of theoretical computer science, and their dedication to teaching will forever serve as a guiding example for me in my future career. Sasha joined the faculty during the COVID lockdown, and I had the privilege of taking the best online class I have ever experienced on matrix rigidity. In the past two years, Sasha has treated me as if I were one of his graduate students, including me in project discussions, reading groups, covering my conference expenses, and even extending invitations to
his backyard BBQ parties. Sasha exemplifies how one can be both intelligent and humorous while consistently showing respect for others.

I would not know anything about quantum information without the inclusiveness of the UMD community. Xiaodi Wu’s quantum information processing class introduced me to the enchanting world of quantum information, which I found to be intriguing as it encompasses interdisciplinary fields such as computer science, physics, and mathematics. I was fortunate to have been included in the Hamiltonian simulation project alongside Yuan Su, Minh Tran, Andrew Childs, and Nathan Wiebe. I would like to extend a special gratitude to Yuan for his exceptional patience in providing detailed explanations during every meeting.

I have been lucky to work with Yao Ji and Henry Lamm, both of whom I had known during our time at ASU, on the quantum simulation of lattice fields, which eventually became an essential component of this thesis. Our meetings were consistently engaging, characterized by not only physics discussions but also impromptu conversations on a range of fun social-economic topics.

I wholeheartedly express my gratitude to Nikhil Mande for generously dedicating a vast amount of his time to mentor me in the proper ways of conducting TCS research. I still feel guilty for not addressing all the comments he made in our shared notes. Nevertheless, his constructive critiques continue to resonate in my mind. Our daily coffee breaks, filled with interesting discussions, on the rooftop of Saint Mary’s Hall will always be remembered.

I have been fortunate to engage in industry internships that have greatly expanded my perspective within the realm of quantum computing and allowed me to delve into in-depth projects. I extend my gratitude to Peter Johnson and Guoming Wang for their hospitality during my internship at Zapata Computing in the summer of 2022. While there, I acquired invaluable insights into the potential of shallow quantum
circuits through collaboration with Daniel Stilck-França and Ruizhe Zhang. I am deeply appreciative of Aarthi Sundaram and Guang Hao Low for hosting me during my internship at Microsoft in the fall of 2022. This led me to contribute to the development of quantum RAM. I learned from their invaluable mentorship on the art of conducting impactful research. I extend my appreciation to Shouvanik Chakrabarti and Marco Pistoia for hosting me as an intern at JPMorgan Chase during the summer of 2023. I gained a substantial understanding of quantum algorithms for optimization tasks. The daily interactions with fellow interns and researchers were always filled with curiosity and energy. I am grateful to Pratik Worah and Renato Paes Leme for welcoming me as a student researcher at Google Research during my final semester at Georgetown. The theoretical machine-learning challenges they guided me through were very interesting. I hope to complete these projects even after my graduation.

I thank individuals I have had the privilege of engaging in discussions with but not limited to: Arithi Acharya, Omar Amer, Abhinav Anand, Brandon Barton, Joao Basso, Yizhuo Chen, Chi-Ning Chou, Wim Van Dam, Nicolas Delfosse, Zhiyan Ding, Di Fang, Erik Gustafson, Katerina Gratsea, Tianyi Hao, Zichang He, Dylan Herman, Tyler Kharazi, Vadym Kliuchnikov, Robin Kothari, Alexander Kunitsa, Jiaqi Leng, Tongyang Li, Changhao Li, Zhiding Liang, Lin Lin, Diyi Liu, Jin-Peng Liu, Hongbin Liu, Minzhao Liu, Di Luo, Edison Murairi, Mariia Mykhailova, Satyajeet Nargaroge, Pradeep Niroula, Raymond Putra, Ojas Parekh, Arthur Rattew, Soo-Jong Rey, Sidhant Saraogi, Rahul Sarkar, Ruslan Shadyulin, Alexander Sherstov, Jiayu Shen, Kaiyan Shi, Zhixin Song, Jesse Stryker, Chong Sun, Yue Sun, Shree Sureshbabu, Mario Szegedy, Yu Tong, Jiasu Wang, Roeland Wiersema, Jue Xu, Romina Yalovetzky, Chao Yang, Cunlu Zhou.

This dissertation would not have been possible without the presence of extremely friendly faculties and graduate students at the GU computer science department. I
always find the company of graduate students to be engaging and never experience boredom when I am around them. This exceptional group includes but is not limited to Laasya Bangalore, Shabnam Behzad, Nairen Cao, Zheng Chai, Rahel Fainchtein, Karthik Gajulapalli, Kornraphop Kawintiranon, Hrishikesh Kulkarni, Sean MacAvaney, Rupayan Mallick, Satyajeet Nagargoje, Sidhant Saraogi, Sajad Sotudeh, Samuel King, Shuo Liu, Yaguang Liu, Jakob Prange, Katina Russell, Jianan Su, Zhiwen Tang, Alex Weaver, Shira Wein, Hao-Ren Yao, Chao Yan, Eugene Yang, Mohammad Zaheri, Ce Zhang, Chong Zhang, Jiachi Zhang, and Zhao Zhang. Having you all around has made my journey significantly less stressful.

On the faculty side, I thank Lisa Singh for her “mandatory” weekly tea time gatherings that bring the entire department together, complete with samosas, cupcakes, tacos, teas, and laughs. I thank Ophir Frieder and Nazli Goharian for their dedicated efforts in hosting graduate student research presentation sessions complemented by free food. I thank Bala Kalyanasundaram and Mahe Velauthapillai for always patiently listening to my ramblings when we routinely bumped into each other in the kitchen during lunchtime. I thank Micah Sherr and Muthu Venkitasubramaniam for their willingness to share their insights on parenting when we have crossed paths either in the department hallway or at Hoya Kids Learning Center. I thank the unsung heroes of our department: Ray Essick and Djuana Shields whose prompt assistance in resolving my administrative issues is deeply appreciated.

I would like to extend my deepest gratitude for the unconditional and enduring support from my family at every phase of this journey, from the very beginning. I express my heartfelt thanks to my wife, Yidan Jin, for her endless love. At last, I thank my son for the happiness he has brought into our family. Every moment spent with you is treasured.
# Table of Contents

## Chapter

1 Introduction ................................................................. 1

2 Quantum Query Complexity of $k$-distinctness Function .......... 3
   2.1 Introduction .................................................. 3
   2.2 Overview of the Proofs ...................................... 9
   2.3 Preliminaries .................................................. 17
   2.4 Outline of Proof of Main Theorem ......................... 30
   2.5 Properties of Auxiliary Functions ......................... 37
   2.6 Proof of Theorem 2.4.4 ..................................... 45
   2.7 An Upper Bound ............................................... 55
   2.8 A Dual Polynomial for Threshold Function ............... 59

3 Analysis of Product Formula ........................................... 65
   3.1 First- and Second-order Error Bound ....................... 66
   3.2 Numerical Confirmation of Higher-order Error Bounds ...... 68

4 Quantum Simulation of Lattice QCD .................................... 72
   4.1 Overview and Results ....................................... 72
   4.2 Group Space Decimation via Strong Coupling Expansion ...... 77
   4.3 Supplement Materials for Strong Coupling Expansion ...... 104
   4.4 Group Space Decimation via Character Expansion .......... 116

5 Quantum Algorithm for Ground State Energy Estimation ........ 134
   5.1 Introduction .................................................. 134
   5.2 Low-depth Ground State Energy Estimation ............... 140
   5.3 Future Directions ............................................ 150

6 Unified Theory of Quantum Data Lookup ............................. 156
   6.1 Introduction .................................................. 156
   6.2 Preliminaries .................................................. 161
   6.3 Naive Construction .......................................... 166
   6.4 General QRAM Framework .................................... 184
   6.5 Large Word Size ............................................. 191
   6.6 Long-range Connections ..................................... 193

Bibliography ............................................................... 207
### List of Figures

4.1 A schematic demonstration of $\Omega$ (in green) of $G$ (a sphere) around $1$ (blue point) of the discrete group (shown as points) ........................................ 82

4.2 Example of two plaquettes $u_p$ and $u_q$ where $p \cap q = u_2 = u_8$ .......... 89

4.3 Average energy per plaquette ................................................................. 91

4.4 $\beta_f$ as a function of $\Delta S^{-1}$, the cycle $C$ of $\mathcal{N}$, and $(1 - V_{\{1\}}^4)^{-1}$ ... 96

4.5 $\beta_f/\beta_s$ as a function of $(1 - V_{\{1\}}^4)^{-1}$ ...................................... 97

4.6 Trajectories of $S^n$ ................................ .............................................. 99

4.7 Average energy per plaquette (character expansion) .................................. 122

4.8 Examples of possible trajectories ............................................................. 133

5.1 Landscape of early fault-tolerant GSEE algorithms .................................. 138

5.2 Tradd-off comparison ................................................................................ 154

5.3 Hadamard test circuit ................................................................................ 155

6.1 High-level description of a quantum router ............................................. 162

6.2 Fan-out architecture .................................................................................. 163

6.3 Bucket-brigade architecture ..................................................................... 164

6.4 SELECT-SWAP architecture ..................................................................... 166

6.5 Bucket-brigade circuit and layout ............................................................. 168

6.6 High-level routing scheme for 16 memory locations ................................. 169

6.7 Qubit layout arrangement of bucket-brigade architecture .......................... 170

6.8 The naive activation sequence ................................................................. 175

6.9 Improved activation sequence .................................................................. 175
6.10 High-level scheme for 16 memory locations. 177
6.11 CNOT router circuit. 178
6.12 Teleportation for routing in and out. 181
6.13 GHZ diffusion circuit. 182
6.14 Abstract view of router arrangement using GHZ state. 183
6.15 Modified scheme to reduce qubit count. 184
6.16 The conditional optimal layout. 200
6.17 Linear router layout. 201
6.18 Linear router circuit. 201
6.19 Pauli error propagation. 202
6.20 Generic optimal scheme. 204
6.21 Parallel read out. 205
6.22 Planar layout for parallel readout. 205
6.23 Sequential read out. 206
List of Tables

3.1 Coefficients of the fourth-order Trotter error bound for Hamiltonians with three summands. 71
4.1 Properties of characters. 86
4.2 Property of character $r$ for a general group decimation. 87
4.3 Numerical values of character $r$. 126
4.4 Parameters of discrete subgroups necessary to study the behavior of $\beta_f$. 127
4.5 Character expansion of $\mathbb{V}$ characters in terms of $SU(3)$ characters, and in trace representation. 128
4.6 Character table for $\mathbb{V}$. 129
4.7 Series expansions of $\beta_r$, $x \equiv \beta/6$ up to $O(x^8)$. 130
4.8 $\beta'_r$ as linear combinations of $\beta_{(\lambda,\mu)}$. 131
4.9 $\gamma_i$ computed in terms of $\beta$ to $O(\beta^5)$ with reparameterization invariance. 132
5.1 Estimated circuit cost savings. 139
6.1 Scalings of prior arts and this work in terms of memory size $N$ and word size $b$. 159
6.2 Error types considered in the fine-tuned analysis throughout this work. 171
6.3 Infidelity scaling for $N = 2^n$ with $k = 0$. 196
6.4 Infidelity scaling for $N = 2^n$ with $k = 1/4d'$. 198
6.5 Infidelity scaling for $N = 2^n$ with $k = 1/2d'$. 198
6.6 Infidelity scaling for $N = 2^n$ with $k = 3/4d'$. 199
6.7 Infidelity scaling for $N = 2^n$ with $k = d'$. 199
Chapter 1

Introduction

In this dissertation, we explore various aspects of quantum computing, a paradigm that harnesses the quantum mechanical properties of subatomic particles to perform computations at speeds provably unattainable by classical computers. The beginning of quantum computing marks a significant milestone, with several small-scale quantum computers now accessible to the public, indicating a new era of computational capability. This thesis explores quantum computing at various levels of granularity, beginning with the abstract complexity that studies the limitations of quantum computing, moving down to the algorithm design, and in the end to the detailed construction of quantum circuits.

Quantum query complexity offers a clean setting in which to study the power and limitations of quantum algorithms. In particular, a lower bound on the quantum query complexity of $f$ implies that no quantum algorithm can solve the problem of computing $f$ using fewer queries than the lower bound, establishing a fundamental limit on the algorithm’s efficiency in the quantum model of computation. One technique to prove quantum query lower bounds is via a notion called approximate degree: a lower bound on the approximate degree of a function $f$ implies a quantum query complexity lower bound for $f$. In Chapter 2, we improved the approximate degree lower bound of the $k$-distinctness Boolean function and also provided an upper bound when $k$ is at most polylogarithmic in the input size.
Next in Chapter 3, we develop a theory of Trotter error which offers tighter error bounds than previous methods by directly considering operator commutativity. This theory yields improved algorithms for quantum simulations, it facilitates simulations where complexity is independent of system size for local observables in power-law interacting systems.

In Chapter 4, our exploration extends into the practical application of quantum computers in high-energy physics, particularly through the digitization of gauge theories for simulation on quantum computers. This work highlights the special ability of quantum computing to deal with complex quantum gauge theories that classical computers cannot handle.

In Chapter 5, we study the application of quantum computing in chemistry and materials science. We develop an optimized algorithm for ground state energy estimation, reducing the resource cost from exponential to linear in terms of precision. This not only slashes the gate count and circuit depth required for hardware implementation but also offers a scalable solution that aligns with the trajectory toward fault-tolerant quantum computing.

At last in Chapter 6, we work out the design and implementation of the quantum lookup table—an essential gadget in the execution of quantum algorithms. By proposing a comprehensive framework, we achieve a versatile structure capable of adapting to varying qubit connectivity schemes. This not only shows sublinear infidelity scaling but also sets a new benchmark in resource efficiency.

Through these contributions, we hope to lay the groundwork for advancing quantum computing towards practical utility.
Chapter 2

Quantum Query Complexity of $k$-distinctness Function

An open problem that is widely regarded as one of the most important in quantum query complexity is to resolve the quantum query complexity of the $k$-distinctness function on inputs of size $N$. While the case of $k = 2$ (also called Element Distinctness) is well-understood, there is a polynomial gap between the known upper and lower bounds for all constants $k > 2$. Specifically, the best known upper bound is $O\left(N^{(3/4)-1/(4k)}\right)$ [23], while the best known lower bound for $k \geq 2$ is $\tilde{\Omega}\left(N^{2/3} + N^{(3/4)-1/(4k)}\right)$ [1, 38].

For any constant $k \geq 4$, we improve the lower bound to $\tilde{\Omega}\left(N^{(3/4)-1/(4k)}\right)$. This yields, for example, the first proof that 4-distinctness is strictly harder than Element Distinctness. Our lower bound applies more generally to approximate degree.

As a secondary result, we give a simple construction of an approximating polynomial of degree $\tilde{O}(N^{3/4})$ that applies whenever $k \leq \text{polylog}(N)$.

2.1 Introduction

In quantum query complexity, a quantum algorithm is given query access to the bits of an unknown input $x$, and the goal is to compute some (known) function $f$ of $x$ while minimizing the number of bits of $x$ that are queried. In contrast to classical query complexity, quantum query algorithms are allowed to make queries.

\footnote{The presentation in this chapter is based on the results obtained in [102].}
in superposition, and the algorithm is not charged for performing unitary operations that are independent of \( x \). Quantum query complexity is a rich model that allows for the design of highly sophisticated algorithms and captures much of the power of quantum computing. Indeed, most quantum algorithms were discovered in or can easily be described in the query setting.

An open problem that is widely regarded as one of the most important in quantum query complexity [97] is to resolve the complexity of the \( k \)-distinctness function. For this function, the input \( x \) specifies a list of \( N \) numbers from a given range of size \( R \), and the function evaluates to TRUE if there is any range item that appears \( k \) or more times in the list. The case \( k = 2 \) corresponds to the complement of the widely-studied \textit{Element Distinctness} function, whose complexity is known to be \( \Theta(N^{2/3}) \) [1, 10].

For general values of \( k \), the best known upper bound on the quantum query complexity of \( k \)-distinctness is \( O\left(N^{3/4-1/(2k+2-4)}\right) \), due to a highly sophisticated algorithm of Belovs [23]. Belovs’ algorithm is based on the so-called learning graph framework in quantum algorithm design, and improves over an earlier upper bound of \( O(N^{k/(k+1)}) \) due to Ambainis [10] that is based on quantum walks over the Johnson graph.

For a long time, the best known lower bound on the quantum query complexity of \( k \)-distinctness was \( \Omega(N^{2/3}) \) for any \( k \geq 2 \), due to Aaronson and Shi [1], with refinements given by Kutin [87] and Ambainis [8]. This lower bound is tight for \( k = 2 \) (matching Ambainis’ upper bound [10]), but it is not known to be tight for any \( k > 2 \). Recently, Bun, Kothari, and Thaler [38] proved a lower bound of \( \tilde{\Omega}(N^{3/4-1/(2k)}) \).

For purposes of this introduction, \( N \) and \( R \) are assumed to be of the same order of magnitude (up to a factor depending on \( k \) alone). For simplicity throughout this section, we state our bounds purely in terms of \( N \), leaving unstated the assumption that \( R \) and \( N \) are of the same order of magnitude.

Throughout this manuscript, we associate \(-1\) with logical TRUE and \(+1\) with logical FALSE.
for constant $k$. This improved over the prior lower bound of $\Omega(N^{2/3})$ for any constant $k \geq 7$. Furthermore, combined with Belovs’ upper bound, this established that for sufficiently large constants $k$, the exponent in the quantum query complexity of $k$-distinctness approaches $3/4$ from below. However, the precise rate at which the quantum query complexity approaches $N^{3/4}$ remains open: there is a polynomial gap between the upper and lower bounds for any constant $k$, and indeed there is a qualitative difference between the inverse-exponential dependence on $k$ in the exponent of $N^{3/4-1/(2k+2-4)}$ (the known upper bound), and the inverse-linear dependence in the known lower bound of $N^{3/4-1/(2k)}$.

In this work, our main result improves the lower bound from $\tilde{\Omega}(N^{3/4-1/(2k)})$ to $\tilde{\Omega}(N^{3/4-1/(4k)})$. While this bound is qualitatively similar to the lower bound of [38], it offers a polynomial improvement for every constant $k \geq 4$. Perhaps more significantly, for $k \in \{4, 5, 6\}$, it is the first improvement over Aaronson and Shi’s $\Omega(N^{2/3})$ lower bound that has stood for nearly 20 years.

The $\epsilon$-error approximate degree of a Boolean function $f : \{-1, 1\}^n \rightarrow \{-1, 1\}$, denoted $\widetilde{\deg}_\epsilon(f)$, is the least degree of a real polynomial $p$ such that $|p(x) - f(x)| \leq \epsilon$ for all $x \in \{-1, 1\}^n$. The standard setting of the error parameter is $\epsilon = 1/3$, and the $(1/3)$-approximate degree of $f$ is denoted $\widetilde{\deg}(f)$ for brevity.

As famously observed by Beals et al. [21], the quantum query complexity of a function $f$ is lower bounded by (one half times) the approximate degree of $f$. Hence, any lower bound on the approximate degree of $f$ implies that (up to a factor of 2) the same lower bound holds for the quantum query complexity of $f$.

As with prior lower bounds for $k$-distinctness [1, 8, 38, 87], our $k$-distinctness lower bound is in fact an approximate degree lower bound (on the natural Boolean function

Throughout this manuscript, $\tilde{O}$, $\tilde{\Omega}$ and $\tilde{\Theta}$ notations are used to hide factors that are polylogarithmic in $N$. 5
induced by \( k \)-distinctness on \( N \lceil \log_2 R \rceil \) bits, where \( R \) denotes the size of the range.

Our analysis is a substantial refinement of the lower bound analysis of Bun et al. [38].

**Theorem 2.1.1 (Informal version of Theorem 2.4.1 and Corollary 2.4.2)**

For any constant \( k \geq 2 \), the approximate degree and quantum query complexity of the \( k \)-distinctness function with domain size \( N \) and range size \( R \geq N \) is \( \tilde{\Omega}(N^{3/4 - 1/(4k)}) \).

**Remark 2.1.2** Theorem 2.1.1 provides an approximate degree lower bound for constant error \( \epsilon = 1/3 \). A recent result of Sherstov and Thaler [124, Theorem 3.4] transforms any constant-error approximate degree lower bound for \( k \)-distinctness, into a lower bound for vanishing error \( \epsilon = o(1) \). Specifically, combining Theorem 2.1.1 and [124, Theorem 3.4] yields that for constant \( k \), the \( \epsilon \)-error approximate degree of \( k \)-distinctness is at least \( \tilde{\Omega} \left( N^{3/4 - 1/(4k)} \log^{1/4+1/(4k)}(1/\epsilon) \right) \), for all \( \epsilon \in [(1/3)^N, 1/3] \).

Recall that for constant \( k \), the best known approximate degree upper bound for \( k \)-distinctness, due to Belovs, is \( O \left( N^{3/4 - 1/(2^k+2-4)} \right) \). For non-constant values of \( k \), the upper bound implied by Belovs’ algorithm grows exponentially with \( k \). That is, the Big-Oh notation in the upper bound hides a leading factor of at least \( 2^{ck} \) for some positive constant \( c \). Consequently Belovs’ result is \( N^{3/4+\Omega(1)} \) for any \( k \geq \Omega(\log N) \). Furthermore, the bound becomes vacuous (i.e., linear in \( N \)) for \( k \geq c \log N \) for a large enough constant \( c > 0 \).

Our secondary result improves this state of affairs by giving a \( \tilde{O}(N^{3/4}) \) approximate degree upper bound that holds for any value of \( k \) that grows at most polylogarithmically with \( N \).

Belovs’ approximate degree upper bound was recently reproved by Sherstov [123], who made the exponential dependence on \( k \) explicit (see, e.g., [123, Theorem 6.6]). To clarify, Belovs’ result is in fact a quantum query upper bound, which in turn implies an approximate degree upper bound. Sherstov’s proof avoids quantum algorithms, and hence does not yield a quantum query upper bound.
Theorem 2.1.3 (Informal) For any \( k \leq \text{polylog}(N) \), the approximate degree of \( k \)-distinctness is \( \tilde{O}(N^{3/4}) \).

We mention that for any \( k \geq 2 \), the approximating polynomials for \( k \)-distinctness that follow from prior works [10, 23, 123] are quite complicated, and in our opinion there has not been a genuinely simple construction of any \( O(N^{3/4}) \)-degree approximating polynomials recorded in the literature, even for the case of \( k = 2 \) (i.e., Element Distinctness). Accordingly, we feel that Theorem 2.1.3 has didactic value even for constant values of \( k \) (though the \( \tilde{O}(N^{3/4}) \) approximate degree upper bound that it achieves is not tight for any constant \( k \geq 2 \)).

To clarify, Theorem 2.1.3 does not yield a quantum query upper bound, but only an approximate degree upper bound. Indeed, it remains an interesting open question whether the quantum query complexity of \( k \)-distinctness is sublinear in \( N \) for all \( k = \text{polylog}(N) \) (see Section 2.1.1 for further discussion).

Our proof of Theorem 2.1.3 is a simple extension of a result of Sherstov [123, Theorem 1.3] that yielded an \( O(N^{3/4}) \) approximate degree upper bound for a different function called Surjectivity. In Section 2.2.2 below, we explain the main observations necessary to obtain Theorem 2.1.3 via the technique used to prove the upper bound for Surjectivity.

2.1.1 Discussion and Open Problems

The most obvious and important open question is to finish resolving the approximate degree and quantum query complexity of \( k \)-distinctness for any \( k > 2 \). Currently, the upper and lower bounds qualitatively differ in their dependence on \( k \), with the upper

---

Surjectivity is the function that interprets its input as a list of \( N \) numbers from a given range of size \( R \), and evaluates to TRUE if and only if every range element appears at least once in the list.
bound having an exponent of the form $3/4 - \exp(-O(k))$ and the lower bound having an exponent of the form $3/4 - \Omega(1/k)$. It seems very likely that major new techniques will be needed to qualitatively change the form of either the upper or lower bound. In particular, on the lower bounds side, our analysis is based on a variant of a technique called dual block composition (see Section 2.2.1), and we suspect that we have reached the limit of what is provable for $k$-distinctness using this technique and its variants.

We remark here that Liu and Zhandry [97] recently showed that the quantum query complexity of a certain search version of $k$-distinctness (defined over randomly generated inputs) is $\Theta(n^{1/2-1/(2^k-1)})$. This inverse-exponential dependence on $k$ is tantalizingly reminiscent of Belovs’ upper bound for $k$-distinctness. This may be construed as mild evidence that $3/4 - \exp(-O(k))$ is the right qualitative bound for $k$-distinctness itself.

A very interesting intermediate goal is to establish any polynomial improvement over the long-standing $\Omega(n^{2/3})$ lower bound for 3-distinctness. This would finally establish that 3-distinctness is strictly harder than Element Distinctness (such a result is now known for all $k \geq 4$ due to Theorem 2.1.1).

It would also be interesting to resolve the quantum query complexity of $k$-distinctness for $k = \text{polylog}(N)$. Although this question may appear to be of specialized interest, we believe that resolving it could shed light on the relationship between approximate degree and quantum query complexity. Indeed, while any quantum algorithm for a function $f$ can be turned into an approximating polynomial for $f$ via the transformation of Beals et al. [21], no transformation in the reverse direction is possible in general [9]. This can be seen, for example, because the quantum query complexity of Surjectivity is known to be $\Omega(N)$ [22, 122], but its approximate degree is $O(N^{3/4})$ [38, 123]. Nonetheless, approximate degree and quantum query complexity turn out to coincide for most functions that arise naturally (Surjectivity remains the
only function that exhibits a separation, without having been specifically constructed for that purpose. In our opinion, this phenomenon remains mysterious, and it would be interesting to demystify it. For example, could one identify special properties of approximating polynomials that would permit a reverse-Beals-et-al. transformation to turn that polynomial into a quantum query algorithm? Perhaps an $\tilde{O}(N^{3/4})$ upper bound for $(\text{polylog}(N))$-distinctness could be derived in this manner. Such an upper bound (even for $(\log N)$-distinctness) would yield improved quantum query upper bounds for min-entropy estimation [93]. On the other hand, due to our Theorem 2.1.3, any $N^{3/4+\Omega(1)}$ lower bound for $(\text{polylog}(N))$-distinctness would require moving beyond the polynomial method.

2.1.2 Roadmap

We give a high-level overview of the proofs of our lower bound and upper bound in Sections 2.2.1 and 2.2.2, respectively. Section 2.3 covers preliminaries. The proof of our main theorem (Theorem 2.1.1) is spread over Sections 2.4-2.6. Section 2.4 gives a detailed, technical outline of the proof, Section 2.5 establishes some auxiliary lemmas, and Section 2.6 contains the heart of the proof. Finally, Section 2.7 proves Theorem 2.1.3.

2.2 Overview of the Proofs

In this section we give an overview of the proofs of our lower bound and upper bound.

There are works in this general direction, notably [13], which shows that a certain technical refinement of approximate degree, called approximation by completely bounded forms, characterizes quantum query complexity. But to our knowledge these works have not yielded any novel quantum query upper bounds for any specific function. We remark that the positive-weights adversary method is also incapable of proving such a result due to the certificate complexity barrier.
Throughout this subsection we assume that \( k \geq 2 \) is an arbitrary but fixed constant.

Let \( \text{THR}_N^k \) denote the function on \( N \)-bit inputs that evaluates to \(-1\) on inputs of Hamming weight at least \( k \), and evaluates to \( 1 \) otherwise. For \( N \leq n \), let \( \{-1,1\}^n \) denote the subset of \( \{-1,1\}^n \) consisting of all inputs of Hamming weight at most \( N \). For any function \( f_n : \{-1,1\}^n \to \{-1,1\} \), let \( f_n^\leq N \) denote the partial function obtained by restricting the domain of \( f \) to \( \{-1,1\}^n \), and let \( \deg(f_n^\leq N) \) denote the least degree of a real polynomial \( p \) such that \( |p(x) - f_n(x)| \leq 1/3 \) for all \( x \in \{-1,1\}^n \).

Simplifying very slightly, prior work by Bun and Thaler [35] (building on an important lemma of Ambainis [8]) implied that for \( k \geq 2 \) the approximate degree of \( k \)-distinctness is equivalent to \( \deg(f_n^\leq N) \) for \( f = \text{OR}_R \circ \text{THR}_N^k \). Here, \( g_n \circ h_m \) denotes the function on \( n \cdot m \) bits obtained by block-composing \( g \) and \( h \), i.e., \( g \circ h \) evaluates \( h \) on \( n \) disjoint inputs and feeds the outputs of all \( n \) copies of \( h \) into \( g \).

Bun et al. [38] proved their \( \tilde{\Omega}(N^{3/4-1/(2k)}) \) lower bound for \( \deg(f_n^\leq N) \) via the method of dual polynomials. This is a technique for proving approximate degree lower bounds that works by constructing an explicit solution to a certain linear program capturing the approximate degree of any function. Specifically, a dual witness to the fact that \( \deg(f_n^\leq N) \geq d \) is a function \( \psi : \{-1,1\}^{RN} \to \mathbb{R} \) satisfying the following properties (this dual formulation is standard, and can be found, for example, in [119]).

First, \( \psi \) must be uncorrelated with all polynomials \( p \) of degree at most \( d \), i.e., \( \langle \psi, p \rangle = 0 \) for all such polynomials \( p \), where \( \langle \psi, p \rangle = \sum_{x \in \{-1,1\}^{RN}} \psi(x)p(x) \). Such a \( \psi \) is said to have pure high degree at least \( d \).
Second, $\psi$ must be well-correlated with $f$, i.e., $\langle \psi, f \rangle \geq (1/3) \cdot \|\psi\|_1$, where $\|\psi\|_1 := \sum_{x \in \{-1, 1\}^n} |\psi(x)|$. Finally, $\psi$ must equal 0 on inputs in $\langle -1, 1 \rangle^N \setminus \langle -1, 1 \rangle^N \leq N$.

To simplify greatly, Bun et al. [38] constructed their dual witness for $(\text{OR}_R \circ \text{THR}_N^k) \leq N$ roughly as follows. They took a dual witness $\Psi$ for the fact that $\widetilde{\deg}(\text{OR}_R) \geq \Omega(R^{1/2})$ [34, 110, 133] and a dual witness $\phi$ for the fact that $\text{THR}_N^k$ also has large approximate degree, and they combined $\Psi$ and $\phi$ in a certain manner (introduced in prior works [91, 121, 125]) to get a dual witness for the composed function $(\text{OR}_R \circ \text{THR}_N^k) \leq N$. The technique used to combine $\Psi$ and $\phi$ is often called dual block composition, and is denoted $\Psi \star \phi$. Dual block composition is defined as follows (below, each $x_i \in \{-1, 1\}$):

$$(\Psi \star \phi)(x_1, \ldots, x_R) = 2^R \cdot \Psi(\text{sgn}(\phi(x_1)), \ldots, \text{sgn}(\phi(x_R))) \cdot \prod_{i=1}^R |\phi(x_i)|/\|\phi\|_1.$$ 

Here, $\text{sgn}(r)$ equals $-1$ if $r < 0$ and equals $+1$ if $r > 0$. To show that $\Psi \star \phi$ is a dual witness for the fact that the approximate degree of $(\text{OR}_R \circ \text{THR}_N^k) \leq N$ is at least $d$, it is necessary to show that $\Psi \star \phi$ has pure high degree at least $d$, and that $\Psi \star \phi$ is well-correlated with $(\text{OR}_R \circ \text{THR}_N^k) \leq N$. It is known that pure high degree increases multiplicatively under the $\star$ operation, and hence the pure high degree calculation for $\Psi \star \phi$ is straightforward. In contrast, the correlation calculation is the key technical challenge and bottleneck in the analysis of [38]. Our key improvement over their work

To clarify, this entire outline is a major simplification of the actual dual witness construction in [38]. The details provided in the outline of this introduction are chosen to highlight the key technical issues that we must address in this work. Amongst other simplifications in this outline, the actual dual witness from [38] is not $\Psi \star \phi$, but rather a “post-processed” version of $\Psi \star \phi$, where the post-processing step is used to ensure that the dual witness evaluates to 0 on all inputs of Hamming weight more than $N$.

It is irrelevant how one defines $\text{sgn}(0)$ because if $\phi(x_i) = 0$ for any $i$, the product $\prod_{i=1}^R |\phi(x_i)|/\|\phi\|_1$ forces $\Psi \star \phi$ to 0. For this reason, the remainder of the discussion in this section implicitly assumes that $\phi(x_i) \neq 0$ for all $i \in \{1, \ldots, R\}$. 

11
is to modify the construction of the dual witness in a manner that allows for an improved correlation bound.

At a very high level, what we do is replace the dual block composition $\Psi \ast \phi$ from the construction of [38] with a variant of dual block composition introduced by Sherstov [120]. Sherstov specifically introduced this variant to address the correlation issues that arise when attempting to use dual block composition to prove approximate degree lower bounds for composed functions, and he used it to prove direct sum and direct product theorems for approximate degree. However, we have to modify even Sherstov’s variant of dual block composition in significant ways to render it useful in our context. We now attempt to give an informal sense of our modification and why it is necessary.

For block-composed functions $g \circ h$, the rough idea of any proof attempting to show that $\langle \Psi \ast \phi, g \circ h \rangle$ is large is to hope that the following approximate equality holds:

$$\langle \Psi \ast \phi, g \circ h \rangle \approx \langle \Psi, g \rangle.$$  \hspace{1cm} (2.1)

If Equation (2.1) holds even approximately, then the correlation analysis of $\Psi \ast \phi$ is complete, since the assumption that $\Psi$ is a dual witness for the high approximate degree of $g$ implies that the right hand side is large.

Equation (2.1) in fact holds with exact equality if $\phi$ agrees in sign with $h$ at all inputs, i.e., if $\langle \phi, h \rangle = \|\phi\|_1$ [91, 121]. Unfortunately, the fact that $\phi$ is a dual witness for the large approximate degree of $h$ implies only a much weaker lower bound on $\langle \phi, h \rangle$, namely that

$$\langle \phi, h \rangle \geq (1/3) \cdot \|\phi\|_1.$$ \hspace{1cm} (2.2)

Variants of dual block composition related to the one introduced in [120] have played important roles in other recent works on approximate degree lower bounds, e.g., [36, 124].
In general, Equation (2.2) is not enough to ensure that Equation (2.1) holds even approximately.

A rough intuition for why Equation (2.1) may fail to hold is the following. The definition of $\Psi \star \phi$ feeds $(\text{sgn}(\phi(x_1)), \ldots, \text{sgn}(\phi(x_R)))$ into $\Psi$. One can think of $\text{sgn}(\phi(x_i))$ as $\phi$’s “prediction” about $h(x_i)$, and the fact that $\langle \phi, h \rangle \geq (1/3) \cdot \|\phi\|_1$ means that for an $x_i$ chosen at random from the probability distribution $|\phi|/\|\phi\|_1$, this prediction is correct with probability at least $2/3$. Unfortunately, there are values of $x_i$ for which $\text{sgn}(\phi(x_i)) \neq h(x_i)$, meaning that $\phi$’s predictions can sometimes be wrong. In this case, on feeding $\text{sgn}(\phi(x_i))$ into $\Psi$, dual block composition is “feeding an error” into $\Psi$, and this can cause $\Psi \star \phi$ to “make more errors” (i.e., output a value on an input that disagrees in sign with $g \circ h$ on that same input) than $\Psi$ itself.

That is, there are two reasons $\Psi \star \phi$ may make an error: either $\Psi$ itself may make an error (let us call this Source 1 for errors), and/or one or more copies of $\phi$ may make an error (let us call this Source 2 for errors).

The first source of error is already fully accounted for in the right hand side of Equation (2.1). The second source of error is not, and this is the reason that Equation (2.1) may fail to hold even approximately.

Roughly speaking, while Equation (2.2) guarantees that $\text{sgn}(\phi(x_i))$ is not “an error” for each $i$ with good probability (i.e., probability at least $2/3$), that still means that with very high probability, $\text{sgn}(\phi(x_i))$ will be in error (i.e., not equal to $h(x_i)$) for a constant fraction of blocks $i \in \{1, \ldots, R\}$. Any one of these errors could be enough to cause a Source 2 error.

Fortunately for us, $g = \text{OR}_R$ has low $(-1)$-certificate complexity, meaning that on inputs $x$ in $\text{OR}_R^{-1}(-1)$, to certify that indeed $x \in \text{OR}_R^{-1}(-1)$, it is sufficient to identify

---

There may be inputs $x = (x_1, \ldots, x_n)$ to $\Psi \star \phi$ that could be classified as both Source 1 and Source 2 errors. For purposes of this high-level introduction, it is not important whether such inputs get classified as Source 1 or Source 2 errors for $\Psi \star \phi$. 

13
just one coordinate of $x$ that equals $-1$. This renders certain kinds of sign-errors made by $\phi$ benign. Specifically, letting $S = \{x: \phi(x) < 0\}$ and $E^- = S \cap f^{-1}(1)$ denote the false-negative errors made by $\phi$, the low $(-1)$-certificate complexity of $\text{OR}_R$ means that it is okay if “a constant fraction of the negative values output by $\phi$ are in error”. That is, so long as

$$\left( \sum_{x \in E^-} |\phi(x)| \right) / \left( \sum_{x \in S} |\phi(x)| \right) = 1 - \Omega(1), \quad (2.3)$$

the contribution of “false negative errors made by $\phi$” to actual Source 2 errors made by $\Psi \star \phi$ is low.

However, the situation is starkly different for “false positive errors” made by $\phi$; while $\text{OR}_R$ has certificates of size 1 for inputs in $\text{OR}_R^{-1}(-1)$, the certificate complexity of the (unique) input in $\text{OR}_R^{-1}(+1)$ is $R$. That is, letting $T = \{x: \phi(x) > 0\}$ and $E^+ = T \cap f^{-1}(-1)$, for Equation (2.1) to hold even approximately for $g = \text{OR}_R$, it is essential that

$$\left( \sum_{x \in T} |\phi(x)| \right) / \left( \sum_{x \in T} |\phi(x)| \right) \ll 1/R. \quad (2.4)$$

Accordingly, Bun et al. [38] obtain their lower bound for $k$-distinctness by using a dual witness $\phi$ for $h = \text{THR}_N^k$ that satisfies Equation (2.4). Using a dual with such few false positive errors causes [38] to lose an additive $1/(2k)$ term in the exponent of $N$ in their final degree bound, relative to what they would obtain if Equation (2.2) were sufficient to ensure that Equation (2.1) approximately held.

As previously mentioned, Sherstov [120] introduced a variant of dual block composition intended to handle Source 2 errors that might have otherwise rendered Equation (2.1) false. Specifically, Sherstov proposed multiplying $(\Psi \star \phi)(x)$ by a low-degree polynomial $p_\eta(x)$ intended to “kill” any inputs $x$ that may contribute Source 2 errors (here, $\eta$ is a parameter, and we will explain shortly how the value of $\eta$ is ultimately chosen). Specifically, $p_\eta$ “counts” the number of blocks $x_i$ of $x$ such that $\text{sgn}(\phi(x_i)) \neq h(x_i)$,
and \( p_\eta \) is defined (through polynomial interpolation) to evaluate to 0 if this number is any integer between 1 and \( \eta \). This has the effect of eliminating all Source 2 errors made by \( \Psi \circ \phi \) on inputs \( x \) for which at most \( \eta \) copies of \( \phi \) make an error. That is, \( p_\eta \) kills all inputs \( x \) in the set

\[
U_\eta := \{ x = (x_1, \ldots, x_R) : \sgn(\phi(x_i)) \neq h(x_i) \text{ for between 1 and } \eta \text{ values of } i \}.
\]

Note that multiplying \( \Psi \circ \phi \) by \( p_\eta \) has the additional, unfortunate effect of distorting the values that \( \Psi \circ \phi \) takes on other inputs; bounding the effect of this distortion is one challenge that Sherstov’s analysis (as well as our own analysis in this work) has to address.

The intuition is that, so long as most Source 2 errors made by \( \Psi \circ \phi \) are caused by inputs in the set \( U_\eta \), then multiplying \( \Psi \circ \phi \) by \( p_\eta \) should eliminate the otherwise devastating effects of most Source 2 errors. So the remaining challenge is to choose a dual witness \( \phi \) for \( h \) guaranteeing that indeed most Source 2 errors are caused by inputs in \( U_\eta \). More precisely, \( \phi \) must be chosen to ensure that, with respect to the product distribution \( \prod_{i=1}^{R} |\phi(x_i)|/\|\phi\|_1 \), it is very unlikely that more than \( \eta \) copies of \( \phi \) make an error on their input \( x_i \).

To this end, it is implicit in Sherstov’s analysis that Equation (2.1) approximately holds with \( (\Psi \circ \phi) \cdot p_\eta \) in place of \( \Psi \circ \phi \) so long as

\[
\left( \sum_{x \in E^{-}\cup E^+} |\phi(x)| \right)/\|\phi\|_1 \ll \eta/R. \tag{2.5}
\]

Notice that this is exactly Equation (2.4), except that the right hand side has crucially increased by a factor of \( \eta \) (also, Equation (2.5) counts both false-positive and false-negative errors, as opposed to just false-positive errors, which is a key discrepancy that we address below). The bigger that \( \eta \) is set, the less stringent is the requirement
of Equation (2.5). However, it turns out that, in order to ensure that \((\Psi \ast \phi) \cdot p_\eta\) has pure high degree close to that of \(\Psi \ast \phi\) itself, \(\eta\) must be set to a value that is noticeably smaller than the pure high degree of \(\Psi\). Ultimately, to obtain the strongest possible results, \(\eta\) gets set to some constant \(C < 1\) times the pure high degree of \(\Psi\).

In order to bring Sherstov’s ideas to bear on \(k\)-distinctness, we have to modify his construction as follows. The key issue (alluded to above) is that Sherstov’s construction is not targeted at functions \(g \circ h\) where \(g\) has low \((-1)\)-certificate complexity, and it is essential that we exploit this low certificate complexity in the correlation analysis to improve on the \(k\)-distinctness lower bound from [38]. Essentially, we modify Sherstov’s definition of \(p_\eta\) to “ignore” all false negative errors (which as explained above are benign in our setting because \(g = \text{OR}_R\) has low \((-1)\)-certificate complexity). Rather we have \(p_\eta\) only “count” the false positive errors and kill any inputs where this number is between 1 and \(\eta\).

We are able to show that with this modification, it is sufficient to choose a dual witness \(\phi\) for \(\text{THR}^k_N\) satisfying

\[
\left(\sum_{x \in T^+} |\phi(x)| \right) / \left(\sum_{x \in T^+} |\phi(x)| \right) \ll \eta/R.
\]  

(2.6)

We end up setting \(\eta \approx O(\sqrt{R})\) for our lower bound, hence the denominator on the right hand side of this inequality represents a quadratic improvement compared to that on the right hand side of Equation (2.4). This improvement ultimately enables us to improve the lower bound from \(\tilde{\Omega}(N^{3/4-1/(2k)})\) to \(\tilde{\Omega}(N^{3/4-1/(4k)})\).

The actual calculations required to establish the sufficiency of Equation (2.6) are quite involved, and we provide a more detailed proof overview in Section 2.4 to help the reader make sense of them.
2.2.2 The Upper Bound

Recall from Section 2.2.1 that the approximate degree of $k$-distinctness is (essentially) equivalent to $\tilde{\deg}(f_{RN}^{\leq N})$ for $f = OR_R \circ THR_N^k$. Similarly, the approximate degree of the Surjectivity function is (essentially) equivalent to $\tilde{\deg}(f_{RN}^{\leq N})$ for $f = AND_R \circ OR_N$. Sherstov proved an upper bound of $O(R^{1/4} \cdot N^{1/2})$ for this latter quantity.

Up to polylogarithmic factors, in Theorem 2.1.3 we achieve an identical upper bound for $k$-distinctness, for any $k \leq \text{polylog}(N)$. To do so, we make the following easy observations. First, in order to apply Sherstov’s construction to a function $f = g \circ h$, it is enough that $g$ have approximate degree $O(\sqrt{R})$, and that $h$ be exactly computed as a linear combination of conjunctions, where the coefficients in the linear combination have $\ell_1$-norm at most quasipolynomially large in $N$. Second, we observe that for $k \leq \text{polylog}(N)$, $THR_N^k$ is exactly computed by such a linear combination of conjunctions. Together, these observations are enough to apply Sherstov’s construction for Surjectivity to obtain the approximate degree upper bound of Theorem 2.1.3 for $k$-distinctness.

2.3 Preliminaries

Notation. Let $N$, $n$ and $m$ be positive integers, $N \leq n$. For $z \in \langle -1, 1 \rangle^n$, let $|z|$ represent the Hamming weight of $z$, i.e., the number of $-1$’s in $z$. Define $(\langle -1, 1 \rangle^n)^{\leq N} := \langle x \in \langle -1, 1 \rangle^n : |x| \leq N \rangle$. For any function $f : (\langle -1, 1 \rangle^n) \rightarrow \mathbb{R}$, denote by $f^{\leq N}$ the partial function that is defined on $(\langle -1, 1 \rangle^n)^{\leq N}$ and agrees with $f$ on all such inputs.

Define $\text{sgn} : \mathbb{R} \rightarrow \langle -1, 1 \rangle$ by $\text{sgn}(x) = 1$ for all non-negative $x$, and $-1$ otherwise. All logarithms in this work are base 2 unless otherwise specified. Let $1^n$ (respectively,
\(-1^N\) denote the \(n\)-bit string \((1, 1, \ldots, 1)\) (respectively, \((-1, -1, \ldots, -1)\)). For strings
\(a \in \langle -1, 1 \rangle^m\) and \(b \in \langle -1, 1 \rangle^n\), we denote by \(a, b\) the \((m + n)\)-bit string formed by the
concatenation of \(a\) and \(b\). We use the notation \([n]\) to denote the set \(\langle 1, 2, \ldots, n \rangle\).

For any function \(f : \langle -1, 1 \rangle^n \to \mathbb{R}\), define \(\|f\|_1 = \sum_{x \in \langle -1, 1 \rangle^n} |f(x)|\). For an event
\(E\), the corresponding indicator function is
\[
I[E] = \begin{cases} 
1 & \text{if } E \text{ holds,} \\
0 & \text{otherwise.} 
\end{cases} \tag{2.7}
\]

For any function \(\psi : \langle -1, 1 \rangle^m \to \mathbb{R}\) such that \(\|\psi\|_1 = 1\), let \(\mu_\psi\) be the distribution
on \((-1, 1)^m\), defined by
\[
\mu_\psi(x) = |\psi(x)|. \tag{2.8}
\]

**Definition 1** For any integer \(n > 0\), any function \(\psi : \langle -1, 1 \rangle^m \to \mathbb{R}\) such that
\(\|\psi\|_1 = 1\), and any \(w \in \langle -1, 1 \rangle\), let \(\mu_\psi\) be the probability distribution \(\mu_\psi\) conditioned
on the event that \(\text{sgn}(\psi(x)) = w\). For any \(z \in \langle -1, 1 \rangle^n\), let \(\mu_z\) denote the probability
distribution \((\mu_\psi)^\otimes n\) conditioned on the event that \(\text{sgn}(\psi(x_i)) = z_i\) for all \(i \in [n]\).

We omit the dependence of \(\mu_z\) on \(\psi\) since \(\psi\) will typically be clear from context.

Note that \(\mu_z\) as defined above is a product distribution given by
\[
\mu_z(x_1, \ldots, x_n) = \prod_{i=1}^n \mu_{z_i}(x_i). \tag{2.9}
\]

**Definition 2** For \(\eta \in [0, 1]\), let \(\Pi(\eta_1, \ldots, \eta_n)\) be the product distribution on \((-1, 1)^n\)
where the \(i\)th bit of the string equals \(-1\) with probability \(\eta_i\), and \(1\) with probability \(1 - \eta_i\).

**Lemma 2.3.1** Let \(n\) be any positive integer, \(p : \langle -1, 1 \rangle^n \to \mathbb{R}\) be a multilinear polynomial,
and \(\eta_1, \ldots, \eta_n \in [0, 1]\). For \(x = (x_1, \ldots, x_n)\) drawn from the product distribution
\(\Pi(\eta_1, \ldots, \eta_n)\) defined in Definition 2, we have
\[
\mathbb{E}_{\Pi(\eta_1, \ldots, \eta_n)}[p(x_1, \ldots, x_n)] = p(1 - 2\eta_1, \ldots, 1 - 2\eta_n). \tag{2.10}
\]
Any function \( f : \langle -1, 1 \rangle^n \rightarrow \mathbb{R} \) has a unique multilinear representation \( f = \sum_{S \subseteq [n]} \hat{f}(S)\chi_S \), where for any \( S \subseteq [n] \), the function \( \chi_S : \langle -1, 1 \rangle^n \rightarrow \langle -1, 1 \rangle \) is defined by \( \chi_S(x) = \prod_{i \in S} x_i \). Hence, \( \|\hat{f}\|_1 = \sum_{S \subseteq [n]} |\hat{f}(S)| \). It follows that for any function \( \phi : \langle -1, 1 \rangle^n \rightarrow \mathbb{R} \), there exists a unique multilinear polynomial \( \tilde{\phi} : \mathbb{R}^n \rightarrow \mathbb{R} \) such that \( \tilde{\phi}(x) = \phi(x) \) for all \( x \in \langle -1, 1 \rangle^n \).

2.3.1 Functions of Interest

Define the function \( \text{OR}_N : \langle -1, 1 \rangle^N \rightarrow \langle -1, 1 \rangle \) to equal 1 if \( x = \mathbf{1}^N \), and -1 otherwise.

Define the Threshold function \( \text{THR}_k^N : \langle -1, 1 \rangle^N \rightarrow \langle -1, 1 \rangle \) to equal 1 for inputs of Hamming weight less than \( k \), and -1 otherwise.

**Definition 3 (k-distinctness)** For integers \( k, N, R \) with \( k \leq N \), define the function \( \text{DIST}_{N,R}^k : [R]^N \rightarrow \langle -1, 1 \rangle \) by \( \text{DIST}_{N,R}^k(s_1, \ldots, s_N) = -1 \) iff there exists an \( r \in [R] \) and distinct indices \( i_1, \ldots, i_k \) such that \( s_{i_1} = \cdots = s_{i_k} = r \). When necessary, the domain of the function can be viewed as \( \langle -1, 1 \rangle^{N \log R} \).

Given any functions \( f_n : \langle -1, 1 \rangle^n \rightarrow \langle -1, 1 \rangle \) and \( g_m : \langle -1, 1 \rangle^m \rightarrow \langle -1, 1 \rangle \), we define the function \( f_n \circ g_m : \langle -1, 1 \rangle^{nm} \rightarrow \langle -1, 1 \rangle \) as

\[
\begin{align*}
f_n \circ g_m(x_{11}, \ldots, x_{1m}, x_{21}, \ldots, x_{2m}, \ldots, x_{n1}, \ldots, x_{nm}) \\
= f_n(g_m(x_1), g_m(x_2), \ldots, g_m(x_n)), x_i \in \langle -1, 1 \rangle^m \text{ for all } i \in [n].
\end{align*}
\]

We drop subscripts when the arities of the constituent functions are clear.

2.3.2 Notions of Approximation

**Definition 4 (Approximate degree)** For any function \( f : \langle -1, 1 \rangle^n \rightarrow \mathbb{R} \), any integer \( N \leq n \), and any \( \epsilon \in [0, 1] \), define the \( \epsilon \)-approximate degree of \( f \leq N \) to be

\[
\widetilde{\deg}_\epsilon(f \leq N) = \min_{p:|p(x) - f(x)| \leq \epsilon, \forall x \in \langle -1, 1 \rangle^n, |x| \leq N} \deg(p).
\]
When the subscript is dropped, $\epsilon$ is assumed to equal $1/3$. When the superscript is dropped in $f^{\leq N}$, then $N$ is assumed to equal $n$.

**Definition 5** For any finite subset $X \subseteq \mathbb{R}^n$, any function $f : X \to \mathbb{R}$, and any integer $d \geq 0$, define

$$E(f, d) := \min_{p : \deg(p) \leq d} \left\{ \max_{x \in X} |f(x) - p(x)| \right\}.$$  

**Definition 6 (Correlation)** Consider any function $f : \langle -1, 1|^{n} \to \mathbb{R}$ and $\psi : \langle -1, 1|^{n} \to \mathbb{R}$. Define the correlation between $f$ and $\psi$ to be

$$\langle f, \psi \rangle = \sum_{x \in \langle -1, 1|^{n}} f(x)\psi(x).$$

**Definition 7 (Pure high degree)** For $\phi : \langle -1, 1|^{n} \to \mathbb{R}$, we say that the pure high degree of $\phi$, which we denote by $\text{phd}(\phi)$, is $d$ if $d \geq 0$ is the largest integer for which $\langle \phi, p \rangle = 0$ for any polynomial $p : \langle -1, 1|^{n} \to \mathbb{R}$ of degree strictly less than $d$.

For any Boolean function $f : \langle -1, 1|^{m} \to \langle -1, 1|$ and function $\psi : \langle -1, 1|^{m} \to \mathbb{R}$, $\|\psi\|_1 = 1$, let

$$\epsilon_{f,\psi}^+ := \Pr_{\mu_{\psi}}[f(x)\psi(x) < 0|\psi(x) > 0], \quad \epsilon_{f,\psi}^- := \Pr_{\mu_{\psi}}[f(x)\psi(x) < 0|\psi(x) < 0]. \quad (2.11)$$

Define $\epsilon_{f,\psi} = \epsilon_{f,\psi}^+ + \epsilon_{f,\psi}^-.$

**Definition 8** For any functions $f : \langle -1, 1|^{n} \to \langle -1, 1|$ and $\psi : \langle -1, 1|^{n} \to \mathbb{R}$, let

$$E^+(f, \psi) := \{x \in \langle -1, 1|^{n} : f(x)\psi(x) < 0, \psi(x) > 0\},$$

$$E^-(f, \psi) := \{x \in \langle -1, 1|^{n} : f(x)\psi(x) < 0, \psi(x) < 0\}.$$
We define the false positive error between $f$ and $\psi$ to be

$$
\delta_{f,\psi}^+ := \sum_{x \in E^+(f,\psi)} |\psi(x)|
$$

and false negative error to be

$$
\delta_{f,\psi}^- := \sum_{x \in E^-(f,\psi)} |\psi(x)|.
$$

We observe the following simple connection between $\delta_{f,\psi}^+$ ($\delta_{f,\psi}^-$) and $\epsilon_{f,\psi}^+ (\epsilon_{f,\psi}^-)$.

**Claim 2.3.2** For any Boolean function $f : \langle -1, 1 \rangle^m \to \langle -1, 1 \rangle$ and any function $\psi : \langle -1, 1 \rangle^m \to \mathbb{R}$ with $\|\psi\|_1 = 1$, $\text{phd}(\psi) \geq 1,$

$$
\epsilon_{f,\psi}^+ = 2\delta_{f,\psi}^+, \quad \epsilon_{f,\psi}^- = 2\delta_{f,\psi}^-.
$$

(2.12)

**Proof.**

$$
\delta_{f,\psi}^+ = \sum_{x \in E^+(f,\psi)} |\psi(x)| \quad \text{by Definition 8}
$$

$$
= \Pr_{x \sim \mu_\psi} [x \in E^+(f,\psi)] \quad \text{by Equation (2.8)}
$$

$$
= \Pr_{x \sim \mu_\psi} [f(x)\psi(x) < 0 \land \psi(x) > 0] \quad \text{by Definition 8}
$$

$$
= \Pr_{x \sim \mu_\psi} [\psi(x) > 0] \cdot \Pr_{x \sim \mu_\psi} [f(x)\psi(x) < 0 | \psi(x) > 0]
$$

$$
= \frac{\epsilon_{f,\psi}^+}{2}. \quad \text{since } \langle \psi, 1 \rangle = 0 \text{ and } \sum_x |\psi(x)| = 1 \text{ implies } \Pr_{\mu_\psi}[\psi(x) > 0] = 1/2
$$

The equality $\epsilon_{f,\psi}^- = 2\delta_{f,\psi}^-$ can be proved similarly.

By linear programming duality, we have the following standard equivalence between lower bounds on approximate degree and existence of “dual polynomials". See, for example, [37].

**Lemma 2.3.3** Let $f : \langle -1, 1 \rangle^n \to \langle -1, 1 \rangle$ be any function. For any integer $0 \leq j \leq n$, we have $\widetilde{\deg}_e(f^{\leq j}) > d$ if and only if there exists a “dual polynomial" $\phi : \langle -1, 1 \rangle^n \to \mathbb{R}$ satisfying the following properties.
\[ \sum_{x \in \{-1,1\}^n} |\phi(x)| = 1. \]

\[ \text{phd}(\phi) > d. \]

\[ \langle f, \phi \rangle > \epsilon. \]

\[ \phi(x) = 0 \text{ for all } |x| > j. \]

We say that \( \phi \) is a dual polynomial witnessing the fact that \( \deg_\epsilon (f^{\leq j}) > d \). For brevity, when \( \epsilon \) and \( d \) are clear from context, we say that \( \phi \) is a dual polynomial for \( f^{\leq j} \).

\( \check{\text{Spalek}} \) [133] exhibited an explicit dual witness for OR (existence of a dual witness for OR was already implicit from the work of Nisan and Szegedy [110]).

Claim 2.3.4 (Implicit in [110]) There exists a constant \( c \in (0,1] \) such that for any integer \( n \geq 0 \), there exists a function \( \theta : \{-1,1\}^n \rightarrow \mathbb{R} \) satisfying

\[ \|\theta\|_1 = 1, \]

\[ \text{phd}(\theta) \geq c\sqrt{n}, \]

\[ \langle \theta, \text{OR}_n \rangle \geq 3/5. \]

We also require the following error reduction theorem for approximate degree.

Lemma 2.3.5 ([33]) Let \( f : \{-1,1\}^n \rightarrow \{-1,1\} \) be any (possibly partial) Boolean function and let \( 0 < \epsilon < 1 \). Then,

\[ \tilde{\deg}_\epsilon (f) = \tilde{\deg}(f) \cdot O(\log(1/\epsilon)). \]

The statement in [33] only deals with total functions. It can be seen that the proof works for partial functions too.
2.3.3 Dual Polynomials and Dual Block Composition

Bun et al. [38] exhibited a dual witness for the approximate degree of the $k$-threshold function. Their dual witness additionally satisfies a decay condition, meaning that it places very little mass on inputs of large Hamming weight. The following claim, which gives a preliminary construction towards their dual witness for $\text{THR}_N^k$, is a mild modification of [37, Proposition 54].

Claim 2.3.6 (Modification of [37, Proposition 54]) Let $k, T, N \in \mathbb{N}$ with $2 \leq k \leq T$. There exist constants $c_1, c_2 \in (0, 1]$ and a function $\omega_T : [T] \cup \{0\} \to \mathbb{R}$ such that all of the following hold.

\[
\sum_{\omega_T(t) > 0, t \geq k} |\omega_T(t)| \leq \frac{1}{48 \cdot 4^k \sqrt{N \log N}}. \tag{2.13}
\]

\[
\sum_{\omega_T(t) < 0, t < k} |\omega_T(t)| \leq \left( \frac{1}{2} - \frac{2}{4^k} \right). \tag{2.14}
\]

\[
\|\omega_T\|_1 := \sum_{t=0}^{T} |\omega_T(t)| = 1. \tag{2.15}
\]

For all polynomials $q : \mathbb{R} \to \mathbb{R}$,

\[
\deg(q) < c_1 \sqrt{4^{-k} k^{-1} T N^{-1/(2k)} \log^{-1} N} \implies \sum_{t=0}^{T} \omega_T(t)q(t) = 0. \tag{2.16}
\]

For all $t \in [T], |\omega_T(t)| \leq \frac{\sigma \exp(-\beta t)}{t^2} \quad \text{for } \sigma = (2k)^k, \quad \beta = \frac{c_2}{\sqrt{4^k k T N^{1/(2k)} \log N}}. \tag{2.17}
\]

Although the proof follows along the same lines as that of [37], we provide a proof in the appendix for completeness.

The next claim yields a dual polynomial for $\text{THR}_N^k$, and we omit its proof.

Claim 2.3.7 (Modification of [37, Proposition 55]) Let $k, T, N \in \mathbb{N}$ with $2 \leq k \leq T \leq N$, and let $\omega_T$ be as constructed in Claim 2.3.6, with constants $c_1, c_2$. Define
\[\psi_T : (-1, 1)^N \rightarrow \mathbb{R} \text{ by } \psi_T(x) = \omega_T(|x|)/(N) \text{ for } x \in ((-1, 1)^N)^{\leq T} \text{ and } \psi_T(x) = 0 \text{ otherwise. Then}\]

\[\delta^+_{\text{THR}^k_N, \psi_T} \leq \frac{1}{48 \cdot 4^k \sqrt{N} \log N} \] (2.18)

\[\delta^-_{\text{THR}^k_N, \psi_T} \leq \frac{1}{2} - \frac{2}{4^k} \] (2.19)

\[\|\psi_T\|_1 = 1 \] (2.20)

For any polynomial \(p : (-1, 1)^N \rightarrow \mathbb{R},\)

\[\deg(p) < c_1 \sqrt{4^{-k}k^{-1}TN^{-1/(2k)} \log^{-1} N} \implies \langle \psi_T, p \rangle = 0 \] (2.21)

For all \(t \in [n],\)

\[\sum_{|x| = t} |\psi_T(x)| \leq \frac{(2k)^k \exp \left( -c_2 t / \sqrt{4^k k T N^{1/(2k)} \log N} \right)}{t^2}. \] (2.22)

Towards proving approximate degree lower bounds for composed functions, one might hope to combine dual polynomials of the constituent functions in some way to obtain a dual polynomial for the composed function. A series of works \([91, 121, 125]\) introduced the notion of “dual block composition”, which is a powerful method of combining dual witnesses.

**Definition 9 (Dual block composition)** Let \(\theta : (-1, 1)^n \rightarrow \mathbb{R}, \phi : (-1, 1)^m \rightarrow \mathbb{R}\) be any functions satisfying \(\|\theta\|_1 = \|\phi\|_1 = 1\) and \(\text{phd}(\phi) \geq 1.\) Let \(x = (x_1, \ldots, x_n)\) where each \(x_i \in (-1, 1)^m.\) Define the dual block composition of \(\theta\) and \(\phi,\) denoted \(\theta \star \phi,\) to be

\[\theta \star \phi(x) = 2^n \theta(\text{sgn}(\phi(x_1)), \ldots, \text{sgn}(\phi(x_n))) \prod_{i=1}^n |\phi(x_i)|.\]

Sherstov [121] showed that dual block composition preserves \(\ell_1\)-norm and that pure high degree is multiplicative (also see [91]). Bun and Thaler [35] observed that dual block composition is associative.
Lemma 2.3.8 Let $\phi : \langle -1, 1 \rangle^{m_\phi} \rightarrow \mathbb{R}, \theta : \langle -1, 1 \rangle^{m_\theta} \rightarrow \mathbb{R}$ be any functions. Then,

Preservation of $\ell_1$-norm: If $\|\theta\|_1 = 1, \|\phi\|_1 = 1$ and $\langle \phi, 1 \rangle = 0$, then

$$\|\theta \star \phi\|_1 = 1.$$  \tag{2.23}

Multiplicativity of pure high degree:

$$\text{phd}(\theta) > D, \text{phd}(\phi) > d \implies \text{phd}(\theta \star \phi) > Dd.$$  \tag{2.24}

Associativity: For every $\psi : \langle -1, 1 \rangle^{m_\psi} \rightarrow \mathbb{R}$, we have

$$(\phi \star \theta) \star \psi = \phi \star (\theta \star \psi).$$  \tag{2.25}

It was shown in [37] that for any dual polynomial $\Phi$, and $\psi_T$ as constructed in Claim 2.3.7, the dual block composed function $\Phi \star \psi_T$ satisfies a “strong dual decay” condition.

Claim 2.3.9 ([37, Proposition 31]) Let $R$ be sufficiently large and $k \leq T \leq R$ be any positive integer. Fix $\sigma = (2k)^k$ and let $N = [20\sqrt{\sigma}R]$. Let $\Phi : \langle -1, 1 \rangle^R \rightarrow \mathbb{R}$ be any function with $\|\Phi\|_1 = 1$ and $\psi_T : \langle -1, 1 \rangle^N \rightarrow \mathbb{R}$ as defined in Claim 2.3.7. Then

$$\sum_{x \notin \langle -1, 1 \rangle^{RN} \leq N} |(\Phi \star \psi_T)(x)| \leq (2NR)^{-2\Delta}$$  \tag{2.26}

for some $\Delta \geq \frac{\beta \sqrt{\sigma} R}{4\ln^2 R}$ for $\beta = c_2 / \sqrt{4^k kTN^{1/(2k)} \log N}$.

We now define a simple but important function $\phi$ that we use in our construction of a dual witness for $\text{DIST}^k_{N,R}$. This function was first used in the context of dual block composition by Bun and Thaler [34].

---

They in fact showed that $\Psi \star \psi$ satisfies this strong decay condition for any $\psi$ satisfying a corresponding “weak decay” condition. However for this work, we only require this statement for $\psi = \psi_T$ as constructed in Claim 2.3.7.
Claim 2.3.10 ([34]) Define \( \phi : \{-1,1\}^n \rightarrow \mathbb{R} \) as

\[
\phi(x) = \begin{cases} 
-1/2 & \text{if } x = -1^n \\
1/2 & \text{if } x = 1^n \\
0 & \text{otherwise.}
\end{cases}
\]  

(2.27)

Then, \( \text{phd}(\phi) = 1 \).

Bun et al. [37], slightly extending a result in [34], showed that on dual block composing \( \phi \) and \( \psi \), where \( \phi \) is defined as in Claim 2.3.10, the correlation of the dual block composed witness \( \phi \star \psi \) with \( \text{OR}_M \circ f \) amplifies the correlation of \( f \) with \( \psi \) as follows.

Lemma 2.3.11 ([37, Proposition 56]) Let \( f : \langle -1,1 \rangle^n \rightarrow \langle -1,1 \rangle \) and \( \psi : \langle -1,1 \rangle^n \rightarrow \mathbb{R} \) be any functions with \( \| \psi \|_1 = 1 \). For every \( M \in \mathbb{N} \) and \( \phi : \langle -1,1 \rangle^M \rightarrow \mathbb{R} \) as defined in Claim 2.3.10, we have

\[
\delta^+_{\text{OR}_M \circ f, \phi \star \psi} \leq M \delta^+_{f, \psi},
\]  

(2.28)

\[
\delta^-_{\text{OR}_M \circ f, \phi \star \psi} \leq \frac{1}{2} (2 \delta^-_{f, \psi})^M.
\]  

(2.29)

2.3.4 Some Polynomials

In this section we list out a few polynomials that we require, along with their properties.

Lemma 2.3.12 ([120, Lemma 3.1]) For any \( \tau_1, \ldots, \tau_n \in [0,1) \), define \( \nu = \Pi(\tau_1, \ldots, \tau_n) \) and \( \tau = \max\{\tau_1, \ldots, \tau_n\} \). For any \( \eta \in \{0,1,\ldots,n-1\} \), let \( p_\eta : [-1,1]^n \rightarrow \mathbb{R} \) be the unique degree-\( \eta \) multilinear polynomial that satisfies

\[
p_\eta(z) = (-1)^{\eta} \prod_{i=1}^{\eta} (|z| - i), \forall z \in \langle -1,1 \rangle^n .
\]  

(2.30)

26
Then,

\[ p_\eta(1^n) = \eta! , \quad \text{(2.31)} \]
\[
\| \hat{p}_\eta \|_1 \leq \eta! \left( \frac{n + \eta}{\eta} \right) , \quad \text{(2.32)}
\]
\[
\mathbb{E}_\nu[|p_\eta(z)|] \leq p_\eta(1^n) \nu(1^n) (1 + A) , \quad \text{where } A := \left( \frac{n}{\eta + 1} \right) \frac{\tau^{\eta+1}}{(1 - \tau)^n} . \quad \text{(2.33)}
\]

Furthermore, \( p_\eta(z) \geq 0 \) for all \( z \in \langle -1, 1 \rangle^n \) provided that \( \eta \) is even.

It is easy to show that for any multilinear polynomial \( p : \mathbb{R}^n \to \mathbb{R} \), we have \( \max_{y \in \langle -1, 1 \rangle^n} |p(y)| \leq \| \hat{p} \|_1 \). When applied to the function in the previous lemma, we obtain

**Claim 2.3.13** For \( p_\eta \) defined as in Lemma 2.3.12, \( \max_{y \in \langle -1, 1 \rangle^n} |p_\eta(y)| \leq \eta! \left( \frac{n+\eta}{\eta} \right) \).

Finally, we require a lemma, implicit in a result of Razborov and Sherstov [117] (also see [35, Proposition 21] for a formulation similar to the one we require).

**Lemma 2.3.14 (Implicit in [117])** Let \( N \geq R \) be positive integers, \( \Delta \in \mathbb{R}^+ \), and \( \theta : \langle -1, 1 \rangle^{RN} \to \mathbb{R} \) be any polynomial such that

\[
\sum_{x \notin \langle -1, 1 \rangle^{RN} \leq N} |\theta(x)| \leq (2NR)^{-\Delta}.
\]

For any positive integer \( D < \Delta \), there exists a function \( \nu : \langle -1, 1 \rangle^{RN} \to \mathbb{R} \) such that

- \( \text{phd}(\nu) > D \)
- \( \| \nu \|_1 \leq 1/10 \)
- \( |x| > N \Rightarrow \nu(x) = \theta(x) \).

Lemma 2.3.14 helps us convert a dual polynomial \( \theta \) with little mass on large Hamming weight inputs to a dual polynomial \((\theta - \nu)/\|\theta - \nu\|_1\) with no mass on large Hamming weight inputs without affecting the pure high degree by much.
**Definition 10** For any integer \( d \geq 0 \), let \( T_d : \mathbb{R} \to \mathbb{R} \) denote the degree-\( d \) Chebyshev polynomial, defined recursively as follows.

\[
T_0(x) = 1 \\
T_1(x) = x \\
T_d(x) = 2xT_{d-1}(x) - T_{d-2}(x).
\]

We now observe a simple well-known fact about Chebyshev polynomials whose proof we include for completeness.

**Claim 2.3.15** For any \( d \geq 0 \), consider the \( d \)'th Chebyshev polynomial \( T_d : \mathbb{R} \to \mathbb{R} \) as defined in Definition 10, and write its expansion \( T_d(x) = \sum_{i=0}^{d} a_i x^i \). Then,

\[
\sum_{i=0}^{d} |a_i| \leq 3^d. \tag{2.34}
\]

**Proof.** We prove this by induction.

Let \( S_d \) denote \( \sum_{i=0}^{d} |a_i| \) where \( a_i \)'s are the coefficients in the expansion \( T_d(x) = \sum_{i=0}^{d} a_i x^i \). By Definition 10, the hypothesis is satisfied for \( d = 0, 1 \). Next suppose the hypothesis is true for all \( d \leq k \) for some \( k \geq 1 \). By the recursive definition in Definition 10, we have \( S_{k+1} \leq 2S_k + S_{k-1} \leq 2 \cdot 3^k + 3^{k-1} = 3^{k-1}(6 + 1) < 3^{k+1} \).

We also require the following well-known properties of Chebyshev polynomials.

**Fact 2.3.16** For any integer \( d \geq 0 \),

\[
|T_d(x)| \leq 1 \quad \quad |x| \leq 1 \tag{2.35}
\]

\[
T_d(1 + \epsilon) \geq 1 + d^2 \epsilon \quad \quad \epsilon \geq 0. \tag{2.36}
\]

**Definition 11** For any positive integer \( n \), any polynomial \( p : (-1,1]^n \to \{0,1\} \) that is of the form

\[
\left( \prod_{i \in A} \frac{1 + x_i}{2} \right) \left( \prod_{j \in B} \frac{1 - x_j}{2} \right) \tag{2.37}
\]

for some sets \( A, B \subseteq [n] \), is called a conjunction.
It can be observed that the product of conjunctions is a conjunction.

**Claim 2.3.17 ([123, Corollary 4.7])** Let $n \leq N$ be any positive integers, and $A, B$ be any subsets of $[N]$. Define $f : \langle -1, 1 \rangle^N \rightarrow \langle 0, 1 \rangle$ by

$$f(x) = \left( \prod_{i \in A} \frac{1 + x_i}{2} \right) \left( \prod_{j \in B} \frac{1 - x_j}{2} \right).$$

Then, for any integer $d \geq 0$, we have

$$E(f, d) \leq \exp\left( -\frac{cd^2 n}{n} \right)$$

for some absolute constant $c$.

**Definition 12** Consider any positive integer $n$ and any function $f : \langle -1, 1 \rangle^n \rightarrow \mathbb{R}$.

Define the conjunction norm of $f$, which we denote by $\rho(f)$, to be

$$\min \{ \sum_{A \subseteq [n]} \sum_{B \subseteq [n]} |C_{A,B}| : f(x) = \sum_{A \subseteq [n]} \sum_{B \subseteq [n]} C_{A,B} \left( \prod_{i \in A} \frac{1 + x_i}{2} \right) \left( \prod_{j \in B} \frac{1 - x_j}{2} \right), \quad C_{A,B} \in \mathbb{R} \}.$$

We now state some simple observations about the conjunction norm which we do not prove here. See, for example, [123, Proposition 2.4].

**Fact 2.3.18** Let $m, n$ be positive integers, $f, g : \langle -1, 1 \rangle^n \rightarrow \mathbb{R}$ be any functions, and $p : \mathbb{R} \rightarrow \mathbb{R}$ be any degree-$m$ polynomial of the form $p(x) = \sum_{i=0}^{m} a_i x^i, a_i \in \mathbb{R}$. Then $\rho$ is well defined and satisfies

$$\rho(a \cdot f) = |a| \rho(f), \quad \text{for any } a \in \mathbb{R}, \quad (2.38)$$

$$\rho(f + g) \leq \rho(f) + \rho(g), \quad (2.39)$$

$$\rho(f \cdot g) \leq \rho(f) \cdot \rho(g), \quad (2.40)$$

$$\rho(p \circ g) \leq (\max\{1, \rho(g)\})^m \cdot \sum_{i=0}^{m} |a_i|. \quad (2.41)$$

The version in [123] deals with functions whose domain is $\langle 0, 1 \rangle^N \subseteq \mathbb{R}$. The statement there can easily be seen to imply the statement in this work.
2.4 Outline of Proof of Main Theorem

Our main theorem is as follows.

**Theorem 2.4.1** For $R \in \mathbb{N}$ sufficiently large, $2 \leq k \leq \frac{\log R}{4}$, and some $N = \Theta(k^{k/2}R)$,

$$\widetilde{\deg}(\text{DIST}^k_{N,R+N}) = \Omega\left(\frac{1}{4k^2} \cdot \frac{1}{\log^{7/2} R} \cdot R^{\frac{3}{4} - \frac{1}{8\pi}}\right). \quad (2.42)$$

Ambainis [8] showed that the approximate degree of functions that are symmetric (both with respect to range elements and with respect to domain elements) is the same for all range sizes greater than or equal to $N$. As a corollary, we obtain the following.

**Corollary 2.4.2** For $R \in \mathbb{N}$ sufficiently large, $2 \leq k \leq \frac{\log R}{4}$, and some $N = \Theta(k^{k/2}R)$,

$$\widetilde{\deg}(\text{DIST}^k_{N,N}) = \Omega\left(\frac{1}{4k^2} \cdot \frac{1}{\log^{7/2} R} \cdot R^{\frac{3}{4} - \frac{1}{8\pi}}\right). \quad (2.43)$$

We require the following relation between approximate degree of $k$-distinctness and a related Boolean function; this relationship follows from [37, Proposition 21 and Corollary 26].

**Claim 2.4.3 ([37])** Let $N, R \in \mathbb{N}$ and $2 \leq k \leq N$ be any integer. Then for any $\epsilon > 0$,

$$\widetilde{\deg}_\epsilon(\text{DIST}^k_{N,R+N}) = \Omega\left(\frac{1}{\log R} \cdot \widetilde{\deg}_\epsilon(\text{OR}_R \circ \text{THR}_N^k)^{\leq N}\right). \quad (2.44)$$

There are several different conventions used in the literature when defining the domain of functions such as $k$-distinctness. The convention used by Ambainis [8] considers the input to be specified by $N \cdot R$ variables $y_{1,1}, \ldots, y_{N,R}$, where $y_{i,j} = -1$ if and only if the $i$th list item in the input equals range element $j$ (i.e., it is promised that for each $i$, $y_{i,j} = -1$ for exactly one $j$). We use the convention that the input is specified by $N[\log_2 R]$ bits. It is well known (and not hard to show) that conversion between the two conventions affects approximate degree by at most a factor of $[\log_2 R]$. 

30
To prove Theorem 2.4.1, Claim 2.4.3 implies that it suffices to prove a lower bound on \( \deg(\text{OR}_R \circ \text{THR}_N^k)^\leq N \).

**Theorem 2.4.4** For \( R \in \mathbb{N} \) sufficiently large, \( 2 \leq k \leq \frac{\log R}{4} \), and some \( N = \Theta(k^{k/2}R) \),

\[
\tilde{\deg}( (\text{OR}_R \circ \text{THR}_N^k)^\leq N ) = \Omega \left( \frac{1}{4k^2} \cdot \frac{1}{\log^{5/2} R} \cdot R^{3/4 - \frac{1}{4k}} \right) .
\]

(2.45)

Note that the theorems above continue to yield non-trivial lower bounds for some values of \( k = \omega(1) \). However for ease of exposition, we assume throughout this section that \( k \geq 2 \) is an arbitrary but fixed constant.

Towards proving Theorem 2.4.4, we construct a dual witness \( \Gamma \) satisfying the following four conditions.

- **Normalization:** \( \| \Gamma \|_1 = 1 \),
- **Pure high degree:** There exists a \( D = \tilde{\Omega} \left( R^{3/4 - \frac{1}{4k}} \right) \) such that for every polynomial \( p : \langle -1, 1 \rangle^R \to \mathbb{R} \) of degree less than \( D \), we have \( \langle p, \Gamma \rangle = 0 \),
- **Correlation:** \( \langle \Gamma, (\text{OR}_R \circ \text{THR}_N^k) \rangle > 1/3 \),
- **Exponentially little mass on inputs of large Hamming weight:**

\[
\sum_{x \notin \langle -1, 1 \rangle^R} \left| \Gamma(x) \right| \leq (2NR)^{-\tilde{\Omega} \left( R^{3/4 - \frac{1}{4k}} \right)} \text{ for all } x \notin \langle -1, 1 \rangle^R^\leq N .
\]

Next, Lemma 2.3.14 implies existence of a function \( \nu \) that equals \( \Gamma \) on \( x \notin \langle -1, 1 \rangle^R \), has pure high degree \( \tilde{\Omega} \left( R^{3/4 - \frac{1}{4k}} \right) \), and \( \| \nu \|_1 \leq 1/10 \). The function \( \mathcal{W} : \langle -1, 1 \rangle^R \to \mathbb{R} \) defined by \( \mathcal{W}(x) := \frac{\Gamma(x) - \nu(x)}{\| \Gamma - \nu \|_1} \) then satisfies the conditions in Equations (2.75), (2.76), (2.77) and (2.78) (see Section 2.6.2 for proofs). Theorem 2.4.4 then follows by Lemma 2.3.3 and Lemma 2.3.5.
The rest of this section is devoted towards providing a sketch of how we construct such a dual witness $\Gamma$. In the next subsection we first sketch an outline of the approximate degree lower bound in [38], and in the subsequent subsection we elaborate on where our approach differs from theirs. Section 2.5 presents auxiliary lemmas that will be used in the formal proof of Theorem 2.4.4, while Section 2.6 contains the proof itself.

2.4.1 Prior Work

At a high level, we follow the same outline as followed in [38], who exhibited a dual witness $\Lambda$ witnessing $\deg(\text{DIST}^k_{N,R}) = \tilde{\Omega}(R^{3/4 - \frac{1}{2k}})$ for the same ranges of $k, N, R$ that we consider. In this section we sketch their construction. Their dual witness takes the form $\Lambda = \theta \ast \phi \ast \psi$, where $\theta, \phi, \psi$ each have $\ell_1$-norm 1 and additionally satisfy the properties below.

- The function $\psi$ satisfies:
  - The false positive error between $\text{THR}^k_N$ and $\psi$ is $O(1/N)$.
  - The false negative error between $\text{THR}^k_N$ and $\psi$ is at most $\frac{1}{2} - \frac{2}{4^k}$.
  - The pure high degree of $\psi$ is $\tilde{\Omega}(R^{1/4} N^{-1/(2k)})$.
  - $\psi$ satisfies a “weak decay condition”, viz. $\sum_{|x| = t} |\psi(x)| \leq \sigma \exp(-\beta t)/t^2$ for some constant $\sigma$ (for general $k$, the value of $\sigma$ only depends on $k$), and $\beta = \tilde{\Omega}(R^{1/4} N^{1/(2k)})$.

- The function $\phi$ is defined on $4^k$ inputs, and is defined as in Claim 2.3.10.

- $\theta$ is constructed as in Claim 2.3.4 with $n = R/4^k$. 
The facts that $\|\Lambda\|_1 = 1$ and $\text{phd}(\Lambda) = \tilde{\Omega}(R^{3/4}N^{-1/(2k)})$ follow immediately from the definitions of $\theta, \phi, \psi$, and the fact that dual block composition preserves $\ell_1$-norm and causes pure high degree to increase multiplicatively (Lemma 2.3.8).

Next they use the fact that dual block composition is associative (Equation (2.25)) to express $\Lambda$ as $(\theta \star \phi) \star \psi$ and conclude using Claim 2.3.9 that $\Lambda$ places exponentially small (in $R^{3/4}^{-1/2}N^{-1/2k}$) mass on inputs in $\langle -1, 1 \rangle^{RN}$ of Hamming weight larger than $N$.

It remains to show the correlation bound, i.e., $\langle \Lambda, \text{OR}_R \circ \text{THR}_N^k \rangle > 1/3$. For the correlation analysis it is convenient to view $\Lambda$ as $\theta \star (\phi \star \psi)$. The following is the outline of their correlation analysis.

1. By construction, $\delta_{\text{THR}_N^k, \psi}^+ = O(1/N)$ and $\delta_{\text{THR}_N^k, \psi}^- \leq \frac{1}{2} - \frac{2}{4k}$.

2. By Lemma 2.3.11, the false positive error between $\text{OR}_k \circ \text{THR}_N^k$ and $\phi \star \psi$ remains $O(1/N)$, whereas the false negative error between $\text{OR}_k \circ \text{THR}_N^k$ and $\phi \star \psi$ becomes a small enough constant.

3. As mentioned in Section 2.2.1, the very low $(-1)$-certificate complexity of $\text{OR}_R$ renders false-negative errors benign. Thus the false-negative and false-positive error rates achieved in the last bullet point are sufficient to ensure $\langle \theta \star (\phi \star \psi), \text{OR}_{R/4} \circ (\text{OR}_k \circ \text{THR}_N^k) \rangle \geq 1/3$ by showing $\langle \theta \star (\phi \star \psi), \text{OR}_{R/4} \circ (\text{OR}_k \circ \text{THR}_N^k) \rangle \approx \langle \theta, \text{OR}_{R/4} \rangle$.

Roughly, where we improve over this prior work is in item 3 above. Whereas [38] needed a false-positive error rate for $\phi \star \psi$ of $O(1/N)$ to ensure that their final dual witness $\Lambda$ is well-correlated with $\text{OR}_R \circ \text{THR}_N^k$, we modify the construction of $\Lambda$ so that a false-positive error rate of roughly $1/\sqrt{N}$ suffices to ensure good correlation of the final dual witness with $\text{OR}_R \circ \text{THR}_N^k$. 

33
2.4.2 Our Construction

As in the previous section, our construction of $\Gamma$ is also based on three dual witnesses. The functions $\theta, \phi$ are exactly the same as in the previous section. Our $\psi$ is a fairly straightforward modification of the one described in the previous section, that has a larger pure high degree, at the cost of a worse false positive error. A little more formally, our functions $\theta, \phi, \psi$ have $\ell_1$-norm equal to 1, and additionally satisfy the following.

- The function $\psi$ satisfies:
  - The false positive error between $\text{THR}_N^k$ and $\psi$ is $\tilde{O}(1/\sqrt{N})$.
  - The false negative error between $\text{THR}_N^k$ and $\psi$ is at most $\frac{1}{2} - \frac{2}{4^k}$.
  - The pure high degree of $\psi$ is $\tilde{\Omega}(R^{1/4}N^{-1/(4k)})$.
  - $\psi$ satisfies a “weak decay condition”, viz. $\sum_{|x|=t} |\psi(x)| \leq \sigma \exp(-\beta t)/t^2$ for some constant $\sigma$ (for general $k$, the value of $\sigma$ only depends on $k$), and $\beta = \tilde{\Omega}(R^{1/4}N^{1/(4k)})$.

- The function $\phi$ is defined on $4^k$ inputs, and is defined as in Claim 2.3.10.

- $\theta$ is constructed as in Claim 2.3.4 with $n = R/4^k$.

If we were to define $\Gamma = \theta \ast \phi \ast \psi$, all the analyses from the previous section would work, except for the correlation analysis, which fails. To fix this, our main technical contribution is to not use dual block composition, but rather a variant of it inspired by a result of Sherstov [120]. Our function $\Gamma$ takes the form $\Gamma = \theta \bullet (\phi \ast \psi)$, where $\bullet$
denotes our variant of dual block composition. In a little more detail, 

\[ \Gamma(x_1, \ldots, x_{R/4^k}) := \]

\[ \frac{1}{\nu(1 - 2\epsilon^+, \ldots, 1 - 2\epsilon^+)} \cdot (\theta \ast (\phi \ast \psi))(x_1, \ldots, x_{R/4^k}) \cdot \nu(\alpha(x_1), \ldots, \alpha(x_{R/4^k})), \]

for 

\[ \epsilon^+ = \epsilon^+_{\text{OR}_k \circ \text{THR}_N, \phi \ast \psi} \]

\[ \epsilon^- = \epsilon^-_{\text{OR}_k \circ \text{THR}_N, \phi \ast \psi} \]

\(\eta\) is a parameter that we set later, \(p_\eta\) is defined as in Lemma 2.3.12, and \(\alpha\) is a function whose definition we elaborate on later in this section.

We first give a very high-level idea of how we prove the required properties of \(\Gamma\), and then elaborate on the definitions of \(\eta, p_\eta\) and \(\alpha\).

- **Normalization:** Following along similar lines as [120, Claim 6.2], we prove that \(\|\Gamma\|_1 = 1\) by modifying the proof that dual block composition preserves \(\ell_1\)-norm, crucially exploiting properties of \(p_\eta\) and \(\alpha\) (see Claim 2.5.5). 

- **Pure high degree:** Using our definition of \(p_\eta\) and \(\alpha\), one can show (Claim 2.5.6) that the pure high degree of \(\theta \bullet (\phi \ast \psi)\) is at least \((\text{phd}(\theta) - \eta)\text{phd}(\phi \ast \psi)\). The value of \(\eta\) is chosen to be \(\text{phd}(\theta)/2\) so that this quantity is the same order of magnitude as \(\text{phd}(\theta)\text{phd}(\phi \ast \psi) = \text{phd}(\theta)\text{phd}(\psi)\), which is \(\tilde{\Omega}(R^{3/4}N^{-1/(4k)})\).

- **Exponentially little mass on inputs of large Hamming weight:** By a similar argument as sketched in the last section, it can be shown that the mass placed by \((\theta \ast \phi) \ast \psi\) on inputs of Hamming weight larger than \(N\) is exponentially small in \(\tilde{\Omega}(R^{3/4}N^{-1/(4k)})\). Since \(\theta \bullet (\phi \ast \psi) := \frac{1}{\nu(1 - 2\epsilon^+, \ldots, 1 - 2\epsilon^+)} \cdot (\theta \ast (\phi \ast \psi))(x_1, \ldots, x_{R/4^k}) \cdot \nu(\alpha(x_1), \ldots, \alpha(x_{R/4^k}))\), it suffices to show that the maximum absolute value
of $\frac{p_\eta(\alpha(x_1),\ldots,\alpha(x_{R/4k}))}{p_\eta(1-2\epsilon^+,\ldots,1-2\epsilon^+)}$ is at most exponentially large in $R^{\frac{1}{4}-\frac{1}{4k}}$, which we do in Claim 2.6.5.

- **Correlation:** Conceptually, the function $p_\eta : \langle -1, 1 \rangle^{R/4k} \to \mathbb{R}$ can be viewed as one that “corrects” $\theta \ast (\phi \ast \psi)$: it “counts” the number of false positives fed to it by $\phi \ast \psi$, and changes the output of $\theta \ast (\phi \ast \psi)$ to 0 on inputs where this number is any integer between 1 and $\eta$. The function $\alpha : \langle -1, 1 \rangle^N \to \mathbb{R}$ acts as the function that, in a sense, indicates whether or not $\phi \ast \psi$ is making a false positive error.

  - **Detecting errors:** The function $\alpha$ takes three possible output values: it outputs $-1$ for $x \in E^+(\text{OR}_{4k} \circ \text{THR}_N^k, \phi \ast \psi)$ and outputs either 1 or a value very close to 1 for $x \notin E^+(\text{OR}_{4k} \circ \text{THR}_N^k, \phi \ast \psi)$. This definition of $\alpha$ is our biggest departure from Sherstov’s construction in [120]; Sherstov defined $\alpha$ to output $-1$ for both false-positive and false-negative errors, whereas our $\alpha$ only outputs $-1$ for false-positive errors.

  - **Zeroing out errors:** Define the function $p_\eta$ to be (the unique multilinear extension of) the function that outputs 0 if its input has Hamming weight between 1 and $\eta$. Recall that our construction considers the dual witness

    $$
    \frac{1}{p_\eta(1-2\epsilon^+,\ldots,1-2\epsilon^+)}(\theta \ast (\phi \ast \psi))(x_1,\ldots,x_{R/4k}) \cdot p_\eta(\alpha(x_1),\ldots,\alpha(x_{R/4k})),
    $$

    and the purpose of multiplying $\theta \ast (\phi \ast \psi)$ by $p_\eta$ is for $p_\eta$ to zero out most inputs in which one or more false-positive errors are being fed by $\phi \ast \psi$ into $\theta$ (see Equation (9)).

    Unfortunately, $p_\eta$ is nonzero on inputs of Hamming weight more than $\eta$. Hence, in terms of the correlation analysis, a key question that must be addressed is: what fraction of the $\ell_1$-mass of $\theta \ast (\phi \ast \psi)$ is placed on inputs
where more than \( \eta \) copies of \( \phi \star \psi \) make a false-positive error? We need this fraction to be very small, because multiplying by \( p_\eta \) fails to zero out such inputs.

Note that under the distribution defined by \(|\phi \star \psi|\), the expected number of false positive errors fed into \( \theta \) is \((R/4^k) \cdot \epsilon^+\). Since we have set \( \eta = O(\sqrt{R}/(4 \cdot 4^k)) \), it suffices to have \( \epsilon^+ \ll 1/(c\eta) \) for some large enough constant \( c \) to conclude that with high probability (over the distribution \(|\phi \star \psi|\)), the number of false positive errors fed into \( \theta \) is at most a small constant times \( \eta \). It turns out that this value of \( \epsilon^+ \) is indeed attained by \( \phi \star \psi \), since the false positive error between \( \text{THR}_N^k \) and \( \psi \) was set to be \( \tilde{O}(1/\sqrt{N}) = \tilde{O}(1/\sqrt{R}) \) to begin with. Thus, with high probability, multiplying \( \theta \star (\phi \star \psi) \) by \( p_\eta \) successfully zeros out all but an exponentially small fraction of the errors made by \( \theta \star (\phi \star \psi) \) that can be attributed to false-positive errors made by \( \phi \star \psi \). This intuitive proof outline is formalized in Claim 2.6.3, which in turn is a formalization of Equation (2.1) that holds with the setting of parameters mentioned above.

### 2.5 Properties of Auxiliary Functions

Given any function \( f : \langle -1,1 \rangle^m \to \langle -1,1 \rangle \) and \( \psi : \langle -1,1 \rangle^m \to \mathbb{R}, \|\psi\|_1 = 1 \), let \( \epsilon^+ = \epsilon^+_{f,\psi} \) and \( \epsilon^- = \epsilon^-_{f,\psi} \) as defined in Equation (2.11). Define the function \( \alpha_{f,\psi} : \langle -1,1 \rangle^m \to \mathbb{R} \) as

\[
\alpha_{f,\psi}(x) := \begin{cases} 
1 =: a^+ & \text{if } \psi(x)f(x) > 0, \psi(x) > 0 \\
\frac{1-2\epsilon^+ - \epsilon^-}{1-\epsilon^-} =: a^- & \text{if } \psi(x)f(x) > 0, \psi(x) < 0 \\
-1 & \text{if } \psi(x)f(x) < 0, \psi(x) > 0 \\
1 & \text{if } \psi(x)f(x) < 0, \psi(x) < 0.
\end{cases}
\] (2.46)
For the remaining sections, for $z_i \in \langle -1, 1 \rangle$, $a^{z_i} = a^+$ if $z_i = 1$, and $a^{z_i} = a^-$ if $z_i = -1$.

**Claim 2.5.1** For any integer $m > 0$, any functions $f : \langle -1, 1 \rangle^m \to \langle -1, 1 \rangle$ and $\psi : \langle -1, 1 \rangle^m \to \mathbb{R}$ such that $\|\psi\|_1 = 1$, let $\alpha = \alpha_{f, \psi} : \langle -1, 1 \rangle^m \to \mathbb{R}$ be as defined in Equation (2.46). Then for any integer $n > 0$, any $z$ in $\langle -1, 1 \rangle^n$, and all $i \in [n]$,

$$E_{(x_1, \ldots, x_n) \sim \mu_z}[\alpha(x_i)] = 1 - 2\epsilon^+_f.$$  \hspace{1cm} (2.47)

**Proof.** Let $\epsilon^+ = \epsilon^+_f$ and $\epsilon^- = \epsilon^-_f$.

$$E_{\mu_z}[\alpha(x_i)] = E_{\mu_z}[\alpha(x_i)]$$

by Equation (2.9)

$$= \begin{cases} 
\epsilon^+ \cdot -1 + (1 - \epsilon^+) \quad & \text{if } z_i = 1 \\
\epsilon^- \cdot 1 + (1 - \epsilon^-) \frac{1 - 2\epsilon^+ - \epsilon^-}{1 - \epsilon^-} \quad & \text{if } z_i = -1 
\end{cases}$$

by Definition 1 and Equation (2.46)

$$= 1 - 2\epsilon^+.$$  

Consider any positive integer $m$, functions $f : \langle -1, 1 \rangle^m \to \langle -1, 1 \rangle$ and $\psi : \langle -1, 1 \rangle^m \to \mathbb{R}$, and any integers $\eta < n$. By Claim 2.5.1, Equation (2.9) and the fact that $p_{\eta} : [-1, 1]^n \to \mathbb{R}$ as defined in Lemma 2.3.12 is multilinear, it holds for all $z \in \langle -1, 1 \rangle^n$ that

$$E_{\mu_z}[p_{\eta}(\alpha(x_1), \ldots, \alpha(x_n))] = p_{\eta}(1 - 2\epsilon^+_f, \ldots, 1 - 2\epsilon^+_f).$$  \hspace{1cm} (2.48)

Let

$$b^+ := 0, \quad b^- := \frac{\epsilon^+_f}{1 - \epsilon^-_f},$$  \hspace{1cm} (2.49)

and $a^+, a^-$ be as defined in Equation (2.46). For the remaining sections, for $z_i \in \langle -1, 1 \rangle$, $b^{z_i} := b^+$ if $z_i = 1$ and $b^{z_i} := b^-$ if $z_i = -1$. Then, by multilinearity of $p_{\eta}$ and Definition 2, for any $i \in [n]$ and any $c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n \in [-1, 1]$ we have

$$E_{w \sim \Pi(b^{z_i})}[p_{\eta}(c_1, \ldots, c_{i-1}, w, c_{i+1}, \ldots, c_n)] = p_{\eta}(c_1, \ldots, c_{i-1}, a^{z_i}, c_{i+1}, \ldots, c_n),$$  \hspace{1cm} (2.50)
since $1 - 2b^+ = 1 = a^+$ and $1 - 2b^- = \frac{1 - \epsilon^+ \epsilon^-}{1 - \epsilon^+ \epsilon^-} = a^-$. We also obtain that

$$\mathbb{E}_{(w_1, \ldots, w_n) \sim \Pi(b^{\pm 1}, \ldots, b^{\pm n})}[p_\eta(w_1, \ldots, w_n)] = p_\eta(a^{\pm 1}, \ldots, a^{\pm n}), \quad (2.51)$$

by Lemma 2.3.1. We now state the setting for our next few claims.

Assumptions for Claim 2.5.2, Claim 2.5.3, Claim 2.5.4, Claim 2.5.5: Let $m, n$ be any positive integers, $\eta < n$ be any even positive integer, and $f : \langle -1, 1 \rangle^m \rightarrow \langle -1, 1 \rangle$ be any function. Let $\zeta : \langle -1, 1 \rangle^n \rightarrow \mathbb{R}$ be such that $\langle \zeta, OR_n \rangle > \delta$ and $\|\zeta\|_1 = 1$, and $\xi : \langle -1, 1 \rangle^m \rightarrow \mathbb{R}$ be any function such that $\|\xi\|_1 = 1$ and $\text{phd}(\xi) \geq 1$. Let $p_\eta : \langle -1, 1 \rangle^n \rightarrow \mathbb{R}$ be as defined in Lemma 2.3.12, let $\alpha = \alpha_{f, \xi} : \langle -1, 1 \rangle^m \rightarrow \mathbb{R}$ be as defined in Equation (2.46), and define the distribution $\mu_{\xi}$ over $\langle -1, 1 \rangle^{nm}$ as in Equation (2.8). Let $\epsilon^+ = \epsilon_{f, \xi}^+$, $\epsilon^- = \epsilon_{f, \xi}^-$, $\epsilon = \epsilon^+ + \epsilon^-$, and $A = \left( \frac{n}{\eta+1} \right)^{(\epsilon^+)^{\eta+1}}$.

Claim 2.5.2

$$\zeta(1^n)\mathbb{E}_{x \sim \mu_{1^n}}[p_\eta(\alpha(x_1), \ldots, \alpha(x_n)) OR(f(x_1), \ldots, f(x_n))] \geq p_\eta(1 - 2\epsilon^+, \ldots, 1 - 2\epsilon^+) (\zeta(1^n) - |\zeta(1^n)|2A). \quad (2.52)$$

Claim 2.5.3

$$\sum_{z \neq 1^n} \zeta(z) \mathbb{E}_{\mu_{\eta}}[p_\eta(\alpha(x_1), \ldots, \alpha(x_n)) OR(f(x_1), \ldots, f(x_n))] \geq p_\eta(1 - 2\epsilon^+, \ldots, 1 - 2\epsilon^+)
\left( \sum_{z \neq 1^n} \zeta(z) OR(z) - \left( 2 - 2 \left( \frac{1 - \epsilon^+ - \epsilon^-}{1 - \epsilon^+} \right) (1 - A) \right) \sum_{z \neq 1^n} |\zeta(z)| \right). \quad (2.53)$$

Claim 2.5.4 If $A < 1$, then,

$$\langle OR \circ f, (\zeta \circ \xi)(p_\eta \circ \alpha) \rangle \geq p_\eta(1 - 2\epsilon^+, \ldots, 1 - 2\epsilon^+) \left( \delta - \left( 2 - 2 \left( \frac{1 - \epsilon^+ - \epsilon^-}{1 - \epsilon^+} \right) (1 - A) \right) \right). \quad (2.54)$$
We first prove Claim 2.5.4 using Claim 2.5.2 and Claim 2.5.3, and prove those claims later. \textit{Proof.} \\
\begin{align*}
\langle OR \circ f, (\zeta \star \xi)(p_\eta \circ \alpha) \rangle &= \sum_{x \in \{-1, 1\}^{mn}} (OR \circ f)(x)(\zeta \star \xi)(p_\eta \circ \alpha)(x) \\
&= \sum_{x \in \{-1, 1\}^{mn}} OR(f(x_1), \ldots, f(x_n))2^n \langle \text{sgn}(\xi(x_1)), \ldots, \text{sgn}(\xi(x_n)) \rangle_{E_\mu} p_\eta(\alpha(x_1), \ldots, \alpha(x_n)) \prod_{i=1}^{n} |\xi(x_i)| \\
&= \sum_{x \in \{-1, 1\}^{n}} \zeta(z) \left( \sum_{z \neq 1} \prod_{i=1}^{n} |\xi(x_i)| \right)
\end{align*}

by Definition 9

\begin{align*}
&= \sum_{z \in \{-1, 1\}^{n}} \zeta(z) \left( \sum_{z \neq 1} \prod_{i=1}^{n} |\xi(x_i)| \right) \\
&= \sum_{z \in \{-1, 1\}^{n}} \zeta(z) \left( \prod_{i=1}^{n} |\xi(x_i)| \right)
\end{align*}

by Definition 1 and \( \text{Pr}_{x_i \sim \mu_\xi}[\text{sgn}(x_i) = 1] = \text{Pr}_{x_i \sim \mu_\xi}[\text{sgn}(x_i) = -1] = 1/2 \) since \( \text{phd}(\xi) \geq 1 \)

\begin{align*}
&\geq p_\eta(1 - 2 \epsilon^+, \ldots, 1 - 2 \epsilon^+) \left( \zeta(1^n)\text{OR}(1^n) - 2|\zeta(1^n)|A + \sum_{z \neq 1^n} \zeta(z)\text{OR}(z) \right) \\
&- \left( 2 - 2 \left( \frac{1 - \epsilon^+ - \epsilon^-}{1 - \epsilon^+} \right) (1 - A) \right) \sum_{z \neq 1^n} |\zeta(z)| \quad \text{by Claims 2.5.2, 2.5.3 and OR}(1^n) = 1 \\
&= p_\eta(1 - 2 \epsilon^+, \ldots, 1 - 2 \epsilon^+) \left( \sum_{z \neq 1^n} \zeta(z)\text{OR}(z) - 2|\zeta(1^n)|A - \left( 2 - 2 \left( \frac{1 - \epsilon^+ - \epsilon^-}{1 - \epsilon^+} \right) (1 - A) \right) \sum_{z \neq 1^n} |\zeta(z)| \right) \\
&\geq p_\eta(1 - 2 \epsilon^+, \ldots, 1 - 2 \epsilon^+) \left( \delta - \max \left\{ 2A, 2 - 2 \left( \frac{1 - \epsilon^+ - \epsilon^-}{1 - \epsilon^+} \right) (1 - A) \right\} \right) \\
&\geq p_\eta(1 - 2 \epsilon^+, \ldots, 1 - 2 \epsilon^+) \left( \delta - 2 - 2 \left( \frac{1 - \epsilon^+ - \epsilon^-}{1 - \epsilon^+} \right) (1 - A) \right)
\end{align*}

where the last inequality holds because \( \left( 2 - 2 \left( \frac{1 - \epsilon^+ - \epsilon^-}{1 - \epsilon^+} \right) (1 - A) \right) - 2A = (1 - A) \left( 2 - 2 \left( \frac{1 - \epsilon^+ - \epsilon^-}{1 - \epsilon^+} \right) \right) > 0 \) since \( \left( \frac{1 - \epsilon^+ - \epsilon^-}{1 - \epsilon^+} \right) < 1 \), and \( A < 1 \). Next we prove Claim 2.5.2. \textit{Proof.} [Proof of Claim 2.5.2] Recall that \( \mu_{1^n} \) is the distribution \( \mu_\xi \) conditioned on the event that \( \text{sgn}(\xi(x_i)) = 1 \) for all \( i \in [n] \). Note that for all \( x_1, \ldots, x_n \) in the support of \( \mu_{1^n} \) such that \( I[(f(x_1), \ldots, f(x_n)) = 1^n] \) (which means \( f(x_i) = 1 \) for all \( i \in [n] \)), we have by the definition of \( a^z_i \) in Equation (2.46), that \( \alpha(x_i) = a^+ \) for
all $i \in [n]$. Hence,

$$
\mathbb{E}_{\mu_1^n}[p_\eta(\alpha(x_1), \ldots, \alpha(x_n)) I[(f(x_1), \ldots, f(x_n)) = 1^n]]
$$

$$
= \Pr_{x \sim \mu_1^n}[(f(x_1), \ldots, f(x_n)) = 1^n] p_\eta(a^+, \ldots, a^+)
$$

$$
= \left(\prod_{i=1}^{n} \Pr_{\mu_1^i}[f(x_i) = 1]\right) p_\eta(a^+, \ldots, a^+)
$$  

by Equation (2.9)

$$
= \left(\prod_{i=1}^{n} (1 - \epsilon^+)^n \mathbb{E}_{w \sim \Pi(b^+, \ldots, b^+)}[p_\eta(w)]\right)
$$  

by Equation (2.11) and Equation (2.51)

$$
\geq (1 - \epsilon^+)^n \mathbb{P}_{w \sim \Pi(b^+, \ldots, b^+)}[w = 1^n] p_\eta(1^n)
$$

since $p_\eta(w) \geq 0$ for all $w \in \{-1, 1\}^n$ by Lemma 2.3.12

$$
= (1 - \epsilon^+)^n p_\eta(1^n),
$$

(2.55)

where the last line follows by Definition 2 and Equation (2.49). Next,

$$
|\mathbb{E}_{\mu_1^n}[p_\eta(\alpha(x_1), \ldots, \alpha(x_n)) OR(f(x_1), \ldots, f(x_n))] - p_\eta(1 - 2\epsilon^+, \ldots, 1 - 2\epsilon^+)|
$$

$$
= \mathbb{E}_{\mu_1^n}[p_\eta(\alpha(x_1), \ldots, \alpha(x_n)) (OR(f(x_1), \ldots, f(x_n)) - 1)]
$$  

by Equation (2.48)

$$
= 2\mathbb{E}_{\mu_1^n}[p_\eta(\alpha(x_1), \ldots, \alpha(x_n))(1 - I[(f(x_1), \ldots, f(x_n)) = 1^n])]
$$

$$
\leq 2\mathbb{E}_{\mu_1^n}[p_\eta(\alpha(x_1), \ldots, \alpha(x_n))] - 2(1 - \epsilon^+)^n p_\eta(1^n)
$$

(2.56)

by Equation (2.55). Hence, by Equation (2.56),

$$
\zeta(1^n) \mathbb{E}_{\mu_1^n}[p_\eta(\alpha(x_1), \ldots, \alpha(x_n)) OR(f(x_1), \ldots, f(x_n))]
$$

$$
\geq \zeta(1^n) p_\eta(1 - 2\epsilon^+, \ldots, 1 - 2\epsilon^+)
$$

$$
- |\zeta(1^n)| \left(2\mathbb{E}_{\mu_1^n}[p_\eta(\alpha(x_1), \ldots, \alpha(x_n))] - 2(1 - \epsilon^+)^n p_\eta(1^n)\right)
$$

$$
= p_\eta(1 - 2\epsilon^+, \ldots, 1 - 2\epsilon^+) \left(\zeta(1^n) - |\zeta(1^n)| \left(2 - \frac{2(1 - \epsilon^+)^n p_\eta(1^n)}{p_\eta(1 - 2\epsilon^+, \ldots, 1 - 2\epsilon^+)}\right)\right)
$$  

by Equation (2.48)

$$
\geq p_\eta(1 - 2\epsilon^+, \ldots, 1 - 2\epsilon^+) (\zeta(1^n) - |\zeta(1^n)| 2A),
$$

(2.57)
where the last inequality follows as we have by Equation (2.33) and the fact that \( p_\eta \) is non-negative on all Boolean inputs (Lemma 2.3.12) that

\[
\mathbb{E}_{\Pi(\epsilon^+,...,\epsilon^+)}[p_\eta(z)] \leq p_\eta(1^n)(1 - \epsilon^+)^n(1 + A),
\]

which by Lemma 2.3.1 implies that

\[
\frac{2p_\eta(1^n)(1 - \epsilon^+)^n}{p_\eta(1 - 2\epsilon^+,...,1 - 2\epsilon^+)} \geq 2(1 + A)^{-1} \geq 2(1 - A),
\]

for all \( A \geq 0 \). We now prove Claim 2.5.3. **Proof.** [Proof of Claim 2.5.3]

We first introduce some notation that we use in this proof. For any \( i \in [n] \) and \( r \in [-1, 1] \), let \( y^i(r) \) denote the \( n \)-bit string \((1 - 2\epsilon^+,...,1 - 2\epsilon^+,r,1 - 2\epsilon^+,...,1 - 2\epsilon^+)\), where \( r \) is in the \( i \)'th position. It is easy to verify from its definition that \( p_\eta \) is symmetric on \((-1, 1)^n\). Hence, for any \( i \in [n] \),

\[
p_\eta(y^i(1))(1 - \epsilon^+) = \mathbb{E}_{w \sim \Pi(\epsilon^+,...,\epsilon^+)}[p_\eta(w, 1)](1 - \epsilon^+)
\]

by Lemma 2.3.1

\[
\geq \mathbb{P}_{w \sim \Pi(\epsilon^+,...,\epsilon^+)}[w = 1^{n-1}] \ p_\eta(1^n)(1 - \epsilon^+)
\]

since \( p_\eta(w, 1) \geq 0 \) for all \( w \in (-1, 1)^{n-1} \) by Lemma 2.3.12

\[
=p_\eta(1^n)(1 - \epsilon^+)^n,
\]

where the last equality follows from Definition 2. For any \( z \neq 1^n \), let \( i \in [n] \) be an index such that \( z_i = -1 \). Fix any \( z \neq 1^n \). Note that by Equation (2.46) and Equation (2.9), \( \alpha(x_i) = a^- \) for all \( x_i \) in the support of \( \mu_{z_i} \) satisfying \( f(x_i) = -1 \).

The notation \( i_z \) is more accurate, but we drop the dependence on \( z \) to avoid clutter. The underlying \( z \) will be clear from context.
Hence,

\[ \mathbb{E}_{x \sim \mu_z} [p_\eta(\alpha(x_1), \ldots, \alpha(x_n)) I[f(x_i) = -1]] = \Pr_{\mu_z}[f(x_i) = -1] p_\eta(y^i(a^-)) \]

by Claim 2.5.1

\[ = \Pr_{\mu_z}[f(x_i) = -1] \mathbb{E}_{w \sim \Pi(b^-)} [p_\eta(y^i(w))] \]

by Equation (2.50)

\[ = (1 - \epsilon^-) \mathbb{E}_{w \sim \Pi(b^-)} [p_\eta(y^i(w))] \]

by Definition 1 the definition of \( \epsilon^- \) in Equation (2.11)

\[ \geq (1 - \epsilon^-) \left( 1 - \frac{\epsilon^+}{1 - \epsilon^-} \right) p_\eta(y^i(1)) \]

by Equation (2.49) and Definition 2 and \( p_\eta \) is non-negative on \((-1, 1]^n\) (Lemma 2.3.12)

\[ = (1 - \epsilon^- - \epsilon^+) p_\eta(y^i(1)). \]  \hspace{1cm} (2.61)

Next,

\[ |\mathbb{E}_{\mu_z} [p_\eta(\alpha(x_1), \ldots, \alpha(x_n)) (\text{OR}(f(x_1), \ldots, f(x_n)) - \text{OR}(z))]| \]

\[ = |\mathbb{E}_{\mu_z} [p_\eta(\alpha(x_1), \ldots, \alpha(x_n)) (\text{OR}(f(x_1), \ldots, f(x_n)) + 1)]| \]

since \( \text{OR}(z) = -1, \forall z \neq 1^n \)

\[ \leq 2 \mathbb{E}_{\mu_z} [p_\eta(\alpha(x_1), \ldots, \alpha(x_n)) (1 - I[f(x_i) = -1])] \]

since \( p_\eta \) is non-negative on \((-1, 1]^n\) by Lemma 2.3.12

\[ \leq 2 \mathbb{E}_{\mu_z} [p_\eta(\alpha(x_1), \ldots, \alpha(x_n))] - 2(1 - \epsilon^- - \epsilon^+) p_\eta(y^i(1)), \]  \hspace{1cm} (2.62)
where the last inequality follows by next applying Equation (2.61). Finally,

\[
\sum_{z \not\in \Omega_{\varepsilon}} \mathbb{E}_{\mu_z} [p_\eta(\alpha(x_1), \ldots, \alpha(x_n)) | OR(f(x_1), \ldots, f(x_n))] | \zeta(z)
\geq \sum_{z \not\in \Omega_{\varepsilon}} |\zeta(z)| p_\eta(y'(1 - 2\epsilon^+)) \geq \sum_{z \not\in \Omega_{\varepsilon}} |\zeta(z)| (2p_\eta(y'(1 - 2\epsilon^+)) - 2(1 - \epsilon^- - \epsilon^+) p_\eta(y'(1)))
\]

by Equation (2.62) and Equation (2.48)

\[
p_\eta(1 - 2\epsilon^+, \ldots, 1 - 2\epsilon^+) \left( \sum_{z \not\in \Omega_{\varepsilon}} |\zeta(z)| OR(z) - \left(2 - 2 \left(\frac{1 - \epsilon^+ - \epsilon^-}{1 - \epsilon^+}\right) \frac{1 - \epsilon^+ p_\eta(y'(1))}{p_\eta(y'(1 - 2\epsilon^+))} \right) \sum_{z \not\in \Omega_{\varepsilon}} |\zeta(z)| \right)
\]

by Equation (2.60)

\[
p_\eta(1 - 2\epsilon^+, \ldots, 1 - 2\epsilon^+) \left( \sum_{z \not\in \Omega_{\varepsilon}} |\zeta(z)| OR(z) - \left(2 - 2 \left(\frac{1 - \epsilon^+ - \epsilon^-}{1 - \epsilon^+}\right) \frac{1 - \epsilon^+ p_\eta(y'(1))}{p_\eta(y'(1 - 2\epsilon^+))} \right) \sum_{z \not\in \Omega_{\varepsilon}} |\zeta(z)| \right).
\]

by Equation (2.59)

Finally, we require a closed form expression for \(\| (\zeta * \xi)(p_\eta \circ \alpha) \|_1\).

**Claim 2.5.5**

\[
\| (\zeta * \xi)(p_\eta \circ \alpha) \|_1 = p_\eta(1 - 2\epsilon^+, \ldots, 1 - 2\epsilon^+).
\]

The proof of the claim follows along the lines as that of [120, Claim 6.2], but we provide the proof for completeness. **Proof.** Consider the distribution \(\mu\) on \((-1, 1)^n\) defined by \(\mu(x_1, \ldots, x_n) = \prod_{i=1}^n \mu_i(x_i)\). Since \(\text{phd}(\xi) \geq 1\), we conclude that the string \((\text{sgn}(\xi(x_1)), \ldots, \text{sgn}(\xi(x_n)))\) is uniformly distributed in \((-1, 1)^n\) when \((x_1, \ldots, x_n)\) is sampled from \(\mu\). Hence, we have

\[
\| (\zeta * \xi)(p_\eta \circ \alpha) \|_1 = \sum_{x \in (-1, 1)^n} 2^n \zeta(\text{sgn}(\xi(x_1)), \ldots, \text{sgn}(\xi(x_n))) p_\eta(\alpha(x_1), \ldots, \alpha(x_n)) \prod_{i=1}^n |\xi(x_i)|
\]

\[
= \sum_{x \in (-1, 1)^n} |\zeta(z)| \mathbb{E}_{\mu_z} [p_\eta(\alpha(x_1), \ldots, \alpha(x_n))]
\]

\[
= \sum_{x \in (-1, 1)^n} |\zeta(z)| \mathbb{E}_{\mu_z} [p_\eta(\alpha(x_1), \ldots, \alpha(x_n))]
\]

since \(p_\eta\) is non-negative on \((-1, 1)^n\) by Lemma 2.3.12

\[
= p_\eta(1 - 2\epsilon^+, \ldots, 1 - 2\epsilon^+) \sum_{z \in (-1, 1)^n} |\zeta(z)|
\]

by Equation (2.48)

\[
= p_\eta(1 - 2\epsilon^+, \ldots, 1 - 2\epsilon^+). 
\]

since \(\|\zeta\|_1 = 1\)
Claim 2.5.6 Let $\Psi : (-1, 1]^n \to \mathbb{R}$, $\Lambda : (-1, 1]^m \to \mathbb{R}$, and $f : (-1, 1]^m \to \mathbb{R}$ be any functions. For any positive integer $\eta$, let $\alpha = \alpha_{f, \Lambda} : (-1, 1]^m \to \mathbb{R}$ be as defined in Equation (2.46), and $p_\eta : (-1, 1]^n \to \mathbb{R}$ defined in Lemma 2.3.12. Then

$$\text{phd}((\Psi \star \Lambda) \cdot (p_\eta \circ \alpha)) > (\text{phd}(\Psi) - \eta) \cdot \text{phd}(\Lambda).$$

(2.65)

The proof follows along the same lines as that of [120, Equation (6.7)] and we omit it.

2.6 Proof of Theorem 2.4.4

Towards proving Theorem 2.4.4, it suffices to exhibit a dual polynomial (see Lemma 2.3.3) that has $\ell_1$-norm 1, sufficiently large pure high degree, good correlation with $(\text{OR}_R \circ \text{THR}_N^k) \leq N$, and places no mass outside $(\langle -1, 1 \rangle^N_{R}) \leq N$. We first define a function $\Gamma$ (Definition 13) that satisfies the first three properties above, and additionally satisfies a strong decay condition. In Section 2.6.2 we use $\Gamma$ to construct a dual polynomial $\mathcal{W}$, via Lemma 2.3.14, satisfying all the requisite properties. We now set several key variables.

- Let $R$ be sufficiently large and fix $k \leq (\log R)/4$. Set $T = \sqrt{R}$, $\eta = \left(\frac{c}{2} \sqrt{\frac{R}{4^k}}\right) - 1$ where $c \in (0, 1]$ is the constant from Claim 2.3.4 (assume without loss of generality that $\eta$ is even), $\sigma = (2k)^k$, $c_1, c_2 \in (0, 1]$ are constants fixed in the next bullet point, $\beta = \frac{c_2}{\sqrt{4^k k T N^{1/(2k)}} \log N}$, $\Delta = \frac{\beta \sqrt{\sigma R}}{4 \ln^2 R} = \frac{c_2 R}{4 \ln^2 R} \sqrt{4^k k T N^{1/(2k)}} \log N$, $N = \lceil 20 \sqrt{\sigma R} \rceil$.

- Let $\omega_T : [T] \cup \{0\} \to \mathbb{R}$ be a function that satisfies the conditions in Claim 2.3.6 and let $c_1, c_2$ be the constants for which the claim holds. Let $\psi : (-1, 1]^N \to \mathbb{R}$ be defined by $\psi(x) = \omega_T(|x|)/\binom{N}{|x|}$ if $|x| \leq T$, and 0 otherwise.
Let \( \theta : \langle -1, 1 \rangle^{R/4^k} \rightarrow \mathbb{R} \) be any function satisfying the conditions in Claim 2.3.4 for \( n = R/4^k \) (note that \( R/4^k > 0 \) since \( k < (\log R)/2 \)).

Let \( \phi : \langle -1, 1 \rangle^{4^k} \rightarrow \mathbb{R} \) be the function defined in Claim 2.3.10 with \( n = 4^k \).

Let \( p_\eta : [-1, 1]^{R/4^k} \rightarrow \mathbb{R} \) be as defined in Lemma 2.3.12.

Let \( \alpha := \alpha_{\text{OR}_{4^k} \circ \text{THR}_{N/4}^k, \phi \ast \psi} : \langle -1, 1 \rangle^{4^k N} \rightarrow \mathbb{R} \) be as defined in Equation (2.46).

Let \( \epsilon^+ := \epsilon^+_{\text{OR}_{4^k} \circ \text{THR}_{N/4}^k, \phi \ast \psi}, \epsilon^- := \epsilon^-_{\text{OR}_{4^k} \circ \text{THR}_{N/4}^k, \phi \ast \psi}, \) and \( \epsilon := \epsilon^+ + \epsilon^- \).

We next define the function \( \Gamma \).

**Definition 13** Let \( \Gamma : \langle -1, 1 \rangle^{NR} \rightarrow \mathbb{R} \) be defined by

\[
\Gamma(x_1, \ldots, x_{R/4^k}) := \frac{(\theta \ast (\phi \ast \psi))(x_1, \ldots, x_{R/4^k}) \cdot p_\eta(\alpha(x_1), \ldots, \alpha(x_{R/4^k}))}{p_\eta(1 - 2\epsilon^+, \ldots, 1 - 2\epsilon^+)} ,
\]

where each \( x_i \in \langle -1, 1 \rangle^{4^k N} \).

**2.6.1 Properties of \( \Gamma \)**

We now show that \( \Gamma \) satisfies the following four properties.

- \( \langle \Gamma, \text{OR}_R \circ \text{THR}_{N/4}^k \rangle > 1/3 \).

- \( \|\Gamma\|_1 = 1 \).

- \( \text{phd}(\Gamma) = \Omega \left( \frac{1}{4^k k^2} \cdot \frac{1}{\sqrt{\log R}} \cdot R^{3/4 - 1/4^k} \right) \).

- \( \sum_{x \in \langle -1, 1 \rangle^{RN} \leq N} |\Gamma(x)| \leq (2NR)^{-2(\Delta - \sqrt{R})} \).

We show the required lower bound on \( \text{phd}(\Gamma) \).

**Claim 2.6.1**

\[
\text{phd}(\Gamma) = \Omega \left( \frac{1}{4^k k^2} \cdot \frac{1}{\sqrt{\log R}} \cdot R^{3/4 - 1/4^k} \right) .
\]
Proof.

\[ \text{phd}(\Gamma) = \text{phd}((\theta \ast (\phi \ast \psi))(p_\eta \circ \alpha)) \] by Definition 13

\[ \geq (\text{phd}(\theta) - \eta) \cdot \text{phd}(\phi \ast \psi) \] by Claim 2.5.6, using \( \Psi = \theta, \Lambda = \phi \ast \psi, \) and \( f = \text{OR}_{4k} \circ \text{THR}_N^k \)

\[ \geq \frac{c}{2} \sqrt{\frac{R}{4^k}} \cdot \text{phd}(\phi) \cdot \text{phd}(\psi) \] by Claim 2.3.8, Claim 2.3.4, and since \( \eta = \left( \frac{c}{2} \sqrt{\frac{R}{4^k}} \right) - 1 \)

\[ \geq \frac{c}{2} \sqrt{\frac{R}{4^k}} \cdot c_1 \sqrt{4^{-k-1}TN^{-1/(2k)} \log^{-1} N} \] by Claim 2.3.10 and Equation (2.21)

\[ = \frac{cc_1}{2} \sqrt{\frac{RT}{4^{2k}kN^{1/(2k)} \log N}} \]

\[ = \frac{cc_1}{2} \sqrt{\frac{1}{\log N} \left( \frac{1}{4^{2k}k} \sqrt{\frac{RT}{N^{1/2k}}} \right)} \]

\[ = \frac{cc_1}{2} \sqrt{\frac{1}{\log 20 + (1/2) \cdot k \log(2k) + \log R} \sqrt{\frac{1}{4^{2k}k} \sqrt{R \sqrt{N}}} \left( \frac{1}{20 \sqrt{(2k)^k R)^{1/2k}}} \right)} \]

using \( T = \sqrt{R} \) and \( N = 20 \sqrt{(2k)^k R} \)

\[ \geq \frac{cc_1}{2^{9/8}} \cdot \frac{1}{\sqrt{k \log R}} \cdot \frac{1}{4^k \cdot 20^{1/(4k)} \cdot k^{5/8}} \cdot R^{3/4 - 1/(4k)} \]

since \( k \log R > \log 20 + 1/2 \cdot k \log(2k) + \log R \) for sufficiently large \( R \)

\[ = \frac{cc_1}{2^{9/8}} \cdot \frac{1}{4^k \cdot 20^{1/(4k)} \cdot k^{5/8} \cdot \sqrt{\log R}} \cdot R^{3/4 - 1/(4k)} \]

\[ \geq \frac{cc_1}{60} \cdot \frac{1}{\sqrt{\log R}} \cdot \frac{1}{4^k k^2} \cdot R^{3/4 - 1/(4k)}. \] since \( 1/20^{1/(4k)} > 1/20, \) for all \( k \geq 2 \)

We then show that the function \( \phi \ast \psi \) has large correlation with \( \text{OR}_{4^k} \circ \text{THR}_N^k \), the following analysis is essentially the same as in [37, Proposition 55].
Claim 2.6.2

\[ \epsilon_{OR_4 \circ THR^k_N, \phi \star \psi}^+ \leq \frac{1}{24 \sqrt{R \log R}}, \quad (2.68) \]

\[ \epsilon_{OR_4 \circ THR^k_N, \phi \star \psi}^- \leq e^{-4}. \quad (2.69) \]

Proof.

\[ \epsilon_{OR_4 \circ THR^k_N, \phi \star \psi}^+ = 2 \delta_{OR_4 \circ THR^k_N, \phi \star \psi}^+ \quad \text{by Claim 2.3.2} \]

\[ \leq 2 \cdot 4^k \cdot \delta_{THR^k_N, \psi}^+ \quad \text{by Equation (2.28), using } M = 4^k \]

\[ \leq \frac{1}{24 \sqrt{N \log N}} \quad \text{by Equation (2.18)} \]

\[ \leq \frac{1}{24 \sqrt{R \log R}}. \quad \text{since } N = \lceil 20 \sqrt{\sigma R} \rceil > R \]

Next,

\[ \epsilon_{OR_4 \circ THR^k_N, \phi \star \psi}^- = 2 \delta_{OR_4 \circ THR^k_N, \phi \star \psi}^- \quad \text{by Claim 2.3.2} \]

\[ \leq (2 \delta_{THR^k_N, \psi}^-)^{4^k} \quad \text{by Equation (2.29) using } M = 4^k \]

\[ \leq \left(1 - \frac{4}{4^k}\right)^{4^k} \quad \text{by Equation (2.19)} \]

\[ \leq e^{-4}. \quad \text{since } (1 - 1/n)^n \leq 1/e \text{ for all } n \geq 1 \]

Claim 2.6.3 The function \( \Gamma \) satisfies

\[ \|\Gamma\|_1 = 1, \]

\[ \langle \Gamma, (OR_R \circ THR^k_N) \rangle > 1/3. \]

Proof. The conditions of Claim 2.5.5 are satisfied with \( n = R/4^k, m = 4^k N, f = OR_4 \circ THR^k_N, \zeta = \theta, \xi = \phi \star \psi, \eta = \left(\frac{\xi}{\sqrt{4^k}}\right) - 1. \) Hence by Claim 2.5.5,

\[ \|\Gamma\|_1 = \frac{\|((\theta \star (\phi \star \psi))(p_\eta \circ \alpha))\|_1}{p_\eta(1 - 2\epsilon^+, \ldots, 1 - 2\epsilon^+)} = 1. \]
Define \( A = \left( \frac{R/4^k}{\eta+1} \right)^{(e^+)^{\eta+1}} \). If \( A < 1 \), then the conditions of Claim 2.5.4 are satisfied with the same parameters mentioned in the beginning on this proof.

We first show that \( A < 1 \), and then invoke Claim 2.5.4. To avoid clutter, define \( \gamma = \eta + 1 = \frac{e}{2} \sqrt{\frac{R}{4^k}} \).

\[
A = \left( \frac{R/4^k}{\eta+1} \right)^{(e^+)^{\eta+1}} \frac{(e^+)^{\eta+1}}{(1-e^+)R/4^k} \\
\leq \left( \frac{Re}{4^k} \right)^{\gamma} \left( \frac{1}{24\sqrt{R}\log R} \right)^{\gamma} \left( 1 - \frac{1}{24\sqrt{R}\log R} \right)^{-R/4^k} \\
\leq \left( \frac{e}{24} \right)^{\gamma} \left( \frac{\sqrt{R}}{4^k \gamma \log R} \right)^{\gamma} \cdot 3^{\sqrt{R}/(4^k24\log R)} \\
\leq \left( \frac{e}{12} \right)^{\gamma} \left( \frac{1}{c \sqrt{4^k \log R}} \right)^{\gamma} \cdot 3^{\sqrt{R}/(4^k24\log R)} \\
= \left( \frac{e \cdot 3^{1/(12c \sqrt{4^k \log R})}}{12c \sqrt{4^k \log R}} \right)^{\gamma} \\
\leq (e/48)^{\gamma} \quad \text{since} \quad 3^{1/(12c \sqrt{4^k \log R})} \leq 2 \quad \text{and} \quad 12c \sqrt{4^k \log R} \geq 8 \quad \text{for sufficiently large} \ R \\
\leq 1/16. \quad \text{(2.70)}
\]
Thus, the conditions in Claim 2.5.4 are satisfied. By the definition of $\Gamma$, we have

$$\langle \Gamma, (\text{OR}_R \circ \text{THR}_N^k) \rangle = \frac{\langle (\theta \ast (\phi \ast \psi)) \cdot (\text{OR}_R \circ \alpha), \text{OR}_{R/4^k} \circ (\text{OR}_{4^k} \circ \text{THR}_N^k) \rangle}{p_\eta(1 - 2\epsilon^+, \ldots, 1 - 2\epsilon^+)}$$

$$\geq \delta - \left(2 - 2\left(\frac{1 - \epsilon^+ - \epsilon^-}{1 - \epsilon^+}\right)(1 - A)\right)$$

by Claim 2.5.4

$$\geq 3/5 - \left(2\frac{\epsilon^-}{1 - \epsilon^+} + 2A\left(\frac{1 - \epsilon^+ - \epsilon^-}{1 - \epsilon^+}\right)\right)$$

since $\delta \geq 3/5$ by Claim 2.3.4

$$\geq 3/5 - \left(2e^{-4}\frac{1}{1 - \frac{1}{24\sqrt{R \log R}}} + 2A\right)$$

by Claim 2.6.2 and $\frac{1 - \epsilon^+ - \epsilon^-}{1 - \epsilon^+} < 1$

$$> 3/5 - 1/8 - 1/8$$

by Equation (2.70) and since $R$ is sufficiently large

$$> 1/3.$$  

We last show the strong decay property. We first state and prove a property of $p_\eta$ that we require.

**Claim 2.6.4**

$$p_\eta(1 - 2\epsilon^+, \ldots, 1 - 2\epsilon^+) > 1.$$  

(2.71)
Proof.

\[ p_\eta(1 - 2\epsilon^+, \ldots, 1 - 2\epsilon^+) = \mathbb{E}_{w \sim \Pi(\epsilon^+, \ldots, \epsilon^+)}[p_\eta(w)] \]

\[ \geq \Pr_{\Pi(\epsilon^+, \ldots, \epsilon^+)}\left[ w = 1^{R/4^k} \right] p_\eta(1^{R/4^k}) \]

since \( p_\eta \) is non-negative on \((-1, 1)^{R/4^k}\) by Lemma 2.3.12

\[ = (1 - \epsilon^+)^{R/4^k} \eta! \]

by Equation (2.31)

\[ \geq \left( 1 - \frac{1}{24\sqrt{R \log R}} \right)^{R/4^k} \cdot 2^{\frac{R}{4^k} - 1} \]

by Equation (2.68) and using \( \eta = \frac{\epsilon}{2} \sqrt{\frac{R}{4^k}} - 1 \)

\[ > \left( \frac{1}{3} \right)^{\left( \frac{\sqrt{R}}{4^k 24 \log R} \right)} \cdot 2^{\sqrt{R}/(4^k 4) - 1} \]

since \( R \) is sufficiently large and \( (1 - 1/n)^n < 1/e \) for \( n > 0 \)

\[ = \frac{2^{\sqrt{R}/4^k \cdot \log^3 3}}{2} > 2^{\sqrt{R}/(24 \log R)} \cdot 1 \]

since \( R \) is sufficiently large and \( k < (\log R)/4 \).

We next show that \( \Gamma \) satisfies a particular decay property.

**Claim 2.6.5** The function \( \Gamma \) defined in Definition 13 satisfies

\[ \sum_{x \notin (-1,1)^{R^N}} |\Gamma(x)| \leq (2NR)^{-2(\Delta - \sqrt{R})}. \]  \hspace{1cm} (2.73)

**Proof.** First note that by Definition 13 and Claim 2.6.4, it suffices to show the same decay property for \((\theta \star (\phi \star \psi)) \cdot (p_\eta \circ \alpha)(x)\), that is, \( \sum_{x \notin (-1,1)^{R^N}} |(\theta \star (\phi \star \psi)) \cdot (p_\eta \circ \alpha)(x)| \leq (2NR)^{-2(\Delta - \sqrt{R})} \).

By associativity of dual block composition (Equation (2.25)), \( \theta \star \phi \star \psi = (\theta \star \phi) \star \psi \).

Recall that \( \psi : (-1,1)^N \to \mathbb{R} \) is defined as \( \psi(x) = \omega_T(\|x\|)/(N_{|x|}) \) if \( |x| \leq T \), and 0 otherwise, for \( \omega_T \) satisfying the conditions in Claim 2.3.6. Hence, \( \psi \) satisfies the conditions of Claim 2.3.7 and also those in Claim 2.3.9. Hence using Claim 2.3.9 with \( \Phi = \theta \star \phi \), we have

\[ \sum_{x \notin (-1,1)^{R^N}} |((\theta \star \phi) \star \psi)(x)| \leq (2NR)^{-2\Delta}. \]  \hspace{1cm} (2.74)
For any \( x \in \langle -1, 1 \rangle^{RN} \), we write \( x = (x_1, \ldots, x_{R/4k}) \), where \( x_i \in \langle -1, 1 \rangle^{4kN} \), for all \( i \).

\[
\sum_{x \notin \langle -1, 1 \rangle^{RN} \leq N} |(\theta \ast (\phi \ast \psi)) \cdot (p_\eta \circ \alpha)(x)| \\
= \sum_{x \notin \langle -1, 1 \rangle^{RN} \leq N} |(\theta \ast \phi) \ast \psi)(x)| |p_\eta(\alpha(x_1), \ldots, \alpha(x_{R/4k}))| \\
\leq \max_{y \in [-1, 1]^{R/4k}} |p_\eta(y)| \sum_{x \notin \langle -1, 1 \rangle^{RN} \leq N} |(\theta \ast \phi) \ast \psi)(x)| \\
\text{since } \alpha(w) \in [-1, 1] \text{ for all } w \in \langle -1, 1 \rangle^{4kN} \text{ by Equation (2.46)} \\
\leq (2NR)^{-2\Delta \eta} \left( \frac{R^{4k} + \eta}{\eta} \right) \text{ by Claim 2.3.13 and Equation (2.74)} \\
\leq (2NR)^{-2\Delta} \left( c \sqrt{\frac{R}{4k+1}} \right) \left( \frac{2eR}{c \sqrt{R/4k+1}} \right)^{c \sqrt{R/4k+1}} \\
\text{since } \eta = c \sqrt{R/4k+1} - 1 < R/4k, \text{ and } \left( \frac{a}{b} \right) \leq (ae/b)^b \\
\leq (2NR)^{-2\Delta \sqrt{R}} \left( \frac{8eR}{c \sqrt{R/4k+1}} \right)^{\sqrt{R/4k+1}} \\
\leq (2NR)^{-2\Delta (8eR/c) \sqrt{R}} \\
\leq (2NR)^{-2(\Delta - \sqrt{R})}, \text{ since } R \text{ (and hence } N \text{) is sufficiently large}
\]

2.6.2 Final Dual Polynomial

We now prove Theorem 2.4.4.

Proof.[Proof of Theorem 2.4.4]

We exhibit a function \( W : \langle -1, 1 \rangle^{RN} \rightarrow \mathbb{R} \) satisfying

\[
W(x) = 0, \forall x \notin \langle -1, 1 \rangle^{RN} \leq N, \quad \text{(2.75)}
\]

\[
\|W\|_1 = 1 \quad \text{(2.76)}
\]

\[
\langle W, (OR_R \circ THR^k_N) \rangle > 7/33, \quad \text{(2.77)}
\]
\[
\text{phd}(W) = \Omega\left(\frac{1}{4k^2} \cdot \frac{1}{\log^{5/2} R} \cdot R^{\frac{3}{4} - \frac{1}{4k}}\right).
\] (2.78)

The theorem then follows by Lemma 2.3.3 and Lemma 2.3.5. Towards the construction of such a \( W \), first note that by Claim 2.6.5 and Lemma 2.3.14 there exists a function \( \nu : (-1,1)^{\mathbb{R}N} \rightarrow \mathbb{R} \) that satisfies the following properties.

\[|x| > N \Rightarrow \nu(x) = \Gamma(x),\] (2.79)

\[\text{phd}(\nu) \geq 2(\Delta - \sqrt{R}) - 1,\] (2.80)

\[\|\nu\|_1 \leq \frac{1}{10}.\] (2.81)

Define \( W : (-1,1)^{\mathbb{R}N} \rightarrow \mathbb{R} \) by

\[W(x) := \frac{\Gamma(x) - \nu(x)}{\|\Gamma - \nu\|_1}.\] (2.82)

For any \( x \notin (-1,1)^{\mathbb{R}N} \), we have \( W(x) = \frac{\Gamma(x) - \nu(x)}{\|\Gamma - \nu\|_1} = 0 \) by Equation (2.79). This justifies Equation (2.75).

Equation (2.76) immediately follows from Equation (2.82).

To justify Equation (2.77), we have

\[
\langle W, \text{OR}_R \circ \text{THR}^k_N \rangle = \frac{1}{\|\Gamma - \nu\|_1} \left(\langle \Gamma, \text{OR}_R \circ \text{THR}^k_N \rangle - \langle \nu, \text{OR}_R \circ \text{THR}^k_N \rangle\right)
\]

by Equation (2.82)

\[\geq \frac{1}{\|\Gamma - \nu\|_1} \left(1/3 - \langle \nu, \text{OR}_R \circ \text{THR}^k_N \rangle\right) \geq \frac{1}{\|\Gamma - \nu\|_1} \left(1/3 - \|\nu\|_1\right) \geq \frac{1}{\|\Gamma - \nu\|_1} \frac{7}{30} \geq \frac{7}{33}.
\]

since \( \|\Gamma - \nu\|_1 \leq \|\Gamma\|_1 + \|\nu\|_1 \leq \frac{11}{10} \) by the triangle inequality.
We have from Equation (2.82) that
\[ \text{phd}(W) = \text{phd} \left( \begin{array}{c} \Gamma(x) - \nu(x) \\ \|\Gamma - \nu\|_1 \end{array} \right) \]
\[ = \text{phd}(\Gamma(x) - \nu(x)) \]  
\[ \geq \min\{\text{phd}(\Gamma), \text{phd}(\nu)\}. \] (2.85)

From Equation (2.80) we have
\[ \text{phd}(\nu) \geq 2(\Delta - \sqrt{R}) - 1 \]  
\[ = 2 \left( \frac{c_2 R}{4 \ln^2 R} \sqrt{\frac{(2k)^k}{4^k kT N^{1/(2k)} \log N} - \sqrt{R}} \right) - 1 \]
\[ \geq 2 \left( \frac{c_2}{4} \frac{1}{\log^2 R \sqrt{\log N}} \cdot \left( \frac{k}{2} \right)^{k/2} \frac{1}{k^{1/2}} \cdot \frac{R^{3/4}}{N^{1/(4k)}} - \sqrt{R} \right) - 1 \] 
\[ \text{substituting the value of } \Delta \]
\[ \geq 2 \left( \frac{c_2}{4} \frac{1}{\log^2 R \sqrt{\log N}} \cdot \left( \frac{k}{2} \right)^{k/2} \frac{1}{k^{1/2}} \cdot \frac{R^{3/4}}{201/(4k) 2^{1/8} k^{1/8} R^{1/(4k)} - \sqrt{R}} \right) - 1 \]
\[ \text{using } T = \sqrt{R} \text{ and } \ln R < \log R \]
\[ \geq 2 \left( \frac{c_2}{217/8} \cdot \frac{1}{\log^2 R \sqrt{\log N}} \cdot \left( \frac{k}{2} \right)^{k/2} \frac{1}{k^{9/8}} \cdot \frac{R^{3/4}}{201/(4k) 2^{1/8} k^{1/8} R^{1/(4k)} - \sqrt{R}} \right) - 1 \]
\[ \text{substituting the value of } N \text{ and using } k \log R > \log N \text{ for sufficiently large } R \]
\[ \geq 2 \left( \frac{c_2}{226/8} \cdot \frac{1}{\log^5/2 R} \cdot \frac{1}{201/(4k)} \cdot R^{3/4 - 1/(4k)} - \sqrt{R} \right) - 1 \]
\[ \text{since } \left( \frac{k}{2} \right)^{k/2} \frac{1}{k^{9/8}} \geq \frac{1}{2^{9/8}} \text{ for all } k \geq 2 \]
\[ \geq 2 \left( \frac{c_2}{320} \cdot \frac{1}{\log^5/2 R} \cdot R^{3/4 - 1/(4k)} - \sqrt{R} \right) - 1 \]  
\[ \geq \frac{c_2}{320} \cdot \frac{1}{\log^5/2 R} \cdot R^{3/4 - 1/(4k)} - 1 \]  
\[ \text{since } \sqrt{R} \leq \frac{c_2}{640} \cdot \frac{1}{\log^5/2 R} \cdot R^{3/4 - 1/(4k)} \text{ for } k \geq 2, \text{ for sufficiently large } R \]
\[ = \Omega \left( \frac{1}{4k^2} \cdot \frac{1}{\log^5/2 R} \cdot R^{3/4 - 1/(4k)} \right). \] (2.89)

Therefore by Claim 2.6.1 and Equation (2.85), we have
\[ \text{phd}(W) = \Omega \left( \frac{1}{4k^2} \cdot \frac{1}{\log^5/2 R} \cdot R^{3/4 - 1/(4k)} \right), \]
justifying Equation (2.78) and finishing the proof.

2.7 An Upper Bound

We extend ideas from Sherstov’s upper bound on the approximate degree of surjectivity [123] to prove an approximate degree upper bound for \( k \)-distinctness, where \( k \) is not necessarily a constant. We first note that it suffices to show an approximate degree upper bound on \( (\text{OR}_R \circ \text{THR}_N^k)^{\leq N} \).

**Claim 2.7.1** For any positive integers \( k, R, N \),

\[
\widetilde{\deg} \left( \text{DIST}^k_{N,R} \right) \leq \widetilde{\deg} \left( (\text{OR}_R \circ \text{THR}_N^k)^{\leq N} \right) \cdot O(\log R) \tag{2.90}
\]

Claim 2.7.1 has essentially appeared in multiple prior works, e.g., [35, Equation 4], [37, Section 3.4.1], [123, Section 6]. Claim 2.7.1 is a converse to Claim 2.4.3, but is far more straightforward to prove than Claim 2.4.3. Claim 2.7.1 follows from the fact that \( \text{DIST}^k_{N,R} \) can be written as an OR over all \( R \) range items \( j \) of the function that tests whether \( k \) or more copies of \( i \) appear in the input list. In more detail, for \( i \in [N] \) and \( j \in [R] \), let \( y_{i,j}(x) = -1 \) if the \( i \)th item of the input list equals range item \( j \). Note that \( y_{i,j}(x) \) is a function of degree at most \( \lceil \log_2 R \rceil \) in \( x \). Moreover,

\[
\text{DIST}^k_{N,R} = (\text{OR}_R \circ \text{THR}_N^k)(y_{1,1}(x), y_{2,1}(x), \ldots, y_{R,N}(x)).
\]

Claim 2.7.1 follows.

The following is our main theorem in this section.

**Theorem 2.7.2** For any positive integers \( k, R, N \), with \( k \leq N/2 \),

\[
\widetilde{\deg} \left( (\text{OR}_R \circ \text{THR}_N^k)^{\leq N} \right) = O(N^{1/2}R^{1/4}\sqrt{k\log N}).
\]
For any integers $N \geq i \geq 0$, define the function $\text{EXACT}^i_N : \langle -1, 1 \rangle^N \to \langle 0, 1 \rangle$ by

$$\text{EXACT}^i_N(x) = \begin{cases} 1 & |x| = i \\ 0 & \text{otherwise.} \end{cases}$$

Note that

$$\text{EXACT}^i_N(x) = \sum_{S \subseteq [N] : |S| = i} \prod_{u \in S} \left( \frac{1 - x_u}{2} \right) \prod_{v \notin S} \left( \frac{1 + x_v}{2} \right). \quad (2.91)$$

Recall that for integers $N \geq k \geq 0$, the function $\text{THR}^k_N : \langle -1, 1 \rangle^N \to \langle -1, 1 \rangle$ is defined by

$$\text{THR}^k_N(x) = \begin{cases} -1 & |x| \geq k \\ 1 & \text{otherwise.} \end{cases}$$

We have

$$\text{THR}^k_N(x) = 2 \left( \sum_{i=0}^{k-1} \text{EXACT}^i_N(x) \right) - 1 \quad (2.92)$$

since exactly one summand outputs 1 if the Hamming weight of $x$ is less than $k$, and all summands output 0 otherwise.

For integers $m, R \geq 0$, define a degree-$m$ polynomial $p : \langle -1, 1 \rangle^R \to \mathbb{R}$ by

$$p(x) = \frac{2}{T_m \left( 1 + \frac{1}{R} \right)} \cdot T_m \left( \frac{\sum_{i=1}^{R} x_i}{R} + \frac{1}{R} \right) - 1. \quad (2.93)$$

Note that when $|x| = 0$, we have $\sum_{i=1}^{R} x_i = R$, and hence $p(x) = 1$. When $|x| > 0$, we have $\frac{\sum_{i=1}^{R} x_i}{R} + \frac{1}{R} \in [-1, 1]$, and by Equation (2.35) this implies $T_m \left( \frac{\sum_{i=1}^{R} x_i}{R} + \frac{1}{R} \right) \in [-1, 1]$, and thus $p(x) \in \left[ -1 - \frac{2}{1 + (m^2/R)}, -1 + \frac{2}{1 + (m^2/R)} \right]$ by Equation (2.36). The next claim immediately follows.

**Claim 2.7.3** The degree-$m$ polynomial $p$ defined in Equation (2.93) uniformly approximates $\text{OR}_R$ to error $\frac{2}{1 + (m^2/R)}$. 56
We are now ready to prove our final upper bound.

Proof.[Proof of Theorem 2.7.2] Let \( m \geq 1 \) be an integer parameter to be fixed later and let \( T_m \) be the degree-\( m \) Chebyshev polynomial. Thus by Claim 2.7.3, the function \( \text{OR}_R \circ \text{THR}^k_N \) is approximated pointwise to error \( \frac{2}{1+(m^2/R)} \) by the degree-\( m \) polynomial \( p : (-1, 1)^{RN} \rightarrow \mathbb{R} \) defined by

\[
p(x) = \frac{2}{T_m(1 + \frac{1}{R})} \cdot T_m \left( \frac{1}{R} + \frac{1}{R} \sum_{j=1}^{R} \text{THR}^k_N(x_{j,1}, \ldots, x_{j,N}) \right) - 1
\]

\[
= \frac{2}{T_m(1 + \frac{1}{R})} \cdot T_m \left( \frac{1}{R} - 1 + \frac{2}{R} \sum_{j=1}^{R} \sum_{i=0}^{k-1} \text{EXACT}^i_N(x_{j,1}, \ldots, x_{j,N}) \right) - 1
\]

by Equation (2.92)

\[
= \frac{2}{T_m(1 + \frac{1}{R})} \cdot T_m \left( \frac{1}{R} - 1 + \frac{2}{R} \sum_{j=1}^{R} \sum_{i=0}^{k-1} \left( \sum_{S \subseteq [N]: |S| = i} \Pi_{u \in S} \left( \frac{1 - x_{j,u}}{2} \right) \Pi_{v \notin S} \left( \frac{1 + x_{j,v}}{2} \right) \right) \right)
\]

by Equation (2.91)

For simplicity of notation, define

\[
C_{j,S} := \prod_{u \in S} \left( \frac{1 - x_{j,u}}{2} \right) \prod_{v \notin S} \left( \frac{1 + x_{j,v}}{2} \right).
\]  

(2.94)
We next show an upper bound on $\rho(p)$ (recall that $\rho(p)$ is the conjunction norm of $p$ defined in Definition 12).

$\rho(p) = \left| \frac{2}{T_m(1 + \frac{1}{R})} \right| \cdot \rho \left( T_m \left( \frac{1}{R} - 1 + \frac{2}{R} \sum_{j=1}^{R} \sum_{i=0}^{k-1} \left( \sum_{S \subseteq \{N\} : |S| = i} C_{j,S} \right) \right) \right)$

by Equation (2.38)

$\leq 2 \cdot 3^m \cdot \rho \left( \frac{1}{R} - 1 + \frac{2}{R} \sum_{j=1}^{R} \sum_{i=0}^{k-1} \left( \sum_{S \subseteq \{N\} : |S| = i} C_{j,S} \right) \right)^m$

by Equation (2.41), Equation (2.34), and $T_m(1 + \frac{1}{R}) > 1$

$\leq 2 \cdot 3^m \cdot \left( \frac{1}{R} - 1 \right) + \rho \left( \frac{2}{R} \sum_{j=1}^{R} \sum_{i=0}^{k-1} \left( \sum_{S \subseteq \{N\} : |S| = i} C_{j,S} \right) \right)^m$

by Equation (2.39)

$\leq 2 \cdot 3^m \cdot \left( 1 + \frac{2}{R} \sum_{j=1}^{R} \rho \left( \sum_{i=0}^{k-1} \left( \sum_{S \subseteq \{N\} : |S| = i} C_{j,S} \right) \right) \right)^m$

by Equation (2.38) and Equation (2.39)

$\leq 2 \cdot 3^m \cdot \left( 1 + 2 \cdot k \left( \frac{N}{k} \right) \right)^m$

by Equation (2.39) and $\rho(C_{j,S})$ is at most 1

$\leq \left( c_1 \cdot k \left( \frac{N}{k} \right) \right)^m$

by Equation (2.95)

for some positive constant $c_1$. By Claim 2.3.17, we have the following. For each conjunction $f$ there is a degree-$d$ polynomial $p_f$ such that $|p_f(x) - f(x)| \leq 2^{-c d^2/N}$ for all $x \in (-1, 1]^{RN}$ for some positive constant $c$. By construction, $\deg(p) = m$ and $|p(x) - (\text{OR}_R \circ \text{THR}^k_N)(x)| \leq 2/ \left( 1 + \frac{m^2}{R} \right)$ for all $x \in (-1, 1]^{RN}$. By the triangle
inequality, we obtain that for any integers \( m, d \geq 0 \),
\[
E \left( (\text{OR}_R \circ \text{THR}_N^k)^{\leq N}, d \right) \leq \frac{2}{1 + \frac{m^2}{R}} + \rho(p) \cdot 2^{-c \cdot d^2 / N}
\]
\[
\leq \frac{2}{1 + \frac{m^2}{R}} + 2^{m \log(c_1 k(N))} \cdot 2^{-c \cdot d^2 / N} \quad \text{by Equation (2.95)}
\]
\[
\leq \frac{2}{7} + 2^{\sqrt{6R} \log(c_1 k(N)) - c \cdot d^2 / N} \quad \text{setting } m = \sqrt{6R}
\]
\[
\leq \frac{2}{7} + 2^{\sqrt{6R} \log(k) - c \cdot d^2 / N} \quad \text{for sufficiently large } N
\]
\[
\leq \frac{1}{3} \quad \text{for } d = \frac{4}{3} \cdot R^{1/4} \sqrt{Nk \log N}
\]

Hence there is a polynomial of degree \( \frac{4}{3} \cdot R^{1/4} \sqrt{Nk \log N} \) that approximates \((\text{OR}_R \circ \text{THR}_N^k)^{\leq N}\) within error 1/3, and the theorem follows.

Combining Claim 2.7.1 and Theorem 2.7.2 immediately yields an upper bound on the approximate degree of \( k \)-distinctness.

**Corollary 2.7.4** For any positive integers \( R, N \) and \( k \leq N/2 \),
\[
\widetilde{\deg} \left( \text{DIST}_{k, N, R}^k \right) = O(\sqrt{kN^{1/2} R^{1/4} \log R \sqrt{\log N}}).
\]

Recall (cf. Corollary 2.4.2) that Ambainis [8] showed that, for all functions that are symmetric both with respect to range elements and with respect to domain elements, the approximate degree is the same for all range sizes greater than or equal to \( N \). This implies that the upper bound in Corollary 2.7.4 can be refined to
\[
\widetilde{\deg} \left( \text{DIST}_{k, N, R}^k \right) = O(\sqrt{kN^{1/2} \min\{N, R\}^{1/4} \log R \sqrt{\log N}}).
\]

### 2.8 A Dual Polynomial for Threshold Function

In this section, we prove Claim 2.3.6. We require the following well-known combinatorial identity. For a proof, see, for example, [111].
Fact 2.8.1 Let \( N \in \mathbb{N} \) and let \( p : \mathbb{R} \rightarrow \mathbb{R} \) be any polynomial of degree less than \( N \).

Then,

\[
\sum_{i=0}^{N} (-1)^i \binom{N}{i} p(i) = 0.
\]

Proof.[Proof of Claim 2.3.6]

Let \( E_+ := \{ t : \omega(t) > 0, t \geq k \} \), and \( E_- := \{ t : \omega(t) < 0, t < k \} \). By normalizing, it suffices to construct a function \( \omega : [T] \cup \langle 0 \rangle \rightarrow \mathbb{R} \) such that

\[
\sum_{t \in E_+} |\omega(t)| \leq \frac{1}{48 \cdot 4^k \sqrt{N} \log N} : \|\omega\|_1  \tag{2.96}
\]

\[
\sum_{t \in E_-} |\omega(t)| \leq \left( \frac{1}{2} - \frac{2}{4^k} \right) : \|\omega\|_1  \tag{2.97}
\]

For all univariate polynomials \( q : \mathbb{R} \rightarrow \mathbb{R} \),

\[
\deg(q) < c_1 \sqrt{4^{-k} k^{-1} T N^{-1/(2k)}} \log^{-1} N \implies \sum_{t=0}^{T} \omega(t) q(t) = 0  \tag{2.98}
\]

\[
|\omega(t)| \leq \frac{(2k)^k \exp \left( -c_2 t / \sqrt{4^k k^{1/2} T N^{1/(2k)} \log N} \right) \|\omega\|_1}{t^2} \forall t = 1, 2, \ldots, T.  \tag{2.99}
\]

Let \( \ell = 100 k \lceil N^{1/(2k)} 4^k \log N \rceil \), and let \( m = \lfloor \sqrt{T/\ell} \rfloor \). Define the set

\[
S = \{ 1, 2, \ldots, k \} \cup \{ \ell i^2 : 0 \leq i \leq m \}.
\]

Note that \( |S| = k + m + 1 \geq m = (1/10) \sqrt{4^{-k} k^{-1} T N^{-1/(2k)} \log^{-1} N} \).

Define the polynomial \( \omega : [T] \cup \langle 0 \rangle \rightarrow \mathbb{R} \) by

\[
\omega(t) = \frac{(-1)^{T-t-m+1}}{T!} \binom{T}{t} \prod_{r \in ([T] \cup \langle 0 \rangle) \setminus S} (t-r).
\]

The signs are chosen so that \( \omega(k) < 0 \), because in the expression

\[
\omega(k) = \frac{(-1)^{T-k-m+1}}{T!} \binom{T}{k} \prod_{r \in ([T] \cup \langle 0 \rangle) \setminus S} (k-r),
\]

60
the number of terms in the product is $|(T \cup \{0\}) \setminus S| = T - k - m$, and each term in the product is negative for $k = 0$.

Let $q$ be any univariate polynomial of degree less than $|S| - 1$. Then,

$$
\sum_{t=1}^T \omega(t)q(t) = \frac{(-1)^T}{T!} \sum_{t=1}^T (-1)^t \left( T \atop t \right) \prod_{r \in (T \cup \{0\}) \setminus S} (t - r) \cdot q(t)
$$

since $(-1)^t = (-1)^t$ for all integer $t$

$$
= \frac{(-1)^{T-m+1}}{T!} \sum_{t=1}^T (-1)^t \left( T \atop t \right) p(t)
$$

where $p(t) := \prod_{r \in (T \cup \{0\}) \setminus S} (t - r) \cdot q(t)$

$$
= 0
$$

by Fact 2.8.1

where we could use Fact 2.8.1 since $\deg(p) \leq \deg(q) + \deg(\prod_{r \in (T \cup \{0\}) \setminus S} (t - r)) \leq |(T \cup \{0\})| - |S| + \deg(q) < T + 1 - |S| + |S| - 1 = T$.

Since $|S| - 1 = k + m > m = (1/10)\sqrt{4^{-k}k^{-1}TN^{-1/(2k)} \log^{-1} N}$, we conclude that $\omega$ satisfies Equation (2.98) for $c_1 = 1/10$. We now show that Equation (2.99) holds.

For $t = 1, \ldots, k$, we have

$$
\frac{(2k)^k \exp \left(-c_2 t/\sqrt{4^k k T N^{1/(2k)} \log N} \right)}{t^2} \geq \frac{(2k)^k \exp \left(-c_2 \sqrt{k} \right)}{k^2} \geq 1
$$

as long as $c_2 \leq 1/2$ and $k \geq 2$. Since $|\omega(t)| \leq \|\omega\|_1$, the bound holds for $t = 1, \ldots, k$.

Next, note that $\omega(t) = 0$ for $t \notin S$. For $t \in S$, we have

$$
|\omega(t)| = \frac{1}{T!} \cdot \frac{T!}{t!(T-t)!} \prod_{r \in (T \cup \{0\}) \setminus S} |t - r| \cdot \prod_{r \in S \setminus \{t\}} |t - r| 
$$

$$
= \frac{1}{t!(T-t)!} \cdot \prod_{r \in (T \cup \{0\}) \setminus \{t\}} |t - r| 
$$

$$
= \frac{1}{t!(T-t)!} \cdot \prod_{r \in S \setminus \{t\}} |t - r| = \prod_{r \in S \setminus \{t\}} \frac{1}{|t - r|}.
$$
Thus,

\[
|\omega(t)| = \begin{cases} 
\prod_{r \in S \setminus \{t\}} \frac{1}{|t-r|} & \text{for } t \in S, \\
0 & \text{otherwise.}
\end{cases}
\]

For \( t \in \{0, 1, \ldots, k\} \), we observe that

\[
|\omega(t)| \leq k! \cdot \prod_{i=1}^{m} (\ell i^2 - k) \leq (k) \cdot \prod_{i=1}^{m} (\ell i^2 - t) \leq \binom{k}{t}. 
\]

(2.100)

Meanwhile, for \( t = \ell j^2 \) with \( j \geq 1 \), we get

\[
|\omega(t)| = \frac{k! \cdot \prod_{i=1}^{m} (\ell i^2 - k)}{\prod_{i=1}^{k} (\ell j^2 - i) \cdot \prod_{i \in \{m \cup \{0\} \setminus \{j\}} |\ell i^2 - \ell j^2|} 
\]

\[
\leq \frac{k! \cdot \prod_{i=1}^{m} \ell i^2}{(\ell j^2 - k)^k \cdot \prod_{i \in \{m \cup \{0\} \setminus \{j\}} \ell (i + j)|i - j|} 
\]

\[
= \frac{2 \cdot k!}{(\ell j^2 - k)^k} \cdot \frac{(m!)^2}{(m + j)!(m - j)!}. 
\]

The first factor is bounded above by

\[
\frac{2 \cdot k!}{(\ell - k)^k} j^{2k}. 
\]

Since \( \ell \geq 2k \) by our choice of \( \ell \), and \( k \geq 2 \), this expression is at most

\[
\frac{k^k}{(\ell/2)^k j^4} = \frac{(2k)^k}{\ell^k \cdot j^4}. 
\]

We control the second factor by

\[
\frac{(m!)^2}{(m + j)!(m - j)!} = \frac{m}{m + j} \cdot \frac{m - 1}{m + j - 1} \cdot \ldots \cdot \frac{m - j + 1}{m + 1} 
\]

\[
\leq \left( \frac{m}{m + j} \right)^j 
\]

\[
\leq \left( 1 - \frac{j}{2m} \right)^j 
\]

\[
\leq e^{-j^2/2m}, 
\]

62
where the last inequality uses the fact that \( 1 - x \leq e^{-x} \) for all \( x \). Hence,

\[
\frac{|\omega(\ell j^2)|}{|\omega(k)|} \leq \frac{(2k)^k}{\ell^k \cdot j^4} \cdot e^{-j^2/2m}. \tag{2.101}
\]

This immediately yields

\[
\frac{|\omega(\ell j^2)|}{\|\omega\|_1} \leq \frac{|\omega(\ell j^2)|}{|\omega(k)|} \leq \frac{(2k)^k}{(\ell j^2)^2} \cdot e^{-\ell j^2/(2\ell m)},
\]

If we choose \( c_2 < 1/20 \), we have \( \frac{1}{2\ell m} \geq \frac{1}{2\sqrt{T\ell}} > \frac{c_2}{\sqrt{4kTN^{1/(2k)} \log N}} \) since \( \ell = 100k[N^{1/(2k)}4^k \log N] \). This establishes Equation (2.99) for all \( t = \ell j^2 > k \). Moreover, by Equation (2.101),

\[
\sum_{t > k} |\omega(t)| \leq |\omega(k)| \cdot \sum_{j=1}^{m} \frac{(2k)^k}{\ell^k \cdot j^4} \cdot e^{-j^2/2m}
\leq \left( \frac{2k}{\ell} \right)^k \cdot |\omega(k)| \cdot \sum_{j=1}^{m} \frac{1}{j^4}
< \frac{(2k)^k}{(100kN^{1/(2k)}4^k \log N)^k} \cdot \frac{\pi^4}{50} \cdot |\omega(k)| \quad \text{since } \sum_{j=1}^{\infty} 1/j^4 < \pi^4/50
= \frac{1}{50k\sqrt{N}4^k \log N} \cdot \frac{1}{50/\pi^4} \cdot |\omega(k)|
\leq \frac{1}{50^2\sqrt{N}4^k \log N} \cdot \frac{1}{50/\pi^4} \cdot |\omega(k)| \quad \text{for all } k \geq 2
\leq \frac{|\omega(k)|}{48 \cdot 4^k \cdot \sqrt{N} \log N}. \tag{2.102}
\]

Hence, since \( \omega(k) < 0 \),

\[
\sum_{t \in E_+} |\omega(t)| \leq \sum_{t > k} |\omega(t)| \leq \frac{|\omega(k)|}{48 \cdot 4^k \cdot \sqrt{N} \log N} \leq \frac{\|\omega\|_1}{48 \cdot 4^k \cdot \sqrt{N} \log N},
\]

which gives Equation (2.96).

Finally, to establish Equation (2.97), we combine Equation (2.100) and Equation (2.102) to obtain

\[
\frac{\|\omega\|_1}{|\omega(k)|} \leq \sum_{t=0}^{k} \binom{k}{t} + \frac{1}{48 \cdot 4^k \cdot \sqrt{N} \log N} < 2^k + 1 < \frac{1}{2} \cdot 4^k. \tag{2.103}
\]

63
We calculate

\[
\frac{\|\omega\|_1}{2} - \sum_{t \in E_-} |\omega(t)| = \frac{1}{2} \left( \sum_{t: \omega(t) < 0} |\omega(t)| + \sum_{t: \omega(t) > 0} |\omega(t)| \right) - \sum_{t \in E_-} (-\omega(t))
\]

\[
= \sum_{t: \omega(t) < 0} (-\omega(t)) - \sum_{t \in E_-} (-\omega(t))
\]

since \( \langle \omega, \mathbf{1} \rangle = 0 \), so \( \sum_{t: \omega(t) < 0} |\omega(t)| = \sum_{t: \omega(t) > 0} |\omega(t)| \)

\[
= \sum_{t: \omega(t) < 0, t \geq k} (-\omega(t)) \quad \text{since } E_- = \{ t: \omega(t) < 0, t < k \}
\]

\[\geq -\omega(k).\]

Rearranging and applying the bound in Equation (2.103),

\[
\sum_{t \in E_-} |\omega(t)| \leq \left( \frac{1}{2} + \frac{\omega(k)}{\|\omega\|_1} \right) \cdot \|\omega\|_1 \leq \left( \frac{1}{2} - 2 \cdot 4^{-k} \right) \cdot \|\omega\|_1.
\]
Product formulas offer a streamlined method for breaking down the decomposing the evolution of a sum of operators. Introduced during the study of Lie groups in the late 19th century, the Lie product formula marked the beginning of exploring more complex operators and advanced approximations. Initially a topic within pure mathematics, product formulas have since been widely applied in fields like applied mathematics, physics, and theoretical computer science.

We delve into the use of product formulas for quantum system simulations. It has long been acknowledged that these formulas play a critical role in digital quantum simulation and quantum Monte Carlo methods. Yet, the understanding of their error scaling remains limited, with existing error estimates often far exceeding actual observations, even in simulations of relatively simple systems.

Our research introduces a new perspective on Trotter error, leveraging the commutativity between operator components to establish more precise error bounds. Unlike prior research, which focused on systems characterized by geometric locality or Lie-algebraic structures, our approach imposes no such constraints. We showcase several instances where product formulas not only rival but sometimes surpass the latest simulation techniques. Our findings are supported by numerical analyses, indicating that these bounds are also close to optimal regarding constant factors.

The main result of the work is the following theorem:

The presentation in this chapter is based on the results obtained in [43].
Theorem 3.0.1 (Trotter error with commutator scaling) Let \( H = \sum_{\gamma=1}^{\Gamma} H_{\gamma} \) be an operator consisting of \( \Gamma \) summands and \( t \geq 0 \). Let \( \mathcal{S}(t) \) be a \( p \)th-order \( \Upsilon \)-stage product formula. Define \( \tilde{\alpha}_{\text{comm}} = \sum_{\gamma_1, \gamma_2, \ldots, \gamma_{p+1}} \| [H_{\gamma_{p+1}}, \ldots, [H_{\gamma_2}, H_{\gamma_1}]] \| \). Then, the additive error \( \mathcal{A}(t) \) and the multiplicative error \( \mathcal{M}(t) \), defined by \( \mathcal{S}(t) = e^{tH} + \mathcal{A}(t) \) and \( \mathcal{S}(t) = e^{tH}(I + \mathcal{M}(t)) \), can be asymptotically bounded as
\[
\| \mathcal{A}(t) \| = O\left( \tilde{\alpha}_{\text{comm}} t^{p+1} e^{3\Upsilon \sum_{\gamma=1}^{\Gamma} \|H_{\gamma}\|} \right), \quad \| \mathcal{M}(t) \| = O\left( \tilde{\alpha}_{\text{comm}} t^{p+1} e^{4\Upsilon \sum_{\gamma=1}^{\Gamma} \|H_{\gamma}\|} \right).
\]

(3.1)

Furthermore, if \( H_{\gamma} \) are anti Hermitian,
\[
\| \mathcal{A}(t) \| = O\left( \tilde{\alpha}_{\text{comm}} t^{p+1} \right), \quad \| \mathcal{M}(t) \| = O\left( \tilde{\alpha}_{\text{comm}} t^{p+1} \right).
\]

(3.2)

The theoretical derivation can be found in [43], and in this thesis, we include the numerical confirmation for error bounds with small prefactors.

3.1 First- and Second-order Error Bound

We establish error limits for both the first-order Lie-Trotter formula and the second-order Suzuki formula, drawing on the methodologies presented in previous works. This process begins by evaluating the Trotter error when decomposing the progression of a Hamiltonian consisting of just two components. This foundational analysis then serves as a stepping stone to extend our examination to more complex Hamiltonians that include a multitude of operator elements. The accuracy of our derived bounds is notably high, as they align with the initial term of the Baker-Campbell-Hausdorff (BCH) series, with only minor deviations accounted for by the application of the triangle inequality. This approach ensures that our error estimations are not just theoretical but closely reflect practical outcomes, making them a reliable resource for understanding and applying these formulas in computational physics and related fields.
Let $H = A + B$ be a two-term Hamiltonian. The evolution under $H$ for time $t$ is given by $e^{-itH} = e^{-it(A+B)}$, which we decompose using the first-order Lie-Trotter formula $\mathcal{S}_1(t) = e^{-itB}e^{-itA}$. We first construct the differential equation

$$\frac{d}{dt} \mathcal{S}_1(t) = -iH \mathcal{S}_1(t) + e^{-itB}(e^{itB}iAe^{-itB} - iA)e^{-itA}$$

(3.3)

with initial condition $\mathcal{S}_1(0) = I$.

$$\mathcal{S}_1(t) = e^{-itH} + \int_0^t d\tau_1 e^{-i(t-\tau_1)H} e^{-ir_1B}(e^{ir_1B}iAe^{-ir_1B} - iA)e^{-ir_1A}.$$  

(3.4)

Altogether, we have the representation

$$\mathcal{S}_1(t) = e^{-itH} + \int_0^t d\tau_1 \int_0^{\tau_1} d\tau_2 e^{-i(t-\tau_1)H} e^{-ir_1B}e^{ir_2B}[iB,iA]e^{-ir_2B}e^{-ir_1A}$$

(3.5)

and the error bound

$$\|\mathcal{S}_1(t) - e^{-itH}\| \leq \frac{|t|^2}{2} \|[B,A]\|.$$ 

(3.6)

We bootstrap this bound to analyze a general Hamiltonian $H = \sum_\gamma H_\gamma$. By the triangle inequality,

$$\left\| \prod_{\gamma=1}^\Gamma e^{-itH_\gamma} - e^{-it \sum_{\gamma=1}^\Gamma H_\gamma} \right\|$$

$$\leq \sum_{\gamma_1=1}^\Gamma \left\| e^{-it \sum_{\gamma_2=\gamma_1+1}^\Gamma H_{\gamma_2}} \prod_{\gamma_1=1}^{\gamma_1} e^{-itH_{\gamma_1}} - e^{-it \sum_{\gamma_2=\gamma_1}^\Gamma H_{\gamma_2}} \prod_{\gamma_2=1}^{\gamma_1-1} e^{-itH_{\gamma_2}} \right\|$$

$$= \sum_{\gamma_1=1}^\Gamma \left\| e^{-it \sum_{\gamma_2=\gamma_1+1}^\Gamma H_{\gamma_2}} e^{-itH_{\gamma_1}} - e^{-it \sum_{\gamma_2=\gamma_1}^\Gamma H_{\gamma_2}} \right\|$$

$$\leq \frac{|t|^2}{2} \sum_{\gamma_1=1}^\Gamma \left\| \sum_{\gamma_2=\gamma_1+1}^\Gamma H_{\gamma_2}, H_{\gamma_1} \right\|.$$ 

This gives us the following:

**Lemma 3.1.1 (Tight error bound for the first-order Lie-Trotter formula)**

Let $H = \sum_\gamma^\Gamma H_\gamma$ be a Hamiltonian consisting of $\Gamma$ summands and $t \in \mathbb{R}$. Let
\[ S_1(t) = \prod_{\gamma=1}^{\Gamma} e^{-itH_{\gamma}} \text{ be the first-order Lie-Trotter formula. Then, the additive Trotter error can be bounded as} \]
\[ \| S_1(t) - e^{-itH} \| \leq \frac{|t|^{2}}{2} \sum_{\gamma_1=1}^{\Gamma} \left\| \left[ \sum_{\gamma_2=\gamma_1+1}^{\Gamma} H_{\gamma_2}, H_{\gamma_1} \right] \right\|. \tag{3.7} \]

A generalization of this analysis gives an error bound for the second-order Suzuki formula with a small prefactor. For the two-term case, our goal is to decompose the evolution \( e^{-itH} = e^{-it(A+B)} \) using the product formula \( S_2(t) = e^{-t\frac{i}{2}A}e^{-itB}e^{-t\frac{i}{2}A} \). The result is the following lemma, where the derivation can be found in [43].

**Lemma 3.1.2 (Tight error bound for the second-order Suzuki formula)**

Let \( H = \sum_{\gamma=1}^{\Gamma} H_{\gamma} \) be a Hamiltonian consisting of \( \Gamma \) summands and \( t \in \mathbb{R} \). Let \( S_2(t) = \prod_{\gamma=1}^{\Gamma} e^{-i\frac{t}{2}H_{\gamma}} \prod_{\gamma=1}^{\Gamma} e^{-i\frac{t}{2}H_{\gamma}} \) be the second-order Suzuki formula. Then, the additive Trotter error can be bounded as
\[
\| S_2(t) - e^{-itH} \| \leq \frac{|t|^{3}}{12} \sum_{\gamma_1=1}^{\Gamma} \left\| \left[ \sum_{\gamma_3=\gamma_1+1}^{\Gamma} H_{\gamma_3}, \left[ \sum_{\gamma_2=\gamma_1+1}^{\Gamma} H_{\gamma_2}, H_{\gamma_1} \right] \right] \right\| + \frac{|t|^{3}}{24} \sum_{\gamma_1=1}^{\Gamma} \left\| H_{\gamma_1}, \left[ H_{\gamma_1}, \sum_{\gamma_2=\gamma_1+1}^{\Gamma} H_{\gamma_2} \right] \right\|. \tag{3.8} \]

### 3.2 Numerical Confirmation of Higher-order Error Bounds

In the previous section, we confirmed that our evaluation aligns with the established, precise error margins for both the first- and second-order formulas. Moving forward, we propose heuristic methods aimed at establishing higher-order Trotter error bound that maintain minimal prefactors. Specifically, we apply these strategies to the fourth-order formula, which, despite its benefits for simulating systems of smaller scale, lacks a comprehensive error analysis. Additionally, we put our derived bounds to the test by conducting numerical simulations on systems characterized by nearest-neighbor and power-law interactions. Our analysis throughout assumes that \( H \) is a
Hermitian operator and focuses on the evolution $e^{-itH}$ for $t \in \mathbb{R}$. This approach not only extends the utility of higher-order Trotter formulas but also enhances their applicability in practical quantum simulations, particularly in scenarios where precise error management is crucial.

We consider a Hamiltonian $H = A + B$ consisting of two summands. This models systems with nearest-neighbor interactions where summands are grouped in an even-odd pattern. The ideal evolution under $H$ for time $t$ is $e^{-itH}$, which we decompose using the fourth-order product formula $S_4(t)$. It is defined by

$$S_2(t) := e^{-i t A} e^{-i t B} e^{-i t A},$$

$$S_4(t) := [S_2(u_2 t)]^2 S_2((1 - 4 u_2 t)[S_2(u_2 t)]^2,$$

with $u_2 := 1/(4 - 4^{1/3})$.

Following the technique presented in [43], we can reach the following lemma.

**Lemma 3.2.1** Let $H = A + B$ be a Hamiltonian consisting of two summands. Decompose the ideal evolution $e^{-itH}$ under $H$ for time $t \in \mathbb{R}$ using the fourth-order Suzuki formula $S_4(t)$. Then,

$$\| S_4(t) - e^{-itH} \| \leq |t|^5 \left( 0.0047 \| [A, [A, [A, [B, A]]]] \| + 0.0057 \| [A, [A, [B, [B, A]]]] \| + 0.0046 \| [A, [B, [A, [B, A]]]] \| + 0.0074 \| [A, [B, [B, [B, A]]]] \| + 0.0097 \| [B, [A, [A, [B, A]]]] \| + 0.0097 \| [B, [A, [B, [B, A]]]] \| + 0.0173 \| [B, [B, [A, [B, A]]]] \| + 0.0284 \| [B, [B, [B, [B, A]]]] \| \right).$$

While our analysis for the first- and second-order Trotter formulas is supported by rigorous proof of their tight error bounds, the same level of certainty does not extend to the higher-order cases. Nonetheless, our numerical findings indicate that the error bounds we propose are nearly precise for one-dimensional Heisenberg models, whether
they involve nearest-neighbor or power-law interactions. This suggests that while
our bounds for these more complex formulas lack formal proof, they are practically
relevant and potentially very accurate. We anticipate that further research will either
theoretically confirm the closeness of our bounds to the true errors or refine them
through additional numerical analyses. Such advancements would greatly benefit the
field, enhancing our understanding of quantum simulation accuracy and the reliability
of higher-order Trotter formulas in simulating quantum systems.

A generalization of this approach analyzes Hamiltonians with three summands,
which is relevant for certain nearest-neighbor and power-law systems where terms are
ordered in an X-Y-Z pattern.

Lemma 3.2.2 Let $H = H_1 + H_2 + H_3$ be a Hamiltonian consisting of three summands.
Decompose the ideal evolution $e^{-itH}$ under $H$ for time $t \in \mathbb{R}$ using the fourth-order
Suzuki formula $S_4(t)$. Then,

$$
\| S_4(t) - e^{-itH} \| \leq t^5 \sum_{i,j,k,l,m=1}^{3} c_{i,j,k,l,m} \| [H_i, [H_j, [H_k, [H_l, H_m]]]] \|, \tag{3.10}
$$

where the coefficients $c_{i,j,k,l,m}$ are given by Table 3.1.
Table 3.1: Coefficients of the fourth-order Trotter error bound for Hamiltonians with three summands.

<table>
<thead>
<tr>
<th>Commutator</th>
<th>Coefficient</th>
<th>Commutator</th>
<th>Coefficient</th>
<th>Commutator</th>
<th>Coefficient</th>
</tr>
</thead>
<tbody>
<tr>
<td>([H_1, [H_1, H_2, H_1]])</td>
<td>0.0047</td>
<td>([H_1, [H_1, [H_2, H_1]])]</td>
<td>0.0047</td>
<td>([H_1, [H_1, [H_2, H_3, H_1]])]</td>
<td>0.0043</td>
</tr>
<tr>
<td>([H_1, [H_2, [H_2, H_1]])]</td>
<td>0.0057</td>
<td>([H_1, [H_1, [H_2, H_3, H_1]])]</td>
<td>0.0057</td>
<td>([H_1, [H_1, [H_2, H_3, H_2]])]</td>
<td>0.0057</td>
</tr>
<tr>
<td>([H_1, [H_1, [H_3, H_1]])]</td>
<td>0.0057</td>
<td>([H_1, [H_1, [H_3, H_2, H_1]])]</td>
<td>0.0057</td>
<td>([H_1, [H_1, [H_3, H_2, H_3]])]</td>
<td>0.0057</td>
</tr>
<tr>
<td>([H_1, [H_2, H_1, H_1]])</td>
<td>0.0046</td>
<td>([H_1, [H_2, [H_1, H_3, H_1]])]</td>
<td>0.0046</td>
<td>([H_1, [H_3, [H_1, H_3, H_2]])]</td>
<td>0.0035</td>
</tr>
<tr>
<td>([H_1, [H_2, H_2, H_1]])</td>
<td>0.0074</td>
<td>([H_1, [H_2, [H_2, H_3, H_1]])]</td>
<td>0.0070</td>
<td>([H_1, [H_3, [H_2, H_3, H_2]])]</td>
<td>0.0046</td>
</tr>
<tr>
<td>([H_1, [H_2, H_3, H_1]])</td>
<td>0.0082</td>
<td>([H_1, [H_2, [H_2, H_3, H_1]])]</td>
<td>0.0082</td>
<td>([H_1, [H_3, [H_3, H_3, H_2]])]</td>
<td>0.0074</td>
</tr>
<tr>
<td>([H_1, [H_3, H_1, H_1]])</td>
<td>0.0046</td>
<td>([H_2, [H_3, [H_1, H_3, H_1]])]</td>
<td>0.0150</td>
<td>([H_2, [H_1, [H_1, H_3, H_1]])]</td>
<td>0.0141</td>
</tr>
<tr>
<td>([H_1, [H_3, H_2, H_1]])</td>
<td>0.0070</td>
<td>([H_2, [H_3, [H_2, H_3, H_1]])]</td>
<td>0.0161</td>
<td>([H_2, [H_1, [H_2, H_3, H_1]])]</td>
<td>0.0161</td>
</tr>
<tr>
<td>([H_1, [H_3, H_3, H_1]])</td>
<td>0.0082</td>
<td>([H_2, [H_3, [H_3, H_3, H_1]])]</td>
<td>0.0150</td>
<td>([H_2, [H_1, [H_3, H_3, H_1]])]</td>
<td>0.0141</td>
</tr>
<tr>
<td>([H_2, [H_1, H_1, H_3, H_1]])</td>
<td>0.0150</td>
<td>([H_2, [H_3, [H_1, H_3, H_1]])]</td>
<td>0.0161</td>
<td>([H_2, [H_1, [H_2, H_3, H_1]])]</td>
<td>0.0161</td>
</tr>
<tr>
<td>([H_2, [H_1, H_2, H_3, H_1]])</td>
<td>0.0161</td>
<td>([H_2, [H_3, [H_2, H_3, H_1]])]</td>
<td>0.0239</td>
<td>([H_2, [H_2, [H_1, H_3, H_1]])]</td>
<td>0.0212</td>
</tr>
<tr>
<td>([H_2, [H_1, H_3, H_1, H_1]])</td>
<td>0.0315</td>
<td>([H_2, [H_3, [H_3, H_3, H_1]])]</td>
<td>0.0306</td>
<td>([H_2, [H_2, [H_2, H_3, H_1]])]</td>
<td>0.0290</td>
</tr>
<tr>
<td>([H_2, [H_2, H_3, H_1, H_1]])</td>
<td>0.0303</td>
<td>([H_2, [H_3, [H_3, H_1, H_1]])]</td>
<td>0.0303</td>
<td>([H_2, [H_2, [H_3, H_3, H_1]])]</td>
<td>0.0303</td>
</tr>
<tr>
<td>([H_2, [H_3, H_3, H_1, H_1]])</td>
<td>0.0179</td>
<td>([H_2, [H_3, [H_1, H_3, H_1]])]</td>
<td>0.0179</td>
<td>([H_3, [H_2, [H_1, H_3, H_1]])]</td>
<td>0.0153</td>
</tr>
<tr>
<td>([H_2, [H_3, H_2, H_1, H_1]])</td>
<td>0.0232</td>
<td>([H_2, [H_3, [H_2, H_3, H_1]])]</td>
<td>0.0206</td>
<td>([H_3, [H_3, [H_2, H_3, H_1]])]</td>
<td>0.0179</td>
</tr>
<tr>
<td>([H_2, [H_3, H_3, H_1, H_1]])</td>
<td>0.0259</td>
<td>([H_2, [H_3, [H_3, H_3, H_1]])]</td>
<td>0.0241</td>
<td>([H_3, [H_3, [H_3, H_3, H_1]])]</td>
<td>0.0241</td>
</tr>
<tr>
<td>([H_2, [H_1, H_1, H_1, H_1]])</td>
<td>0.0204</td>
<td>([H_3, [H_1, [H_1, H_3, H_1]])]</td>
<td>0.0204</td>
<td>([H_3, [H_1, [H_1, H_3, H_1]])]</td>
<td>0.0186</td>
</tr>
<tr>
<td>([H_2, [H_1, H_2, H_1, H_1]])</td>
<td>0.0225</td>
<td>([H_3, [H_1, [H_1, H_3, H_1]])]</td>
<td>0.0225</td>
<td>([H_3, [H_1, [H_1, H_3, H_1]])]</td>
<td>0.0217</td>
</tr>
<tr>
<td>([H_2, [H_1, H_3, H_1, H_1]])</td>
<td>0.0225</td>
<td>([H_3, [H_1, [H_3, H_3, H_1]])]</td>
<td>0.0225</td>
<td>([H_3, [H_1, [H_3, H_3, H_1]])]</td>
<td>0.0225</td>
</tr>
<tr>
<td>([H_2, [H_1, H_3, H_1, H_1]])</td>
<td>0.0423</td>
<td>([H_3, [H_1, [H_3, H_3, H_1]])]</td>
<td>0.0423</td>
<td>([H_3, [H_1, [H_3, H_3, H_1]])]</td>
<td>0.0377</td>
</tr>
<tr>
<td>([H_3, [H_2, H_2, H_1, H_1]])</td>
<td>0.0585</td>
<td>([H_3, [H_2, [H_2, H_3, H_1]])]</td>
<td>0.0571</td>
<td>([H_3, [H_2, [H_2, H_3, H_1]])]</td>
<td>0.0537</td>
</tr>
<tr>
<td>([H_3, [H_2, H_3, H_1, H_1]])</td>
<td>0.0502</td>
<td>([H_3, [H_3, [H_2, H_3, H_1]])]</td>
<td>0.0502</td>
<td>([H_3, [H_3, [H_2, H_3, H_1]])]</td>
<td>0.0502</td>
</tr>
<tr>
<td>([H_3, [H_2, H_3, H_1, H_1]])</td>
<td>0.0423</td>
<td>([H_3, [H_3, [H_1, H_3, H_1]])]</td>
<td>0.0423</td>
<td>([H_3, [H_3, [H_1, H_3, H_1]])]</td>
<td>0.0377</td>
</tr>
<tr>
<td>([H_3, [H_3, H_2, H_1, H_1]])</td>
<td>0.0681</td>
<td>([H_3, [H_3, [H_2, H_3, H_1]])]</td>
<td>0.0641</td>
<td>([H_3, [H_3, [H_2, H_3, H_1]])]</td>
<td>0.0601</td>
</tr>
<tr>
<td>([H_3, [H_3, H_3, H_1, H_1]])</td>
<td>0.0648</td>
<td>([H_3, [H_3, [H_3, H_3, H_1]])]</td>
<td>0.0621</td>
<td>([H_3, [H_3, [H_3, H_3, H_1]])]</td>
<td>0.0628</td>
</tr>
</tbody>
</table>
Quantum chromodynamics (QCD) is the theory that describes strong interactions that give rise to protons and neutrons via an $SU(3)$ gauge theory. In the last fifty years, impressive ab-initio predictions have become possible by discretizing QCD on a spacetime lattice with a fixed lattice spacing $a$, sampling with classical Monte Carlo techniques, and then performing extrapolations back to the continuum limit with multiple values of $a$.

Our work used group space decimation and character expansion which, on the one hand, have fixed qubit costs per gauge link while on the other hand, maintain gate costs that scale polynomially with the total number of qubits required on a full lattice. We showed progress toward efficient QCD simulation schemes on quantum computers with control of error that arises from discrete gauge group representation on quantum circuits.

4.1 Overview and Results

Large-scale quantum computers can simulate nonperturbative quantum field theories which are intractable classically [58]. Alas, Noisy Intermediate-Scale Quantum (NISQ) era systems will be limited both in qubits and circuit depths. Whether any gauge theory simulations in this period are possible depends upon efficient formulations. The presentation in this chapter is based on the results obtained in [77, 78].
situation is similar to the early days of lattice field theory when computer memory was limited and the cost of storing $SU(3)$ elements was prohibitive.

For fermionic fields, relatively efficient mappings to quantum registers are known [80, 132, 141, 148] evidenced by most existing quantum calculations being fermionic [83, 88, 104]. The bosonic nature of gauge fields preclude exact mappings, but many proposals exist with different costs [4, 5, 20, 32, 42, 69, 84, 101, 118, 127, 129, 130, 145, 146, 149]. Digitizing reduces symmetries – either explicitly or through finite-truncations [149]. These breakings mean a priori the original model may not be recovered in the continuum limit [41, 72, 73, 85, 113]. Further, choices of digitization may limit the use of classical resources for Euclidean simulations or state preparation. In summary, the understanding of resource costs, systematic errors, and the continuum limit for these proposals is poorly known today.

We start by introducing some key concepts in the theory of lattice QCD, and then discuss our main results in the following subsections.

**Gauge theory** denotes any theory that has an internal gauge group (e.g., $U(1)$ for electromagnetism). Gauge group then leads to gauge symmetry which manifests as charge conservation (electric charge conservation as an example) in particle interactions and therefore plays central role in theoretical physics. To simulate the dynamics of gauge theories on computers, it is necessary to study their discretized counterpart — lattice gauge theory. The basic idea of a lattice gauge theory is to convert a quantum theory problem to a statistical one by using imaginary time $\tau$. Hence the four-dimensional spacetime becomes a four-dimensional Euclidean space which can be discretized into a "lattice" with the vertices occupied by matter particles (quarks, electrons, etc.) and the lines connecting them representing the gauge (force) fields/boson (gluons, photons, etc.). This Euclidean spacetime lattice can be understood as the
analytic continuation of the trotterized time-evolution of a quantum field theory from $t \to i\tau$, effectively turning path integrals into partition functions.

A **Wilson loop** is a fundamental object in a gauge theory constructed from gauge fields. It plays a crucial role in understanding the inner structures of hadrons such as protons and neutrons. It has been studied extensively in classical lattice calculations and is also currently the main object of interest for applications of quantum computing to high energy physics.

In lattice theory, a **plaquette** is the smallest closed structure on a four-dimensional Euclidean lattice. It usually takes the shape of a two-dimensional square on a standard lattice.

Group space decimation represents a systematic way to study the truncation errors in discrete subgroup digitization of gauge theories. Together with the ability to perform classical simulations of this approximation for time-independent quantities, it is possible to study the errors introduced nonperturbatively. Provided equal developments in other schemes in the near future, direct comparisons of digitizations will become possible whereas at present they are not. Such nonperturbative comparisons are critical for understanding the optimal encoding and resource requirements of simulating gauge theories on quantum devices.

### 4.1.1 Strong Coupling Expansion

Our earlier result [77] is a scheme for digitizing the $SU(N)$ gauge group of effective action to any arbitrary order through group space decimation. In particular, we give a detailed illustration of finding the digitized action to the third order in the strong coupling. This makes the representation of gauge action by quantum registers possible since only a finite number of gauge group elements are required.
Result 1 Let $S[U] = -\sum_p \text{Re Tr}(U_p)$ be the Wilson action, where $U_p$ indicates a product of four $SU(N)$ elements of a single plaquette. The decimated action to the third order including only the single plaquette contributions is expressed as in [77, Eq. (21)].

The high-level idea is to approximate the partition function over a continuous gauge group $G$ by an effective one over the discrete subgroup $H$ of $G$. Let $U \in G$, $u \in H$ and $\Omega$ be the neighborhood of $1 \in H$ [77, Fig. (1)]. For any $U \in G$, there exists a unique $u \in H$ and $\epsilon \in \Omega$ such that $U = u\epsilon$, where we may treat $\epsilon$ as the error of approximating $U$ by $u$. In this way the partition function integrating over $G$ can be written, without approximation, as a summation over $H$ and integration over fluctuations $\epsilon \in \Omega$:

$$Z = \int_G DU \, e^{-S[U]} = \sum_{u \in H} \int_{\Omega} D\epsilon \, e^{-S[u, \epsilon]}, \quad (4.1)$$

where the continuous action $S[U]$ is replaced by its unique discrete counterpart $S[u, \epsilon]$.

The scheme we systematized is a principled way that generates effective decimated action to any arbitrary order. We investigate the behavior of discrete action up to the third order of the coupling expansion for three distinct gauge groups $U(1)$, $SU(2)$, and $SU(3)$. We perform numerical simulations [77, Section 5] on $SU(3)$ of which we found the ground state energy at the nonperturbative regime. We derive the discretization error of the coupling expansion [77, Section 6].

Prior approaches to action decimation have limitations that result in a large error in the perturbative regime. Our approach takes the following measures to address this issue. Our integration over $\epsilon \in \Omega$ has controlled precision by the number of Monte-Carlo sampling in determining the effective couplings, whereas in [60, 61] the integration region was approximated by a polytope in the hyperspace. The uncontrolled
error becomes unacceptable for higher-order approximations. As a quantitative analysis, we show that the multi-plaquette contributions can be systematically neglected. This drastically reduces the number of quantum resources required for a targeted error. We study the effectiveness of the large coupling expansion and discuss how this expansion formally works. This provides some insights into the higher-order behavior of the decimated action. We demonstrate a strong dependence between the freezing point of the decimated action and a particular function of the fundamental character. This serves as a guide for estimating the freezing point for any decimated action.

4.1.2 Character Expansion

Our later result [78] is a scheme for digitizing the $SU(N)$ gauge group of Non-Abelian action to any arbitrary order through character expansion. Unlike the group space decimation method where finding higher-order approximation requires tedious analytical analysis and Monte-Carlo computations, the character expansion scheme can easily produce the effective action to any order through software packages as time permits. Hence gauge field simulation becomes plausible for targeted error.

**Result 2** Let $S[U] = -\sum_p \frac{\beta}{N} \text{Re Tr}(U_p)$ be the Wilson action, where $U_p$ indicates a product of four $SU(N)$ elements of a single plaquette. The character expanded action to the fifth order including only the single plaquette contributions is expressed as in [78, Eq. (6)], where the coefficients $\gamma_i$ are summarized in Tab. I.

The general idea is to approximate the partition function, which can be written as a series expansion over infinitely many $SU(3)$ characters, by an effective one over a finite number of $\mathbb{V}$ group characters. Schematically, the $SU(3)$ character expansion
of the exponentiated Wilson action reads,
\[
e^{-S[U]} = \sum_{\{\lambda,\mu\}:\lambda+\mu \leq 9} \beta_{\{\lambda,\mu\}} \chi_{\{\lambda,\mu\}}(U) + \cdots, \quad U \in SU(3), \quad \lambda \geq \mu \geq 0, \quad (4.2)
\]
with \(\cdots\) representing the higher-order contributions for which we neglect hereafter. This truncation is sufficient for our current goal of accuracy. Also for the defined Wilson action, each expansion coefficient \(\beta_{\{\lambda,\mu\}}\) are calculable as an infinite sum in terms of Bessel functions. Thus we could obtain an effective partition function over \(V\) by matching the following ansatz
\[
e^{\tilde{S}[u]} = \sum_{r} \beta'_{r} \chi'_{r}(u), u \in S(1080) \quad (4.3)
\]
to Eq. (4.2) hence determining the effective action \(\tilde{S}\) to the target accuracy.

This alternative scheme provides not only a principled but also an efficient way to generate effective actions to any arbitrary order. We investigate the behavior of the effective action over \(V\) up to the fifth order in the strong coupling as an approximation of the Wilson action over \(SU(3)\) and accompany it with numerical simulations. Together with the group decimation procedure, this method provides a theoretical framework for systematically improving the Hamiltonian formalism ideal for simulation on quantum devices with fixed qubit costs.

4.2 Group Space Decimation via Strong Coupling Expansion

In this work, we systematize the proposal of replacing continuous gauge groups \(G\) by their discrete subgroups \(H\) \([4, 69]\) by deriving lattice actions using the group space decimation procedure of \([60, 61]\). After deriving the general third-order action, we will investigate the behavior of discretizing three distinct gauge groups \(U(1), SU(2),\) and \(SU(3)\). We begin by reviewing the discrete subgroup approximation in Section 4.2.1. In Section 4.2.2 we discuss the general aspects of the group space
decimation procedure. Following that, in Section 4.2.3 we derive the decimated action up to 3rd order. Numerical results for $\mathbb{V}$ using the decimated actions are presented in Section 4.2.4. Section 4.2.5 studies the continuous group limit, and we conclude in Sec. 4.2.9.

4.2.1 Discrete Subgroups

Approximating gauge theories by replacing $G \rightarrow H$ was explored in the early days of Euclidean lattice field theory. The viability of the $\mathbb{Z}_n$ subgroups replacing $U(1)$ were studied in [48, 49]. Further studies of the crystal-like discrete subgroups of $SU(N)$ were performed [28, 29, 115], including with fermions [139, 140]. These studies met with mixed success depending on the group and action tested.

The fundamental issue of group discretization can be understood by considering the Wilson gauge action

$$S[U] = -\sum_p \frac{\beta}{N} \text{Re} \text{Tr}(U_p),$$

where $U_p$ indicates a plaquette of continuous group gauge links $U$ (for discrete groups, $u_p$ denotes plaquettes and $u$ denotes links). As $\beta \rightarrow \infty$, links near the group identity $1$ dominate, i.e. $U \approx 1 + \varepsilon$, where $\varepsilon$ can be arbitrarily small. Therefore the gap $\Delta S = S[1 + \varepsilon] - S[1]$ goes to zero smoothly. For discrete groups, $\varepsilon$ has a minimum given by the nearest elements $\mathcal{N}$ to $1$, and thus $\Delta S = S[\mathcal{N}] - S[1] > 0$. This strongly suggests a phase transition at some critical $\beta_f = c/\Delta S$, where $c \approx \mathcal{O}(1)$ depends on spacetime dimensionality, gauge group, and entropy. For $U(1) \rightarrow \mathbb{Z}_n$ in 4d, $\beta_f = \frac{0.78}{1 - \cos(2\pi/n)}$ [115]. Above $\beta_f$, all field configurations but $u = 1$ are exponentially suppressed. Thus, $H$ fails to approximate $G$ for $\beta > \beta_f$. Another way to understand this behavior follows [62], where some discrete theories are shown equivalent to continuous groups.
coupled to a Higgs field. The Higgs mechanism introduces a new phase missing from the continuous gauge theory when $\beta \to \infty$.

Both arguments suggest $H$ be viewed as an effective field theory for $G$ with a UV-cutoff at $\Lambda_f$. Provided the typical separation of scales of physics $m_{IR} \ll \Lambda_f$, the approximation could be reliable up to $O(m_{IR}/\Lambda_f)$ effects.

In lattice calculations, one replaces $\Lambda_f$ by a fixed lattice spacing $a = a(\beta)$ which shrinks as $\beta \to \infty$ for asymptotically free theories. To control errors when extrapolating to $a \to 0$, one should simulate in the scaling regime of $a \ll m_{IR}^{-1}$. We denote the onset of the scaling regime by $a_s$, and $\beta_s$. For $a_f(\beta_f) \sim \Lambda_f^{-1}$, errors from the discrete group approximation would be small if $a$ can be reduced such that $m_{IR}^{-1} \gg a \gtrsim a_f$ i.e. $\beta_s \leq \beta_f$.

In the case of $U(1)$ with $\beta_s = 1$, $\mathbb{Z}_{n>5}$ satisfies $\beta_f > \beta_s$. For non-Abelian groups, only a finite set of crystal-like subgroups exist. $SU(2)$ has three: the binary tetrahedral $\mathbb{B}T$, the binary octahedral $\mathbb{B}O$, and the binary icosahedral $\mathbb{B}I$. While $\mathbb{B}T$ has $\beta_f = 2.24(8)$, $\mathbb{B}O$ and $\mathbb{B}I$ have $\beta_f = 3.26(8)$ and $\beta_f = 5.82(8)$ respectively [4], above $\beta_s = 2.2$. Hence, $\mathbb{B}O$ and $\mathbb{B}I$ appear useful for $SU(2)$.

For the important case of $SU(3)$ with $\beta_s = 6$, there are five crystal-like subgroups with the Valentiner group $\mathbb{V}$ with 1080 elements. For all subgroups, $\beta_f < \beta_s$, with $\mathbb{V}$ having $\beta_f = 3.935(5)$ [4] and thus appear inadequate. Other work [95] has shown that extending to a subset with the midpoints between elements of $\mathbb{V}$ raises $\beta_f \approx 7$. However this require more qubits and – potentially more worrisome– sacrifices gauge symmetry completely which is dangerous on quantum computers [127].

To decrease $a_f$, adding additional terms to Eq. (4.4) was attempted [4, 16, 29, 48, 57, 60, 61, 63, 74], although only in [4, 29] were Monte Carlo calculations undertaken.

---

This name is most common in the mathematical literature [46, 131]. It has also referred to as $S(1080)$ [4, 29, 60, 61] or $\Sigma_{3\times360}$ [70].
for $SU(3)$. Two reasons suggest this would help. First, additional terms which have a continuum limit $\propto \text{Re} \text{Tr} F_{\mu\nu} F^{\mu\nu}$, but take different values on the element of $H$ (e.g. $|\text{Tr}(u_p)|^2 - 1$), change $\Delta S$ and thus $a_f$. Second, new terms can reduce finite-$a$ errors as in Symanzik improvement.

The term usually added was the adjoint trace, giving

$$S[u] = -\sum_p \left( \frac{\beta_{\{1\}}}{3} \text{Re} \text{Tr}(u_p) + \frac{\beta_{\{1,-1\}}}{8} |\text{Tr}(u_p)|^2 \right),$$

(4.5)

where $u_p \in \mathbb{V}$, and the first term is normalized so for $\beta_{\{1,-1\}} = 0$, the $S[u]$ matches the Wilson action (with $\beta_{\{1\}} = \beta$). In these works, no relationship was assumed between $\beta_{\{1\}}$ and $\beta_{\{1,-1\}}$. That Eq. (4.5) improves the viability of $\mathbb{V}$ over the Eq. (4.4). For a different action,

$$S[u] = -\sum_p \left( \frac{\beta_0}{3} \text{Re} \text{Tr}(u_p) + \beta_1 \text{Re} \text{Tr}(u_p^2) \right),$$

(4.6)

smaller values of $a_f$ were demonstrated in [4].

With these actions, the dimensionless product $T_c \sqrt{t_0}$ of the pseudocritical temperature and the Wilson flow parameter were found to agree in the continuum with $SU(3)$, allowing one to set the scale of those calculations. $a > 0.08$ fm was achieved without the effects of $a_f$ being seen. This suggest that $\mathbb{V}$ can reproduce $SU(3)$ in the scaling region with a modified action, such that practical quantum computations of $SU(3)$ could be performed. While promising, the choice of new terms was ad-hoc and left unclear how to systematically improve or analyze effectiveness. In the next section, we systematically derive lattice actions for $H$, discovering that the terms added in these two actions are in fact the first terms generated.

4.2.2 Group Space Decimation

Our ultimate goal is to approximate the path integral of group $G$ faithfully by a discrete subgroup $H$ by replacing the integration over $G$ by a summation over $H$. 

80
Group space decimation can be understood in analogy to Wilsonian renormalization, where we integrate out continuous field fluctuations instead of UV modes. The typical method used with discrete subgroup approximations is to replace the gauge links $U \in G$ by $u \in H$ such that the action $S[U] \rightarrow S[u]$. This corresponds to simply regularizing a field theory. For strong coupling, this appears sufficient. As $\beta \rightarrow \infty$, correlations between gauge links increase and the average field fluctuation becomes smaller. When the average field fluctuations decrease below the distance between $I$ and $\mathcal{N}$ of the discrete group, freeze-out occurs and the approximation breaks down—similar to probing a regulated theory too close to the cutoff. Therefore, improving this approximation and understanding the systematics can be done by considering these discarded continuous field fluctuations. To do this, instead of performing the replacement $U \rightarrow u$, we will integrate out the continuous fluctuations, following the decimation formalism developed by Flyvbjerg [60, 61]. He derived the second order decimated action for $U(1)$, $SU(2)$, and $SU(3)$. An important general feature of the decimated action though is missing from this second order action—while new terms are generated at each order, until third order no coefficient of an existing term is modified. One expects such terms are critical to understanding deviations from the continuous group and therefore we compute them in Sec. 4.2.3.

It is natural to associate every subgroup element $u \in H$ with an unique set, or region, $\Omega_u$ containing all closest continuous group elements $U \in G$:

$$
\Omega_u \equiv \{ U \in G | d(U, u) < d(U, u'), \forall u' \in H \setminus \{u\} \},
$$

(4.7)

where the distance is defined as $d^2(U, u) = \text{Tr} \left( (U - u)^\dagger (U - u) \right)$. By such a definition, the continuous group is fully covered, i.e., $G = \cup_{u \in H} \Omega_u$ and a graphical demonstration of $\Omega \equiv \Omega_I$ can be found in Fig. 4.1. Note that for any $U \in G$, there exist a unique $u \in H$ and $\epsilon \in \Omega$ such that $U = u\epsilon$, where we may treat $\epsilon$ as the error of $u$ approximating
Figure 4.1: A schematic demonstration of $\Omega$ (in green) of $G$ (a sphere) around 1 (blue point) of the discrete group (shown as points). $\mathcal{N}$ for $H$ are given by red points. We have applied the $S^2$ metric to obtain the $\Omega$. In groups representable in two dimensions, this region resembles a polygon while in higher dimensions, it becomes a polytope.

$U$. In this way, without approximation, the Euclidean path integral integrating over $G$ can be written as a summation over $H$ and integration over $\epsilon \in \Omega$:

$$Z = \int_G DU e^{-S[U]} = \sum_{u \in H} \int_\Omega D\epsilon e^{-S[u,\epsilon]}$$

(4.8)

where $Z$ is a functional integral over all gauge links $U$ on the lattice, or equivalently a functional integral over $\epsilon$ and a functional sum over $u$. In this expression, $S[u,\epsilon] = S[U]$ is defined by replacing each gauge link $U$ by $ue$. 

82
We then expand the exponential in the path integral and integrate over \( \epsilon \) producing a moment expansion

\[
Z = \sum_{u \in H} \int_{\Omega} D\epsilon \left( 1 - \beta S[u, \epsilon] + \frac{\beta^2}{2!} S[u, \epsilon]^2 + \cdots \right)
\]

\[
= \sum_{u \in H} \left( 1 - \beta \langle S[u, \epsilon] \rangle + \frac{\beta^2}{2!} \langle S[u, \epsilon]^2 \rangle + \cdots \right),
\]

(4.9)

where we have introduced the notation \( \langle f \rangle = \int_{\Omega} D\epsilon f \) with normalization \( \int_{\Omega} D\epsilon = 1 \).

What we are really after is an expansion for the action \( S[U] \), writing \( Z \) in terms of a cumulant expansion

\[
Z = \sum_{u \in H} \exp \left( -\sum_{n=1}^{\infty} \frac{\beta^n}{n!} \mathcal{J}_n[u] \right),
\]

(4.10)

allows us to match Eq. (4.9) with (4.10) to obtain an effective action. In this way, after integrating over \( \epsilon \), the contributions to the action depend only on the discrete group gauge link \( u \) and the effective action can be defined as

\[
S[u] \equiv \sum_n \frac{\beta^n}{n!} \mathcal{J}_n[u].
\]

(4.11)

Up to \( \mathcal{O}(\beta^3) \) one has

\[
\mathcal{J}_1[u] = \langle S[u, \epsilon] \rangle,
\]

(4.12)

\[
\mathcal{J}_2[u] = -\langle S[u, \epsilon]^2 \rangle + \langle S[u, \epsilon]^2 \rangle,
\]

(4.13)

\[
\mathcal{J}_3[u] = \langle S[u, \epsilon]^3 \rangle - 3\langle S[u, \epsilon] \rangle \langle S[u, \epsilon]^2 \rangle + 2\langle S[u, \epsilon]^2 \rangle.
\]

(4.14)

One may worry about poor convergence in the region of interest \( \beta \geq \beta_s \geq 1 \). As will be discussed more thoroughly in Sec. 4.2.5, \( \beta^n \) terms are suppressed by powers of the average field fluctuation. Thus, the size of the discrete group, which determines the size of field fluctuations integrated out, also determines the series convergence.

Starting with the second order terms computed in Refs. [60, 61], the decimated action generates multi-plaquette contributions. Their inclusion in quantum simulations brings substantial non-locality which requires high qubit connectivity and
increases circuit depth. Luckily these contributions will be shown to be small in Sec. 4.2.3.

In the following section, we will calculate Eq. (4.12) to (4.14) in terms of linear combination of the group characters starting from the Wilson action of Eq. (4.4):

$$S[U] \equiv -\sum_p \frac{\beta}{N} \text{Re} \text{Tr}(U_p) = -\sum_p \frac{\beta}{N} \text{Re} \chi_{\{1\}}.$$  (4.15)

Here we introduced $\chi_r$, the character of the group representation $r$. This is the natural basis for the decimated action. All characters required for our $\beta^3$ calculation are in Table 4.1. In the interest of deriving a decimated action for general gauge groups, we have chosen a nonstandard basis for $U(1)$ and $SU(2)$. This allows for one general scheme for $U(N)$ and $SU(N)$ groups. This basis is not linearly independent and relations between representations exist. This dependence is typically used to write $U(1)$ and $SU(2)$ in reduced sets of representations. We have collated relations between the over complete basis in Section 4.2.7.

In deriving the decimated action, integrating out the field fluctuations require us to reduce expressions of the form $\langle \epsilon_i \epsilon_j \cdots \epsilon_{i_n} \rangle$. To simplify these, we use an identity derived in [47] for $SU(N)$ and $U(N)$ groups for any integer $n \leq N$. The necessary relations for $n \leq 3$ are found in Appendix 4.2.6. From these identities, we are left with expectation values of $\chi_r$ over $\Omega$

$$V_r \equiv \frac{1}{d_r} \langle \text{Re} \chi_r \rangle,$$  (4.16)

where $d_r$ is the dimension of representation $r$.

For $U(1) \to \mathbb{Z}_n$, there is only one representation at each order of the cumulant expansion, $V\{ h \} = \langle \epsilon^h \rangle$. These terms can be computed analytically by a change of

---

84
variables $\epsilon = e^{i\phi}$ [61]:

$$V_{(h)} = \frac{1}{V_0} \int \limits_{-\pi}^{\pi} d\phi e^{i\phi h} = \frac{n}{\pi h} \sin \left( \frac{\pi h}{n} \right)$$

(4.17)

with $h = 1, 2, \ldots$ being integers and the normalization constant $V_0 = \int_{\Omega} d\epsilon e^{\epsilon} = \frac{2\pi}{n}$.

Extending this to non-abelian groups, e.g. $SU(N)$, $\Omega$ becomes a high-dimensional polytope in $SU(N)$ space. In [60], the $V_r$ for $\mathbb{B}$ and $\mathbb{V}$ were computed up to second order by approximating these polytopes with hyperspheres to two significant figures. It is crucial to remove these approximations for our purpose because the uncertainty $\delta V_r \sim \mathcal{O}(1\%)$ is magnified in the coupling constants of the decimated action. These couplings are combinations of powers of $V_r$ with extreme cancellations making the fraction errors grow rapidly. Hence we avoid the hypersphere approximation and numerically compute all the $V_r$ necessary for the 3rd order actions to $\mathcal{O}(0.1\%)$. (Results found in Table 4.1.)

4.2.3 ORDER-BY-ORDER DECIMATION

In this section, we summarize the derivation of the decimated action order-by-order. Further details can be found in Appendix 4.2.8. The first order is relatively straightforward, and only contains a single plaquette term. Working from Eq. (4.12)

$$\beta \mathcal{S}_1[u] = -\frac{\beta}{N} \langle \text{Re Tr} (u_1 \epsilon_1 u_2 \epsilon_2 (u_3 \epsilon_3)^\dagger (u_4 \epsilon_4)^\dagger) \rangle$$

$$= -\frac{\beta}{N} \text{Re} (u_{1ab} u_{2cd} u_{3ef} u_{4gh} \langle \epsilon_{1bc} \rangle \langle \epsilon_{2de} \rangle \langle \epsilon_{3fg} \rangle \langle \epsilon_{4ha} \rangle).$$

(4.18)

After applying Eq. (4.34), $\mathcal{S}_1[u]$ depends only on $u$:

$$\beta \mathcal{S}_1[u] = -V_4^{(1)} \frac{\beta}{N} \text{Re} (u_{1ab} u_{2cd} u_{3ef} u_{4gh} \delta_{bc} \delta_{de} \delta_{fg} \delta_{ha})$$

$$= -V_4^{(1)} \frac{\beta}{N} \text{Re} \chi_{(1)} \equiv -\beta_{(1)}^{(1)} \frac{1}{N} \text{Re} \chi_{(1)},$$

(4.19)

where $\beta_r^{(n)}$ is the $n$-th order term in front of $\frac{1}{d_r} \text{Re} \chi_r$. 

85
Table 4.1: Properties of characters. The dimension, $d_r$, the character $\chi_r$, and $V_r[G \to H] = d_r^{-1} \langle \text{Re} \chi_r \rangle$ of character $r$ for the decimations $U(1) \to \mathbb{Z}_n$, $SU(2) \to \mathbb{B}[2]$, and $SU(3) \to \mathbb{V}$. We have followed the normalizations in Table 14 of [55].

<table>
<thead>
<tr>
<th>$r$</th>
<th>$d_r$</th>
<th>$\chi_r$</th>
<th>$V_r[U(1) \to \mathbb{Z}_n]$</th>
<th>$V_r[SU(2) \to \mathbb{B}[2]]$</th>
<th>$V_r[SU(3) \to \mathbb{V}]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>{1}</td>
<td>$N$</td>
<td>$\text{Tr}(U)$</td>
<td>$\frac{n}{2} \sin \left(\frac{n\pi}{2}\right)$</td>
<td>0.964748(2)</td>
<td>0.83414(6)</td>
</tr>
<tr>
<td>{2}</td>
<td>$\frac{N(N+1)}{2}$</td>
<td>$\frac{1}{2} \left(\text{Tr}(U) + \text{Tr}(U^2)\right)$</td>
<td>$\frac{n}{2n} \sin \left(\frac{2n\pi}{n}\right)$</td>
<td>0.90798(3)</td>
<td>0.62874(11)</td>
</tr>
<tr>
<td>{1, 1}</td>
<td>$\frac{N^2 - 1}{2}$</td>
<td>$\frac{1}{2} \left(\text{Tr}(U) - \text{Tr}(U^2)\right)$</td>
<td>—</td>
<td>1</td>
<td>0.83414(6)</td>
</tr>
<tr>
<td>{1, -1}</td>
<td>$\frac{N(N+1)(N+2)}{6}$</td>
<td>$\frac{1}{6} \left(\text{Tr}(U)^3 + 2 \text{Tr}(U) + 3 \text{Tr}(U^2) \text{Tr}(U)\right)$</td>
<td>$\frac{n}{2n} \sin \left(\frac{2n\pi}{n}\right)$</td>
<td>0.90798(3)</td>
<td>0.65971(10)</td>
</tr>
<tr>
<td>{3}</td>
<td>$\frac{N(N+1)(N+2)}{6(N-1)}$</td>
<td>$\frac{1}{6} \left(\text{Tr}(U)^3 + 2 \text{Tr}(U) + 3 \text{Tr}(U^2) \text{Tr}(U)\right)$</td>
<td>—</td>
<td>0.964748(2)</td>
<td>0.65971(10)</td>
</tr>
<tr>
<td>{2, 1}</td>
<td>$\frac{N(N^2-1)}{6}$</td>
<td>$\frac{1}{3} \left(\text{Tr}(U) - \text{Tr}(U^3)\right)$</td>
<td>—</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>{1, 1, 1}</td>
<td>$\frac{N(N-3)(N-2)}{6}$</td>
<td>$\frac{1}{6} \left(\text{Tr}(U)^3 + 2 \text{Tr}(U) + 3 \text{Tr}(U^2) \text{Tr}(U)\right)$</td>
<td>—</td>
<td>0.83257(2)</td>
<td>0.46693(13)</td>
</tr>
<tr>
<td>{2, -1}</td>
<td>$\frac{N(N-1)(N+2)}{6}$</td>
<td>$\frac{1}{6} \left(\text{Tr}(U)^3 + 2 \text{Tr}(U) + 3 \text{Tr}(U^2) \text{Tr}(U)\right)$</td>
<td>—</td>
<td>0.83257(2)</td>
<td>0.46693(13)</td>
</tr>
<tr>
<td>{1, 1, -1}</td>
<td>$\frac{N(N+1)(N-2)}{2}$</td>
<td>$\frac{1}{2} \left(\text{Tr}(U) \text{Tr}(U^\dagger) + \text{Tr}(U^2) \text{Tr}(U^\dagger)\right) - \text{Tr}(U)$</td>
<td>$\frac{n}{2} \sin \left(\frac{2n\pi}{n}\right)$</td>
<td>—</td>
<td>0.62874(11)</td>
</tr>
</tbody>
</table>
Table 4.2: Property of character $r$ for a general group decimation.

$\beta, G \to H$ of character $r$ for a general group decimation. For completeness, we have included the 4 two-plaquette terms derived in [60, 61] at second order labeled as $2r, 2i, 2t$ and $2u$.

<table>
<thead>
<tr>
<th>$r$</th>
<th>$\beta_r$</th>
</tr>
</thead>
<tbody>
<tr>
<td>${0}$</td>
<td>$V_{(1)}^4 \beta + \frac{1}{8N^2} [4V_{(1)}^8 - 2V_{(1)}^4 - V_{(1)}(1,-1) - V_{(1)}^{(2)}] \beta^3$</td>
</tr>
<tr>
<td>${1}$</td>
<td>$\frac{N+1}{8N^2} [V_{(2)}^4 - V_{(1)}^8] \beta^2$</td>
</tr>
<tr>
<td>${2}$</td>
<td>$\frac{N}{8N^2} [V_{(2)}^4 - V_{(1)}^8] \beta^2$</td>
</tr>
<tr>
<td>${1,1}$</td>
<td>$\frac{N^2 - 1}{N^2} [V_{(2)}^4 - V_{(1)}^8] \beta^2$</td>
</tr>
<tr>
<td>${1, -1}$</td>
<td>$\frac{(N+1)(N+2)}{6N^2} [V_{(2)}^4 - V_{(1)}^8] \beta^2$</td>
</tr>
<tr>
<td>${2, 1}$</td>
<td>$\frac{(N^2 - 1)}{6N^2} [V_{(2)}^4 - V_{(1)}^8] \beta^2$</td>
</tr>
<tr>
<td>${1, 1, 1}$</td>
<td>$\frac{(N-1)(N-2)}{6N^2} [V_{(2)}^4 - V_{(1)}^8] \beta^2$</td>
</tr>
<tr>
<td>${2, -1}$</td>
<td>$\frac{(N-1)(N+2)}{16N^2} [V_{(2)}^4 - V_{(1)}^8] \beta^2$</td>
</tr>
<tr>
<td>${1, 1, -1}$</td>
<td>$\frac{(N+1)(N-2)}{16N^2} [V_{(2)}^4 - V_{(1)}^8] \beta^2$</td>
</tr>
<tr>
<td>${2r}$</td>
<td>$\frac{1}{2} V_{(1)}^4 [\frac{1}{4} V_{(2)}^{(4)} + \frac{1}{3} V_{(1,1)} + \frac{1}{2} V_{(1,-1)} - V_{(1)}^{(2)}] \beta^2$</td>
</tr>
<tr>
<td>${2i}$</td>
<td>$\frac{1}{2} V_{(1)}^4 [\frac{1}{4} V_{(2)}^{(4)} + \frac{1}{3} V_{(1,1)} + \frac{1}{2} V_{(1,-1)} - V_{(1)}^{(2)}] \beta^2$</td>
</tr>
<tr>
<td>${2t}$</td>
<td>$\frac{1}{2} V_{(1)}^4 [\frac{1}{4} V_{(2)}^{(4)} + \frac{1}{3} V_{(1,1)} + \frac{1}{2} V_{(1,-1)} - V_{(1)}^{(2)}] \beta^2$</td>
</tr>
<tr>
<td>${2u}$</td>
<td>$\frac{1}{4N^2} V_{(1)}^4 [1 - V_{(1,-1)}] \beta^2$</td>
</tr>
</tbody>
</table>

It is comforting that at $O(\beta)$, no new terms are generated in $S[u]$. This allows for rescaling $\beta_{(1)}^{(1)} \to \beta$, recovering the procedure of directly replacing $U \to u$ in the Wilson action. Although this rescaling is permitted, $V_{(1)} < 1$ contains content about the approximation $G \to H$. As the number of elements of $H$ increases, $\Omega$ shrinks and $V_{(1)} \to 1$. This means $V_{(1)}$ quantifies how densely $H$ covers $G$ and thus the minimal fluctuation size. Since $\beta_{(1)}^{(1)} = V_{(1)}^4 \beta$, decreases in $V_{(1)}$ signals the poorness of using Eq. (4.19) alone. This is discussed further in Sec. 4.2.5.
We now proceed to calculate the second order decimated action while fixing a few typos in [60] along the way. The second order decimated action $S_2[u] = -\langle S[u, \epsilon]\rangle^2 + \langle S[u, \epsilon]\rangle^2$ depends upon two plaquettes $U_p = U_1 U_2 U_3^1 U_4^+$ and $U_q = U_5 U_6 U_7^1 U_8^+$. A natural decomposition of $S_2[u]$ can be made into three terms based on how the two plaquettes $p$ and $q$ are related: $p = q$ (one-plaquette contribution), $p \cap q = 1$-link (two-plaquette contribution), and $p \cap q = 0$-links. To all orders, the $p \cap q = 0$ contributions to the decimated action vanish.

For the case of $p = q$, we conclude that it is:

$$\frac{1}{2!} \beta^2 S_2[u]_{1p} = -\beta^{(2)}_{(0)} - \beta^{(2)}_{(2)} \frac{2}{N(N+1)} \text{Re} \chi^{(2)}$$

$$- \beta^{(2)}_{(1,1)} \frac{2}{N(N-1)} \text{Re} \chi^{(1,1)}$$

$$- \beta^{(2)}_{(1,-1)} \frac{1}{N^2 - 1} \chi^{(1,-1)},$$

where the $\beta^{(2)}_r$ can be found in Table 4.2.

Next, we calculate the case of $p \cap q = 1$-link for the second order decimation. Contracting the $\delta$’s in Eqs. (4.35) and (4.36), where unlike Eq. (4.48), we only identify one link as the same between the two plaquettes. This leads to the following expression,

$$\frac{1}{2!} \beta^2 S_2[u]_{2p}$$

$$= -\beta_{(2r)} \frac{1}{N} \text{Re} [\chi^{(1)}(u_p)] - \beta_{(2i)} \frac{1}{N} \text{Im} [\chi^{(1)}(u_p)]$$

$$- \beta_{(2i)} \frac{1}{N} \text{Im} [\chi^{(1)}(u_q)]$$

$$- \beta_{(2t)} \frac{1}{N} \text{Re} [\chi^{(1)}(u_{p\neq q})] - \beta_{(2u)} \frac{1}{N} \text{Re} [\chi^{(1)}(u_{p\neq q})],$$

where we have used the fact that all the $V_r$’s are real due to our choice of the integration region. The explicit expressions for the couplings are found in Table 4.2. Note that this expression is also applicable to $U(1)$.

We would now like to comment on how the two-plaquette – and general multiplaquette – terms contributes to the $S[u]$. It would be desirable if these terms
could be neglected, because they require substantial quantum resources. By inspecting Table 4.3, one observes that the two-plaquette $\beta_r$ are $O(0.1)$ or smaller than the single-plaquette terms. The largest coupling, $\beta_{21}$, multiples a term $\text{Im} \chi_1 \text{Im} \chi_1 \approx 0$. Strong cancellations are expected from correlations between the remaining terms (shown in Fig. (4.2)) as evident by the observation $\beta_{2t} \approx -\beta_{2u}$.

We would now like to comment on how the two-plaquette – and general multiplaquette – terms contributes to the $S[u]$. It would be desirable if these terms could be neglected, because they require substantial quantum resources. By inspecting Table 4.3, one observes that the two-plaquette $\beta_r$ are $O(0.1)$ or smaller than the single-plaquette terms. The largest coupling, $\beta_{21}$, multiples a term $\text{Im} \chi_1 \text{Im} \chi_1 \approx 0$. Strong cancellations are expected from correlations between the remaining terms (shown in Fig. (4.2)) as evident by the observation $\beta_{2t} \approx -\beta_{2u}$.

$$S[u] = \sum_p \left( \beta_{(1)}^{(1)} + \beta_{(1)}^{(3)} \right) \frac{1}{N} \text{Re}(\chi_{(1)}) - \beta_{(0)}^{(2)} - \beta_{(2)}^{(2)} \frac{2}{N(N + 1)} \text{Re} \chi_{(2)} - \beta_{(1,1)}^{(2)} \frac{2}{N(N - 1)} \text{Re} \chi_{(1,1)}$$

$$- \beta_{(1,-1)}^{(2)} \frac{1}{N^2 - 1} \text{Re} \chi_{(1,-1)} - \beta_{(3)}^{(3)} \frac{6}{N(N + 1)(N + 2)} \text{Re} \chi_{(3)} - \beta_{(2,1)}^{(3)} \frac{3}{N(N^2 - 1)} \text{Re} \chi_{(2,1)}$$

$$- \beta_{(1,1,1)}^{(3)} \frac{6}{N(N - 1)(N - 2)} \text{Re} \chi_{(1,1,1)} - \beta_{(2,1,1)}^{(3)} \frac{2}{N(N - 1)(N + 2)} \text{Re} \chi_{(2,1,1)}$$

$$- \beta_{(1,1,-1)}^{(3)} \frac{2}{N(N + 1)(N - 2)} \text{Re} \chi_{(1,1,-1)} .$$

(4.22)
where $\beta_r$ are in Table 4.2. Note that this $S[u]$ is correct for any $G \to H$. Referring to Eqs. (4.39), (4.40), and (4.41), for a given $G$ simplifications occur. For $SU(3)$, with

$$
\beta_r \equiv \sum_n \frac{1}{n!} \beta_r^{(n)} ,
$$

this corresponds to:

$$
S[u] = \sum_p - (\beta_{\{1\}} + \beta_{\{1,1\}}) \frac{1}{3} \text{Re} \chi_{\{1\}} - (\beta_{\{0\}} + \beta_{\{1,1,1\}})
$$

$$
- (\beta_{\{2\}} + \beta_{\{1,1,-1\}}) \frac{1}{6} \text{Re} \chi_{\{2\}}
$$

$$
- (\beta_{\{1,-1\}} + \beta_{\{2,1\}}) \frac{1}{8} \chi_{\{1,-1\}}
$$

$$
- \frac{\beta_{\{3\}}}{10} \text{Re} \chi_{\{3\}} - \frac{\beta_{\{2,-1\}}}{15} \text{Re} \chi_{\{2,-1\}} .
$$

For $U(1)$ and $SU(2)$, we refer the reader to Section 4.2.7.

### 4.2.4 Results for $V$

As a demonstration, we simulated Eq. (4.24) to each order in $\beta$ for $SU(3) \to V$. For these computations $10^2$ configurations separated by $10^3$ sweeps were collected on a $4^4$ lattice and plotted in Fig. 4.3. In the figure, we compare the average energy per plaquette $\langle E_0 \rangle$ versus the coupling, $\beta_{\{1\}}$ as defined in Eq. (4.23), which multiplies the Wilson term $\text{Re} \chi_1$. For $SU(3)$, this corresponds to $\beta$, and $\beta_{\{1\}} + \beta_{\{1,1\}}$ for $V$.

Naively, $\langle E_0 \rangle$ is monotonic in $a$. Including $O(\beta^2)$ terms, we observe a clear reduction in $\langle E_0 \rangle$ and thus an improvement over the Wilson action for small $a$. This suggests promise in this systematic approach. As will be discussed in Sec. 4.2.5, it also supports the effectiveness of the previously studied ad-hoc actions. Instead of freezing out, the theory approaches a non-zero value of $\langle E_0 \rangle$.

At $O(\beta^3)$, $\langle E_0 \rangle$ displays non-monotonic behavior due to the negative coefficient of $\chi_1$ at $\beta^3$. This suggests the higher order terms (4th order and beyond) required to match Eq. (4.9) and (4.10) are dominating the action.
Figure 4.3: Average energy per plaquette. \( \langle E_0 \rangle = 1 - \text{Re} \langle \text{Tr} U_p \rangle / 3 \), vs \( \tilde{\beta}_1 \) on 4\( ^4 \) lattice for \( V \) action with corrections of: (■) \( O(\beta^1) \), (●) \( O(\beta^2) \), and (▲) \( O(\beta^3) \). The black line is the \( SU(3) \) result.

Taken together, the \( O(\beta^n) \) results suggests that the decimation procedure, formulated as a strong coupling expansion, converges to the continuous theory slowly. Sufficiently large order calculations would suppress the higher order contributions in the form \( \beta^n/n! \) for a reasonable range of \( \beta \). While an \( O(\beta^4) \) calculation would undoubtedly be insightful to understanding this convergence, other approaches such as introducing “counter-terms” to absorb some higher-order contributions, or instead using a character expansion may prove fruitful. It also may prove useful to take the expansion in Eq. (4.10) as an effective theory where each character is subject to field redefinitions. While these possibilities are interesting to investigate, they are certainly beyond the scope of this work. We therefore leave them for future studies.
4.2.5 Finite Group Effects

With Eq. (4.22), it is possible for us to investigate systematically the effect of replacing the continuous group by its finite subgroup. In order to proceed, it is useful to introduce a new parameter which approximately represents the field fluctuations. To do this, consider the representation of a continuous group lattice gauge link in terms of the corresponding generators \( \lambda_a \) in the adjoint representation, \( U = e^{i\lambda_a A_a} \), where a summation over color indices \( a \) is implied. In this form, we see that the gauge fields correspond to amplitudes in each of the generators. For \( \epsilon \in \Omega \), inserting its small parameter expansion \( \epsilon \approx 1 + i\lambda_a A_a - \frac{1}{2}(\lambda_a A_a)^2 + \ldots \) into Eq. (4.16) gives

\[
V_r \approx 1 - \int_{\Omega} DA \left( c_r^{(2)} \sum_a A_a^2 + \ldots \right),
\]

where \( DA \) is a measure over all \( A_a \) which respects gauge symmetry and \( c_r^{(n)} \) are representation and group-dependent constants. From this, we see that as the subgroup \( H \) incorporates more elements, the size of \( \Omega \) approaches 0 and \( V_r \to 1 \) from below.

This means that for finite \( \Omega \) the domain size of \( A_a \) that grives rise to \( \Omega \) is an indicator for deviations from \( G \) of \( H \). Flyvbjerg defines a parameter \( R \) as the radius of a hypersphere with equal volume to \( \Omega \) to get a handle on the domain of \( A_a \). This allows him to approximate \( V_r \) analytically [60, 61]. Here, we can use this idea to roughly understand the scaling of \( V_r \).

For \( U(1) \to \mathbb{Z}_n \), the hypersphere is exactly \( \Omega \) and \( R \) cleanly defines \( \epsilon \leq R = \pi/n \). Beyond \( U(1) \), the connection between \( \Omega \) and a single value of \( R \) is complicated because the \( \Omega \) of \( H \) form polytopes in the hypervolume of their continuous partner (see Fig. 4.1 for a clear demonstration). In this case, while one could take \( \Omega \) to be contained by a hypersphere centered at \( 1 \) whose boundary incorporates elements of the nearest neighbors of \( 1 \) in \( H \), making some element of the hypersphere not included in \( \Omega \). On the other hand, there exists a largest hypersphere centered at \( 1 \) that only
contains elements in $\Omega$. In this way, we define an upper and lower bound for $R$. Note, this is different from [60, 61] where the polytopes of $H$ were always approximated by hyperspheres with definite radii. For SU(2) with $H$, we find $0.09 \leq R^2 \leq 0.15$ which can be compared to $R_{\text{sphere}}^2 = 0.12$ of [60, 61]. In the case of SU(3) with $V$, $0.42 \leq R^2 \leq 0.93$ compared to $R_{\text{sphere}}^2 = 0.62$.

While superficially the cumulant expansion has appeared as a strong-coupling expansion in $\beta$, the actual behavior is controlled by both $\beta$ and $R$ with $R$ controlling $V_r$. As pointed out in [60, 61], the leading order behavior for small $R$ for a given power of $\beta^\alpha$ ($\alpha > 0$) is actually $O([\beta R^2]^{\alpha} R^{-2})$. Therefore one would predict that the relative smallness of $R^2$ for $H$ compare to $V$ signals that $\beta_f$ should be larger for $H$ which is indeed the case.

For subgroups of $SU(3)$, this scaling behavior becomes unsatisfactory because $R^2 \sim 1$. It is possible to study this breakdown in $U(1) \to \mathbb{Z}_n$ where the systematic effect of decimation can be studied in detail both because errors can be made arbitrarily small for large $n$ and because $V_r$ and $\beta_r$ are known analytically. In terms of $R$, one can expand the $\beta_r$ for the $U(1)$ action of Eq. (4.46) to find:

$$
\beta_{\{0\}} \approx \left(\frac{R^2}{3} - \frac{19R^4}{90} + \ldots\right) \beta^2,
$$

(4.26)

$$
\beta_{\{1\}} + \beta_{\{1,1,-1\}} \approx \left(1 - \frac{2R^2}{3} + \frac{R^4}{5} + \ldots\right) \beta
$$

$$
+ \left(- \frac{17R^4}{90} + \frac{311R^6}{945} + \ldots\right) \beta^3,
$$

(4.27)

$$
\beta_{\{2\}} \approx \left(- \frac{R^2}{3} + \frac{53R^4}{90} + \ldots\right) \beta^2,
$$

(4.28)

$$
\beta_{\{3\}} \approx \left(\frac{17R^4}{90} - \frac{1609R^6}{2835} + \frac{46303R^8}{56700}
- \frac{77603R^{10}}{103950} + \ldots\right) \beta^3.
$$

(4.29)
The first thing to note is that the $\mathcal{O}([\beta R^2]^{\alpha} R^{-2})$ scaling found in [60, 61] continues to the third order. One might be tempted to use this leading behavior to estimate the $\beta_f$ or the radius of convergence of this series, but this would be incorrect. Instead, it behooves one to note that for both 2nd and 3rd order contributions, the subleading terms $[R^2]^k R^{-2}$ with $k > \alpha$ initially grow until a $1/k!$ factor dominates over all the other factors.

But what is the origin of this behavior? For simplicity, we can understand this behavior by considering the expansion of $V_{4m}$ which form $\beta_r$. The specific combination of $V_{4m}$ dictated by the cumulant expansion ensures that orders lower than $\mathcal{O}([\beta R^2]^{\alpha} R^{-2})$ cancel in $\beta_r$. The $j$ representation contributes to $\beta_{\{r_1, \cdots, r_k\}}$ in the form of $V_{4m_{\{j_1, \cdots, j_l\}}} \cdots V_{4m_{\{j_{1}, \cdots, j_l\}}} \cdots$ under the constraint $|r| = m_i \tilde{j}_i$ where $|r| = |r_1| + \cdots + |r_k|$ and $\tilde{j}_i = |j_1^i| + \cdots + |j_l^i|$. One might worry that studying the expansion of $V_{4m}$ isn’t representative, but one can verify that the scaling behavior observed below persists in $\beta_r$, although the numerical factors become cumbersome. For $V_{4m} \equiv V_{4m_{\{j_1, \cdots, j_l\}}}$, $\tilde{j} = |j_1| + \cdots |j_l|$, we have

$$V_{4m} \approx 1 - \frac{2}{3} m(\tilde{j} R)^2 + \frac{1}{45} (10 m^2 - m)(\tilde{j} R)^4 + \mathcal{O}(m^3(\tilde{j} R)^6)$$

(4.30)

from which, we see that the coefficients of the $[R^2]^k R^{-2}$ contributions to $\beta_r$ are accompanied by a factor $\propto \frac{1}{k!} m^{k-1} \tilde{j}^{2k-2}$. While the factorials ensure the series converges, $\beta_r$ for higher representations $r$ have larger $m$, $\tilde{j}$, or both leading to higher order terms in the expansion being large for moderate $R$. This helps explaining why $\mathbb{Z}_4$ with the Wilson action fails to replicate $U(1)$ substantially above $\beta = 1$ – while the naive scaling would suggest $R \lesssim \sqrt{\beta^{1-k}}$ would be enough to suppress higher representations, in reality a stronger bound of $\max\{ \frac{1}{k!} m^{k-1} (\tilde{j} R)^{2k-2} \}_{1 \leq \tilde{j} \leq |r|} \lesssim 1$ for $\forall \beta_r$ is required for all subleading terms to be small. Considering the range of $m$ with fixed $|r|, \tilde{j}$, the bound is strictest when $|r| = \tilde{j}$ yielding $R \lesssim 1/|r|^{3/2}$ in order for the lowest
order contribution to dominate such that \( R \lesssim \sqrt{\beta^{\alpha}} \) provides a reasonable estimate for the range of \( \beta \) where the decimated action provides a reasonable approximation for its continuous partner. While these conditions are satisfied for \( B\mathbb{I} \), they are violated for \( \mathbb{V} \) in which case the dominant term in the \( R \) expansion isn’t clear.

Another feature observed in the \( R \) expansion of the \( \mathbb{Z}_n \) group is that because \( V_r \propto \sin rR \), the sign of the \( \mathcal{O}([rR]^k) \) terms oscillate, and therefore the sign of \( \beta_r^{(n)} \) can depend sensitively on \( R \). Since \( \text{Re} \chi_r(1) > \text{Re} \chi_r(\mathcal{N}) \), where \( \mathcal{N} \) is the nearest neighbors of \( \mathcal{K} \) in \( H \) (see Fig. 4.1), the overall sign of \( \beta_r^{(n)} \) determines whether or not the \( r \)-th term in the action enters the frozen phase in the limit of \( \beta \to \infty \). This behavior is observed in Fig. 4.6 where \( \beta_{(1)}^{(1,2)} > 0 \) but \( \beta_{(1)}^{(3)} < 0 \).

From the behavior observed in \( U(1) \), we can improve the quantitative understanding of how well \( H \) can approximate \( G \), even when \( \beta_r \) are not known analytically. Clearly, \( V_r \to 1 \) indicates that the \( R \to 0 \), and in that limit the two actions would agree. Therefore, the difference between the two actions \( S_G - S_H \approx \beta \chi(1)(U) - \beta(1)\chi(1)(u) \approx (1 - V_{(1)}^4)\beta \chi(1)(u) \) serves as an indicator of \( \beta_f \).

This proxy can be compared to others in the literature. The simplest estimate is \( \beta_f^{-1} \propto \Delta S = \text{Re Tr}(1) - \text{Re Tr}(\mathcal{N}) \) \cite{115}. While this estimate finds monotonic behavior for discrete groups of \( U(1) \) and \( SU(2) \), different \( \mathcal{O}(1) \) factors are needed. It also fails completely for \( SU(3) \), as seen in the left panel of Fig. 4.4.

Observing the differing \( \mathcal{O}(1) \) factors, \cite{115} suggested a different estimate. For discrete Non-abelian subgroups near \( \beta_f \), \( S[u] \) is dominated by contributions from \( u_p = \mathcal{N} \). From duality arguments, the action near \( \beta_f \) could be approximately rewritten as a \( \mathbb{Z}_C \) action where \( C \) is the minimal cycle such that \( u^C = 1 \) for all \( u \subset \mathcal{N} \). Since \( C = n \) for \( \mathbb{Z}_n \), these arguments predict a single curve \( \beta_f \approx 0.78/(1 - \cos(2\pi/C)) \) directly from the study of \( \beta_f \) in \( \mathbb{Z}_n \) for all discrete subgroups. The discrepancy between \( SU(2) \) and \( U(1) \) was reduced from \( \sim 300\% \) to \( \sim 50\% \). The authors of \cite{115} warned
Figure 4.4: $\beta_f$ as a function of $\Delta S^{-1}$, the cycle $C$ of $\mathcal{N}$, and $(1 - V_{(1)}^4)^{-1}$. Note that for the subgroups of $U(1)$ and $SU(2)$, monotonic behavior is observed for all three variables, but only for $(1 - V_{(1)}^4)^{-1}$ are the subgroups of $SU(3)$ monotonic.

that this approximation could be poor for $SU(3)$ albeit without numerical evidence. Since then $\beta_f$ for the subgroups of $SU(3)$ have been found and as anticipated, this estimator proves to be poor as presented in the center of Fig. 4.4. In the plot on the right of Fig. 4.4, $\beta_f$ is plotted as a function of $(1 - V_{(1)}^4)^{-1}$. We find that monotonic, linear behavior is observed within the uncertainties for each continuous group. Best fit lines have been included for each group to guide the eye. This suggests that our estimator captures some of the non-perturbative behavior near the freezing transition better than $\Delta S^{-1}$ or $C$. Physics of the different groups differ, as signaled by their different scaling regimes. If we divide $\beta_f$ by a rough estimate of $\beta_s = [1, 2.2, 6]$ for $U(1), SU(2), SU(3)$ respectively, we might expect to further remove some of this group dependence. Doing so in Fig. 4.5, we find that $SU(2)$ and $SU(3)$ collapse onto a single line and $U(1)$ within 25%.

Using our higher order results, one can then gain insight into the effectiveness of the ad-hoc actions of $V$. Each of these actions corresponds to terms that are generated at 2nd order in the decimated action. The first ad-hoc action used in [4] can be
Figure 4.5: $\beta_f/\beta_s$ as a function of $(1 - V_{(1)}^4)^{-1}$. 
rewritten as

\[
S[u] = -\sum_p \left( \frac{\beta_0}{3} \text{Re} \, \text{Tr}(u_p) + \beta_1 \text{Re} \, \text{Tr}(u_p^2) \right),
\]

\[
= -\sum_p \left( (\beta_0 - 3\beta_1) \frac{1}{3} \text{Re} \, \chi_{\{1\}} + (6\beta_1) \frac{1}{6} \text{Re} \, \chi_{\{2\}} \right),
\]

(4.31)

where we have used \( \beta_1 = a\beta_0 + b \) with \( a = -0.1267 \) and \( b = 0.253 \). For an unpublished action of

\[
S[u] = -\sum_p \left( \frac{\tilde{\beta}_{\{1\}}}{3} \text{Re} \, \chi_{\{1\}} + \frac{\tilde{\beta}_{\{1,1\}}}{8} \text{Re} \, \chi_{\{1,\} - 1} \right) \quad (4.32)
\]

where \( \tilde{\beta}_{\{1\}} = a\tilde{\beta}_{\{1\}} + b \) with \( a = -0.587 \) and \( b = 1.80 \). The trajectory parameters were chosen to be parallel to the freezing point at large \( \beta_0 \) by eye. From Fig. 4.6, we see that in both ad-hoc actions, reasonably agreement is found for intermediate \( \beta \) for the 3rd order action. Here \( \beta \) is the coefficient in front of \( \text{Re} \, \chi_{\{1\}} \) for the ad-hoc actions. The ad-hoc trajectories are known to poorly reflect \( G \) at low \( \beta \), because they lack curvature to fix the known requirements at \( \beta = 0 \). At large \( \beta \), we expect higher order terms in the cumulant expansion to become relevant and thus disagreement is expected to occur. This surprising agreement in the intermediate region of \( \beta \) suggests that actions formed by neglecting terms in the cumulant expansion are optimized in their character basis by setting the couplings to results given by the resuming higher order contributions in cumulant expansion with fluctuations \( G/H \) integrated out.

**4.2.6 Creutz Identities**

A useful identity was derived in [47] for \( SU(N) \) and \( U(N) \) groups such that for any integer \( n \leq N \)
Figure 4.6: Trajectories of $S^n$. The open circles indicate the boundary between the frozen and unfrozen phases obtained on $2^4$ lattices.

$$\langle \varepsilon_{i_1j_1} \cdots \varepsilon_{i_nj_n} \rangle = c_1 \varepsilon_{i_1A_1^1 \ldots A_{N-1}^1} \varepsilon_{j_1A_1^1 \ldots A_{N-1}^1} \times \cdots \times \varepsilon_{i_nA_n^1 \ldots A_{N-1}^1} \varepsilon_{j_nA_n^1 \ldots A_{N-1}^1}$$

$$+ c_2 \varepsilon_{i_1i_2A_1^1 \ldots A_{N-2}^1} \varepsilon_{j_1j_2A_1^1 \ldots A_{N-2}^1} \times \cdots \times \varepsilon_{i_nA_n^{n-1} \ldots A_{N-1}^{n-1}} \varepsilon_{j_nA_n^{n-1} \ldots A_{N-1}^{n-1}} + \cdots$$

$$+ c_{B_n} \varepsilon_{i_1i_2 \ldots i_nA_1^1 \ldots A_{N-n}^1} \varepsilon_{j_1j_2 \ldots j_nA_1^1 \ldots A_{N-n}^1},$$

(4.33)

where $\varepsilon$ is Levi-Civita symbol, $A_i^j$ are the contracted dummy indices, and $B_n$ is the Bell number accounting for the number of ways that one can put the open indices $i_k, j_l$ on $\varepsilon$ such that no $i_k$ and $j_l$ appear in the same $\varepsilon$. In [47], Eq. (4.33) was derived for integrating over the entire group $G$. Hence in our case, we need to determine the constants $c_i$’s when integrating only over $\Omega$ for $\langle \varepsilon_{ij} \rangle, \langle \varepsilon_{ij} \varepsilon_{kl} \rangle, \langle \varepsilon_{ij} \varepsilon_{kl} \varepsilon_{mn} \rangle, \langle \varepsilon_{ij} \varepsilon_{kl} \varepsilon_{mn} \rangle$, with $i, j, k, l, m, n \in [N]$. This is done by contracting the tensor structure on each side of Eq. (4.33) with products of Kronecker delta’s and solving the resulting linear equations.
At first order, only one integral is needed:

\[ \langle \epsilon_{ij} \rangle = V_1 \delta_{ij}. \]  

(4.34)

At second order, there are two relations

\[ \langle \epsilon_{ij} \epsilon_{kl} \rangle = \frac{1}{2} \left( V_{(2)} + V_{(1,1)} \right) \delta_{ij} \delta_{kl} + \frac{1}{2} \left( V_{(2)} - V_{(1,1)} \right) \delta_{il} \delta_{jk}, \]  

(4.35)

and

\[ \langle \epsilon_{ij} \epsilon_{kl}^\dagger \rangle = V_{(1,1)} \delta_{ij} \delta_{kl} + \frac{1}{N} (1 - V_{(1,1)}) \delta_{il} \delta_{jk}. \]  

(4.36)

At third order, there are four structures, but by complex conjugation one can reduce this to two unique ones:

\[ \langle \epsilon_{ij} \epsilon_{kl} \epsilon_{mn} \rangle = \frac{1}{6} \left( V_{(3)} + 4V_{(2,1)} + V_{(1,1,1)} \right) \delta_{ij} \delta_{kl} \delta_{mn} \]  

\[ + \frac{1}{6} \left( V_{(3)} - V_{(1,1,1)} \right) \left( \delta_{il} \delta_{jk} \delta_{mn} + \delta_{in} \delta_{jm} \delta_{kl} + \delta_{ij} \delta_{kn} \delta_{lm} \right) \]  

\[ + \frac{1}{6} \left( V_{(3)} - 2V_{(2,1)} + V_{(1,1,1)} \right) \left( \delta_{in} \delta_{jk} \delta_{lm} + \delta_{il} \delta_{kn} \delta_{jm} \right), \]  

(4.37)

\[ \langle \epsilon_{ij} \epsilon_{kl} \epsilon_{mn}^\dagger \rangle = \frac{1}{2} \left( V_{(2,1)} + V_{(1,1,1)} \right) \delta_{ij} \delta_{kl} \delta_{mn} + \frac{1}{2} \left( V_{(2,1)} - V_{(1,1,1)} \right) \delta_{il} \delta_{jk} \delta_{mn} \]  

\[ + \left( \frac{N}{(N-1)(N+1)} V_{(1)} - \frac{1}{2(N+1)} V_{(2,1)} - \frac{1}{2(N-1)} V_{(1,1,1)} \right) \]  

\[ \times \left( \delta_{in} \delta_{jm} \delta_{kl} + \delta_{ij} \delta_{kn} \delta_{lm} \right) \]  

\[ + \left( -\frac{1}{(N-1)(N+1)} V_{(1)} - \frac{1}{2(N+1)} V_{(2,1)} + \frac{1}{2(N-1)} V_{(1,1,1)} \right) \]  

\[ \times \left( \delta_{in} \delta_{jk} \delta_{lm} + \delta_{il} \delta_{kn} \delta_{jm} \right). \]  

(4.38)

4.2.7 GROUP PROPERTIES

For a given group, the general basis is overcomplete. These leads to simplifications in our derivations for a given group. Here we present the related characters for three groups of relative importance: \( U(1), SU(2), SU(3) \).  

100
For $U(1)$, the resulting identities are

\[
\chi\{1\} = -\chi\{1,1,-1\}, \quad \chi\{1,\pm 1\} = \chi\{2,\pm 1\} = \chi\{1,1,1\} = 0. \quad (4.39)
\]

For $SU(2)$, one finds that

\[
\chi\{1\} = \chi\{2,1\}, \quad \chi\{2\} = \chi\{1,-1\}, \quad \chi\{1,1\} = 1, \quad \chi\{1,1,-1\} = 0, \quad \chi\{3\} = \chi\{2,-1\},
\]

and for $SU(3)$, the set of dependent representations needed up to third order in the cumulant expansion are

\[
\chi\{1\} = \chi\{1,1\}, \quad \chi\{2\} = \chi\{1,1,-1\}, \quad \chi\{1,-1\} = \chi\{2,1\}, \quad \chi\{1,1,1\} = 1. \quad (4.41)
\]

Another important set of identities are those which relate products of $\text{Re} \chi_r$ to sum of $\text{Re} \chi_r$. They are easily enough derived, but we display a few key ones here:

\[
(\text{Re} \chi_{\{1\}})^2 = \frac{1}{2} \text{Re}(\chi\{2\} + \chi\{1,1\} + \chi\{1,-1\} + 1), \quad (4.42)
\]

\[
\text{Re} \chi\{1\} \text{ Re} \chi\{2\} = \frac{1}{2} \text{Re}(\chi\{1\} + \chi\{2,1\} + \chi\{2,-1\} + \chi\{3\}), \quad (4.43)
\]

\[
\text{Re} \chi\{1\} \text{ Re} \chi\{1,1\} = \frac{1}{2} \text{Re}(\chi\{1\} + \chi\{1,1,1\} + \chi\{1,1,-1\} + \chi\{2,1\}), \quad (4.44)
\]

\[
\text{Re} \chi\{1\} \text{ Re} \chi\{1,-1\} = \text{Re}(\chi\{1\} + \chi\{2,-1\} + \chi\{1,1,-1\}). \quad (4.45)
\]

Applying all the simplifications in Eq. (4.22) for specific groups, we write $S[u]$ for $U(1)$ and $SU(2)$ respectively. For $U(1)$:

\[
S[u] = \sum_p - (\beta\{1\} - \beta\{1,1,-1\}) \text{Re} \chi\{1\} - \beta\{0\}
\]

\[
- \beta\{2\} \text{Re} \chi\{2\} - \beta\{3\} \text{Re} \chi\{3\}. \quad (4.46)
\]
For $SU(2)$:

$$S[u] = \sum_p - \left( \beta_{(1)} + \beta_{(2,1)} \right) \frac{1}{2} \text{Re} \chi_{(1)} - \left( \beta_{(0)} + \beta_{(1,1)} \right)$$

$$- \left( \beta_{(2)} + \beta_{(1,-1)} \right) \frac{1}{3} \text{Re} \chi_{(2)}$$

$$- \left( \beta_{(3)} + \beta_{(2,-1)} \right) \frac{1}{4} \text{Re} \chi_{(3)} .$$  \hspace{1cm} (4.47)

### 4.2.8 Derivation of the Decimated Action

In this appendix, we expand upon the derivation of the decimated action. First, for the second-order term in Eq. (4.13), there are three terms which we decomposed based on the number of links that the two plaquettes $p, q$ shared. For case $p = q$ reads:

$$\beta^2 \langle S[u, \epsilon] \rangle^2 = \frac{\beta^2}{N^2} \langle \text{Re} \left( \text{Tr} \left( u_1 \epsilon_1 u_2 \epsilon_2 (u_3 \epsilon_3 \dagger (u_4 \epsilon_4 \dagger) \right) \right) \rangle \text{Re} \left( \text{Tr} \left( u_1 \epsilon_1 u_2 \epsilon_2 (u_3 \epsilon_3 \dagger (u_4 \epsilon_4 \dagger) \right) \right)$$

$$= \frac{\beta^2}{2 N^2} \left( |V_{(1,1)}|^4 \text{Re} \chi_{(1,1)} + |V_{(2)}|^4 \text{Re} \chi_{(2)} + V_{(1,1)} V_{(2)} \chi_{(1,1)} + 1 \right) ,$$  \hspace{1cm} (4.48)

where we have utilized Eqs. (4.35) and (4.36) to contract the $u$'s after integration. The second term of Eq. (4.13) is obtained from first order action of Eq. (4.19) which reads,

$$\beta^2 \langle S[u, \epsilon] \rangle^2 = \left( \frac{1}{N} \beta^2 V_{(1)}^4 \text{Re} \chi_{(1)} \right)^2 = \frac{1}{2 N^2} \beta^2 V_{(1)}^8 \left( \text{Re} \chi_{(2)} + \text{Re} \chi_{(1,1)} + \chi_{(1,-1)} + 1 \right) ,$$  \hspace{1cm} (4.49)

where we have used Eq. (4.42).

For the third-order terms of Eq. (4.14), as discussed we need only consider when the three plaquettes are identical. This will be done term by term, where the first term is:

$$\beta^3 \langle S[u, \epsilon] \rangle^3 = - \frac{\beta^3}{N^3} \langle \text{Re} \text{Tr}(u_1 \epsilon_1 u_2 \epsilon_2 (u_3 \epsilon_3 \dagger (u_4 \epsilon_4 \dagger)) \text{Re} \text{Tr}(u_5 \epsilon_5 u_6 \epsilon_6 (u_7 \epsilon_7 \dagger (u_8 \epsilon_8 \dagger)) \text{Re} \text{Tr}(u_9 \epsilon_9 u_{10} \epsilon_{10} (u_{11} \epsilon_{11} \dagger (u_{12} \epsilon_{12} \dagger))))$$

$$= - \frac{\beta^3}{2 N^2} \left( V_{(1)}^4 \text{Re} \chi_{(1)} + V_{(2,1)}^4 \text{Re} \chi_{(2,1)} + \frac{V_{(1,1,1)}^4}{2} \text{Re} \chi_{(1,1,1)} + \frac{V_{(2,-1)}^4}{2} \text{Re} \chi_{(2,-1)} + \frac{V_{(1,1,-1)}^4}{2} \text{Re} \chi_{(1,1,-1)} + 3 V_{(1)}^4 \text{Re} \chi_{(1,1,1)} \right) .$$  \hspace{1cm} (4.50)
For the mixed-order term in Eq. (4.14):
\[
-3\beta^3 \langle S[u, \epsilon] \rangle \langle S[u, \epsilon] \rangle^2 = \frac{3\beta^3 V_{(1)}^4}{2N^3} \text{Re} \chi_{(1)} \left[ V_{(2)}^4 \text{Re} \chi_{(2)} + V_{(1,1)}^4 \text{Re} \chi_{(1,1)} + V_{(1,-1)}^4 \chi_{(1,-1)} + 1 \right]
\]
\[
= \frac{3\beta^3 V_{(1)}^4}{4N^3} \left[ (V_{(1)}^4 + 2V_{(1,-1)}^4 + V_{(2)}^4 + 2) \text{Re} \chi_{(1)} + (V_{(1,1)}^4 + 2V_{(1,-1)}^4) \text{Re} \chi_{(1,1,-1)} + (V_{(1)}^4 + V_{(2)}^4) \text{Re} \chi_{(2,1)} + V_{(1,1)}^4 \text{Re} \chi_{(1,1,1)} + (2V_{(1)}^4 + V_{(2)}^4) \text{Re} \chi_{(2,-1)} + V_{(2)}^4 \text{Re} \chi_{(3)} \right],
\]
where the second line was simplified with the identities from Appendix 4.2.7. The final term in Eq. (4.14) follows from another identity:
\[
2\beta^3 \langle S[u, \epsilon] \rangle^3 = -2\beta^3 \frac{V_{(1)}^4}{N^3} (\text{Re} \chi_{(1)})^3
\]
\[
= -\frac{\beta^3 V_{(1)}^4}{2N^3} \left( \text{Re} \chi_{(3)} + 2 \text{Re} \chi_{(2,1)} + \text{Re} \chi_{(1,1,1)} + 6 \text{Re} \chi_{(1)} + 3 \text{Re} \chi_{(2,-1)} + 3 \text{Re} \chi_{(1,1,-1)} \right).
\]

4.2.9 Summary

In this work, we used the cumulant expansion to develop a systematic method for studying and improving lattice actions that replace continuous gauge groups by their discrete subgroups. This is a step in the ongoing trek toward developing accurate and efficient digitization on quantum computers. These decimated actions, through the factor $V_{(1)}$, have superior predictive power for finding the freezing transition compared to prior estimators.

We further computed the third-order, single-plaquette contribution for the general group. These higher-order terms are necessary for systematizing the decimation procedure of $SU(3) \to V$ where it has been observed that the inclusion of terms generated in the second-order cumulant expansion with ad-hoc couplings improve the approximation of $SU(3)$. The most immediate work in these directions would be to compute more Euclidean observables (i.e. Wilson flow parameter and pseudocritical temperature) from the full decimated action of Eq. (4.22) and compare them to [4]. Given the large corrections from second to third order for $V$, additional work should be devoted to computing the fourth-order contributions.
In order to move beyond pure gauge theory, it will be necessary to consider quark fields. While the computational resources increase substantially for dynamical quarks, an advantage of the discrete subgroup approximations is that many standard lattice field theory techniques such as \textit{fermionic determinants} and \textit{pseudofermions} can be applied. This was demonstrated in early works on dynamical fermions where $\mathbb{R}$ replaced $SU(2)$ [139, 140].

Another important step in studying the feasibility of this procedure is to explicitly construct the quantum registers and primitive gates à la [89] where smaller discrete groups were investigated. Together with classical lattice results, this would allow for resource counts.

4.3 \textbf{Supplement Materials for Strong Coupling Expansion}

In this section, we show a toy example of the decimation of $U(1)$ to $Z(N)$. We would like to represent a continuous group by its discrete subgroup. Let $G$ be the original group, and $H$ be a subgroup of $G$. For each $U \in G$, there exists $u \in H$ such that $U = u \epsilon$, where $\epsilon$ is a small multiplicative error of $u$ that represents $U$. Hence the measure of integration over all elements in the continuous group $G$ becomes summation over all elements in the discrete group $H$ multiplied by integration of all possible multiplicative errors:

$$\int_G dU = \sum_{u \in H} \int_{\Omega} d\epsilon. \quad (4.53)$$
The partition function becomes:

\[ Z = \int_G dU_1 \ldots dU_L e^{S[U]} \]

\[ = \sum_{u_1 \in H} \cdots \sum_{u_l \in H} \int_\Omega d\epsilon_1 e^{S[u]} \]

\[ = \sum_{u_1 \in H} \cdots \sum_{u_l \in H} S'[u], \quad (4.54) \]

where in the last line we define:

\[ S'[u] = \int_\Omega d\epsilon_1 \cdots \int_\Omega d\epsilon_L e^{S[u]} \]

\[ = \sum_{n=1}^\infty \int_\Omega d\epsilon_1 \cdots \int_\Omega d\epsilon_L S^n[u] \frac{1}{n!} \]

\[ = \sum_{n=1}^\infty S'_n[u], \quad (4.55) \]

here define \( \langle g \rangle := \int_\Omega d\epsilon_1 \cdots \int_\Omega d\epsilon_L g \) and \( S'_n[u] := \langle \frac{S^n[u]}{n!} \rangle_\Omega \), which reconstructed Equation 2.7 in the paper.

Let the continuous group \( G \) to be \( U(1) \) and let the subgroup \( H \subseteq G \) to be \( \mathbb{Z}(N) \).

Let the integration measure \( \Omega \) of \( \epsilon \) to be

\[ \Omega = \{ \epsilon \in U(1) | \epsilon = e^{i\phi}, -\pi/N < \phi \leq \pi/N \}. \quad (4.56) \]

Define the volume \( V_r := \langle \epsilon^r \rangle \), so

\[ V_r = \int_\Omega d\epsilon \epsilon^r = \int_{-\pi/N}^{\pi/N} d\phi \left| \frac{d\epsilon}{d\phi} \right| e^{i\phi r} = \int_{-\pi/N}^{\pi/N} d\phi e^{i\phi r} = \frac{2}{r} \sin \left( \frac{\pi r}{N} \right). \quad (4.57) \]

It can be observed that the integration of the imaginary part of \( \epsilon_r \) vanishes:

\[ \int_\Omega d\epsilon \text{Im}(\epsilon^r) = 0, \quad (4.58) \]

and the integration measure \( d\epsilon \) is real over \( \Omega \):

\[ \int_\Omega d\epsilon = \int_{-\pi/N}^{\pi/N} d\phi \left| \frac{d\epsilon}{d\phi} \right| = \int_{-\pi/N}^{\pi/N} d\phi. \quad (4.59) \]
Note that we need the normalization condition \( \int_{\Omega} d\epsilon = 1 \), but
\[
V_0 = \int_{\Omega} d\epsilon \epsilon^0 = \int_{-\pi/N}^{\pi/N} d\phi = \frac{2\pi}{N},
\]
so we can multiply the factor \( \frac{N}{2\pi} \) to the original \( V_r \):
\[
V_r \rightarrow \frac{N}{2\pi} V_r = \frac{N}{\pi r} \sin\left(\frac{r\pi}{N}\right).
\] (4.60)

### 4.3.1 One-Point Coupling

We proceed to see how the lower order expansion looks like for a particular action
\( S[U] = \beta \sum_p \text{Re}(U_p) \), where it sums over all possible point \( p \) on a lattice. Let \( U = u\epsilon \), by Equation 4.55 the first order approximation for \( S'[u] \) is:
\[
S'_1[u] = \langle S[ue] \rangle = \beta \sum_p \langle \text{Re}(u_p \epsilon_p) \rangle_{\Omega} = \beta \sum_p \langle \text{Re}(u_p \prod_l \epsilon_{p_l}) \rangle_{\Omega}
\]
\[
= \beta \sum_p \left( \prod_{i=1}^{4} \int_{\Omega} d\epsilon_{p_i} \right) \left( \text{Re}(u_p \prod_{l=1}^{4} \epsilon_{p_l}) \right)
\]
\[
\hspace{1cm} \text{(at each point } p \text{ there are 4 links extending from it)}
\]
\[
= \beta \sum_p \text{Re} \left( u_p \prod_{i=1}^{4} \int_{\Omega} d\epsilon_{p_i} \epsilon_{p_i} \right) 
\]
\[
= \beta V_1^4 \sum_p \text{Re}(u_p) 
\]
\[
= \beta_1 \sum_p \text{Re}(u_p),
\] (4.61)

where \( \beta_1 := \beta(V_1)^4 \). By Equation 4.60, we may expand \( \beta_1 \) as:
\[
\beta_1 = \beta \left( \frac{N}{\pi} \sin\left(\frac{\pi}{N}\right) \right)^4
\]
\[
= \beta \left( 1 - \frac{2}{3} \left(\frac{\pi}{N}\right)^2 + \frac{\pi^4}{5N^4} + O\left(\left(\frac{1}{N}\right)^6\right) \right). \hspace{1cm} \text{(by Laurent expansion at } N = \infty)\]
4.3.2 Two-Point Coupling

The two-point coupling constants are calculated from

\[ S'_2[u] = \frac{1}{2} \sum_{p_1,p_2} \beta^2 \langle \text{Re}(u_{p_1} \epsilon_{p_1}) \text{Re}(u_{p_2} \epsilon_{p_2}) \rangle_c \]

\[ = A + B, \quad (4.62) \]

where

\[ A = \frac{1}{2} \beta^2 \sum_{u_{p_1} = u_{p_2} = u_p} \langle \text{Re}(u_{p_1} \epsilon_{p_1}) \text{Re}(u_{p_2} \epsilon_{p_2}) \rangle_c \]

\[ = \frac{1}{2} \beta^2 \sum_p \langle \text{Re}(u_p \epsilon_p) \text{Re}(u_p \epsilon_p) \rangle - \frac{1}{2} \beta^2 \sum_p \langle \text{Re}(u_p \epsilon_{p_1}) \text{Re}(u_p \epsilon_{p_2}) \rangle \bigg|_{\epsilon_{p_1} \neq \epsilon_{p_2}} \]

\[ = \frac{\beta^2}{2} \sum_p \left( \prod_{i=1}^{4} \mathcal{N} \int_{-\pi/N}^{\pi/N} d\phi_i \right) \text{Re} \left( u_p \prod_{j=1}^{4} e^{i\phi_j} \right) \text{Re} \left( u_p \prod_{k=1}^{4} e^{i\phi_k} \right) \]

\[ - \frac{\beta^2}{2} \sum_p \left( \prod_{i=1}^{8} \mathcal{N} \int_{-\pi/N}^{\pi/N} d\phi_i \right) \text{Re} \left( u_p \prod_{j=1}^{8} e^{i\phi_j} \right) \text{Re} \left( u_p \prod_{j=5}^{8} e^{i\phi_j} \right). \quad (4.63) \]

Since \( \text{Re}(x \ast y) = \text{Re}(x) \text{Re}(y) - \text{Im}(x) \text{Im}(y) \):

\[ A = \frac{1}{2} \beta^2 \sum_p \left( \prod_{i=1}^{4} \mathcal{N} \int_{-\pi/N}^{\pi/N} d\phi_i \right) \left( \text{Re}(u_p) \text{Re} \left( \prod_{j=1}^{4} e^{i\phi_j} \right) - \text{Im}(u_p) \text{Im} \left( \prod_{j=1}^{4} e^{i\phi_j} \right) \right)^2 \]

\[ - \frac{\beta^2}{2} \sum_p \left( \prod_{i=1}^{8} \mathcal{N} \int_{-\pi/N}^{\pi/N} d\phi_i \right) \left( \text{Re}(u_p) \text{Re} \left( \prod_{j=1}^{8} e^{i\phi_j} \right) - \text{Im}(u_p) \text{Im} \left( \prod_{j=1}^{8} e^{i\phi_j} \right) \right) \times \left( \text{Re}(u_p) \text{Re} \left( \sum_{j=5}^{8} \phi_j \right) - \text{Im}(u_p) \text{Re} \left( \sum_{j=5}^{8} \phi_j \right) \right) \]

\[ = \frac{1}{2} \beta^2 \sum_p \left( \prod_{i=1}^{4} \mathcal{N} \int_{-\pi/N}^{\pi/N} d\phi_i \right) \left( \text{Re}^2(u_p) \cos^2 \left( \sum_{j=1}^{4} \phi_{p_j} \right) + \text{Im}^2(u_p) \sin^2 \left( \sum_{j=1}^{4} \phi_{p_j} \right) \right) \]

\[ - \frac{\beta^2}{2} \sum_p \left( \prod_{i=1}^{8} \mathcal{N} \int_{-\pi/N}^{\pi/N} d\phi_i \right) \left( \text{Re}(u_p) \cos \left( \sum_{j=1}^{4} \phi_j \right) - \text{Im}(u_p) \sin \left( \sum_{j=1}^{4} \phi_{p_j} \right) \right) \times \left( \text{Re}(u_p) \cos \left( \sum_{j=5}^{8} \phi_j \right) - \text{Im}(u_p) \sin \left( \sum_{j=5}^{8} \phi_{p_j} \right) \right). \]

\[ (4.64) \]
where in the first line of last equation we used the fact that \( \sin(2x) = 2 \sin(x) \cos(x) \). Hence now \( \mathcal{A} \) can be reduced to:

\[
\mathcal{A} = \frac{1}{2} \beta^2 \sum_p \left( \prod_{i=1}^{N} \int_{-\pi/N}^{\pi/N} d\phi_i \right) \left\{ \frac{1}{2} \text{Re}^2(u_p) \left[ 1 + \cos \left( 2 \sum_{j=1}^{4} \phi_j \right) \right] + \frac{1}{2} \text{Im}^2(u_p) \left[ 1 - \cos \left( 2 \sum_{j=1}^{4} \phi_j \right) \right] \right\} \\
- \frac{\beta^2}{2} \sum_p \left( \prod_{i=1}^{N} \int_{-\pi/N}^{\pi/N} d\phi_i \right) \text{Re}^2(u_p) \cos \left( \sum_{j=1}^{4} \phi_j \right) \cos \left( \sum_{j=5}^{8} \phi_j \right)
\]

\[
= \frac{1}{4} \beta^2 \sum_p \{ \text{Re}^2(u_p) + \text{Im}^2(u_p) + (\text{Re}^2(u_p) - \text{Im}^2(u_p)) (\epsilon^2)^8_{\Omega} \} - \frac{1}{2} \beta^2 \sum_p \text{Re}^2(u_p) (\epsilon)^8_{\Omega}
\]

\[
= \frac{1}{4} \beta^2 \sum_p \{ \text{Re}^2(u_p) + \text{Im}^2(u_p) + (\text{Re}^2(u_p) - \text{Im}^2(u_p)) V^4_{1} \} - \frac{1}{2} \beta^2 \sum_p \text{Re}^2(u_p) V^8_{1}
\]

\[
\equiv \sum_p \{ \beta_0 + \beta_2 \text{Re}(u_p^2) \} .
\]

(4.65)

where

\[
\beta_0 = \frac{1}{4} \beta^2 (1 - V^8_{1}) , \quad \beta_2 = -\frac{1}{4} \beta^2 (V^8_{1} - V^4_{2})
\]

(4.66)

and the minus sign comes from the requirement of removing the disconnected diagrams. Note that the term proportional to \( V^8_{1} \) is necessary to have \( \lim_{N \to \infty} \mathcal{A} \to 0 \) since the decimation of the \( U(1) \) group must be identical to the original \( U(1) \) group at the \( N \to \infty \) limit which implies only the one-point coupling survives.

\[
\mathcal{B} = \frac{1}{2} \beta^2 \sum_{p \neq q} \langle \text{Re}(u_p \epsilon_p) \text{Re}(u_q \epsilon_q) \rangle_c
\]

\[
= \frac{1}{2} \beta^2 \sum_{\epsilon_p \cap \epsilon_q = \text{one link}} \langle \text{Re}(u_p \epsilon_p) \text{Re}(u_q \epsilon_q) \rangle - \frac{1}{2} \beta^2 \sum_{\epsilon_p \cap \epsilon_q = \emptyset} \langle \text{Re}(u_p \epsilon_p) \text{Re}(u_q \epsilon_q) \rangle .
\]

(4.67)
\[ C = \frac{1}{2} \beta^2 \sum_{p \neq q} \int d\phi_p d\phi_{p_2} d\phi_{q_3} d\phi_{q_4} d\phi_{q_5} d\phi_{q_6} d\phi_{\ell} d\phi_k \delta(\phi_{\ell} + \phi_k) \]

\[
\Re(u_p) \Re(u_q) \cos(\sum_i \phi_{p_i} + \phi_{\ell}) \cos(\sum_i \phi_{q_i} + \phi_k) \\
+ \Im(u_p) \Im(u_q) \sin(\sum_i \phi_{p_i} + \phi_{\ell}) \sin(\sum_i \phi_{q_i} + \phi_k) \\
= \frac{1}{2} \beta^2 \sum_{p \neq q} \int d\Phi \Re(u_p) \Re(u_q) \cos(\sum_i \phi_{p_i} + \phi_{\ell}) \cos(\sum_i \phi_{q_i} - \phi_{\ell}) \\
+ \Im(u_p) \Im(u_q) \sin(\sum_i \phi_{p_i} + \phi_{\ell}) \sin(\sum_i \phi_{q_i} - \phi_{\ell}), \tag{4.68}
\]

where \( \delta(\phi_{\ell} + \phi_k) \) comes from the fact that two loops centering at \( p \) and \( q \) are in opposite direction on the shared edge.

\[ D = \frac{1}{2} \beta^2 \sum_{p \neq q} \int d\phi_{p_1} \ldots d\phi_{p_4} d\phi_{q_1} \ldots d\phi_{q_4} \Re(u_p) \Re(u_q) \cos(\sum_i \phi_{p_i}) \cos(\sum_i \phi_{q_i}) \\
= \frac{1}{2} \beta^2 \sum_{p \neq q} \Re(u_p) \Re(u_q) V_1^6. \tag{4.70} \]
Combining the results for $A$ and $B$, the second order correction term reads:

$$S_2'[u] = \frac{1}{4} \beta^2 \sum_p \left\{ 1 - V_1^8 + (V_2^4 - V_1^8) \Re(u_p^2) \right\}$$

$$+ \frac{1}{4} \beta^2 \sum_{p \neq q} \left( \Im(u_p) \Im(u_q) V_1^6 (V_2 - 1) + \Re(u_p) \Re(u_q) V_1^6 (1 + V_2 - 2V_1^2) \right).$$

(4.71)

Let us now address the appearance of minus term. Starting from Equation (2.5) in [61],

$$\exp \left[ \sum \tilde{S}(u) \right] = \left( \prod_{\ell} \int_{\Omega} d\epsilon_{\ell} \right) \exp \left[ \sum_p S(u_p \prod_{\ell} \epsilon_{\ell}) \right]$$

$$= \prod_p \left( \prod_{\ell} \int_{\Omega} d\epsilon_{\ell} \right) \exp \left[ S(u_p \prod_{\ell} \epsilon_{\ell}) \right]$$

(4.72)

$$\exp \left[ \sum \tilde{S}(u) \right] := \exp \left[ \sum_{n=1}^{\infty} \tilde{S}_n[u] \right]$$

(4.73)

and expanding both sides of Equation 4.72 and 4.73, we have,

$$1 + \left( \sum_{n=1}^{\infty} \tilde{S}_n(u) \right) + \frac{1}{2!} \left( \sum_{n=1}^{\infty} \tilde{S}_n(u) \right)^2 + \ldots$$

$$= \prod_{\ell} \int_{\Omega} d\epsilon_{\ell} \left( 1 + \sum_p S(u_p \epsilon_p) + \frac{1}{2!} \sum_{p,q} S(u_p \epsilon_p) S(u_q \epsilon_q) + \ldots \right)$$

(4.74)

identifying terms of the same order on each side of the equation, we find a set of equations,

$$\begin{cases} 
\tilde{S}_1(u) = \sum_p \left( \prod_{\ell} \int_{\Omega} d\epsilon_{\ell} \right) S(u_p \prod_{\ell} \epsilon_{\ell}), \\
\tilde{S}_2(u) = \frac{1}{2!} \sum_{p,q} \prod_{\ell} \int_{\Omega} d\epsilon_{\ell} S(u_p \prod_{\ell} \epsilon_{\ell}) S(u_q \prod_{\ell} \epsilon_{\ell}) - \frac{1}{2!} \tilde{S}_1^2(u), \\
\cdots 
\end{cases}$$

(4.75)

$\ell$ denotes all possible links in the lattice.
where \( \Omega \) represents a gauge loop circling lattice a point \( p \) and its edges are parameterized by \( \epsilon_{p\ell} \). Note that we have used the normalization condition \( \prod_{\ell} \int_{\Omega} d\epsilon_{\ell} = 1 \). The above equation demonstrates the true meaning of connected part in \( \langle \ldots \rangle_c \). To further see the details, let us start again from Equation 4.74 we can read off \( \bar{S}_2(u) \) as:

\[
\bar{S}_2(u) = \prod_{\ell} \int_{\Omega} d\epsilon_{\ell} \frac{1}{2} \beta^2 \sum_{p,q} S(u_p\epsilon_p)S(u_q\epsilon_q) - \frac{1}{2} \beta^2 \bar{S}_1^2. \tag{4.76}
\]

Notice that the \( \prod_{\ell} \) in the above equation covers all possible edges in the grid, including edges that are not adjacent to \( p \) or \( q \). We shall now break the sum \( \sum_{p,q} \) into three cases: \( p = q \), \( p \neq q \) but they share one common link, and \( p \neq q \) where no link is shared:

\[
\bar{S}_2(u) = \frac{1}{2} \beta^2 \sum_p \prod_{\ell} \int_{\Omega} d\epsilon_{\ell} S(u_p\epsilon_p)S(u_p\epsilon_p) + \frac{1}{2} \beta^2 \sum_{p \neq q} \prod_{\ell} \int_{\Omega} d\epsilon_{\ell} S(u_p\epsilon_p)S(u_q\epsilon_q)
+ \frac{1}{2} \beta^2 \sum_{p \neq q \mid p \cap q = \emptyset} \prod_{\ell} \int_{\Omega} d\epsilon_{\ell} S(u_p\epsilon_p)S(u_p\epsilon_p) - \frac{1}{2} \bar{S}_1^2. \tag{4.77}
\]

Now for the link \( \epsilon_{\ell} \) that is not adjacent to the points \( p \) or \( q \), it contributes only a factor of 1 because we defined \( \int_{\Omega} d\epsilon = 1 \). Therefore,

\[
\bar{S}_2(u) = \frac{1}{2} \beta^2 \sum_p \prod_{\ell}^4 \int_{\Omega} d\epsilon_{\ell} S(u_p\epsilon_p)S(u_p\epsilon_p) + \frac{1}{2} \beta^2 \sum_{p \neq q} \prod_{\ell} \int_{\Omega} d\epsilon_{\ell} S(u_p\epsilon_p)S(u_q\epsilon_q)
+ \frac{1}{2} \sum_{p \neq q \mid p \cap q = \emptyset} \prod_{\ell}^8 \int_{\Omega} d\epsilon_{\ell} S(u_p\epsilon_p)S(u_p\epsilon_p) - \frac{1}{2} \beta^2 \bar{S}_1^2. \tag{4.78}
\]
But we can also classify the last term as three cases, so

\[
\tilde{S}_2(u) = \frac{1}{2} \beta^2 \sum_p \prod_{\ell}^4 \int_{\Omega} d\epsilon_{\ell} S(u_p\epsilon_p) S(u_p\epsilon_p) + \frac{1}{2} \beta^2 \sum_{p \neq q}^7 \prod_{\ell} \int_{\Omega} d\epsilon_{\ell} S(u_p\epsilon_p) S(u_p\epsilon_p)
\]

\[
+ \frac{1}{2} \beta^2 \sum_{p \neq q}^8 \prod_{\ell} \int_{\Omega} d\epsilon_{\ell} S(u_p\epsilon_p) S(u_p\epsilon_p) - \frac{1}{2} \sum_p \tilde{S}_1(u_p) \tilde{S}_1(u_p)
\]

\[
- \frac{1}{2} \sum_{p \neq q} \tilde{S}_1(u_p) \tilde{S}_1(u_q) - \frac{1}{2} \sum_{p \neq q} \tilde{S}_1(u_p) \tilde{S}_1(u_q).
\] (4.79)

Rearrange the terms we get:

\[
\tilde{S}_2(u) = \frac{1}{2} \beta^2 \sum_p \prod_{\ell}^4 \int_{\Omega} d\epsilon_{\ell} S(u_p\epsilon_p) S(u_p\epsilon_p) - \frac{1}{2} \sum_p \tilde{S}_1(u_p) \tilde{S}_1(u_p)
\]

\[
+ \frac{1}{2} \beta^2 \sum_{p \neq q}^7 \prod_{\ell} \int_{\Omega} d\epsilon_{\ell} S(u_p\epsilon_p) S(u_p\epsilon_p) - \frac{1}{2} \sum_{p \neq q} \tilde{S}_1(u_p) \tilde{S}_1(u_q)
\]

\[
+ \frac{1}{2} \beta^2 \sum_{p \neq q}^8 \prod_{\ell} \int_{\Omega} d\epsilon_{\ell} S(u_p\epsilon_p) S(u_p\epsilon_p) - \frac{1}{2} \sum_{p \neq q} \tilde{S}_1(u_p) \tilde{S}_1(u_q)
\] (4.80)

\[
= \mathcal{A} + \mathcal{B}.
\]

this recovers Equation 4.62

4.3.3 HIGHER-ORDER GENERALIZATION FOR $\mathcal{V}$

It is possible to generate the coefficients in front of $V_r^4 \Re \chi^{(r)}$ without considering \(\langle \epsilon_{i+j}, \cdots \epsilon^{\dagger}_{i+j}\rangle\). Take the 4th-order contribution as an example. First, we identify that there are three classes of characters that contribute to the order:

\[
\Xi_1 = \{\chi_{(1,1,1,1)} , \chi_{(2,1,1)} , \chi_{(2,2)} , \chi_{(3,1)} , \chi_{(4)}\}, \quad \Xi_2 = \{\chi_{(1,1,1,-1)} , \chi_{(2,1,-1)} , \chi_{(3,-1)}\},
\]

\[
\Xi_3 = \{\chi_{(1, -1, -1)} , \chi_{(2,-1, -1)} , \chi_{(2,-2)}\}.
\] (4.81)
The coefficients $a_{\{r\}}$ for the first class $\Xi_1$ can be obtained by requiring
\[
a_{\{1,1,1,1\}} : a_{\{2,1,1\}} : a_{\{2,2\}} : a_{\{3,1\}} : a_{\{4\}} = 1 : 3 : 2 : 3 : 1, \tag{4.82}
\]
where the ratios are from the overall constant in the definition of each character. Replacing $\chi_{\{r\}}$ in $\Xi_1$ by their corresponding dimensions yields a result $\propto N^4$ serving as a nontrivial check. Note that the characters in class $\Xi_1$ have weight 4, which equals the sum of all the indices in the subscripts, and therefore receive no corrections from lower order characters, which have at most weight 3 (e.g., $\chi_{\{3\}}, \ldots$). An overall common factor for characters in $\Xi_1$ is determined before multiplying an additional factor of 2 from the c.c. part (i.e., $\chi_{\{4\}} + \cdots + c.c = \chi_{\{4\}} + \chi^*_{\{4\}} + \cdots = 2 \text{Re } \chi_{\{4\}} + \cdots$).

The coefficients for $\Xi_2$ can be obtained in a similar way. The only difference is that in this case, corrections of lower order characters of the weight appear. Namely, we must include two additional characters $\chi_{\{2\}}, \chi_{\{1,1\}}$ to $\Xi_2$, the reason being that the sum of the indices of these two characters’ equals to the sum of the indices of any characters in $\Xi_2$ ($1 + 1 = 2 = 2 + 1 - 1 = \cdots$). This again gives us 5 characters. We now require the characters in $\Xi_2$ to follow the same ratio law that was elaborated previously
\[
a_{\{1,1,1,-1\}} : a_{\{2,1,-1\}} : a_{\{3,-1\}} = 1 : 2 : 1, \tag{4.83}
\]
and finally letting $\sum_{r: \chi_{\{r\}} \in \Xi_2} a_{\{r\}} \times \dim(\chi_{\{r\}}) \propto N^4$ allows us to find the relative ratio of $a_{\{2\}}$ and $a_{\{1,1\}}$ with the rest of $\Xi_2$ characters.

Determining the coefficients in $\Xi_3$ (adjoint) is a bit tricky. In this case, each character is no longer independent of its c.c. partner. This means we must consider $\Xi_3$ and $\Xi_3^*$ together as the character basis since one has to consider all independent

---

Here we have in total 5 polynomials of maximal degree 4 and therefore $a_{\{2\}}$ and $a_{\{1,1\}}$ are completely fixed.
characters that have *equal* number of $U$ and $U^\dagger$ (adjoint) as the complete basis for expanding the corresponding trace structures. Namely, consider,

$$\Xi_3 = \{ \chi_{(1,1,-1,-1)} , \chi^*_{(1,1,-1,-1)} , \chi_{(2,-1,-1,1)} , \chi^*_{(2,-1,-1,1)} , \chi_{(2,-2)} , \chi^*_{(2,-2)} \}, \quad (4.84)$$

and note that $\chi^*_{(1,1,-1,-1)} = \chi_{(-1,1,1,1)} = \chi_{(1,1,-1,-1)}$ and $\chi^*_{(2,-2)} = \chi_{(-2,2)} = \chi_{(2,-2)}$ meaning that there are 4 *independent* characters in $\Xi_3$.

We now require the ratio of the coefficient of *independent* character as follows,

$$a_{(1,1,-1,-1)} : a_{(2,-2)} : a_{(2,-1,1,1)} : a_{(-2,1,1)} = 1 : 1 : 1 : 1 \quad (4.85)$$

where again the numbers on the RHS are from the ratio of the overall constant in character definition. Then imposing the constraint $\sum_i a_{(r)} \times \dim(\chi_{(r)}) \propto N^4$ fixes the ratios of $\chi_{(1,-1)}$ and $\chi_{(0)} = 1$.

$$\beta^4(S[u,e]^4) = \frac{\beta^4}{8N^4} \left\{ V_{(4)}^4 \Re \chi_{(4)} + V_{(1,1,1,1)}^4 \Re \chi_{(1,1,1,1)} + 3V_{(3,1)}^4 \Re \chi_{(3,1)} + 3V_{(2,1,1)}^4 \Re \chi_{(2,1,1)} 
+ 2V_{(2,2)}^4 \Re \chi_{(2,2)} + 4V_{(3,1,1)}^4 \Re \chi_{(3,1,1)} + 4V_{(1,1,1,1)}^4 \Re \chi_{(1,1,1,1)} + 8V_{(2,1,1,1)}^4 \Re \chi_{(2,1,1,1)} 
+ 6V_{(2,-1,-1)}^4 \Re \chi_{(2,-1,-1)} + 3V_{(1,1,-1,1)}^4 \Re \chi_{(1,1,-1,1)} + 3V_{(2,-2)}^4 \Re \chi_{(2,-2)} 
+ 12V_{(2)}^4 \Re \chi_{(2)} + 12V_{(1,1)}^4 \Re \chi_{(1,1)} + 12V_{(1,-1)}^4 \Re \chi_{(1,-1)} + 6 \right\}. \quad (4.85)$$

### 4.3.4 Scheme for Calculating Characters $\chi$

We follow the scheme from [68, Appendix A] to calculate characters of any order. We start by introducing all the necessary definitions, and then follow with a few examples.

Let $W_n$ be the sum of product of trace of $U$ of order $n$:

$$W_n = \frac{1}{n!} \sum_{\sigma \in S_n} \text{Tr}^\sigma(U). \quad (4.86)$$

Thus, we have

$$W_0 = 1, \quad W_1 = \text{Tr}(U), \quad W_2 = \frac{1}{2} \left( \text{Tr}^2(U) + \text{Tr}(U^2) \right),$$

$$W_3 = \frac{1}{6} \left( \text{Tr}^3(U) + 3 \text{Tr}(U^2) \text{Tr}(U) + 2 \text{Tr}(U^3) \right).$$

In other cases, no cross-talks between characters and their c.c. partners. Namely, trace structures generated by characters in $\Xi_1$ cannot be generated by $\Xi_1^*$. 

114
Notice that the coefficients of traces for $W_3$, 1 comes from $(1,2,1) \in S_3$, 3 comes from $(1,3,3) \in S_3$ and 2 comes from $(1,2,3), (1,3,2) \in S_3$. For negative $n$, we replace $U$ by $U^\dagger$:

$$W_{-1} = \text{Tr}(U^\dagger), \quad W_{-2} = \frac{1}{2} \left( \text{Tr}^2(U^\dagger) + \text{Tr}((U^\dagger)^2) \right),$$

$$W_{-3} = \frac{1}{6} \left( \text{Tr}^3(U^\dagger) + 3 \text{Tr}((U^\dagger)^2) \text{Tr}(U^\dagger) + 2 \text{Tr}((U^\dagger)^3) \right).$$

We also include $W_5, W_6$ for further usage:

$$W_5 = \frac{1}{120} \left( \text{Tr}^5(U) + 10 \text{Tr}(U^2) \text{Tr}^3(U) + 15 \text{Tr}^2(U^2) \text{Tr}(U) + 20 \text{Tr}(U^3) \text{Tr}^2(U) + 20 \text{Tr}(U^4) \text{Tr}(U^2) 
+ 24 \text{Tr}(U^5) + 30 \text{Tr}(U^4) \text{Tr}(U) \right),$$

$$W_6 = \frac{1}{720} \left( \text{Tr}^6(U) + 15 \text{Tr}(U^2) \text{Tr}^4(U) + 15 \text{Tr}^3(U^2) + 40 \text{Tr}(U^3) \text{Tr}^3(U) + 40 \text{Tr}^2(U^3) + 45 \text{Tr}^2(U^2) \text{Tr}^2(U) 
+ 90 \text{Tr}(U^4) \text{Tr}^2(U) + 90 \text{Tr}(U^4) \text{Tr}(U^2) + 120 \text{Tr}(U^5) \text{Tr}(U^2) \text{Tr}(U) + 120 \text{Tr}(U^6) + 144 \text{Tr}(U^5) \text{Tr}(U) \right).$$

The character $\chi$ of any order can be specified as $\chi_{l_1,\ldots,l_p;m_1,\ldots,m_q}$, where $l$’s indicate the positive indices and $m$’s indicate the negative indices. It is easy to connect our notation to the notations in [68]:

$$\chi\{2,-2\} = \chi_{2;2}, \quad p = 1, q = 1, l_1 = 2, m_1 = 2,$$

$$\chi\{3,-1\} = \chi_{3;1}, \quad p = 1, q = 1, l_1 = 3, m_1 = 1,$$

$$\chi\{2,-1,-1\} = \chi_{2;1,1}, \quad p = 1, q = 2, l_1 = 2, m_1 = 1, m_2 = 1.$$

For $q = 0$, $\chi_{l_1,\ldots,l_p} = \det M$, where $M$ is defined as follow:

$$M_{ij} = \begin{cases} W_{l_i+j-i} & \text{if } l_i + j - i \geq 0 \\ 0 & \text{if } i + j - i \geq 0 < 0. \end{cases}$$

For $q \neq 0$, $\chi_{l_1,\ldots,l_p;m_1,\ldots,m_q} = (-1)^{pq} \det M$, where $M$ is defined as follow. For $i \in \{1,2,\ldots,p\}$:

$$M_{ij} = \begin{cases} W_{l_i+j-i-q} & \text{if } l_i + j - i - q \geq 0 \\ 0 & \text{if } l_i + j - i - q < 0, \end{cases}$$

115
and for \( i \in \{ p + 1, \cdots, p + q \} \):

\[
M_{ij} = \begin{cases} 
W_{-m_{i-p} + j - i + p} & \text{if } -m_{i-p} + j - i + p \leq 0 \\
0 & \text{if } -m_{i-p} + j - i + p > 0.
\end{cases}
\]

4.4 Group Space Decimation via Character Expansion

The resulting discrepancy from approximations can be analyzed systematically through expansions of various parameters in the same spirit of the modern effective field theory (EFT) approach with a matching procedure. There are two natural ways to attempt the matching between the continuous and discrete groups: classical or quantum improvement. In this section, we examine the former possibility, namely, matching at the classical level the Boltzmann weights \( e^{-S} \) through the character expansion. In Sec. 4.4.1, we summarize the group properties of \( V \), the largest crystallike subgroup of \( SU(3) \). This is followed by Sec. 4.4.2, where we demonstrate the matching via a systematic character expansion. Sec. 4.4.3 is reserved for numerical results with analysis of the viability of character expansion. The paper is finally concluded in Sec. 4.4.4.

4.4.1 Characters of \( V \)

The 1080 elements of the \( SU(3) \) subgroup \( V \) can be classified into 17 conjugacy classes \([59]\), generated by its total 17 independent characters for which we denote as \( \chi'_r \) with \( r = 1, 2, \cdots, 17 \). These 17 characters are linearly related to a subset of \( SU(3) \).
characters $\chi_{(\lambda,\mu)}$ that are organized by two \textit{non-negative} integers $\lambda$ and $\mu$,

$$\chi'_r = \sum_{(\lambda,\mu)} m_{r,(\lambda,\mu)} \chi_{(\lambda,\mu)}, \quad (4.87)$$

where $m_{r,(\lambda,\mu)}$ are a set of integers systematically obtainable by matching the character definitions of the two groups. The explicit linear relations between $\chi'_r$ and $\chi_{(\lambda,\mu)}$ are given in Table 4.5 for $r = 1, 2, \cdots, 9, 12, \cdots, 17$.

It is worth noting that although $\chi'_{10} + \chi'_{11}$ is expressible in terms of $\chi_{(\lambda,\mu)}$ in a simple fashion as given in Table 4.5, individual expressions for $\chi'_{10}$ and $\chi'_{11}$ in terms of $SU(3)$ characters are rather lengthy. We note that, in practice, $\chi'_{10}$ and $\chi'_{11}$ always appear together as $\chi'_{10} + \chi'_{11}$ and thus the absence of their expressions individually leads to no issues in our derivations.

On the other hand, in order to obtain the action of $\chi'_{10}$ and $\chi'_{11}$ on all $V$ elements, we exploit the orthonormality condition of the character representation, allowing us to fix the last elements in the character table in Table 4.6. We point out that the conjugacy classes $C_8$ and $C_9$, both of which are composed of traceless $V$ elements, are distinguishable only through these two characters $\chi'_{10}$ and $\chi'_{11}$, as can be read from Table 4.6.

\subsection*{4.4.2 \textsc{Character Expansion of Wilson Action}}

In this section, we first carry out the character expansion for the Boltzmann weight using the Wilson action to sufficiently high orders in $SU(3)$. The domain of the resulting expansion is then reduced from $SU(3)$ to $V$ with the help of Eq. (4.87) of which the lowest-weight characters are found in Table 4.5. Clearly, this step lowers the

\footnote{We note that in Ref. [77], another notation was adopted for general $SU(N)$ characters labeled by $N$ integers $\{\lambda_1, \lambda_2, \cdots, \lambda_N\}$ with $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_N$. For the special case of $SU(3)$ that is our sole interest throughout this paper, all characters can be denoted by only two \textit{non-negative} integers $(\lambda, \mu)$ [55]. We employ the $(\lambda, \mu)$ convention hereafter.}
theory complexity at the cost of approximation errors which are quantifiable through theoretical and/or numerical means (e.g., [77]). Finally, we derive the effective action \( \tilde{S}(u) \) over \( \mathcal{V} \) by matching \( e^{-\tilde{S}(u)} \) onto the corresponding character expansion.

We start with the pure gauge Wilson action,

\[
S(U) = -\sum_p \frac{\beta}{N} \text{Re} \text{Tr}(U_p), \quad U \in SU(3),
\]

where the summation runs over all plaquettes. \( U_p \) denotes a product of gauge links in the adjoint representation of \( SU(3) \). The resulting Boltzmann weight, \( e^{-S(U)} \), can be decomposed into the orthonormal \( SU(3) \) characters basis,

\[
e^{-S(U)} = \sum_{(\lambda,\mu)} \beta_{(\lambda,\mu)} \chi_{(\lambda,\mu)}(U),
\]

giving rise to a series of character coupling constants \( \beta_{(\lambda,\mu)} \). The resulting partition function central to the classical lattice calculation can therefore be presented as,

\[
Z \equiv \int DU \ e^{-S(U)} = \sum_{(\lambda,\mu)} \int DU \beta_{(\lambda,\mu)} \chi_{(\lambda,\mu)}(U).
\]

For the Wilson action defined in Eq. (4.88), the explicit form of \( \beta_{(\lambda,\mu)} \) can be written as an infinite sum in terms of Bessel functions [55],

\[
\beta_{(\lambda,\mu)}(\beta) = \sum_{n=-\infty}^{\infty} \text{det} \begin{pmatrix}
I_{\rho+n}(\beta \frac{3}{\beta}) & I_{\sigma-1+n}(\beta \frac{3}{\beta}) & I_{n-2}(\beta \frac{3}{\beta}) \\
I_{\rho+1+n}(\beta \frac{3}{\beta}) & I_{\sigma+n}(\beta \frac{3}{\beta}) & I_{n-1}(\beta \frac{3}{\beta}) \\
I_{\rho+2+n}(\beta \frac{3}{\beta}) & I_{\sigma+1+n}(\beta \frac{3}{\beta}) & I_{n}(\beta \frac{3}{\beta})
\end{pmatrix},
\]

where \( \rho = \lambda + \mu, \sigma = \mu, \) and \( I_k \) is the Bessel function of the first kind [55]. Explicit expressions of \( \beta_{(\lambda,\mu)} \) that are relevant for our current study are collected in Table 4.7 in the form of Taylor series of \( \beta \). In practice, we found taking \( |n| \leq 40 \) in Eq. (4.91) is sufficient numerically.
We are now ready to extract the effective action over \( \mathbb{V} \), the finite discrete crystal subgroup of \( SU(3) \). The starting point of our procedure is to substitute \( U \in SU(3) \) on the R.H.S. of Eq. (4.89) by \( u \in \mathbb{V} \), effectively reducing the domain of the character expansion. The \( SU(3) \) characters \( \chi_{(\lambda,\mu)}(U) \) are then mapped to their \( \mathbb{V} \) counterparts \( \chi'_r(u) \) using either Eq. (4.87), or Table 4.6 by solving a system of 17 linear equations. Subsequently, the \( SU(3) \) character couplings \( \beta_{(\lambda,\mu)} \) are also rearranged into \( \mathbb{V} \) character couplings \( \beta'_r \). Detailed relations between \( \beta'_r \) and \( \beta_{(\lambda,\mu)} \) are collected in Table 4.8. The resulting \( \mathbb{V} \) character expansion is finally matched onto the \( \mathbb{V} \) effective action \( \tilde{S}(u) \) as follows,

\[
e^{-\tilde{S}(u)} = \sum_{r=1}^{17} \beta'_r \chi'_r(u), \quad u \in \mathbb{V}. \tag{4.92}
\]

We emphasize that once the order of truncation for the \( SU(3) \) character expansion is determined, the R.H.S of Eq. (4.92) is completely fixed through Eq. (4.87) (or Table 4.5). The relations between \( \beta'_r \) and \( \beta_{(\lambda,\mu)} \) given in Table 4.8 provide a complete basis for \( SU(3) \) character \( \chi_{(\lambda,\mu)} \) expansion up to \( 0 \leq \lambda + \mu \leq 6 \). It is also important to remark that here we have systematically neglected the contribution of \( SU(3) \) elements which are absent in \( \mathbb{V} \), effectively providing us with a "leading-order" approximation. Such approximations are improvable systematically by parametrizing \( U = \epsilon u \) [77] yielding,

\[
Z = \sum_{u \in \mathbb{V}} \sum_{(\lambda,\mu)} \int D\epsilon \beta_{(\lambda,\mu)}(\epsilon u) \chi_{(\lambda,\mu)}(\epsilon u) = \sum_{u \in \mathbb{V}} \sum_{(\lambda,\mu)} \beta_{(\lambda,\mu)} F(V_{(\lambda,\mu)}, \chi_{(\lambda,\mu)}(u)), \tag{4.93}
\]

where

\[
\int D\epsilon \chi_{(\lambda,\mu)}(\epsilon u) = F(V_{(\lambda,\mu)}, \chi_{(\lambda,\mu)}(u)) = \tilde{F}(V'_r, \chi'_r(u)). \tag{4.94}
\]
We have schematically applied relations in Table 4.5 or 4.6 at the second equality in Eq. (4.94), and
\[ V(\lambda,\mu) = \frac{1}{d(\lambda,\mu)} \int_{\Omega} D\epsilon \text{Re} \chi(\lambda,\mu)(\epsilon), \]
where \( d(\lambda,\mu) \) is the dimension of the character \( \chi(\lambda,\mu) \) as defined in [55]. The function \( F(V(\lambda,\mu), \chi(\lambda,\mu)) \), which is linear in \( \chi(\lambda,\mu) \), is obtainable through systematic albeit tedious algebraic manipulations as explicitly demonstrated in [77]. At higher orders, however, it is more advantageous to derive the \( \chi'_r(u) \) dependence of \( \tilde{F}(V'_r, \chi'_r(u)) \) numerically by solving a system of 17 linear equations, generated by \( u \in V \) from 17 different conjugacy classes. The domain of Eq. (4.93) hence reduces to \( V \) leading to
\[ \chi(\lambda,\mu) = \sum_{r=1}^{17} c^r_{(\lambda,\mu)} \chi'_r. \quad (4.95) \]

With the determined values of \( \beta'_i \), we can now reexponentiate to obtain the effective action \( \tilde{S}(u) \) in Eq. (4.92). Rewriting the effective action \( \tilde{S}(u) \) as an expansion in terms of \( \chi'_r \), we obtain the following matching formula from which the coefficients \( \gamma_i \) are fixed to the targeted order in \( \beta \),
\[ \exp(-\tilde{S}(u)) = \exp\left( -\sum_{i=1}^{17} \gamma_i \chi'_i \right) = \sum_{i=1}^{17} \beta'_i \chi'_i, \quad (4.96) \]
which implies
\[ -\sum_{i=1}^{17} \gamma_i \chi'_i = \log \left( 1 + \sum_{i=1}^{17} \beta'_i \chi'_i - 1 \right) \equiv \log (1 + z). \quad (4.97) \]
Coefficients \( \gamma_i \) are then extracted by expanding the R.H.S. with respect to \( z \) and matching onto the L.H.S. in terms of the 17 characters, the completeness of \( \chi'_r \) as a character representation of \( V \) validates
\[ \chi'_i \chi'_j = \sum_{k=1}^{17} c_{ijk} \chi'_k, \quad (4.98) \]
with \( c_{ijk} \) being integers easily calculable from Table 4.6 by solving a system of 17 linear equations with 17 unknowns.

Both \( \beta'_i \) and \( \gamma_i \) are \( \beta \)-dependent.
Substituting Eq. (4.98) into Eq. (4.97) then yields all the coefficients $\gamma_i$ as polynomials of the strong coupling $\beta$. Explicit expressions with parametrization invariance, a general principle for constructing effective actions which we explain below, are summarized in Table 4.9.

Finally, it is important to notice that the original Wilson action $S(U)$ is invariant under reparameterization $\{\beta, U\} \mapsto \{\beta/c, cU\}$ with $c \neq 0$ being an arbitrary constant. This property, which we call reparameterization invariance (RI), is no longer present when the character expansion is truncated at finite orders. We explicitly reintroduce it to remove finite order terms in the effective action $\tilde{S}(u)$ that are destined to sum up to zero. This not only gives us a much simpler expression for the effective action but also helps reduce the computational cost in lattice simulations and should improve agreement with the $SU(3)$ action.

The effective action we have derived from the character expansion in terms of the $\gamma_i$ in Table 4.9 can be compared to the group decimated action, $S_{GD}$, defined by the couplings in Table III of [77]. $S_{GD}$ was only calculated to $O(\beta^3)$ and thus the scaling behavior for certain $\chi'_r$ are unknown. In contrast, using the character expansion we can determine the leading power of $\beta$ for all $\chi'_r$.

Between the two schemes, there are different $\beta$ dependences. In particular, $\chi'_1$ in the character expansion contains only odd powers of $\beta$ while $S_{GD}$ generates all new terms at all orders. When comparing the two ad-hoc modified $V$ actions which individually added $\chi'_4$ and $\chi'_5$ [4, 6], the group decimation procedure suggested no preference – they both are generated at $O(\beta^2)$. Within the character expansion, only $\chi'_4$ appears at $O(\beta^2)$. $\chi'_5$ only arises at $O(\beta^4)$.
4.4.3 Numerical Results

In order to gauge the effectiveness of our approximations, the effective \( V \) action induced by character expansion was simulated at each order in \( \beta \). For these computations \( 10^2 \) configurations separated by \( 10^2 \) sweeps were collected on a \( 4^4 \) lattice. The average energy per plaquette \( \langle E_0 \rangle \) versus \( \beta \) is plotted in Fig. 4.7.

\[
\langle E_0 \rangle = 1 - \text{Re}(\Tr u_p)/3, \text{ vs } \beta \text{ on a } 4^4 \text{ lattice for } V \text{ action with corrections of: } O(\beta^1), O(\beta^2), O(\beta^3), O(\beta^4), \text{ and } O(\beta^5). \text{ The black line is the } SU(3) \text{ result.}
\]

If the effective action behaved as the continuous group action, \( \langle E_0 \rangle \) would be observed to be monotonic in \( \beta \) and be gapless. Note that with the truncation in \( \beta^n \) and imposing the reparameterization invariance condition, the connection between the Wilson action \( \beta \) and the \( \beta \) used in the \( V \) simulations is not linear. For all orders in the character expansion, we find that a gap – corresponding to entering the frozen phase –
exists. This is in contrast to the group decimation approximations of [77] where higher orders never entered the frozen phase. We observe though that when including $O(\beta^2)$ or higher terms, instead of just entering the frozen phase as in the trajectories of $a, b, c$ in Fig. 4.8, these trajectories appear to experience a large drop in $\langle E_0 \rangle$ and then rise again and asymptote to a fixed value. We interpret this as the character expansion approximation producing trajectories of the form $d$ in Fig. 4.8. At sufficiently high order, or with resummation, the trajectory should change to follow $e$, but clearly fifth order is insufficient for this. The convergence to the continuous group results is slow and alternating with $\beta^n$. Despite this, higher-order effective action seems to correspond to a wider range of $\langle E_0 \rangle$ being accessible. We take $\langle E_0 \rangle = \langle E_0(a) \rangle$ to be a simplistic proxy for the obtainable lattice spacing in a discrete group action. While this is not a definitive scale setting, it serves as a first test that without success no further ones should be made. If interpreted this way, $\langle E_0 \rangle = 0$ corresponds to the frozen phase and should be avoided. We observe that while all actions are bounded by $\langle E_0 \rangle \in [0, 1]$, the values within this range that are unobtainable shrink as higher $\beta^n$ are included. For the $O(\beta^5)$ action, it was found to be possible to obtain $0.1 \leq \langle E_0 \rangle \leq 0.5$. These results are promising in that they naively suggest that the action might allow for smaller lattice spacing than the unmodified one - including physics within the scaling regime although scale setting and other observables would be necessary to prove this.

It should be noted that the behavior observed by this expansion is qualitatively different from that of the group decimation procedure of [77]. In that work, the effective actions obtained at various orders of $\beta$ were found to lack the first-order phase-transition behavior of a discrete group, but the range of $\langle E_0 \rangle$ was limited to much larger values of $0.5 - 1$ in the small $\beta$ region.
4.4.4 Conclusion

In this work, we used the character expansion to develop a systematic method for improving lattice actions that replace continuous gauge group $SU(3)$ by its discrete subgroup $V$. Moreover, this method can be generalized to any continuous gauge group $SU(N)$. We also spell out a new principle called reparameterization invariance as a guideline for constructing effective actions, allowing to reduce the cost of computation and match the original action more closely at the same time. This is the ongoing effort toward developing efficient digitization schemes on quantum computers.

We computed to $O(\beta^5)$ for the single-plaquette $V$ action as an approximation of the Wilson action of $SU(3)$. These higher-order terms suggest a different scaling with $\beta$ compared to previous expansions based on group decimation [77] which leads to qualitatively different behavior along the trajectories predicted. While neither method is sufficient to give a monotonic trajectory into the scaling regime, new insight into the relative contribution of new representations into the action have been gained. The higher-order ($O(\beta^2)$) result in this work does not take into account the contribution of quantum fluctuations around $V$ elements. So as expected it deviates from the $SU(3)$ result with a hard truncation in the character expansion. It would be beneficial to include the quantum fluctuation through Table 4.5 in future work to achieve better approximations.

Moreover, while the group decimation procedure was observed to suggest the necessity of introducing two characters at $O(\beta^2)$, the character expansion only requires the adjoint character to be present.

The most immediate next steps are to compute more Euclidean observables (i.e. Wilson flow parameter and pseudocritical temperature and etc.) from the character expansion action to determine the lattice spacings achievable and to compare them
to [4, 6]. Given the large corrections order by order for $V$ and the interesting even versus odd behavior, additional work should be devoted to computing the higher order contributions and corrections induced by fluctuations around $V$ elements - potentially via some resummation technique.

Another obvious step in studying the feasibility of this procedure is to derive the modified Hamiltonian, and explicitly construct the primitive quantum gates à la [3, 89]. Together with classical lattice results, this would allow for complete resource counts for extracting continuum physics.
Table 4.3: Numerical values of character $r$. Numerical values of $\beta_r[G \to H]$ of character $r$ for the decimations $U(1) \to \mathbb{Z}_4$, $SU(2) \to \mathbb{H}$, and $SU(3) \to \mathbb{V}$. For completeness, we have included the 4 two-plaquette terms derived in [60, 61] at second order.

<table>
<thead>
<tr>
<th>$r$</th>
<th>$\beta_r[U(1) \to \mathbb{Z}_4]$</th>
<th>$\beta_r[SU(2) \to \mathbb{H}]$</th>
<th>$\beta_r[SU(3) \to \mathbb{V}]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>${0}$</td>
<td>0.142081$\beta^2$</td>
<td>0.0155979(8)$\beta^2$</td>
<td>0.021267(4)$\beta^2 + 0.0008079(3)\beta^3$</td>
</tr>
<tr>
<td>${1}$</td>
<td>0.657022$\beta + 0.128321\beta^3$</td>
<td>0.866276(8)$\beta - 0.001350(8)\beta^3$</td>
<td>0.48411(13)$\beta + 0.020812(14)\beta^2 - 0.000550(4)\beta^3$</td>
</tr>
<tr>
<td>${2}$</td>
<td>$-0.066855\beta^2$</td>
<td>$-0.02652(3)\beta^2$</td>
<td>$-0.01301(3)\beta^2 - 0.000960(5)\beta^3$</td>
</tr>
<tr>
<td>${1,1}$</td>
<td>$-\beta$</td>
<td>$\beta$</td>
<td>$-\beta$</td>
</tr>
<tr>
<td>${1,-1}$</td>
<td>$-\beta$</td>
<td>$-\beta$</td>
<td>$-0.00999(4)\beta^2 - 0.001202(5)\beta^3$</td>
</tr>
<tr>
<td>${3}$</td>
<td>0.010483$\beta^3$</td>
<td>0.001185(14)$\beta^3$</td>
<td>0.000485(3)$\beta^3$</td>
</tr>
<tr>
<td>${2,1}$</td>
<td>$-\beta$</td>
<td>$\beta$</td>
<td>$-\beta$</td>
</tr>
<tr>
<td>${1,1,1}$</td>
<td>$\alpha$</td>
<td>$\alpha$</td>
<td>$\alpha$</td>
</tr>
<tr>
<td>${2,-1}$</td>
<td>$-\beta$</td>
<td>$\beta$</td>
<td>$\beta$</td>
</tr>
<tr>
<td>${1,1,-1}$</td>
<td>$\alpha$</td>
<td>$\alpha$</td>
<td>$\alpha$</td>
</tr>
<tr>
<td>${2r}$</td>
<td>$-0.173459\beta^2$</td>
<td>0.000102(7)$\beta^2$</td>
<td>$-0.000334(18)\beta^2$</td>
</tr>
<tr>
<td>${2t}$</td>
<td>0.04238$\beta^2$</td>
<td>0.009295(7)$\beta^2$</td>
<td>0.006040(10)$\beta^2$</td>
</tr>
<tr>
<td>${2t}$</td>
<td>0.04238$\beta^2$</td>
<td>$-0.0046477(15)\beta^2$</td>
<td>$-0.002883(19)\beta^2$</td>
</tr>
<tr>
<td>${2u}$</td>
<td>0.13314$\beta^2$</td>
<td>0.0046477(15)$\beta^2$</td>
<td>0.003184(15)$\beta^2$</td>
</tr>
</tbody>
</table>
Table 4.4: Parameters of discrete subgroups necessary to study the behavior of $\beta_f$.

<table>
<thead>
<tr>
<th>$G$</th>
<th>$H$</th>
<th>$\Delta S$</th>
<th>$N$</th>
<th>$C$</th>
<th>$V_{{1}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$U(1)$</td>
<td>$\mathbb{Z}_2$</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>0.6366</td>
</tr>
<tr>
<td></td>
<td>$\mathbb{Z}_4$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>0.9003</td>
</tr>
<tr>
<td></td>
<td>$\mathbb{Z}_{10}$</td>
<td>$3-\sqrt{5}$</td>
<td>2</td>
<td>10</td>
<td>0.9836</td>
</tr>
<tr>
<td>$SU(2)$</td>
<td>$BT$</td>
<td>$\frac{1}{2}$</td>
<td>8</td>
<td>6</td>
<td>0.8939</td>
</tr>
<tr>
<td></td>
<td>$BO$</td>
<td>$\frac{1-\sqrt{2}}{2}$</td>
<td>6</td>
<td>8</td>
<td>0.9309</td>
</tr>
<tr>
<td></td>
<td>$BI$</td>
<td>$\frac{3-\sqrt{5}}{2}$</td>
<td>12</td>
<td>10</td>
<td>0.9648</td>
</tr>
<tr>
<td>$SU(3)$</td>
<td>$S(108)$</td>
<td>$\frac{4}{3}$</td>
<td>18</td>
<td>4</td>
<td>0.7138</td>
</tr>
<tr>
<td></td>
<td>$S(216)$</td>
<td>$\frac{5-\sqrt{5}}{2}$</td>
<td>54</td>
<td>4</td>
<td>0.7557</td>
</tr>
<tr>
<td></td>
<td>$S(648)$</td>
<td>$1 - \frac{1}{3}(\cos\frac{\pi}{5} + \cos\frac{2\pi}{9})$</td>
<td>24</td>
<td>9</td>
<td>0.7855</td>
</tr>
<tr>
<td></td>
<td>$V$</td>
<td>$\frac{5-\sqrt{5}}{2}$</td>
<td>72</td>
<td>5</td>
<td>0.8342</td>
</tr>
</tbody>
</table>
Table 4.5: Character expansion of $\forall$ characters in terms of $SU(3)$ characters, and in trace representation.

<table>
<thead>
<tr>
<th>$\chi'_r \ (\forall)$</th>
<th>$\sum_l \lambda \tau_{r, l}$, $\lambda \mu$</th>
<th>$\chi_l, \mu$</th>
<th>Trace Representation</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\chi'_1(u)$</td>
<td>$\chi_{(0, 0)}(u)$</td>
<td>1</td>
<td>$\text{Tr}(u)$</td>
</tr>
<tr>
<td>$\chi'_2(u)$</td>
<td>$\chi_{(1, 0)}(u)$</td>
<td>$\frac{1}{2}$</td>
<td>$\text{Tr}(u) - \frac{1}{2}$</td>
</tr>
<tr>
<td>$\chi'_3(u)$</td>
<td>$\chi_{(0, 1)}(u)$</td>
<td>$\frac{1}{2}$</td>
<td>$\text{Tr}(u) - 1$</td>
</tr>
<tr>
<td>$\chi'_4(u)$</td>
<td>$\chi_{(1, 1)}(u)$</td>
<td>$\frac{1}{2}$</td>
<td>$\text{Tr}(u) - \frac{1}{2}$</td>
</tr>
<tr>
<td>$\chi'_5(u)$</td>
<td>$\chi_{(2, 0)}(u)$</td>
<td>$\frac{1}{2}$</td>
<td>$\text{Tr}(u) - 1$</td>
</tr>
<tr>
<td>$\chi'_6(u)$</td>
<td>$\chi_{(0, 2)}(u)$</td>
<td>$\frac{1}{2}$</td>
<td>$\text{Tr}(u) - 1$</td>
</tr>
<tr>
<td>$\chi'_7(u)$</td>
<td>$\chi_{(2, 1)}(u)$</td>
<td>$\frac{1}{2}$</td>
<td>$\text{Tr}(u) - 1$</td>
</tr>
<tr>
<td>$\chi'_8(u)$</td>
<td>$\chi_{(1, 2)}(u)$</td>
<td>$\frac{1}{2}$</td>
<td>$\text{Tr}(u) - 1$</td>
</tr>
<tr>
<td>$\chi'_9(u)$</td>
<td>$\chi_{(3, 0)}(u)$</td>
<td>$\frac{1}{2}$</td>
<td>$\text{Tr}(u) - 1$</td>
</tr>
<tr>
<td>$\chi'<em>{10}(u) + \chi'</em>{11}(u)$</td>
<td>$\chi_{(1, 1)}(u) + \chi_{(2, 2)}(u)$</td>
<td>$\frac{1}{2}$</td>
<td>$\text{Tr}(u) - 1$</td>
</tr>
<tr>
<td></td>
<td>+ $\chi_{(3, 0)}(u) - \chi_{(4, 1)}(u)$</td>
<td>$\frac{1}{2}$</td>
<td>$\text{Tr}(u) - 1$</td>
</tr>
<tr>
<td>$\chi'_{12}(u)$</td>
<td>$\chi_{(3, 0)}(u) + \chi_{(2, 2)}(u)$</td>
<td>$\frac{1}{2}$</td>
<td>$\text{Tr}(u) - 1$</td>
</tr>
<tr>
<td></td>
<td>+ $\chi_{(4, 1)}(u) - \chi_{(3, 3)}(u)$</td>
<td>$\frac{1}{2}$</td>
<td>$\text{Tr}(u) - 1$</td>
</tr>
<tr>
<td>$\chi'_{13}(u)$</td>
<td>$-\chi_{(1, 1)}(u) - 2\chi_{(3, 0)}(u)$</td>
<td>$\frac{1}{2}$</td>
<td>$\text{Tr}(u) - 1$</td>
</tr>
<tr>
<td></td>
<td>$-\chi_{(2, 2)}(u) + \chi_{(3, 3)}(u)$</td>
<td>$\frac{1}{2}$</td>
<td>$\text{Tr}(u) - 1$</td>
</tr>
<tr>
<td>$\chi'_{14}(u)$</td>
<td>$\chi_{(3, 1)}(u) - \chi_{(1, 2)}(u)$</td>
<td>$\frac{1}{2}$</td>
<td>$\text{Tr}(u) - 1$</td>
</tr>
<tr>
<td>$\chi'_{15}(u)$</td>
<td>$\chi_{(1, 3)}(u) - \chi_{(2, 1)}(u)$</td>
<td>$\frac{1}{2}$</td>
<td>$\text{Tr}(u) - 1$</td>
</tr>
<tr>
<td>$\chi'_{16}(u)$</td>
<td>$\chi_{(3, 2)}(u) - \chi_{(2, 1)}(u)$</td>
<td>$\frac{1}{2}$</td>
<td>$\text{Tr}(u) - 1$</td>
</tr>
<tr>
<td></td>
<td>$-\chi_{(1, 3)}(u)$</td>
<td>$\frac{1}{2}$</td>
<td>$\text{Tr}(u) - 1$</td>
</tr>
<tr>
<td>$\chi'_{17}(u)$</td>
<td>$\chi_{(2, 3)}(u) - \chi_{(1, 2)}(u)$</td>
<td>$\frac{1}{2}$</td>
<td>$\text{Tr}(u) - 1$</td>
</tr>
<tr>
<td></td>
<td>$-\chi_{(3, 1)}(u)$</td>
<td>$\frac{1}{2}$</td>
<td>$\text{Tr}(u) - 1$</td>
</tr>
</tbody>
</table>

128
Table 4.6: Character table for $\mu_1 = (1 - \sqrt{5})/2; \mu_2 = (1 + \sqrt{5})/2, \omega = (1 + i\sqrt{3})/2, \omega^* = (1 - i\sqrt{3})/2$. The integer in the second row indicates the number of elements in each class, and the letter behind denotes the cycle induced by the class elements.

<table>
<thead>
<tr>
<th>class:</th>
<th>$C_1$</th>
<th>$C_2$</th>
<th>$C_3$</th>
<th>$C_4$</th>
<th>$C_5$</th>
<th>$C_6$</th>
<th>$C_7$</th>
<th>$C_8$</th>
<th>$C_9$</th>
<th>$C_{10}$</th>
<th>$C_{11}$</th>
<th>$C_{12}$</th>
<th>$C_{13}$</th>
<th>$C_{14}$</th>
<th>$C_{15}$</th>
<th>$C_{16}$</th>
<th>$C_{17}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X_1(u)$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$X_2(u)$</td>
<td>3</td>
<td>$\mu_2$</td>
<td>1</td>
<td>$\omega$</td>
<td>$\omega^*$</td>
<td>$-\mu_1 \omega$</td>
<td>$-\mu_1 \omega^*$</td>
<td>0</td>
<td>0</td>
<td>$-\omega$</td>
<td>$-\omega^*$</td>
<td>$\mu_1$</td>
<td>$-\mu_2 \omega$</td>
<td>$-\mu_2 \omega^*$</td>
<td>$-\mu_1 \omega$</td>
<td>$-\mu_2 \omega$</td>
<td>$-\mu_1 \omega^*$</td>
</tr>
<tr>
<td>$X_3(u)$</td>
<td>3</td>
<td>$\mu_2$</td>
<td>1</td>
<td>$\omega^*$</td>
<td>$\omega$</td>
<td>$-\mu_1 \omega^*$</td>
<td>$-\mu_1 \omega$</td>
<td>0</td>
<td>0</td>
<td>$-\omega^*$</td>
<td>$-\omega$</td>
<td>$\mu_1$</td>
<td>$-\mu_2 \omega^*$</td>
<td>$-\mu_2 \omega$</td>
<td>$-\mu_1 \omega^*$</td>
<td>$-\mu_2 \omega^*$</td>
<td>$-\mu_1 \omega$</td>
</tr>
<tr>
<td>$X_4(u)$</td>
<td>8</td>
<td>$\mu_2$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>$\mu_1$</td>
<td>$\mu_1$</td>
<td>$-1$</td>
<td>$-1$</td>
<td>0</td>
<td>0</td>
<td>$\mu_1$</td>
<td>$\mu_2$</td>
<td>$\mu_2$</td>
<td>0</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>$X_5(u)$</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>$-2 \omega^*$</td>
<td>$-2 \omega$</td>
<td>$-\omega^*$</td>
<td>$-\omega$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>$-\omega$</td>
<td>$-\omega^*$</td>
<td>2</td>
<td>$-\omega$</td>
<td>$-\omega^*$</td>
</tr>
<tr>
<td>$X_6(u)$</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>$-2 \omega$</td>
<td>$-2 \omega^*$</td>
<td>$-\omega$</td>
<td>$-\omega^*$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>$-\omega^*$</td>
<td>$-\omega$</td>
<td>2</td>
<td>$-\omega^*$</td>
<td>$-\omega$</td>
</tr>
<tr>
<td>$X_7(u)$</td>
<td>15</td>
<td>0</td>
<td>$-1$</td>
<td>$\omega^*$</td>
<td>$\omega$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>$\omega$</td>
<td>$\omega^*$</td>
<td>0</td>
<td>0</td>
<td>$-1$</td>
<td>$-15 \omega^*$</td>
<td>$-15 \omega$</td>
</tr>
<tr>
<td>$X_8(u)$</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>$-2$</td>
<td>$-2$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>$-2$</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>$X_9(u)$</td>
<td>5</td>
<td>0</td>
<td>$-1$</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>$-1$</td>
<td>2</td>
<td>$-1$</td>
<td>$-1$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>$X_{10}(u)$</td>
<td>5</td>
<td>0</td>
<td>$-1$</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>$-1$</td>
<td>2</td>
<td>$-1$</td>
<td>$-1$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>$X_{11}(u)$</td>
<td>8</td>
<td>$\mu_1$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>$\mu_2$</td>
<td>$\mu_2$</td>
<td>$-1$</td>
<td>$-1$</td>
<td>0</td>
<td>0</td>
<td>$\mu_2$</td>
<td>$\mu_1$</td>
<td>$\mu_1$</td>
<td>0</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>$X_{12}(u)$</td>
<td>9</td>
<td>$-1$</td>
<td>1</td>
<td>1</td>
<td>$-1$</td>
<td>$-1$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>$-1$</td>
<td>$-1$</td>
<td>$-1$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>$X_{13}(u)$</td>
<td>9</td>
<td>$-1$</td>
<td>1</td>
<td>$-\omega^*$</td>
<td>$-\omega$</td>
<td>$\omega^*$</td>
<td>$\omega$</td>
<td>0</td>
<td>0</td>
<td>$-\omega$</td>
<td>$-\omega^*$</td>
<td>$-1$</td>
<td>$\omega$</td>
<td>$\omega$</td>
<td>1</td>
<td>$-9 \omega$</td>
<td>$-9 \omega^*$</td>
</tr>
<tr>
<td>$X_{14}(u)$</td>
<td>9</td>
<td>$-1$</td>
<td>1</td>
<td>$-\omega$</td>
<td>$-\omega^*$</td>
<td>$\omega$</td>
<td>$\omega^*$</td>
<td>0</td>
<td>0</td>
<td>$-\omega^*$</td>
<td>$-\omega$</td>
<td>$-1$</td>
<td>$\omega^*$</td>
<td>$\omega$</td>
<td>1</td>
<td>$-9 \omega^*$</td>
<td>$-9 \omega$</td>
</tr>
<tr>
<td>$X_{16}(u)$</td>
<td>3</td>
<td>$\mu_1$</td>
<td>1</td>
<td>$\omega$</td>
<td>$\omega^*$</td>
<td>$-\mu_2 \omega$</td>
<td>$-\mu_2 \omega^*$</td>
<td>0</td>
<td>0</td>
<td>$-\omega$</td>
<td>$-\omega^*$</td>
<td>$\mu_2$</td>
<td>$-\mu_1 \omega^*$</td>
<td>$-\mu_1 \omega$</td>
<td>$-1$</td>
<td>$-3 \omega$</td>
<td>$-3 \omega^*$</td>
</tr>
<tr>
<td>$X_{17}(u)$</td>
<td>3</td>
<td>$\mu_1$</td>
<td>1</td>
<td>$\omega^*$</td>
<td>$\omega$</td>
<td>$-\mu_2 \omega^*$</td>
<td>$-\mu_2 \omega$</td>
<td>0</td>
<td>0</td>
<td>$-\omega$</td>
<td>$-\omega^*$</td>
<td>$\mu_2$</td>
<td>$-\mu_1 \omega$</td>
<td>$-\mu_1 \omega^*$</td>
<td>$-1$</td>
<td>$-3 \omega$</td>
<td>$-3 \omega^*$</td>
</tr>
</tbody>
</table>
Table 4.7: Series expansions of $\beta_r$, $x \equiv \beta/6$ up to $O(x^8)$.

<table>
<thead>
<tr>
<th>$(\lambda, \mu)$</th>
<th>$\beta_{(\lambda, \mu)}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0, 0)</td>
<td>$1 - x^2 + \frac{x^4}{2} - \frac{11x^6}{72} + \frac{91x^8}{2880} + \cdots$</td>
</tr>
<tr>
<td>(1, 0)</td>
<td>$x + \frac{x^2}{2} - x^3 - \frac{3x^4}{8} + \frac{11x^6}{24} + \frac{11x^8}{80} - \frac{91x^{10}}{720} - \frac{91x^{12}}{2880} + \cdots$</td>
</tr>
<tr>
<td>(1, 1)</td>
<td>$-x^2 + x^4 - \frac{77x^6}{180} + \frac{13x^8}{120} + \cdots$</td>
</tr>
<tr>
<td>(2, 0)</td>
<td>$\frac{x^2}{2} + \frac{x^3}{2} - \frac{5x^4}{12} - \frac{11x^5}{30} + \frac{x^6}{6} + \frac{56x^7}{365} + \frac{59x^8}{1440} + \cdots$</td>
</tr>
<tr>
<td>(2, 1)</td>
<td>$-\frac{x^2}{2} - \frac{5x^4}{24} + \frac{11x^5}{24} + \frac{7x^6}{48} - \frac{13x^7}{72} - \frac{3x^8}{64} + \cdots$</td>
</tr>
<tr>
<td>(3, 0)</td>
<td>$\frac{x^3}{6} + \frac{x^4}{4} - \frac{x^5}{12} - \frac{25x^6}{144} + \frac{x^7}{48} + \frac{113x^8}{2016} + \cdots$</td>
</tr>
<tr>
<td>(2, 2)</td>
<td>$\frac{x^4}{4} - \frac{9x^6}{40} + \frac{27x^8}{320} - \frac{187x^{10}}{10080} + \cdots$</td>
</tr>
<tr>
<td>(3, 1)</td>
<td>$-\frac{x^4}{6} - \frac{2x^5}{15} + \frac{x^6}{8} + \frac{4x^7}{45} - \frac{3x^8}{70} + \cdots$</td>
</tr>
<tr>
<td>(4, 0)</td>
<td>$\frac{x^4}{24} + \frac{x^5}{12} - \frac{53x^6}{1008} + \frac{19x^8}{2880} + \cdots$</td>
</tr>
<tr>
<td>(3, 2)</td>
<td>$\frac{x^5}{12} + \frac{7x^6}{240} - \frac{49x^7}{720} - \frac{3x^8}{160} + \cdots$</td>
</tr>
<tr>
<td>(4, 1)</td>
<td>$-\frac{x^5}{24} - \frac{7x^6}{144} + \frac{x^7}{48} + \frac{29x^8}{960} + \cdots$</td>
</tr>
<tr>
<td>(5, 0)</td>
<td>$\frac{x^6}{120} + \frac{x^7}{48} + \frac{x^8}{180} - \frac{13x^9}{1152} + \cdots$</td>
</tr>
<tr>
<td>(3, 3)</td>
<td>$-\frac{x^6}{36} + \frac{x^8}{45} + \cdots$</td>
</tr>
<tr>
<td>(4, 2)</td>
<td>$\frac{x^6}{48} + \frac{x^7}{72} - \frac{71x^8}{5040} + \cdots$</td>
</tr>
<tr>
<td>(5, 1)</td>
<td>$-\frac{x^6}{120} - \frac{4x^7}{315} + \frac{x^8}{720} + \cdots$</td>
</tr>
<tr>
<td>(6, 0)</td>
<td>$\frac{x^6}{720} + \frac{x^7}{240} + \frac{x^8}{480} + \cdots$</td>
</tr>
</tbody>
</table>
Table 4.8: $\beta_r'$ as linear combinations of $\beta_{(\lambda,\mu)}$.

<table>
<thead>
<tr>
<th>$\beta_r'$</th>
<th>( \beta_{(0,0)} + 2\beta_{(6,0)} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\beta_1$</td>
<td>( \beta_{(1,0)} + \beta_{(5,0)} + \beta_{(5,1)} )</td>
</tr>
<tr>
<td>$\beta_2$</td>
<td>( \beta_{(1,1)} + 2\beta_{(4,1)} + \beta_{(3,3)} + 2\beta_{(6,0)} )</td>
</tr>
<tr>
<td>$\beta_3$</td>
<td>( \beta_{(2,0)} + \beta_{(4,0)} + 2\beta_{(4,2)} + \beta_{(5,1)} )</td>
</tr>
<tr>
<td>$\beta_4$</td>
<td>( \beta_{(2,1)} + \beta_{(3,1)} + 2\beta_{(3,2)} + \beta_{(5,0)} + 2\beta_{(4,2)} + 2\beta_{(5,1)} )</td>
</tr>
<tr>
<td>$\beta_5$</td>
<td>( \beta_{(3,0)} + 2\beta_{(4,1)} + 2\beta_{(3,3)} )</td>
</tr>
<tr>
<td>$\beta_6$</td>
<td>( \beta_{(2,2)} + \beta_{(3,3)} + 2\beta_{(6,0)} )</td>
</tr>
<tr>
<td>$\beta_7$</td>
<td>( \beta_{(2,2)} + 2\beta_{(4,1)} + \beta_{(3,3)} )</td>
</tr>
<tr>
<td>$\beta_8$</td>
<td>( \beta_{(2,2)} + 2\beta_{(4,1)} + 2\beta_{(3,3)} + 2\beta_{(6,0)} )</td>
</tr>
<tr>
<td>$\beta_9$</td>
<td>( \beta_{(3,1)} + \beta_{(4,0)} + \beta_{(3,2)} + 2\beta_{(4,2)} + \beta_{(5,1)} )</td>
</tr>
<tr>
<td>$\beta_{10}$</td>
<td>( \beta_{(2,2)} + \beta_{(3,3)} + 2\beta_{(6,0)} )</td>
</tr>
<tr>
<td>$\beta_{11}$</td>
<td>( \beta_{10} )</td>
</tr>
<tr>
<td>$\beta_{12}$</td>
<td>( \beta_{12} )</td>
</tr>
<tr>
<td>$\beta_{13}$</td>
<td>( \beta_{13} )</td>
</tr>
<tr>
<td>$\beta_{14}$</td>
<td>( \beta_{14} )</td>
</tr>
<tr>
<td>$\beta_{15}$</td>
<td>( \beta_{15} )</td>
</tr>
<tr>
<td>$\beta_{16}$</td>
<td>( \beta_{16} )</td>
</tr>
<tr>
<td>$\beta_{17}$</td>
<td>( \beta_{17} )</td>
</tr>
</tbody>
</table>
Table 4.9: $\gamma_i$ computed in terms of $\beta$ to $\mathcal{O}(\beta^5)$ with reparameterization invariance.

<table>
<thead>
<tr>
<th>$\gamma_i$</th>
<th>$-\frac{1}{18}\beta^2 - 0.00308642\beta^4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\gamma_2$</td>
<td>$\frac{1}{6}\beta + 0.00925926\beta^3 + 0.00174683\beta^5$</td>
</tr>
<tr>
<td>$\gamma_3$</td>
<td>$\gamma_2$</td>
</tr>
<tr>
<td>$\gamma_4$</td>
<td>$-\frac{1}{18}\beta^2 - 0.00308642\beta^4 - 0.000364369\beta^5$</td>
</tr>
<tr>
<td>$\gamma_5$</td>
<td>$-0.000257202\beta^4$</td>
</tr>
<tr>
<td>$\gamma_6$</td>
<td>$\gamma_5$</td>
</tr>
<tr>
<td>$\gamma_7$</td>
<td>$0.00925926\beta^3 - 0.000257202\beta^4 + 0.00524049\beta^5$</td>
</tr>
<tr>
<td>$\gamma_8$</td>
<td>$\gamma_7$</td>
</tr>
<tr>
<td>$\gamma_9$</td>
<td>$-0.000728738\beta^5$</td>
</tr>
<tr>
<td>$\gamma_{10}$</td>
<td>$-0.00308642\beta^4$</td>
</tr>
<tr>
<td>$\gamma_{11}$</td>
<td>$\gamma_{10}$</td>
</tr>
<tr>
<td>$\gamma_{12}$</td>
<td>$-0.00308642\beta^4 - 0.000364369\beta^5$</td>
</tr>
<tr>
<td>$\gamma_{13}$</td>
<td>$\gamma_{12}$</td>
</tr>
<tr>
<td>$\gamma_{14}$</td>
<td>$-0.000257202\beta^4 + 0.00174683\beta^5$</td>
</tr>
<tr>
<td>$\gamma_{15}$</td>
<td>$\gamma_{14}$</td>
</tr>
<tr>
<td>$\gamma_{16}$</td>
<td>$0.00174683\beta^5$</td>
</tr>
<tr>
<td>$\gamma_{17}$</td>
<td>$\gamma_{16}$</td>
</tr>
</tbody>
</table>
Figure 4.8: Examples of possible trajectories. In the unfrozen phase, the lines of constant lattice spacing are represented by the $45^\circ$ gray lines and the color gradient. (a) crosses into the frozen phase at larger lattice spacing compared to (b) which is the $\mathcal{O}(\beta)$ result which replaces $SU(3)$ by $\mathbb{V}$. (c) also enters the frozen phase, but at a smaller $a$ – thus improving the approximation; (d) describes the behavior observed in Fig. 4.3 where the trajectory enters and leaves the frozen phase. The curve (e) remains in the unfrozen phase forever, and asymptotes to a finite $a$ e.g the ad-hoc trajectory of [4]. The final trajectory (f) where the trajectory diverges from the frozen phase has been observed in the group space decimation method [77].
5.1 Introduction

When will quantum computers solve valuable problems that are out of reach for state-of-the-art classical approaches? To understand this future moment of quantum advantage, we must identify what computational problems are most apt and determine what quantum algorithms will be able solve them in the nearest time frame. Despite some recent challenges being illuminated [90], estimating the ground state energy of quantum systems [15] remains one of the leading contenders for the first realization of practical quantum advantage. Solving this problem efficiently with a quantum computer would be of high value to areas including combustion [67], batteries [51, 82], and catalysts [66]. Considering that the progress in quantum hardware has consistently improved, we are urged to investigate: what are the minimal quantum resources needed to realize quantum advantage with ground state energy estimation (GSEE)?

To estimate ground state energy on early quantum computers, researchers have designed more efficient algorithms using fewer qubits, gates, and ancillas. Most of these algorithms are based on the variational quantum eigensolver (VQE) [114]. These algorithms do not have performance guarantees and recent works have identified roadblocks for the practicality of such approaches through the measurement problem.

The presentation in this chapter is based on the results obtained in [138].
[67, 79] and issues with optimization [12, 105]. Yet, quantum algorithms with performance guarantees [15, 18, 54, 94] demand unfortunately-large quantum resources, requiring hundreds of logical qubits and over billions of operations per circuit (e.g. greater than $10^{10}$ T gates [82]). The error correction overhead needed to run such quantum circuits is far beyond what can be realized on today’s hardware. Towards realizing practical quantum advantage sooner, we develop quantum algorithms in the goldilocks regime of having provable performance guarantees while also exponentially reducing the required number of operations.

The operations involved in many GSEE algorithms, including ours, are controlled time evolution operations, $c \exp i H t$. For the algorithms considered, the total number of operations per circuit and the circuit depth are proportional (ignoring logarithmic factors) to the evolution time $t$. We will refer to this measure as the circuit depth. The circuit depth required by a GSEE algorithm is typically costed in terms of $\epsilon$, the target accuracy of the ground state energy estimate, and $\eta$, a lower bound on the overlap of the input state $\rho$ with the ground state. In contrast to previous GSEE methods, the costs of our GSEE algorithms will depend on $\Delta$, a lower bound on the energy gap (i.e. the difference between the smallest and next-smallest eigenvalue of $H$), typically governs the performance of ground state preparation methods [54]. With these parameters established we are able to describe the costs of previous methods for GSEE that aim to minimize the quantum resources. Recently, building upon the ideas of [126], Lin and Tong [94] designed a quantum algorithm for ground state energy estimation with circuit depths scaling as $\tilde{O}(1/\epsilon)$, which requires just a single ancilla qubit and involves no costly circuit operations beyond controlled time evolu-

---

An important caveat for all known ground state energy estimation methods (c.f Table I of [54]) is that if $\eta$ is extremely small, then we have little hope of accurately estimating the ground state energy. Thus, it is common to assume that the Hamiltonian of interest admits a good ground state approximation.
tions. This algorithm requires running the circuits of depth $\tilde{O}(\epsilon^{-1})$ multiple times, leading to a total runtime of $\tilde{O}(\epsilon^{-1}\eta^{-2})$. Later, Dong et al. [54] improved on this result, developing an algorithm with similar characteristics, yet achieving a runtime of $\tilde{O}(\epsilon^{-1}\eta^{-1})$. Both of these methods achieve the so-called Heisenberg-limited scaling in the runtime with respect to $\epsilon$. Meanwhile, Wan et al. [134] combined the ideas in [94] with the principles of randomized Hamiltonian evolution (QDRIFT) [39] to propose a ground state energy estimation algorithm which trades off between number of non-Clifford gates and runtime. Ding and Lin [52] and Ni et al. [108] also discovered low-depth algorithms for phase estimation which achieve the Heisenberg-limited scaling of quantum runtime while having a diminishing prefactor for the maximum circuit depth when the initial state approaches the target eigenstate. There has also been progress in developing low-cost (or low-depth) quantum algorithms for simultaneous estimation of multiple eigenvalues in the past years [53, 56, 92, 112, 126]. Our work is mostly influenced by [94, 126] which promoted the idea of using quantum circuits to general time signals and utilizing the tools from classical signal processing to analyze them. This time series analysis reveals the target property of the spectrum of the Hamiltonian.

All of the GSEE methods prior to ours employ quantum circuits whose depth scales inversely with $\epsilon$ the target accuracy. In the early fault-tolerant setting, this

---

After the first version of this paper was posted on arXiv, Ding and Lin [52] proposed a GSEE algorithm which achieves essentially the same circuit depth and quantum runtime as ours. Although both their algorithm and our algorithm are based on classical postprocessing of the data from Hadamard tests, the specific ways of exploiting such data are quite different. The algorithm of [52] takes a direct data fitting approach and solves nonlinear optimization problems to find the values that best match the observed data. By contrast, we take an indirect Fourier filtering approach and use the data to construct the convolution of the spectral measure and a Gaussian derivative filter, and then infer the ground state energy from the shape of this convolution. The classical computation is simpler here. On the other hand, [52] also proposed techniques for reducing the circuit depth for GSEE when the overlap between the initial state and the ground state is large (without a spectral-gap assumption). This scenario is not considered in this work.
circuit depth requirement may place a limit on the size of problem instances that such methods can accommodate. It is reasonable to assume that early fault-tolerant quantum computers will be limited in number of physical qubits. Larger problem instances require more logical qubits to be encoded in these physical qubits. This entails an increase in the error rate for logical operations (as the code distance has been reduced). This increase in error rate compromises the number of operations that can be implemented per circuit (assuming a fixed circuit error tolerance of the algorithm). To “unlock” larger instances requires running a GSEE algorithm that can succeed with fewer operations per circuit (or less circuit depth). Motivated by these considerations, the question addressed by this work is: is it possible to unlock larger problem instances for early fault-tolerant quantum computers through an exponential improvement in the accuracy-dependence scaling of circuit depth in ground state energy estimation?

We develop and analyze low-depth ground state energy estimation (GSEE) algorithms with high accuracy for which the circuit depth scales exponentially better than $O(1/\epsilon)$. As is typical, the circuit depth and quantum runtime of the algorithm is measured in terms of the number of controlled evolution operations $c\exp(-2\pi i H)$ referred to as Hamiltonian evolution time.

**Theorem 5.1.1 (Low-depth GSEE, informal version)** Let $H$ be a Hamiltonian with spectral gap at least $\Delta$. Suppose we can prepare an initial state $\rho$ such that the overlap with the ground state satisfies $\langle E_0 | \rho | E_0 \rangle \geq \eta$. Given $\Delta$, $\eta$, and sufficiently small $\epsilon$, there exists an algorithm to estimate the ground state energy within accuracy $\epsilon$ with high probability such that:

- The circuit depth, measured in maximal Hamiltonian evolution time, is

$$T_{\text{max}} = O\left(\Delta^{-1} \cdot \text{poly log } \epsilon^{-1} \eta^{-1} \Delta\right).$$  

(5.1)
Figure 5.1: Landscape of early fault-tolerant GSEE algorithms. This figure shows the landscape of early fault-tolerant GSEE algorithms plotted according to their runtime and circuit depth measured in terms of total evolution time ($T_{\text{tot}}$) and maximal evolution time ($T_{\text{max}}$), respectively. The green region indicates the new low-depth regime introduced in this work. The orange dot corresponds to the $\Delta^{-1}$-depth GSEE algorithm (Theorem 5.1.1) when $\Delta = \Delta_{\text{true}}^{-1}$, and the curve shows the smooth trade off between $T_{\text{max}}$ and $T_{\text{tot}}$ described in Corollary 5.1.2. We also remark that the right-most dot which shows an algorithm in [54] requires multiple ancilla qubits and multi-qubit controlled operations, whereas the algorithms in this work and [94, 134] only use a single ancilla qubit. For simplicity, we have ignored all the poly-logarithmic factors.

- The quantum runtime, measured in total Hamiltonian evolution time, is

$$T_{\text{tot}} = O \left( \eta^{-2} \epsilon^{-2} \Delta \cdot \text{poly log} \epsilon^{-1} \eta^{-1} \Delta \right). \quad (5.2)$$

Using the costs established in Theorem 5.1.1, Table 5.1 provides resource estimates that show the reduction in gates per circuit for molecules of industrial interest. The reduction in gates per circuit affords a reduction in the fault-tolerant overhead required to implement ground state energy estimation. These reductions may help to
Table 5.1: Estimated circuit cost savings. This table displays estimated circuit cost savings afforded by Algorithm 2 for two molecules relevant to battery design analyzed in previous work [82]. For these molecules in the cc-pVDZ basis, we can estimate the energy gaps using EOM-CCSD calculations with ORCA software [106, 107]. The target accuracy considered in [82] was $\epsilon = 1$ mHa. The standard approach to quantum phase estimation (ignoring the cost due to imperfect ground state preparation) uses a circuit with $2/\epsilon$ applications of $c \exp(2\pi i H)$ to achieve an $\epsilon$ accurate estimate with high probability. We include the various logarithmic factors (c.f. Algorithm 2) and set an input state overlap value of $\eta = 1/1000$, which is conservative (i.e. lower) relative to the values found in [128]. In the last column we give cost reductions relative to recent methods [94], which use $2/\pi \epsilon$ applications of $c \exp(2\pi i H)$.

<table>
<thead>
<tr>
<th>Molecule</th>
<th>Gap</th>
<th>Gap Lower Bound</th>
<th>Gate Reduction [82]</th>
<th>Gate Reduction [94]</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC</td>
<td>264 ± 20 mHa</td>
<td>244 mHa</td>
<td>43×</td>
<td>16×</td>
</tr>
<tr>
<td>PF₆</td>
<td>468 ± 20 mHa</td>
<td>448 mHa</td>
<td>78×</td>
<td>28×</td>
</tr>
</tbody>
</table>

bring such problem instances within reach of earlier fault-tolerant quantum architectures, potentially realizing quantum advantage sooner.

For some molecules, it might be the case that the runtime of this low depth algorithm is too high to outperform state-of-the-art classical methods for solving the same problem. Our second main result is that we can trade circuit depth for total runtime reduction. This gives a means of speeding up the overall algorithm.

**Corollary 5.1.2** Let $H$ be a Hamiltonian with spectral gap $\Delta_{\text{true}}$. Suppose we can prepare an initial state $\rho$ such that the overlap with the ground state satisfies $\langle E_0 | \rho | E_0 \rangle \geq \eta$. Then for arbitrary $\alpha \in [0, 1]$, given $\Delta_{\text{true}}$, $\eta$ and sufficiently small $\epsilon$, there exists an algorithm to estimate the ground state energy within accuracy $\epsilon$ with high probability such that:
• The circuit depth, measured in maximal Hamiltonian evolution time, is
\[
T_{\text{max}} = \tilde{O} \left( e^{-\alpha} \Delta_{\text{true}}^{-1+\alpha} \right). \tag{5.3}
\]

• The quantum runtime, measured in total Hamiltonian evolution time, is
\[
T_{\text{tot}} = \tilde{O} \left( \eta^{-2} e^{-2+\alpha} \Delta_{\text{true}}^{1-\alpha} \right). \tag{5.4}
\]

Through the era of early fault-tolerant quantum computing, as quantum architectures are able to realize deeper quantum circuits, the trade-off in Corollary 5.1.2 may lead to a crossover point into quantum advantage.

### 5.2 Low-depth Ground State Energy Estimation

Before introducing the method, we define the ground state energy estimation problem. Suppose we are given a classical description of a quantum Hamiltonian \( H \). This Hamiltonian has (unknown) spectral decomposition \( H = \sum_{j=0}^{N-1} E_j |E_j\rangle \langle E_j| \), where \( E_0 < E_1 \leq E_2 \leq ... \leq E_{N-1} \) are the eigenvalues of \( H \), and the \( |E_j\rangle \)'s are orthonormal eigenstates of \( H \). Let \( \rho \) be an easy-to-prepare state (of the same dimension as \( H \)). Let \( p_j := \langle E_j | \rho | E_j \rangle \) be the overlap between \( \rho \) and \( |E_j\rangle \), for \( 0 \leq j \leq N - 1 \). We assume that two numbers \( \eta \in (0, 1) \) and \( \Delta > 0 \) are given such that \( p_0 = \langle E_0 | \rho | E_0 \rangle \geq \eta \) and \( E_1 - E_0 \geq \Delta \). Our goal is to estimate \( E_0 \) with accuracy \( \epsilon \) and confidence \( 1 - \delta \), i.e. to output a sample from a random variable \( \hat{E}_0 \) such that the failure probability satisfies
\[
\mathbb{P} |\hat{E}_0 - E_0| > \epsilon < \delta,
\]
for given small \( \epsilon > 0 \) and \( \delta \in (0, 1) \). Furthermore, we want to achieve this by using limited-depth quantum circuits and classical post-processing of the quantum measurement outcome data.
Our algorithm does not require the Hamiltonian $H$ to be normalized to work, i.e. it does not rely on an assumption like $\|H\| \leq 1$. The circuit depth and quantum runtime of our algorithm will be measured in the maximal and total evolution time of $H$, respectively. Note that the gate complexity of simulating $e^{iHt}$ is proportional to $\|H\| t$. Therefore, rescaling $H$, $\Delta$ and $\epsilon$ by the same constant simultaneously does not change the number of elementary gates in our algorithm.

Time signals from Hadamard tests. In our GSEE algorithm, the role of the quantum computer is simply to provide statistical estimates of $\text{tr} \left[ \rho e^{-iH\tau} \right]$. The quantum circuit we use to generate these estimates is known as a Hadamard test and is shown in Figure 5.3. Labeling this outcome $b \in \{+1, -1\}$, the average value of $b$ output by the Hadamard test circuit is

$$
\mathbb{E}[b] = \text{Re} \left[ \text{tr} \left[ \rho e^{-iH\tau} \right] \right],
$$

when $W = I$ and it is equal to the imaginary part when $W = S^\dagger$ where $S$ is the phase gate. It is helpful to view the quantity $\text{tr} \left[ \rho e^{-iH\tau} \right]$ as a complex-valued time signal, with $\tau$ being the time. This time signal encodes information about the eigenvalues of $H$ and the density operator $\rho$. In particular, if we can determine how this signal depends on the ground state energy $E_0$, then we might be able to estimate $E_0$ from the time signal. Although we are unable to exactly determine the time signal, we can estimate the real and imaginary parts of the signal at any time $\tau$ to within any desired accuracy using sufficiently many Hadamard test measurement outcomes as described above. The time cost of each Hadamard test is proportional to $\tau$ and the total time cost will depend on how many Hadamard tests, or samples, we take over the different chosen times $\tau$. 

141
Filtering the spectrum Here we introduce the method for estimating and processing the signals from the Hadamard test data. The Fourier transform (or frequency signal) of the ideal time signal $\text{tr} \left[ \rho e^{-iH\tau} \right]$ is equal to the so-called spectral measure of $H$ associated with the initial state $\rho$ and is given by

$$p(x) := \sum_{j=0}^{N-1} p_j \delta(x - E_j).$$

(5.7)

Although $p(x)$ itself cannot be determined exactly from Hadamard test data, we explain how to accurately estimate any convolution of $p(x)$ with a filter function $f(x)$. For our purposes, the filter function is used as a tool for organizing the time signal data from a limited time window into useful information about the spectrum of $H$. We briefly explain how to evaluate (or, rather, estimate) the complex number $(f * p)(x)$ for any given value $x$ using low-depth Hadamard test circuits.

Three key features make low-depth convolution estimation possible. First, the convolution can be expressed as a linear combination of $\hat{p}(t) = \text{tr} \left[ \rho e^{-2\pi iHt} \right]$,

$$(f * p)(x) = \int_{-\infty}^{\infty} \hat{f}(t) \hat{p}(t) e^{2\pi ixt} dt,$$

(5.8)

where $\hat{f}(t)$ denotes the Fourier transform of $f(x)$. Second, these traces can be estimated from the Hadamard test data as shown in Eq. 5.6. Third, the circuit depth of each Hadamard test is proportional to $t$. We can limit the circuit depth used in the algorithm and still obtain an accurate estimate of the convolution by judiciously truncating the integral approximation

$$\int_{-\infty}^{\infty} \hat{f}(t) \hat{p}(t) e^{2\pi ixt} dt \approx \int_{-T}^{T} \hat{f}(t) \text{tr} \left[ \rho e^{-2\pi iHt} \right] e^{2\pi ixt} dt.$$  

(5.9)

As explained in detail in Algorithm 1, the strategy we use to estimate $(f * p)(x)$ uses a so-called multi-level Monte Carlo approach. An unbiased estimate of $(f * p)(x)$ is constructed by first (classically) sampling a time $t$ in $[-T, T]$ drawn from a distribution
proportional to $|\hat{f}_T(t)|$. Conditioned on this outcome $t$, a sample is then drawn from each of the real $(W = I)$ and the imaginary $(W = S^\dagger)$ part Hadamard tests with time $t$, returning $X$ and $Y$, respectively. From these outcome data $(t, X, Y)$, we construct a random variable whose average value is equal to $(f * p)(x)$,

$$Z(x; t, X, Y) = \|\hat{f}_T\|_1 e^{2\pi i (tx + \phi(t))} \cdot (X + iY).$$

(5.10)

where $e^{i2\pi \phi(t)} = \hat{f}_T(t)/|\hat{f}_T(t)|$. It is important to note that the samples can be generated ahead of time; the choice of where to evaluate $(f * p)(x)$ can be made after this data is gathered.

Designing the filters  The filter function plays two roles in determining the algorithm performance. First, the shape of the filter determines how easily the ground state energy can be determined from $(f * p)(x)$. Second, the smoothness of the filter determines the severity of the truncation $T$ that can be withstood, and therefore the minimal viable circuit depth. This second role is what affords the exponential reduction in circuit depth of our method.

Estimating the ground state energy from the convolution can be understood through an example. In [94] they choose $f(x)$ to be a periodic Heaviside function. As shown in Figure 5.2, this particular choice of convolution results in a series of steps, the first of which is located at the ground state energy $E_0$. Their algorithm proceeds by using a binary search to locate this first step. The drawback of this approach is that in order to resolve this first step to accuracy $\epsilon$, the truncation order must be $\tilde{O}(1/\epsilon)$. This means that the circuit depth of the Hadamard test scales as $\tilde{O}(1/\epsilon)$. We design a filter function and energy estimation strategy that requires a time window

$$\Theta(x) = \begin{cases} 1 & \text{if } x \in [2k\pi, (2k + 1)\pi) \\ 0 & \text{if } x \in [(2k - 1)\pi, 2k\pi) \end{cases} \quad \forall k \in \mathbb{Z}. $$

143
that scales as $O(\log 1/\epsilon)$. This corresponds to an exponential improvement in the circuit depth dependence on the accuracy.

The key observation for the design of low-depth filter functions is as follows. If a filter function satisfies the following properties, then it can isolate the minimum eigenvalue from the others well and the corresponding convolution can be evaluated easily:

1. The filter function $f(x)$ has an exponentially-decaying tail, i.e., $|f(x)| = \exp -\Omega(|x|)$ for sufficiently large $x$. This ensures that $(f * p)(x) \approx p_0 f(x - E_0)$ for $x$ near $E_0$ (i.e. the interference from the excited states is negligible) and hence we can easily infer $E_0$ from the shape of $f * p$ in this region.

2. The filter function’s Fourier transform $\hat{f}(t)$ also has an exponentially-decaying tail, i.e., $|\hat{f}(t)| = \exp -\Omega(|t|)$ for sufficiently large $t$. This allows $f$ to be well-approximated by a band-limited function, which means that the maximal evolution time in the Hadamard tests will be small.

Based on this observation, a natural choice is the Gaussian filter, defined as:

$$f_\sigma(x) = \frac{1}{\sqrt{2\pi\sigma}} e^{-\frac{x^2}{2\sigma^2}},$$

where $\sigma > 0$ is a parameter to be chosen later. Note that its Fourier transform is another Gaussian kernel (up to some scaling factor):

$$\hat{f}_\sigma(t) = e^{-\frac{1}{2}(\sigma t)^2}.$$

Thus, most of its mass is concentrated within $|t| = O(\sigma^{-1})$. More importantly, by convolving $f_\sigma$ with the spectral measure $p$, we get:

$$(f_\sigma * p)(x) = \sum_{j=0}^{N-1} p_j f_\sigma(x - E_j),$$

where $\sigma > 0$ is a parameter to be chosen later. Note that its Fourier transform is another Gaussian kernel (up to some scaling factor):
which is a mixture of Gaussians. Since the Gaussian filter has an exponentially-decaying tail, if we zoom-in to a neighborhood of $E_0$, the convolution value is dominated by the first Gaussian kernel $p_0 f_\sigma(x - E_0)$. Therefore, the first significant peak of $f_\sigma \star p$ will be close to $E_0$ and GSEE is then reduced to a peak finding problem. Our approach to this problem is to first obtain some $\tilde{E}_0 \in [E_0 - \mathcal{O}(\sigma), E_0 + \mathcal{O}(\sigma)]$ by using a previous algorithm [94]. Then we partition the interval $[\tilde{E}_0 - \mathcal{O}(\sigma), \tilde{E}_0 + \mathcal{O}(\sigma)]$ into a $\mathcal{O}(\epsilon)$-width grid, and estimate the convolution $f_\sigma \star p$ at each grid point. Finally, we output the position of the grid point with maximum convolution value. The complexity of this algorithm depends on $\sigma$, the width of the Gaussian filter, since we can only truncate its spectrum to $[-T, T]$ for $T = \tilde{\Theta}(1/\sigma)$ in order to evaluate the convolution with enough precision. For sufficiently small $\epsilon > 0$, one can take $\sigma = \mathcal{O}(\Delta/\text{polylog}(\Delta \epsilon^{-1} \eta^{-1}))$ such that the algorithm outputs an estimate of $E_0$ within $\epsilon$-additive error. It implies that the maximal Hamiltonian evolution time of our algorithm is $\tilde{O}(1/\Delta)$.

We develop a method for evaluating the convolution of the spectral measure and any filter with bounded band-limit. We prove that if $f_T$ is a function such that $\hat{f}_T$ has support in $[-T, T]$, then one can use the measurement outcomes of $\tilde{O}(\epsilon_1^{-2}\|\hat{f}_T\|_2^2)$ Hadamard tests to estimate $(f_T \star p)(x)$ within accuracy $\epsilon_1 > 0$ (for any given $x$), where $\|\hat{f}_T\|_1$ is the $L^1$ norm of $\hat{f}_T$.

We now apply this result to bound the total evolution time of our algorithm with the Gaussian filter. As we will see, its performance will be sub-optimal, so we will only analyze a more refined version with better performance in detail. For the truncated Gaussian filter

$$f_{\sigma,T}(x) := \int_{-T}^T \hat{f}_\sigma(t)e^{2\pi ixt} dt,$$
we have $\|\hat{f}_{\sigma,T}\|_1 = \mathcal{O}(\sigma^{-1})$, and we need to evaluate the convolution within accuracy $\epsilon_1 = \tilde{\mathcal{O}}(\eta \epsilon^2 \sigma^{-3})$. Thus, by our choice of $\sigma = \tilde{\mathcal{O}}(\Delta)$, the sample complexity is $\tilde{\mathcal{O}}(\eta^{-2} \epsilon^{-4} \sigma^6 \cdot \sigma^{-2}) = \tilde{\mathcal{O}}(\eta^{-2} \epsilon^{-4} \Delta^4)$. Hence, the total evolution time is $T_{\text{tot}} \leq \tilde{\mathcal{O}}(\eta^{-2} \epsilon^{-4} \Delta^4 \cdot T) = \tilde{\mathcal{O}}(\eta^{-2} \epsilon^{-4} \Delta^3)$ as $T = \tilde{\mathcal{O}}(1/\sigma) = \tilde{\mathcal{O}}(1/\Delta)$.

The bottleneck of our total evolution time is the normalized convolution evaluation accuracy $\epsilon_1/\|\hat{f}_T\|_1$ which scales as $\mathcal{O}(\eta \epsilon^2 \sigma^{-2})$ for the Gaussian filter $f_\sigma$. To improve this factor, we switch to the Gaussian derivative filter $g_\sigma$ which is defined as follows:

$$g_\sigma(x) := -\frac{1}{\sqrt{2\pi} \sigma^3}x e^{-\frac{x^2}{2\sigma^2}}.$$  

Since the Gaussian derivative filter has an exponentially-decaying tail, $(g_\sigma * p)(x)$ resembles $p_0 g_\sigma(x - E_0)$ in a neighborhood of $E_0$. In particular, the unique zero point of $g_\sigma * p$ in this region is close to $E_0$.

The Gaussian derivative filter allows for a more favorable normalized convolution evaluation accuracy. On the one hand, the difference between the values of $|(g_\sigma * p)(x)|$ for $x$ that is $\epsilon/2$-close to $E_0$ and for $x$ that is $\epsilon$-far from $E_0$ is $\Omega(\eta \epsilon \sigma^{-3})$. So it suffices to pick $\epsilon_1 = \mathcal{O}(\eta \epsilon \sigma^{-3})$. On the other hand, it is easy to show that $\|\hat{g}_{\sigma,T}\|_1 = \Theta(\sigma^{-2})$. This implies that the required normalized convolution evaluation accuracy for $g_\sigma$ is $\epsilon_1/\|\hat{g}_{\sigma,T}\|_1 = \mathcal{O}(\eta \epsilon \sigma^{-1})$. Moreover, our GSEE and convolution evaluation approaches are general so that they can be easily adapted to the Gaussian derivative filter function with almost the same parameters (i.e., $\sigma = \tilde{\mathcal{O}}(\Delta)$ and $T = \tilde{\mathcal{O}}(1/\sigma)$). Therefore, using $g_\sigma$ in our algorithm, the maximal evolution time remains to be $T_{\text{max}} = \tilde{\mathcal{O}}(\Delta^{-1})$ and the total evolution time is reduced to $T_{\text{tot}} = \tilde{\mathcal{O}}(\eta^{-2} \epsilon^{-2} \Delta)$.

To see this, note that the Taylor expansion for the Gaussian density around 0 up to second order yields

$$f_\sigma(\epsilon) \simeq \frac{1}{\sqrt{2\pi} \sigma} - \frac{\epsilon^2}{2\sqrt{2\pi} \sigma^3}.$$  

This implies that the difference between the values of $(f_\sigma * p)(x) \approx p_0 f_\sigma(x - E_0)$ for $x = E_0$ and $x = E_0 + \epsilon$ can be as small as $\mathcal{O}(\eta \epsilon^2 \sigma^{-3})$. 

146
Ground state energy estimation algorithm Using the Gaussian derivative filter, we describe the algorithm for ground state energy estimation that proves Theorem 5.1.1. This is the first GSEE algorithm that uses $\tilde{O}(\Delta^{-1})$-depth quantum circuits to achieve accuracy $\epsilon$. A detailed presentation of the algorithm can be found in Algorithm 2. This algorithm makes use of the data structure for convolution evaluation in Algorithm 1.

### Algorithm 1 Convolution evaluation data structure.

1. **data structure** FilterSampler
2.  
   **Init**($f_T$) \quad \triangleright \text{Initialize for the filter } f_T
3.  
   **Sample**() \quad \triangleright \text{Sample } \xi \in \mathbb{R} \text{ with probability } \propto |\hat{f}_T(\xi)|
4.  
   **Norm**() \quad \triangleright \text{Return } \|\hat{f}_T\|_1
5.  
   **end data structure**
6.  

7. **data structure** ConvEval
8. **members**
9.  
   $\mathcal{C}(H, \rho, t, W)$ \quad \triangleright \text{Run the circuit in Figure 5.3 with } \tau = 2\pi t \text{ and } W = I \text{ or } S^t
10. 
    $\{(t^{(i)}, z^{(i)})\}_{i \in [S]} \subset \mathbb{R} \times \mathbb{C}$ \quad \triangleright \text{Fourier samples}
11. 
    FilterSampler FS \quad \triangleright \text{Filter function’s sampler}
12. **end members**
13. 

14. **procedure** Init($H, \rho, f_T, \epsilon, \delta, M$) \quad \triangleright \epsilon \text{ is the target accuracy, } \delta \text{ is the tolerable failure probability, } M \text{ is the maximal number of points at which the convolution is evaluated}
15.  
    FS.Init($f_T$)
16.  
    $L \leftarrow \text{FS.Norm}()$
17.  
    $S \leftarrow \left[\frac{L^2 \ln 4M/\delta}{\epsilon^2}\right]$
18.  
    **for** $i \leftarrow 1, 2, \ldots, S$ **do**
19.  
    $t^{(i)} \leftarrow \text{FS.Sample}()$
20.  
    $x^{(i)} \leftarrow \mathcal{C}(H, \rho, t^{(i)}, I)$ \quad \triangleright \text{Hadamard test}
21.  
    $y^{(i)} \leftarrow \mathcal{C}(H, \rho, t^{(i)}, S^t)$ \quad \triangleright \text{Hadamard test}
22.  
    $z^{(i)} \leftarrow L \cdot e^{2\pi i \phi(t^{(i)})}(x^{(i)} + iy^{(i)})$
23.  

24. **procedure** Eval($x$) \quad \triangleright \text{Approximate } (f_T * p)(x) \text{ within accuracy } \epsilon
25.  
    $Z \leftarrow \frac{1}{S} \sum_{i \in [S]} e^{2\pi i t^{(i)}x} \cdot z^{(i)}$
26.  
    **return** $Z$
27. **end data structure**
Algorithm 2: Low-depth ground state energy estimation algorithm.

1: \textbf{procedure} GSEE($H, \rho, \epsilon, \delta, \Delta, \eta$)
2: \hspace{1em} $\sigma \leftarrow \min\left(\frac{0.9\Delta}{\sqrt{2\ln 9\Delta \epsilon^{-1} \eta^{-1}}}, 0.2\Delta\right)$
3: Run the algorithm in [94] on $H$ and $\rho$ to obtain an estimate $\tilde{E}_0$ of $E_0$ such that $|\tilde{E}_0 - E_0| = \tilde{O}(\Delta)$ with high probability.
4: $M \leftarrow \lceil \sigma/\epsilon \rceil + 1$
5: $\tilde{\epsilon} \leftarrow \frac{0.1 \eta}{\sqrt{2\pi\sigma}}$
6: $T \leftarrow \pi^{-1}\sigma^{-1}\sqrt{2\ln 8\pi^{-1}\tilde{\epsilon}^{-1}\sigma^{-2}}$ \hspace{1em} $\triangleright$ Filter band-limit
7: CONVEVAL.INIT($H, \rho, g_{\sigma,T}, \tilde{\epsilon}/2, \delta/2, M$) \hspace{1em} $\triangleright$ Algorithm 1
8: \hspace{1em} \textbf{for} $j = 1, 2, \ldots, M$ \hspace{1em} \textbf{do}
9: \hspace{2em} $x_j \leftarrow \tilde{E}_0 - 0.25\sigma + (0.5\sigma/M) \cdot (j - 1)$
10: \hspace{2em} $h_j \leftarrow \text{CONVEVAL.EVAL}(x_j)$ \hspace{1em} $\triangleright$ Algorithm 1
11: \hspace{2em} $j^* \leftarrow \arg\min_{1 \leq j \leq M} |h_j|$.
12: \hspace{1em} \textbf{return} $x_{j^*}$

The inputs to Algorithm 2 include the Hamiltonian $H$ and initial state $\rho$, a lower bound $\Delta$ on the spectral gap $E_1 - E_0$ of $H$, a lower bound $\eta$ on the overlap between $\rho$ and the ground state $|E_0\rangle$ of $H$ (i.e. $\eta \leq \langle E_0|\rho|E_0\rangle$), the target accuracy $\epsilon$ and confidence $1 - \delta$. The output of the algorithm is an estimate of the ground state energy $E_0$ of $H$. The steps of the algorithm are as follows:

1. **Roughly locate $E_0$**: Run the algorithm of [94] to obtain an estimate $\tilde{E}_0$ of $E_0$ such that $|\tilde{E}_0 - E_0| = \tilde{O}(\Delta)$ with high probability.

2. **Configure filter**: Set the Gaussian derivative filter function to have width $\sigma \in \tilde{O}(\Delta)$ and choose the truncation of the filter to be $T \in \tilde{O}(1/\sigma) = \tilde{O}(1/\Delta)$ (this limits the circuit depth).
3. **Estimate convolution:** For a grid of \( M \in \tilde{O}({\Delta}/\epsilon) \) evenly-spaced energies centered at \( \tilde{E}_0 \) with width \( \tilde{O}(\Delta) \), estimate the Gaussian derivative convolution at each grid point.

   (a) To estimate the Gaussian derivative convolution at each point, for \( \tilde{O}(\eta^{-2}\epsilon^{-2}\Delta^2) \) rounds, draw a time \( t \in [-T,T] \) with probability proportional to \( |\hat{f}_T(t)| \) and run depth \( t \) real and imaginary Hadamard tests to generate binary samples \( X \) and \( Y \).

   (b) Compute \( Z(x; t, X, Y) \) (see Eq. 5.10) for each sample and average to output the convolution estimate at \( x \).

4. **Estimate zero-crossing:** Among the \( M \) convolution estimates, find the estimate closest to zero and report the corresponding energy as the ground state energy estimate.

To realize the results in Corollary 5.1.2, we choose \( \Delta \) between \( \Delta_{\text{true}} \) and \( 1/\epsilon \).

Furthermore, we can easily parallelize our algorithm to reduce the runtime in the regime where \( \Delta \gg \epsilon \). Indeed, as we do a Monte Carlo evaluation of the convolution, we can use several quantum computers in parallel to generate samples and reduce the runtime of the computation. In contrast, in the regime \( \Delta \simeq \epsilon \) it is unclear how to speed up the computation by resorting to parallel quantum computers, as we essentially sample from the distribution a constant number of times. Thus, as the total number of gates required to implement the algorithm in the \( \Delta \gg \epsilon \) regime is smaller than the usual QPE, we envision that it will be possible to run the algorithm reliably in error-corrected devices with a smaller code distance, which translates to a smaller number of physical qubits. And by running the algorithm on various smaller quantum processors in parallel, it will be possible to offset some of the additional cost.
incurred by the quadratically worse dependency on the precision. By combining these two observations, we believe that it will be possible to obtain quantum advantage earlier with the approach advocated by this paper when compared to traditional QPE.

One may wonder if Algorithm 2 still works if $\Delta$ is larger than the spectral gap $E_1 - E_0$. Unfortunately, this is not always the case. To see this, recall that we infer $E_0$ from the shape of the convolution of the spectral measure $p$ and a Gaussian derivative filter $g_\sigma$. We need the filter $g_\sigma$ to be narrow enough so that $(p \ast g_\sigma)(x) \approx p_0 g_\sigma(x - E_0)$ in a neighborhood of $E_0$. Then the unique zero point of $p \ast g_\sigma$ in this region is close to $E_0$. If $\Delta > E_1 - E_0$, then since $\sigma = \tilde{O}(\Delta)$, the filter $g_\sigma$ could be too wide for our purpose, and the functions $p_0 g_\sigma(x - E_0)$ and $p_1 g_\sigma(x - E_1)$ might have significant overlap. Consequently, we can no longer guarantee that $(p \ast g_\sigma)(x) \approx p_0 g_\sigma(x - E_0)$ for $x$ near $E_0$. In other words, $p \ast g_\sigma$ might have a different shape from $g_\sigma$ in the neighborhood of $E_0$. Thus, the current strategy will not work in general. In practice, it may be difficult to decide whether a given $\Delta$ is smaller or larger than $E_1 - E_0$, and this could pose a problem for the application of Algorithm 2. In a recent work [137], we proposed a method to certify the correctness of the outputs of GSEE algorithms (without assuming $\Delta \leq E_1 - E_0$) to mitigate this problem. We leave it as future work to fully resolve this issue.

5.3 Future Directions

In this work, we have introduced a framework for estimating ground state energies using tunable-depth quantum circuits. As shown in Figure 5.1, the algorithms developed in this work are applicable to maximum circuit depths ranging from $\tilde{O}(1/\Delta)$ to $\tilde{O}(1/\epsilon)$. The development of algorithms beyond this range is left for future explo-
ration. While we have made progress in establishing upper bounds over a range of circuit depths, an important future direction is to establish lower bounds on depth-limited ground state energy estimation. This would deepen our understanding of the capabilities and constraints of using depth-limited quantum computers for simulating quantum systems. To this end, one might draw inspiration from Section 2.2 of [56] which derives Cramer-Rao lower bounds on the scaling of the error versus the total quantum cost for estimating a single eigenvalue phase given an eigenstate input. It might be possible to generalize the result to the case where the input state is just close to an eigenstate and a spectral gap of the Hamiltonian is promised.

Our work helps to establish the paradigm of developing quantum algorithms using the tools of classical signal processing [94, 136, 147]. In this approach, the quantum computer produces stochastic signals that encode characteristics of a matrix. This stochastic signal can be processed to learn the matrix properties of interest. The signal processing paradigm is well-suited to developing algorithms for early fault-tolerant quantum computers. Quantum computations with such architectures will be error prone, generating noisy signals. The tools of classical signal processing have been designed to handle such noisy signals and can aid in the design and analysis of robust quantum algorithms [81, 86, 135].

One requirement of the algorithm is that a lower bound on the energy gap must be specified. There exist quantum chemistry methods for estimating the gap (e.g. using the ORCA software [106, 107] as we did for our numerical comparisons). However, such estimates can become inaccurate for large systems. It may be helpful to incorporate a step into the quantum algorithm that estimates this gap. Although this estimation is computationally hard in general [11], many physical systems of interest have structure that make the estimation feasible.
In this work, we did not consider the impact of implementation error on the performance of the algorithm. We expect that our algorithm is able to tolerate some degree of variation between the ideal Hadamard tests and the implemented Hadamard tests. Building off of recent work [86], we believe the algorithm can be operated so as to accommodate such deviations. We leave for future work the investigation of robust quantum algorithms for ground state energy estimation.

The methods introduced here may help to bring the target of useful quantum computing closer to the present. Yet, there is still much work needed to carry out detailed resource estimations that predict the onset of quantum advantage using methods such as those we have introduced. More broadly, our hope is that this work contributes to the general understanding of how to use quantum computers given practical constraints on their capabilities and might inspire the development of quantum algorithms in other application domains.

One may have noticed that GSEE can be also solved by preparing a high-fidelity approximation of the ground state and estimating its energy with respect to the Hamiltonian somehow. However, it is unclear whether such methods can have the same circuit depth and quantum runtime as ours. Specifically, our method requires only $\tilde{O}(\Delta^2/\epsilon^2)$ quantum circuits where each circuit evolves $H$ for $\tilde{O}(1/\Delta)$ time (ignoring $\eta$-dependence). Note that $\Delta \leq E_1 - E_0$ is always no larger than $\|H\|$. We will consider two state-preparation-based strategies below, and both of them require $\Omega(\|H\|^2/\epsilon^2)$ copies of the state to reach accuracy $\epsilon$, which is more costly than our method, especially when $\|H\| \gg \Delta$. In both strategies, let $|\psi\rangle$ be the output of a ground state preparation algorithm.

1. In the first strategy, suppose $H$ has the Pauli decomposition $H = \sum_i a_i P_i$.

   Then with probability $|a_i|/\|\vec{a}\|_1$, where $\|\vec{a}\|_1 = \sum_i |a_i| \geq \|H\|$, we perform the projective measurement \{(\(I + P_i\))/2, (\(I - P_i\))/2\} on $|\psi\rangle$, and multiply the
outcome $\pm 1$ by $a_i/|a_i|$. Then this random variable is an unbiased estimator of $\langle \psi | H | \psi \rangle / \| \vec{a} \|_1$. Thus we need to collect $O(\| \vec{a} \|^2 / \epsilon^2)$ samples to estimate $\langle \psi | H | \psi \rangle$ within accuracy $\epsilon$.

2. In the second strategy, let $U$ be a block-encoding of $H$ with normalization factor $\alpha$, i.e. $\langle 0 | U | 0 \rangle = H/\alpha$. Note that $\alpha \geq \| H \|$. Then we run the Hadamard test with unitary operation $U$ and initial state $| 0 \rangle | \psi \rangle$. Then the outcome of this circuit is an unbiased estimator of $\langle 0 | \langle \psi | U | 0 \rangle | \psi \rangle = \langle \psi | H | \psi \rangle / \alpha$. Hence we need to collect $O(\alpha^2 / \epsilon^2)$ samples to estimate $\langle \psi | H | \psi \rangle$ within accuracy $\epsilon$.

We leave it as an open question to find a state-preparation-based strategy with $\tilde{O}(\Delta^2 / \epsilon^2)$ sample complexity.

In this work, we have focused on estimating a single eigenvalue of the Hamiltonian $H$. But it is likely that our method can be extended to estimate multiple eigenvalues of $H$ simultaneously, under appropriate assumptions about the gaps among the eigenvalues and the overlaps between an input state and the eigenstates. The reason is as follows. One can use the data from the Hadamard tests to construct the convolution of the spectral measure and a Gaussian filter, and under proper conditions, the peaks of this convolution will be close to the eigenvalues of $H$. Then our problem is reduced to finding the peaks of this function. Furthermore, perhaps we can replace the Gaussian filter by a Gaussian derivative filter to gain better efficiency, as in GSEE. In that case, one would need to search for the zero points of the convolution instead of its peaks. We leave it as future work to fully develop this algorithm for simultaneous estimation of multiple eigenvalues of a given Hamiltonian.
Figure 5.2: Tradd-off comparison. This figure qualitatively compares the convolution functions and circuit depths used in the ground state energy estimation method of Ling and Tong [94] (blue curve) and the method developed here (green curve). The blue curve is an example estimate of the approximate cumulative distribution function (see Eq. (16) in [94]), while the green curve is an example estimate of output from Step 3b in the algorithm below. The LT22 method uses a Heaviside convolution, while our method uses a Gaussian derivative convolution. Their method requires a steep jump in the convolution function, which necessitates $\tilde{O}(\frac{1}{\epsilon})$-depth circuits. Our method only requires that the contribution of the excited state energies to the convolution function does not interfere too much with that of the ground state energy. This affords the use of a less-steep convolution function, which only requires $O(1/\Delta)$-depth circuits. The trade-off is that our method requires more samples, leading to an increased total runtime.
Figure 5.3: Hadamard test circuit. Hadamard test circuit parameterized by the Hamiltonian evolution time $\tau$. H is the Hadamard gate and W is either $I$ or $S^\dagger$, where $S$ is the phase gate.
6.1 Introduction

Many quantum algorithms can provide speedups over corresponding classical algorithms. For example, Hamiltonian simulation [18, 19, 24, 25, 26, 99] and quantum machine learning [2, 30, 45, 75, 98, 143]. These algorithms usually require repeated access to classical data, which encodes the problem instance, throughout the computation. Conceptually, a theoretically structured universal model known as a quantum oracle is employed to facilitate this data access. This is natural since most quantum algorithms can be phrased under the oracle query model. For practical quantum advantages, it is essential to detail the implementation of data access methods and ensure they meet specific criteria. However, identifying a feasible implementation for these data access schemes continues to be a challenge.

Quantum lookup table is a generic framework that facilitates the data access procedure for quantum algorithms. In analogy to the classical lookup table that returns data $x_i$ for a specified address bit $i$, the quantum lookup table responds with a superposition of data $\sum_i \alpha_i |i, x_i\rangle$ when queried by a superposition of address bits $\sum_i \alpha_i |i, 0\rangle$. In practice, a classical lookup table is typically realized by Random Access Memory (RAM), providing constant data access time at an almost vanishing error rate. On the quantum side, the quantum lookup table acts as an analogue, extending the quantum oracle in a specific manner. Nonetheless, there are multiple architectures designed to
achieve this implementation, known by various names such as QRAM, QROM, and SELECT-SWAP circuits. In the end, they all accomplish the same function call, but they come with varying trade-offs concerning error rate, query time, and resource cost.

Although the quantum lookup table is critical for quantum algorithms to succeed, it is extremely hard to realize. The challenge of a practical quantum lookup table lies in ensuring fault-tolerant quantum circuits. The quantum circuit usually consists of Clifford gates and T-gates, and synthesizing a high-fidelity T-gate usually involves a resource-intensive process. Thus, reducing the T-gate count without compromising fidelity is paramount in circuit design. Additionally, the efficacy of a quantum lookup table is contingent upon its query time being commensurate with the total runtime of the algorithm; otherwise, the overhead associated with data retrieval could compromise the quantum benefit. A recent study [71] shows that QRAM is error resilient. Therefore, practical quantum lookup tables should uphold this error resilience, aim for a high success rate, and optimize the T-gate count, query duration, and qubit consumption.

For near-term applications, the significance of the T-gate count supersedes circuit depth (query time), especially for circuits with a limited number of available qubits. This is because the restricted number of designated qubits used for T-gate generation results in additional cycles needed to produce the required quantity of T-gates for the circuit, effectively nullifying the benefits of a smaller circuit depth. One might think if one reduces the error of the magic state that generates a T-gate, fewer qubits for the T-gate are necessary, making it seem as though circuit depth holds greater importance. However, with a local layout, the optimal infidelity dependency on T-gate scales sublinearly in memory size which restricts the extent to which magic state distillation can be improved. Hence, it becomes crucial to pinpoint the bottleneck
affecting the actual running time in near-term devices. We shall find the optimal configuration that produces the most efficient overall runtime, taking into account multiple factors rather than relying solely on circuit depth.

Prior circuit architectures include fan-out [109], bucket-brigade [65], and SELECT-SWAP [100] circuit, whose properties are summarized in Table 6.1. These results are all based on the ideal assumption of all-to-all connectivity, where multiple qubit gates can act on distant qubits. In fact, most real-world quantum devices require qubits to be physically adjacent for direct interactions. There have been ongoing works regarding variants of QRAM[7, 144], and review articles [50, 76] on the limitations in the end-to-end implementation. To the best of our knowledge, there is no comprehensive investigation into a resilient quantum lookup table framework for real-world applications that takes into account both resource limitations and local connectivity.

We develop a generic error-resilient quantum lookup table framework, complete with fine-tuned scalings of infidelity, T-gate count, and qubit count. Our framework comprises distinct components during both route-in and route-out procedures with varying parameters, which can be assembled in various configurations to yield different scalings. It turns out that all the prior arts are just one of the special cases of our framework in certain parameter regimes. Our framework permits a smooth transition between local connectivity and all-to-all connectivity when varying the long-range connection budget. We discover the regime of parameters that yield meaningful scalings and also provide a detailed arrangement for qubits layout on a planar surface.

In this work, we assign errors to each gate type present in the circuits. This approach contrasts with the current literature where a generic $\epsilon$ error is uniformly assigned to all gates. By having such fine-tuned gate errors, we distinguish which gate errors significantly influence error scaling. Thus, in real-world applications, it becomes
<table>
<thead>
<tr>
<th>Architecture</th>
<th>Infidelity</th>
<th>T-depth</th>
<th>Qubit</th>
<th>T-gate</th>
<th>Layout</th>
</tr>
</thead>
<tbody>
<tr>
<td>fan-out [109]</td>
<td>$\tilde{O}(N)$</td>
<td>$O(\log N)$</td>
<td>$O(N)$</td>
<td>$O(N)$</td>
<td>all-to-all</td>
</tr>
<tr>
<td>bucket-brigade [71]</td>
<td>$O(\log^2 N)$</td>
<td>$O(\log N)$</td>
<td>$O(N)$</td>
<td>$O(N)$</td>
<td>all-to-all</td>
</tr>
<tr>
<td>SELECT-SWAP [100]</td>
<td>$O(bN)$</td>
<td>$O(\sqrt{N})$</td>
<td>$O(\sqrt{N})$</td>
<td>$O(\sqrt{bN})$</td>
<td>all-to-all</td>
</tr>
<tr>
<td><strong>general single-bit</strong></td>
<td>$\tilde{O}(\frac{2N}{\lambda})$</td>
<td>$O(\frac{N}{\lambda} \log N)$</td>
<td>$O(\log \frac{N}{\lambda} + \lambda)$</td>
<td>$O(\frac{N}{\gamma} + \frac{N}{\lambda} \log \frac{N}{\lambda} + \lambda)$</td>
<td>local, planar</td>
</tr>
<tr>
<td><strong>general multi-bit parallel</strong></td>
<td>$\tilde{O}(\frac{b\sqrt{N}}{\lambda})$</td>
<td>$O(\frac{N}{\lambda} \log N)$</td>
<td>$O(\log \frac{N}{\lambda} + b\lambda)$</td>
<td>$O(\frac{N}{\gamma} + \frac{bN}{\lambda} \log \frac{N}{\lambda} + b\lambda)$</td>
<td>local, planar</td>
</tr>
<tr>
<td><strong>general multi-bit sequential</strong></td>
<td>$\tilde{O}(\frac{b\sqrt{N}}{\lambda} + b^2)$</td>
<td>$O((bN) \log(\frac{N}{\lambda}))$</td>
<td>$O(\log \frac{N}{\lambda} + b\lambda)$</td>
<td>$O(\frac{N}{\gamma} + \frac{N}{\lambda} \log \frac{N}{\lambda} + \lambda)$</td>
<td>local, planar</td>
</tr>
<tr>
<td><strong>single-bit</strong> (Sec. 6.4)</td>
<td>$\tilde{O}(N^{3/4})$</td>
<td>$O(\sqrt{N} \log N)$</td>
<td>$O(\sqrt{N})$</td>
<td>$O(N^{3/4})$</td>
<td>local, planar</td>
</tr>
<tr>
<td><strong>parallel multi-bit</strong> (Sec. 6.5)</td>
<td>$\tilde{O}(bN^{3/4})$</td>
<td>$O(\sqrt{N} \log N)$</td>
<td>$O(b\sqrt{N})$</td>
<td>$O(bN^{3/4})$</td>
<td>local, planar</td>
</tr>
<tr>
<td><strong>sequential multi-bit</strong> (Sec. 6.5)</td>
<td>$\tilde{O}(bN^{3/4} + b^2)$</td>
<td>$O(\sqrt{N} \log(bN))$</td>
<td>$O(b\sqrt{N})$</td>
<td>$O(N^{3/4})$</td>
<td>local, planar</td>
</tr>
</tbody>
</table>

Table 6.1: Scalings of prior arts and this work in terms of memory size $N$ and word size $b$. The $\gamma$ and $\lambda$ are the tuning parameters one can choose, both are powers of 2, $\lambda \in [1, N]$, and $\gamma \in [1, \lambda]$. The types of models studied in this work are in bold. The last four rows show scaling results for the particular choice of $\lambda = \sqrt{N}$, and $\gamma = N^{1/4}$. 
feasible to focus on optimizing the performance of these particular gates to mitigate the bottlenecks in error scaling. Achieving optimal scaling in every dimension is infeasible. Instead, our framework allows one to make trade-offs tailored to their specific requirements and constraint conditions. Our results, based on particular parameter selections, are summarized in Table 6.1 and Theorems below. Detailed scalings will be shown in the later sections.

**Theorem 6.1.1 (Informal version of Theorem 6.4.5 and Corollary 6.4.6 )**

There exists a single-word quantum lookup table that has sublinear scaling in infidelity, T-gate count, and qubit count, with local connectivity.

**Theorem 6.1.2 (Informal version of Theorem 6.5.1 and Theorem 6.5.2)**

For constant word size $b$, there exist multi-word quantum lookup tables that have sublinear scaling in infidelity, T-gate count, and qubit count, with local connectivity.

**Theorem 6.1.3 (Informal version of Corollary 6.6.3 )** With long-range connection, there exists a single-word quantum lookup table whose infidelity can be tuned between $\tilde{O}(N^{1/2})$ and $\tilde{O}(N)$ while maintaining sublinear scalings in T-gate, and qubit count, with local connectivity.

We expect this work to serve as a link that bridges the gap between the current state-of-the-art theoretical quantum lookup table architectures, and guidance toward near-term end-to-end implementations of quantum algorithms [96]. While most literature is optimistic about the wide applications of quantum lookup tables with a logarithmic infidelity assumption, we underscore the importance of considering applications permitting sublinear infidelity scaling, given the limited budget of long-range connectivity on near-term devices.
6.2 Preliminaries

All the circuit designs in this work are assumed to access data addressed by \( n \) bits with a memory of size \( N = 2^n \). We first demonstrate reading a single bit of data before discussing extensions for large word size. Without loss of generality, there are four key characteristics of the quantum lookup table that directly impact its efficiency: circuit depth, qubit count, \( T \)-gate count, and infidelity. The time taken to query a memory location is proportional to the table’s circuit depth. Hence, for any quantum algorithm to claim an advantage over classical algorithms, this depth has to be factored into its overall runtime. For example, to achieve an exponential separation, the circuit depth must scale polylogarithmically in memory size. The qubits in a lookup table design are either used to maintain memory and router status or to act as control or ancilla bits. The current generation of quantum devices are relatively small, often having a few dozen to a few hundred qubits [14, 44, 116]. Considering such constraints in near-to-intermediate term devices, a quantum lookup table design with sublinear qubit scaling becomes highly desirable. \( T \)-gates, essential for designing routers in the presence of superposition queries, are non-Clifford gates that remain difficult to physically implement without substantial resources in most qubit modalities [31, 40]. Hence, in practical circuit design, the \( T \)-gate count needs to be minimized. The infidelity is the probability of failing a single query and it scales as a function of memory size multiplied by a generic gate error \( \varepsilon \). Thus for a constant target query error, lower infidelity provides more gate error tolerance and flexibility for accommodating larger memories.

In classical RAM, a combination of logical gates sends the bus signal to the specific memory location determined by the input address bit and relays the data stored on that memory location to the output register. Similarly, quantum routers (Figure 6.1)
help to navigate the qubit to a memory location determined by the address, after
which the corresponding classical data is loaded onto the bus qubit, and subsequently
the bus qubit is navigated to the output register. The circuit design of the quantum
router plays a pivotal role in determining the properties of a quantum lookup table. In
this section, we review the prior architectures with all-to-all connectivity assumptions.

\[ |a\rangle \]

Router

\[ |b\rangle \]

Left outputRight output

**Figure 6.1:** A high-level description of a quantum router, the router status is set to
\(|a\rangle\). Incident qubit \(|b\rangle\) will be routed to the left (right) when the router state is set
to \(|0\rangle\) (<\|1\rangle).

### 6.2.1 Fan-out Architecture

The fan-out architecture [109], an initial proposal for the QRAM, can be visualized
as a binary tree of depth \(\log N\), where the \(N\) memory locations are situated at the
tree’s leaves (Figure 6.2). Every non-leaf node in this tree functions as a router, which
guides the bus signal to its left or right child. The status of the routers on the \(\ell\)-th
level is determined by the \(\ell\)-th address bit entanglement with the router qubits.

A significant drawback of this architecture is its high linear infidelity. If a single
router gets corrupted, it has the potential to flip all other routers on that same
level, misdirecting the query to an incorrect memory path. Consequently, for error
resilience, it is suboptimal to have all the routers simultaneously entangled with the
addresses bits.
6.2.2 Bucket-brigade Architecture

The bucket-brigade architecture [64] is an improved QRAM proposal over the fan-out architecture. The memory is addressed using a binary tree structure (Figure 6.3). Each level of the tree represents a bit of the address. At each node of the tree, there are control qubits and a quantum router. When a memory address is queried, the control qubits activate a path through the routers to the target memory cell. Only the routers along this path are activated, significantly reducing the number of active routers at any time. This is in contrast to the fan-out architecture where all paths are activated simultaneously. As a result, only the $\log N$ routers in the binary tree are strongly entangled with the address bits, and all other routers are weakly entangled.

A pivotal study by Hann et al. [71] demonstrated a circuit design for the bucket-brigade model yields $O(\log^2 N)$ infidelity and is resilient to generic gate errors. They
observed that the error in some query path remains contained and does not spread to every other branch of the bucket-brigade model thereby letting some of the query paths remain free of fault. This causes the infidelity to scale only with the number of active routers in a query path and circuit depth. However, it assumed all-to-all connectivity, which is not a guaranteed feature on most current hardware. In practice, most quantum modalities will require additional operations and/or qubits to implement interactions between non-adjacent qubits. Precisely accounting for this could result in an undesirable infidelity scaling.

Previous studies did not consider long-range resources like a Bell path. In our research, we delve into a detailed examination of the cost and outcomes linked to the development of a bell path within our planar approach. We emphasize that it is
possible to create an arbitrary error-free Bell path whose infidelity is governed by the number of gates utilized in the distillation protocol. This is significant as it implies that the assumption of all-to-all connectivity is feasible on a planar layout. But simultaneously, our results reveal a critical threshold beyond which QRAM at the physical level fails to be error-resilient. This essentially means achieving logarithmic infidelity scaling is unattainable. The underlying cause is the lack of entanglement distillation. For entanglement distillation to be effective, it must occur below a certain error threshold. Given that the error for long-range gates scales linearly with memory size, for any sufficiently large QRAM, it inevitably surpasses the threshold. Consequently, employing this scheme for physical QRAM on a planar layout is deemed impractical. To meet the threshold, more sophisticated setups, such as including repeaters, are necessary, which will raise costs. We defer the practical implementation of these solutions to future work.

The popularity of QRAM is largely restricted by the large qubit counts predicted for the fault-tolerant computation. A common scenario in implementation is that different gates/operations could contribute different errors to the overall circuit. Hence, differentiating gate error types allows for a more in-depth profiling of which operations hamper overall performance of a model and how one can best harness its full potential.

6.2.3 SELECT-SWAP Architecture

The SELECT-SWAP architecture [100] is structured using a combination of both SELECT and SWAP circuits. A simple SELECT-SWAP circuit is shown in Figure 6.4 in which address bits are partitioned into two sets, each controlling the SELECT and SWAP part of the circuit, respectively. The SELECT circuit activates one of the SWAP circuits using partial address bits, and the activated SWAP circuit then routes
out the qubits stored at the designated memory location specified by the remaining address bits.

| $|a_0\rangle$ | $|a_1\rangle$ | $|a_2\rangle$ | $|0\rangle$ | $|0\rangle$ | $|0\rangle$ |
|----------------|----------------|---------------|------------|------------|------------|
| $x_0$          | $x_2$          | $x_4$         | $x_2$      | $x_6$      | $x_7$      |
|               |               |               |            |            | $|\text{out}\rangle$ |

**Figure 6.4: SELECT-SWAP architecture.** The address bits $|a_0\rangle|a_1\rangle$ are used for the SELECT circuit, and $|a_2\rangle$ is used in the SWAP circuit. For address bits set to $|010\rangle$, the $x_2$ and $x_3$ memory locations are activated in SELECT, and $x_2$ gets swapped out to the output register in SWAP.

While the SELECT circuit is deep, scaling exponentially with the number of control qubits, it uses fewer qubits for its state. The SWAP circuit operates like a chain of routers, directing the desired memory bit to the output register. The SELECT-SWAP circuit has a sublinear scaling in both T-gate and qubit count but suffers from linear infidelity scaling. This greatly limits the number of classical data bits that can be stored for a given quantum algorithm.

### 6.3 Naive Construction

We modify the bucket-brigade circuit design of [71] that assumes all-to-all connectivity by restricting to a planar layout with local connectivity. In Section 6.3.1, we present the planar layout circuit design of the bucket-brigade model to illustrate the concept. We then proceed to conduct a fine-grained analysis for how infidelity scales for this design. In Sections 6.3.3 and 6.3.4, we modify the basic layout to reduce its T count and qubit count, respectively. Even though the methods in this section do not lead to sub-linear scaling for all parameters, they are useful in understanding the building blocks used for our generic construction in upcoming sections.
6.3.1 Planar Layout of Bucket-brigade Model

We provide a circuit design for the bucket-brigade QRAM model, assuming the qubits are laid out on a 2D planar lattice and multi-qubit gates act only on adjacent qubits. We first demonstrate a toy model with two memory locations, where the routing scheme is depicted as a binary tree in Figure 6.5a. To reach the desired memory allocation, a single router $R_0$ is employed to direct the incoming address qubits into the designated memory location, from where the stored data $x_i$ is retrieved and then routed out using the same path.

The circuit description for $R_0$ is illustrated in Figure 6.5b following [71]. The router is composed of four qubits ($t_0$, $in_0$, $L_0$, and $R_0$) and is referred to as a CSWAP router as it uses Controlled-Swaps to route information. Querying the memory is divided into three phases: setting router status, qubit route-in, qubit route-out. The status of a router at depth $\ell$ of the bucket-brigade model is set according to the $\ell$th address bit. For our toy model, $R_0$’s status is set by first storing the address qubit $a_0$ in the incoming register $in_0$ and then swapping it to the status register $t_0$. Once a router’s status is set, it is said to be active and part of a query path. During qubit route-in, the bus qubit is swapped to the desired memory location connected to either $R_0$ or $L_0$ depending on the status in $t_0$. In Figure 6.5b, the circuit for qubit route-out is not explicitly depicted, as it is the qubit-route in circuit in reverse.

The CSWAP router’s four qubits can be arranged in a T-shaped configuration as shown in Figure 6.5c where the qubits are located at the intersections of the grid. This configuration ensures that each router qubit is adjacent to any other router qubit with at most one local swap. The CSWAP gate can be decomposed into a sequence of Clifford and T gates that operate on at most two qubits [100].
Figure 6.5: Bucket-brigade circuit and layout. (a) A high-level bucket-brigade QRAM routing scheme for two memory locations. (b) Circuit for the toy model. It first sets the router status qubit $t_0$ to the address bit $a_0$, and then routes the control bit from the bus to the target location. (c) A planar layout of qubits for the toy model with nearest-neighbor connectivity. (d) Joining two T-shaped routers to form a single H-tree segment.
For the larger memory size of $N = 16$, the high-level bucket-brigade routing scheme is shown in Figure 6.6, where both the route-in and route-out phases follow the same path in the tree. The corresponding planar layout is shown in Figure 6.7 where the input, and bus bits are positioned. The routers are placed on the grid following the H-tree fractal pattern [103] starting from the root at the center and leaves at the boundaries of the grid. The left and right registers of the leaf-level routers send an incoming qubit to the respective memory locations. A pair of T-shaped routers each laid out according to Figure 6.5c can be joined together to form a single H-tree segment as shown in Figure 6.5d.

![Figure 6.6: High-level routing scheme for 16 memory locations.](image)

The recursive expansion of the fractal layout yields an optimal layout that occupies an area of size $O(N)$. Such a layout scheme infidelity, T count, and qubit count scaling linearly with memory size $N$. Clearly, both T count and qubit count are $O(N)$ respectively since the layout uses $O(N)$ CSWAP routers and there are $O(N)$ points in the rectangular grid where each point corresponds to a qubit. We show that infidelity scales linearly in Lemma 6.3.1.

**Lemma 6.3.1** Let $\varepsilon_{\text{max}}$ be the maximum gate error for each time step among all types of gates used in the layout. Then the infidelity of the bucket-brigade QRAM with the planar layout design (Figure 6.7) scales as $O(N\varepsilon_{\text{max}})$. 

169
Proof. We give a high-level idea for the proof here, and an exact proof can be obtained similarly to the one in Ref. [71, Appendix D]. Tree branches in Figure 6.6 can be categorized as either good or bad, based on the presence or absence of errors within the branch. Crucially, errors do not spread from a bad branch to a good branch. This property of error containment within the bucket brigade model forms the foundation of their proof. This property holds regardless of the layout scheme as long as the high-level routing scheme follows Figure 6.6. Indeed, as both the all-to-all connectivity layout and the local connectivity layouts follow this scheme, as with the former case, the error does not propagate from bad branches into good ones.

For each CSWAP router $R_i$, its active time is the time step during which its status qubit $t_i$ needs to be maintained. Since any radius of a volume $N$ ball on a
planar surface is \( O(\sqrt{N}) \), the depth of the circuit is \( O(\sqrt{N}) \), and the active time for each CSWAP router is \( O(\sqrt{N}) \). Multiplying them yields \( O(N\varepsilon_{\text{max}}) \) infidelity.

Note that such a planar layout scheme can be naturally extended to higher dimensions such as a cubic grid for 3D. However we focus only on the planar grid throughout this work.

6.3.2 Fine-grained and Improved Infidelity

Note that Theorem 6.3.1 uses only one term for gate errors and does not differentiate the sources of gate errors. For a more precise accounting of how infidelity depends on the circuit operations, we account for differentiate the error contributions from operations. In this section, we first present a fine-grained analysis of the infidelity associated with the basic layout. Later, we improve on this by changing how long distance SWAPs are performed: using GHZ states instead a series of local SWAP operations. The type of errors that we will consider throughout this work is summarized in Table 6.2.

<table>
<thead>
<tr>
<th>Error type</th>
<th>Symbol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idling/ identity gate</td>
<td>( \varepsilon_I )</td>
</tr>
<tr>
<td>GHZ qubit</td>
<td>( \varepsilon_G )</td>
</tr>
<tr>
<td>Long range</td>
<td>( \varepsilon_L )</td>
</tr>
<tr>
<td>SWAP gate</td>
<td>( \varepsilon_s )</td>
</tr>
<tr>
<td>CSWAP gate</td>
<td>( \varepsilon_{cs} )</td>
</tr>
<tr>
<td>CNOT gate</td>
<td>( \varepsilon_c )</td>
</tr>
<tr>
<td>CCNOT gate</td>
<td>( \varepsilon_{cc} )</td>
</tr>
</tbody>
</table>

Table 6.2: Error types considered in the fine-tuned analysis throughout this work.
**Lemma 6.3.2** The fine-grained infidelity of the bucket-brigade QRAM with the planar layout scheme (Figure 6.7) scales as \(O(N\varepsilon_s + \sqrt{N} \log N\varepsilon_{cs})\).

*Proof.* Each query branch has circuit depth \(O(\sqrt{N})\) with there are \(O(\sqrt{N})\) SWAP gates and \(O(\log N)\) CSWAP routers. A similar argument to Lemma 6.3.1 yields the desired fine-grained infidelity.

Lemma 6.3.2 shows that infidelity scales linearly due to the presence of consecutive SWAP gates, as indicated by the vertices covered by red lines in Figure 6.7. Therefore, it is reasonable to explore strategies aimed at reducing the number of SWAP gates to improve the overall infidelity. One approach to accomplish this is by employing constant depth circuits for long-range operations between non-adjacent qubits.

There are multiple ways to implement a long-range SWAP between two qubits separated by a line of \(m\) qubits (e.g., a single red line in Figure 6.7). One is to use a strongly entangled length-\(m\) GHZ state on the latter as a resource and then performing a long range gate involving the qubits near the endpoint as shown in Ref. [27]. A length-\(m\) GHZ state is

\[
|GHZ\rangle = \frac{|0\rangle^\otimes m + |1\rangle^\otimes m}{\sqrt{2}}.
\] (6.1)

GHZ states of arbitrary length can be accomplished using a constant-depth circuit. Consequently, all the GHZ states utilized for the long-range SWAPs can be generated in place without incurring a substantial overhead. With such modification applied to the basic layout, the circuit depth is reduced from \(O(\sqrt{N})\) to \(O(\log N)\). The error contribution for using the GHZ states in this case is stated below.

**Lemma 6.3.3** For a given GHZ state of length \(m\), the probability that the long-range operation using the GHZ state produces the correct output is \(O((1 - \varepsilon_G)^m)\).

Lemma 6.3.3 shows that despite the constant depth of the quantum teleportation circuit, its error can increase with length of the GHZ state. Hence the infidelity can
be reduced by minimizing the total length of GHZ states used in each query path. Our layout in Figure 6.7 supports this as the total length in any query path scales sub-linearly as $O(\sqrt{N})$.

As this above method would still give a polynomial dependence on $N$ in the infidelity analysis, we also consider performing a long-range SWAP remote qubits using a Bell pair between them as a resource. To obtain a high quality Bell state, we use noisy Bell states, a quantum error correcting code and an entanglement distillation protocol as shown in [142, Section II.D].

**Lemma 6.3.4** Given an $[[\hat{n}, \hat{k}, \hat{d}]]$ quantum error correcting code and $\hat{n}$ noisy Bell pairs with initial error $\varepsilon_i$, there exists a distillation protocol that creates $\hat{k}$ Bell pairs with error $\varepsilon_f < \varepsilon_i$ where $\varepsilon_f = O(\varepsilon_i^d)$. Moreover, when $\varepsilon_i = O(m \cdot \varepsilon_G)$ and $\varepsilon_f < 1$ is a small constant, $d = O(\log m)$.

To perform a long-range SWAP, consider the Bell pair being created on adjacent qubits near the source qubit and one half of it is teleported to be adjacent to the target qubit using the length-$m$ GHZ state where $m = O(\sqrt{N})$ as per our layout. Then, from Theorem 6.3.3 these noisy Bell pairs could have an error $\varepsilon_i \leq O(\sqrt{N} \cdot \varepsilon_G)$ and it is possible to distill a Bell pair with constant error using say, the surface code, with distance $O(\log N)$. For this choice of code, the protocol to distill would have depth $O(d) = O(\log N)$ and the number of noisy Bell pairs used would be $\hat{n} = O(d^2) = O(\log^2 N)$. Combining the two methods together gives the following.

**Corollary 6.3.5** Given two qubits separated by $m$ qubits on a planar grid with local connectivity, GHZ qubit error $\varepsilon_G$ and the error on a distilled Bell pair $\varepsilon_f$, the error on performing a long-range operations between the two qubits is given by

$$\varepsilon_L := \min(m \cdot \varepsilon_G, \varepsilon_f). \quad (6.2)$$
In our discussion on entanglement distillation, we acknowledge that in the worst-case scenario, the depth may increase by a polylogarithmic factor. However, there might be strategies to mitigate this depth increase. Therefore, for the purposes of our analysis, we proceed under the assumption that long-range Bell states are readily available. Creating these long-range Bell paths could introduce a polylogarithmic overhead in the worst case, which is acceptable. The precise implications of this overhead can be explored in future research.

As in [71, Appendix A] we reiterate that the circuit depth $T$ scales as $O(\log N)$, contrary to the naive analysis which suggests that it scales as $O(\log^2 N)$. Crucially, observe that in the setting router status phase, it unnecessary to wait for a parent router’s status to be set before sending the next address qubit to set a child router’s status. In fact, regardless of a router’s depth, the address qubit to set its status can be routed into to the bucket-brigade QRAM a constant number of steps after the qubit to set its parent router’s status has routed in. This parallel procedure results in a desirable $O(\ell)$ time to set the status for the router at level $\ell$, leading overall to an $O(\log N)$ time complexity to set the status of all routers.

Understanding the activation sequence of routers in a query branch is beneficial. It helps comprehend the parallel address setting procedure we described earlier and reveals that not all qubits need to remain active throughout the entire query duration $T$. This property can be incorporated into the fine-tuned infidelity analysis for a tighter bound. Suppose we are given a fixed query branch of depth four, and such branch has routers $R_0, R_1, R_2, R_3$ counting from root to leaf. The naive activation sequence of each router and associated gates are depicted in Figure 6.8, in which the circuit depth $T_i$ increases a constant size hence $\sum_i T_i = O(\log^2(N))$.

By observing the naive activation sequence in Figure 6.8, it is natural to merge the time segment $T_i$ with its neighbors as shown in Figure 6.9. For any larger $i$, it is
Figure 6.8: The naive activation sequence. $T_i$ is the total time setting the address bit for router $R_i$. The green and blue dots indicate the router at the associated time step is in use. The solid rectangle represents a local SWAP operation over the qubits associated with the router, the circle represents a local CSWAP operation, and the dashed rectangle represents a GHZ teleportation swap between qubits associated with parent and child routers.

not hard to observe that each segment takes only a constant number of time steps, hence the total circuit depth is $O(\log N)$.

Figure 6.9: Improved activation sequence.

Theorem 6.3.6 For $N$ memory locations, the improved fine-grained infidelity of the bucket-brigade QRAM with planar layout (Figure 6.6) scales as

$$O \left( \log N \varepsilon_L + \log N \varepsilon_s + \log^2 N \varepsilon_{cs} + \log^2 N \varepsilon_I \right).$$

(6.3)

Proof. For a fixed query branch, we first consider the error contribution from the GHZ teleportation. The contribution of GHZ teleportation error to the probability of
a successful query is
\[ P_G = \prod_{\ell=1}^{\log N} (1 - \varepsilon_G)^{\sqrt{N}/2^{\ell/2}} (T - \ell) = (1 - \varepsilon_G)^{\Omega(\sqrt{N}T)}, \tag{6.4} \]

where \( \sqrt{N}/2^{\ell/2} \) is the number of GHZ qubit connecting \( R_{\ell} \) router to \( R_{\ell+1} \) router, and \( T - \ell \) is the number of times the teleportation happens. This pattern is also evident in Figure 6.9, where the occurrence of GHZ teleportation between \( R_1 \) and \( R_2 \) happens \( T \) times, while between \( R_2 \) and \( R_3 \) it happens \( T - 1 \) times.

Next, consider the error contribution from the local swap operation over qubits associated with individual routers. It can be observed from Figure 6.9 that it takes two local swap operations for the address setting of each router. Hence the contribution of local SWAP error to the probability of a successful query is
\[ P_s = (1 - \varepsilon_s)^{2T} = (1 - \varepsilon_s)^{\Omega(T)}. \tag{6.5} \]

The error contribution of the local CSWAP operation can be analyzed similarly, and its probability contribution toward success is
\[ P_{cs} = \prod_{\ell=1}^{\log N} (1 - \varepsilon_{cs})^{2\ell} = (1 - \varepsilon_{cs})^{\Omega(T^2)}. \tag{6.6} \]

Last, we consider the idling error of the status qubit \( t_{\ell} \) for each router \( R_{\ell} \). The status qubit differs from non-router status qubits or helper GHZ qubits. While those can be reset and remain irrelevant until their next usage, the status qubit must maintain its value immediately after its associated router’s address is settled. The idling time for each \( R_{\ell} \’s \) status qubit \( t_{\ell} \) is the total active time of the router minus the number of CSWAP operations over the qubits of \( R_{\ell} \), then from Figure 6.9 the total idling time for \( R_{\ell} \) is \( O(T - \ell) \). Therefore, the idling qubit error contribution toward total query success probability is
\[ P_I = (1 - \varepsilon_I)^{\Omega(T^2)}. \tag{6.7} \]
Since the total success probability is \( P = P_G \cdot P_s \cdot P_{cs} \cdot P_I \), combining Corollary 6.3.5 with a similar analysis in reference [71, Appendix D] with \( T = O(\log N) \), we obtain the desired infidelity.

![Diagram of a high-level scheme for accessing memory locations](image)

**Figure 6.10:** High-level scheme for 16 memory locations. The router setting shows an example of accessing memory location \( x_4 \).

### 6.3.3 Improve T Count with CNOT Tree

The bucket-brigade planar layout achieves sublinear infidelity, but its T count scales linearly with \( N \). In this section, we present a scheme that reduces the T count by replacing \( O(N) \) many CSWAP routers with CNOT routers that do not require the T gate for implementation.
The high-level router arrangement is depicted in Figure 6.10, with information flowing from top to bottom. Unlike the bucket-brigade model where the same path is used for the entire processes, the qubit routing-in and routing-out processes in this scheme utilize separate sets of routers. The routing-in procedure corresponds to the top half of the tree, while the routing-out procedure corresponds to the bottom half. The routing-in procedure adopts a similar approach to the bucket-brigade scheme but replaces all CSWAP routers beyond level $\frac{\log N}{2}$ with CNOT routers, as illustrated in Figure 6.11a. Each CNOT cluster distributes the same control qubit to its corresponding $\sqrt{N}$ memory locations. Likewise, in the routing-out procedure, the CSWAP routers at deeper levels are replaced by CNOT routers, as depicted in Figure 6.11c. The key distinction is that each CNOT routing-out cluster is linked to a memory location from every routing-in cluster.

![CNOT router circuit](image)

**Figure 6.11: CNOT router circuit.** (a) A single CNOT router for route-in that takes input qubit and sends it to all its child nodes. (b) Circuit for the CNOT router during route-in. (c) A single CNOT router for route-out. It is effectively an XOR gate. (d) Circuit for the CNOT router during route-out.

Now, we demonstrate the correctness of this scheme with the example depicted in Figure 6.10, where the target qubit $x_4$ is routed out. To activate the correct paths for
routing out the target qubit $x_4$ during the address setting phase, we set the CSWAP routers $R_0, R_1, R'_1,$ and $R'_0$ to the appropriate states based on the address bits $|0010\rangle$ associated with the memory location $x_4$. The activated paths are indicated by the green lines. In the routing-in phase, a control qubit $|1\rangle$ is routed from the top router $t_0$ to the first CNOT router $q_1$. Subsequently, the CNOT tree propagates the control qubit, activating all its child memory locations, namely $x_4$, $x_5$, $x_6$, and $x_7$. Note that only the activated memory locations (represented by the blue rectangle) pass down the information stored in their respective locations. Conversely, the inactivated memory locations (depicted by the red rectangle) pass down a $|0\rangle$ qubit to the CNOT routers. By observing the crossover arrangement of CNOT routers in the bottom half, it becomes apparent that each CNOT router at level $\log_2 N$ (namely, $q'_0$, $q'_1$, $q'_2$, and $q'_3$) is able to retrieve one unique $x_i$ from among the $\sqrt{N}$ activated memory locations. In the end, the correct qubit $x_4$ gets selected and routed out by the CSWAP routers $t'_1$ and $t'_0$.

Defining the query branch in this setting can be challenging, but it is evident that each query to memory location $x_i$ relies on the correct passage of qubits from the other $\sqrt{N} - 1$ memory locations which rely on their parent routers being correct. Moreover, it is not possible to have the same fractal pattern for routing out as we have for routing in. This is due to the fact that only the memory locations associated with the same routing-in CNOT cluster are in close proximity to each other within a distance of $N^{1/4}$. Memory locations from different routing-in CNOT clusters are separated by at least $\sqrt{N}$ distance. Therefore, attempting to bring them together using routing-out CNOT clusters would result in a teleportation error depending linearly on $N$, since the total GHZ qubit length is $N$. This argument implies a linear infidelity that we summarize in the next Corollary.
Corollary 6.3.7  The infidelity of QRAM with the planar layout scheme (Figure 6.10) scales as $O(N)$.

This scheme enhances the T count to $O(\sqrt{N})$, but the qubit count and infidelity stay at $O(N)$. As explained earlier, the primary reason for the linear increase in infidelity stems from the fact that the query’s success relies on a large number of memory locations, resulting in a $O(N)$ GHZ error during the routing-out phase. Therefore, an improved scheme design should minimize the correlation between multiple branches in the binary tree for a single query.

6.3.4 Improve Qubit Count with Tree Size Reduction

In this section, we present a scheme that achieves a sublinear qubit count. Figure 6.12 shows a high-level arrangement scheme in which $N$ memory locations are aligned in a square area of size $N$. During the routing-in phase, it requires a depth of $\frac{\log N}{2}$ CSWAP routers to transfer the control qubits to $q_i$. Similarly, during the routing-out phase, a second set of CSWAP routers with a depth of $\frac{\log N}{2}$ is used to retrieve the result qubits from $q'_i$. Each dashed colored box represents a GHZ state of length $\sqrt{N}$. These GHZ states are responsible for either dispersing the control qubit to its corresponding memory locations (vertical ones) or gathering output from memory locations (horizontal ones), similar to the functioning of a routing-out CNOT cluster described in Section 6.3.3. The circuit representing the vertical GHZ teleportation is illustrated in Figure 6.13. It demonstrates that a circuit of constant depth can successfully distribute the control qubit $q_1$ to its $\sqrt{N}$ associated memory locations $x_4, x_5, x_6$, and $x_7$. Similarly, a constant depth circuit can be employed for the horizontal GHZ teleportation process as well.
The GHZ teleportation circuits depicted in Figure 6.13 can maintain a constant depth. This is possible because the GHZ state of any length can be positioned parallel to its corresponding memory qubits. As a result, only a constant number of swap operations are required to transfer the control bit from the GHZ qubits to the memory qubits.

Upon initial observation of Figure 6.12, one might be tempted to consider it as an improvement over the scheme in Figure 6.10 in terms of infidelity, since the CNOT routers, which contribute to linear GHZ errors, are replaced by GHZ teleportation circuits of length $O(\sqrt{N})$. However, it is noteworthy that the positions of each memory
Figure 6.13: GHZ diffusion circuit. Example of passing the state of the \( q_1 \) router to all its children’s memory locations \( x_4, x_5, x_6, \) and \( x_7 \). The gate associated with each \( x_i \) is either a CNOT gate if the memory location \( x_i \) stores 1, or an identity gate otherwise.

location in this figure correspond to their respective positions on a planar surface. Therefore the physical distance from the root CSWAP router \( R_0 \) to the control qubit \( q_i \) is \( \sqrt{N} \). This distance incurs a GHZ teleportation error that scales with \( \sqrt{N} \). Moreover, the correctness of each \( q'_i \) depends on the correctness of all \( \sqrt{N} q_i \)'s. Consequently, this leads to a GHZ error that scales linearly with \( N \).

To inspire qubit usage reduction, we can ignore partial circuits without CSWAP routers and treat them as a black box (Figure 6.14). In the given scenario of \( N = 16 \) memory locations, each intermediate output \( q'_i \) relies on \( \sqrt{N} = 4 \) memory variables
and $\sqrt{N}$ control qubits $q_i$ as follows:

\[
q'_0 = q_0x_1 + q_1x_5 + q_2x_9 + q_3x_{13},
\]
\[
q'_1 = q_0x_2 + q_1x_6 + q_2x_{10} + q_3x_{14},
\]
\[
q'_2 = q_0x_3 + q_1x_7 + q_2x_{11} + q_3x_{15},
\]
\[
q'_3 = q_0x_4 + q_1x_8 + q_2x_{12} + q_3x_{16}.
\]

(6.8)

This implies that to obtain a single intermediate output $q'_i$, it is only necessary to synthesize a partial circuit linked to $\sqrt{N} x_i$'s. Additionally, to acquire all $q_i$'s, the partial circuit can be synthesized sequentially, thereby reducing the overall qubit cost, as depicted in Figure 6.15.

The high-level arrangement depicted in Figure 6.15 may appear to be optimal due to its $O(\sqrt{N})$ qubit count and T count, along with the fact that the GHZ teleportation
Figure 6.15: **Modified scheme to reduce qubit count.** The high-level router arrangement shown in Figure 6.12 is modified to incorporate $O(\sqrt{N})$ memory qubits at each round, with a total of $\sqrt{N}$ rounds.

Error scales with $\sqrt{N}$ when obtaining a single $q'_i$. However, this optimal outcome is only valid under the best-case scenario where only $q'_1$ is required. In the case of a superposition query, where all $q'_i$’s are generated sequentially, the idling error for the qubits holding the values of $q'_i$ will exhibit linear scaling.

**Corollary 6.3.8** *The infidelity of QRAM with the planar layout scheme (Figure 6.15) scales as $O(N)$.***

### 6.4 General QRAM Framework

In this section, we draw inspirations from Sections 6.3.3 and 6.3.4 that reduce T count and qubit count and adapt that to the bucket-brigade planar layout in Section 6.3.1 to obtain the most general framework. We first show the general framework that is robust against X error in Section 6.4.1, and then modify it in Section 6.4.2 to make it robust against any generic error with trade-offs in infidelity.
6.4.1 X Error Resilient Framework

The high-level layout is shown in Figure 6.16. The procedure consists of three stages: Stage I involves setting the address on linear routers, which are termed as such because they do not require branching out and can be arranged linearly in a line within the actual planar setting. During Stage II, the control \( q_i \) is diffused to memory locations whose output is added to the corresponding \( q'_i \) registers. This stage is repeated \( \sqrt{N} \) times, with different CSWAP gates applied to linear routers each time to obtain the appropriate \( q_i \) values. In Stage III, the remaining address bit is set on CSWAP routers, and the corresponding \( q'_i \) values are routed out. The value of \( q'_i \) in this context can be expressed as shown in Equation 6.8.

Before delving into the detailed construction and analysis of each stage, let’s summarize the high-level idea behind why this layout achieves optimal results:

- Unlike the high-level scheme shown in Figure 6.10, which employs a separate set of routers at a different location for the routing out procedure, the CSWAP routers replace CNOT routers \( R'_i \) in place in order to leverage the advantages provided by the fractal layout. This resolves the issue raised in Section 6.3.4, where the routing out procedure using CNOT routers fails to maintain the fractal layout utilized during the routing-in phase. Consequently, it leads to an \( O(N) \) infidelity originating from GHZ teleportation errors.

- This scheme differs from the one in Figure 6.15 by computing all \( q'_i \) concurrently in each round, resulting in idle time scaling as \( O(\sqrt{N}) \) instead of \( O(N) \).

In summary, this new scheme addresses the linear infidelity caused by large GHZ error and idling error discussed in Sections 6.3.3 and 6.3.4, while maintaining sublinear T count and qubit count. The remaining section provides a detailed implementation of each stage.
We first introduce the linear router, denoted by $R$, which differs from the branching SWAP router. It comprises two registers, $t$ and $in$, responsible for status storage and input reception from the parent node. Figure 6.17 illustrates the address bit routing procedure and the planar layout. In this stage, the depth of the linear routers is $\log_2 N$ for $N$ memory locations. This choice allows routing in half of the total $\log N$ address bits, resulting in $\sqrt{N}$ distinct $q_i$ for each round in stage II.

**Lemma 6.4.1** For each time step, let $\varepsilon_s, \varepsilon_I$ be the error of SWAP gate and router status qubit, respectively. For $N$ memory locations, the infidelity of stage I in Figure 6.16 scales as $O(\log^2 N\varepsilon_s + \log^2 N\varepsilon_I)$.

**Proof.** Figure 6.17 demonstrates that setting the address bit into the deepest router takes $\log_2 N + 1$ steps, while the second deepest router requires one less swap. Additionally, once activated, the router status qubit remains active for the entire session. As a result, the total success probability can be expressed as $(1 - \varepsilon_I)^{\Omega(\log^2 N)}(1 - \varepsilon_s)^{\Omega(\log^2 N)}$. Similar to the analysis in Ref. [71], we can derive the desired infidelity.

In stage II, the objective is to compute the intermediate values $q'_i$ through $\sqrt{N}$ repetitions. In each round $i$, the control qubit $q_i$ is set to $|1\rangle$ only when the decimal representation of the first half of the address bits matches $i$. These control qubits are then diffused across $\sqrt{N}$ memory locations, which subsequently send their values to the respective intermediate quantum register $q'_i$. To obtain the correct control qubit $q_i$ for each round, different gate sets are applied to the linear routers, as shown in Figure 6.18.

For each fixed control qubit $q_i$, it diffuses into $\sqrt{N}$ memory locations exactly the way shown in Figure 6.10 using the CNOT routers in Figure 6.11a. When $q_i = |0\rangle$, all the memory locations will output $|0\rangle$, and this value will be added to their corresponding intermediate register $q'$. On the other hand, when $q_i = |1\rangle$, the value
stored in each memory location will be added to $q'$. This addition operation can be achieved using a CNOT gate, where the output from the memory location serves as the control, and $q'$ acts as the target.

Ensuring that errors in the bad branch do not propagate into the good branch is critical since the entire proof of infidelity is built upon this assumption. While the CSWAP router has been shown to be robust against error propagation, we need to establish the same property for the CNOT routers used in this context. The robustness of the CNOT routers against Pauli $X$ errors in this setting is evident from Figure 6.19. It is important to highlight that while the Pauli $Z$ error cannot extend beyond the parent node in the CNOT router, it still presents a phase issue within this specific framework. This arises when the round of repetition matches the decimal representation of the fixed address bits, causing the introduction of a phase factor $-1$ whenever an odd number of $Z$ errors are present. A comparable scenario is also encountered in the scheme presented in Ref. [144, Section V], where the read-out CNOT tree demonstrates resilience to only Pauli $Z$ error.

**Lemma 6.4.2** Assume there is no Pauli $Z$ error in the CNOT tree. For $N$ memory locations, the infidelity of stage II in Figure 6.16 scales as $O(\log N \sqrt{N} \varepsilon_I + \log N \sqrt{N} \varepsilon_{cc} + \log N \sqrt{N} \varepsilon_c + \log N \sqrt{N} \varepsilon_L)$.

**Proof.** There is a total of $\sqrt{N}$ rounds. In each round, the linear router employs a depth of $O(\log N)$ CCNOT gates [17]. The CNOT tree utilizes GHZ qubits of length $O(N^{1/4} \log N)$ due to the fractal nature of the CNOT tree, as well as a similar analysis to Equation 6.4. Additionally, $O(\log N)$ CNOT gates are utilized. The idling time for each $q'_i$ is $O(\log N)$. Combining Corollary 6.3.5 and analysis in Ref. [71], we obtain the desired result.
In the last stage, the CNOT routers used in stage II can be turned into CSWAP routers in place to preserve the fractal layout. This procedure is the same as that of the basic layout shown in Section 6.3.1, hence the infidelity scaling analysis in Theorem 6.3.6 can be adopted here for a smaller memory size circuit.

**Corollary 6.4.3** For \( N \) memory locations, the infidelity of stage II in Figure 6.16 scales as \( O(\log N \varepsilon_L + \log N \varepsilon_s + \log^2 N \varepsilon_{cs} + \log^2 N \varepsilon_I) \).

**Proof.** Use Theorem 6.3.6 with memory size \( \sqrt{N} \).

Now we can bound the infidelity of the whole procedure.

**Theorem 6.4.4** Assume there is no Pauli Z error in the CNOT tree, for \( N \) memory location, the infidelity of QRAM with the layout scheme (Figure 6.16) scales as

\[
O \left( \log N \sqrt{N} (\varepsilon_L + \varepsilon_I + \varepsilon_c + \varepsilon_{cc}) + \log^2 N (\varepsilon_s + \varepsilon_{cs}) \right).
\]

(6.9)

**Proof.** Combining Lemmas 6.4.1, 6.4.2, and Corollary 6.4.3 yield the result.

The qubit count and T count for this scheme are both \( O(\sqrt{N}) \).

### 6.4.2 Generic Error Resilient Framework

In this section, we address the phase issue of the framework (Figure 6.16) in Section 6.4.1 and offer a remedy that preserves sublinear scaling of infidelity, qubit count, and T count.

Assuming only Pauli Z errors occur, the address \( a_i, i \in [\sqrt{N}] \), is fixed to the linear routers \( \mathcal{R} \). In stage II, there are \( \sqrt{N} \) rounds of repetition. For each round \( j \), denoted \( N_j \) the number of Pauli Z errors in the CNOT tree. During round \( i, j = i \), the intermediate value \( q' \) acquires a phase factor of \( (-1)^{N_j} \). This is because in round \( i \) the control qubit \( q_i = |1\rangle \), and the Z error becomes effective on CNOT routers set to
This kind of address-dependent error becomes problematic as discussed in [71]. In contrast, for the basic layout (Figure 6.6) discussed in Section 6.3.1, the presence of Z errors outside the query branch does not pose a problem. This is because the router status qubit is consistently set to $|0\rangle$ for all CSWAP routers that are not part of the query path, rendering any Z error ineffective in those cases.

The preceding analysis indicates that in order to prevent phase errors, it is necessary to designate the entire CNOT tree, where the root node captures the $|1\rangle$ qubit during the process, as part of the query branch, ensuring it remains Z error-free. However, if we require the entire CNOT tree in Figure 6.16 to be entirely Z error-free, the infidelity will exhibit a linear infidelity scaling due to the $\sqrt{N}$ repetitions over the $\sqrt{N}$-sized CNOT tree.

Hence, a viable approach would be to minimize the CNOT tree’s depth depicted in Figure 6.16 by substituting the upper tier of CNOT routers with CSWAP routers. Figure 6.20 showcases an instance of this layout, demonstrating that the address-specific phase error ceases to be an issue when the query branch is error-free. In a broader model with a memory size of $N$, where the address bit length is $n = \log N$, we define $d$ as the number of linear routers $R$, $d'$ as the depth of routing-in CSWAP routers $R$, $n - d - d'$ as the depth of the CNOT tree, and $n - d$ as the depth of the routing-out CSWAP routers. Our objective is to examine the optimal balance between $d$ and $d'$ that results in the most favorable infidelity, T count, and qubit count scaling. The detailed procedure for data lookup is shown in Algorithm 3.

**Theorem 6.4.5** Consider the QRAM with the high-level scheme in Figure 6.20 with $N$ memory locations. Let $n = \log N$, $\lambda = 2^{n-d}$ be the number of intermediate qubits $q_i$ updated each round in phase II, and $\gamma = 2^{n-d-d'}$ be the size of a CNOT tree. The
The infidelity of the QRAM is

\[
O \left( \varepsilon_L \left( \frac{\gamma N}{\lambda} + \frac{N}{\lambda} \log \frac{\lambda}{\gamma} \right) + \varepsilon_s \log \frac{\lambda^2}{\gamma} \right) \\
+ \varepsilon_I \left( \frac{N}{\lambda} \log N \log \frac{N}{\gamma} + \frac{\gamma N}{\lambda} \log N + \log \frac{N}{\gamma} + \log^2 \lambda \right) \\
+ \varepsilon_c \frac{\gamma N}{\lambda} + \varepsilon_{cc} \frac{N}{\lambda} \log N + \varepsilon_{cs} \left( \log^2 \frac{\lambda}{\gamma} + \log^2 \lambda \right) \right) .
\]

(6.10)

Moreover, the T count is \(O(\frac{N}{\gamma} + \frac{N}{\lambda} \log \frac{N}{\lambda} + \lambda)\), and qubit count is \(O(\log \frac{N}{\lambda} + \lambda)\).

**Proof.** First consider stage I, by Theorem 6.3.6 routing-in the address qubits for the CSWAP router has infidelity \(O(d^2 \varepsilon_I + d' \varepsilon_L + d' \varepsilon_s + d^2 \varepsilon_{cs})\). Then for stage II, the infidelity from the gate error is

\[
O \left( 2^d \left( \varepsilon_{cc} d + \varepsilon_L \left( d' + 2^{n-d-d'} \right) + \varepsilon_c 2^{n-d-d'} \right) \right) ,
\]

(6.11)

where the Toffoli gates in linear routers contribute to \(\varepsilon_{cc}\), a routing-in CSWAP path and a CNOT-tree contribute to \(\varepsilon_G\), and the CNOT tree also has CNOT gate error \(\varepsilon_c\). The infidelity from the idling error is

\[
O \left( 2^d \left( \varepsilon_I n \left( d + d' + 2^{n-d-d'} \right) \right) \right) ,
\]

(6.12)

where the terms correspond to the idling qubits in linear routers, CSWAP routers, and intermediate registers \(q'_i\), respectively. Last, for stage III, apply Theorem 6.3.6 we obtain the infidelity of the CSWAP tree as \(O((n-d)^2 \varepsilon_I + (n-d) \varepsilon_L + (n-d) \varepsilon_s + (n-d)^2 \varepsilon_{cs})\). Combining infidelity from all phases, and replacing \(d, d', n\) by \(N, \lambda, \gamma\) yields Equation 6.10.

The T count is

\[
O \left( 2^d(2^{d'} + d) + 2^{n-d} \right) ,
\]

(6.13)

where the second term comes from \(2^d\) repetitions of size \(2^{d'}\) CSWAP routers in stage II and the third term comes from a single run of size \(2^{n-d}\) CSWAP tree in stage III. Replacing \(d, d'\) and \(n\) yields \(O(\frac{N}{\gamma} + \frac{N}{\lambda} \log \frac{N}{\lambda} + \lambda)\) T count.
The depth $2^{n-d}$ CSWAP tree in stage III contributes to the qubit count

$$O(d + 2^{n-d}),$$

which yields $O(\log \frac{N}{\lambda} + \lambda)$ qubit count.

**Corollary 6.4.6** For $N$ memory locations, there exists a generic error-resilient planar QRAM scheme that has $\tilde{O}(N^{\frac{3}{4}})$ infidelity, $O(N^{\frac{3}{4}})$ $T$ count, and $O(\sqrt{N})$ qubit count scaling.

*Proof.* In the planar layout described by the high-level scheme depicted in Figure 6.20, we set $\lambda = \sqrt{N}$ and $\gamma = N^{1/4}$. By substituting these values into Theorem 6.4.5, we obtain the corresponding result.

Corollary 6.4.6 demonstrates that by carefully selecting values for $\lambda$ and $\gamma$, the planar layout depicted in Figure 6.20 can achieve sublinear scaling on infidelity, $T$ count, and qubit count. However, optimizing one aspect’s scaling may lead to less favorable scaling in the others. For instance, if we set $N$ as fixed and choose $\lambda \in [1, N]$ and $\gamma \in [1, \lambda]$, we can pursue infidelity optimization by selecting $\lambda = N$ and $\gamma = \sqrt{N}$. In this case, the infidelity will scale as $\tilde{O}(\sqrt{N})$, while $T$ count and qubit count will exhibit linear scaling, resulting in the same scenario as the basic planar case shown in Figure 6.6. On the other hand, if the goal is to achieve optimal $T$ count, we can set $\lambda = \gamma = \sqrt{N}$. However, this choice will lead to linear infidelity scaling due to the $\sqrt{N}$ repetition of the length $\sqrt{N}$ GHZ qubit shown in Figure 6.16.

### 6.5 Large Word Size

In classical memory architectures, the word size of RAM is typically designed to suit the system’s needs, often mirroring the size of the CPU’s general-purpose registers. This word size signifies the number of bits that can be fetched in a single operation.
Similarly, for quantum systems, our goal is for QRAM to permit access to multiple qubits simultaneously. In the subsequent section, we detail planar layouts for QRAM that exhibit optimal scaling with word size \( b \).

### 6.5.1 Parallel Multi-bit Readout

We can fan out the \( b \) words initially, prior to the introduction of the fractal tree structure, as depicted in Figure 6.21. The signal \( q_i \) is concurrently transmitted to all top-tier qubits \( q'' \) across all instances. Subsequent procedures align precisely with those elaborated in Section 6.4.2, for a single word size.

**Theorem 6.5.1** Consider the QRAM with the high-level scheme in Figure 6.21 with \( N \) memory locations. Let \( b = 2^{d''} \) be the word size, \( n = \log N, \lambda = 2^{n-d} \) be the number of intermediate qubits \( q'_i \) updated each round in phase II, and \( \gamma = 2^{2-d-d'} \) be the size of a CNOT tree. Also, let \( I, T, \) and \( Q \) be the infidelity, \( T \) count, and qubit count of the Pauli error-resilient scheme for the single-word readout in Theorem 6.4.5. The infidelity of the QRAM is \( O(bI) \). Moreover, the \( T \) count is \( O(bT) \), and qubit count is \( O(bQ) \).

**Proof.** Given the block setup for every word \( b \) as depicted in Figure 6.22, the extra GHZ qubits required to transmit the signal \( q_i \) to all \( q'' \) instances is \( O(b2^{n-d}) \). Let \( I_i \) represent the infidelity at stage \( i \) as described in Theorem 6.4.5. In Stage I, the infidelity is \( O(bI_1 + \epsilon_G b2^{2-n+d'}d') \), where the second term emerges from the GHZ error introduced while setting up \( b \) CSWAP router copies at a depth of \( d' \). Moving to Stage II, the infidelity is \( O(bI_2 + 2^d(\epsilon_G b2^{n-d})) \), where the second term is for the instances when the signal \( q_i \) is transmitted to all \( q'' \) counterparts, which occurs \( 2^d \) times. For Stage III, the infidelity remains consistent at \( O(bI_3) \). This is because each word remains in its specific block when the procedure is finished. Aggregating the
infidelities across these stages, we conclude that the total infidelity is $O(bI)$. as all extra GHZ errors get absorbed into $bI$.

The T count is $O(d2^d + b2^{d+d'} + b2^{n-d}) = O(bT)$ as compared with Equation 6.13, and the qubit count is $O(d + b2^{n-d}) = O(bQ)$ as compared to Equation 6.14.

6.5.2 Sequential Multi-bit Readout

**Theorem 6.5.2** Consider the QRAM with the high-level scheme in Figure 6.23 with $N$ memory locations. Let $b = 2^{d''}$ be the word size, $n = \log N$. Also, let $I$, $T$, and $Q$ be the infidelity, T count, and qubit count of the Pauli error-resilient scheme for the single-word readout in Theorem 6.4.5. The infidelity of the QRAM is $\tilde{O}(bI + b^2\epsilon_I)$. Moreover, the $T$ count is $O(T)$, and qubit count is $O(bQ)$.

**Proof.** Before reading out the $b$ memory bits, the analysis follows the same as in Theorem 6.4.5 which yields $O(bI)$ infidelity. There is an additional qubit idling error to be considered. It takes $O(2^{d''} + n - d + d'')$ time to transfer $b$ memory bits out sequentially. The idling qubits are the memory qubits and the CSWAP router status bits, hence the total idling error is $O(\epsilon_I(2^{d''} + d')(2^{d''} + n - d + d'') = \tilde{O}(b^2\epsilon_I)$. The number of CSWAP routers and linear routers is unchanged, hence the $T$ count is $O(T)$. The qubit count is magnified by a factor of $b$, hence the qubit count is $O(bQ)$.

6.6 Long-range Connections

We may allow only a few gates to be able to act on long-distance qubits. By having such an assumption, we will see prior arts with all-to-all connectivity are special cases of our general framework described in Section 6.4.
6.6.1 Bucket-brigade Model

First consider modifying the basic planar layout case in Section 6.3.1 with only CSWAP routers and SWAP gates. It can be observed that in the fractal design in Figure 6.7, for a given branch the number of swap gates connecting $\ell$-th to $\ell+1$-th level router is $O(\sqrt{N}/2^{\lceil k/2 \rceil})$. Suppose we allow the first $k \in \log N$ levels routers to be connected by long-range swap gates in the basic planar layout case in Figure 6.6. Then the depth of the circuit for a given query branch becomes $O(k + \sqrt{N}/2^{\lceil k/2 \rceil})$. This gives a natural transition from all-to-all connectivity to the nearest-neighbor connectivity, as for $k = 0$ the circuit depth is $O(\sqrt{N})$ and for $k = \log(N)$ the circuit depth becomes $O(\log N)$. Now we can have a modified version of Lemma 6.3.2 as follows.

**Corollary 6.6.1** For each time step, let $\varepsilon_s, \varepsilon_{cs}$ be the error of the SWAP gate and CSWAP router, respectively. Consider a basic planar layout with CSWAP routers and SWAP gates in Figure 6.6. Let long-distance swap gates connect the first $k$ level routers. Then the infidelity scales as

$$O \left( \left( k + \sqrt{N}/2^{\lceil k/2 \rceil} \right) \left( \log N \varepsilon_{cs} + \left( k + \sqrt{N}/2^{\lceil k/2 \rceil} \right) \varepsilon_s \right) \right).$$

(6.15)

**Proof.** For a given query branch, the number of CSWAP routers is $O(\log N)$ and the number of SWAP gates is $O(k + \sqrt{N}/2^{\lceil k/2 \rceil})$. The depth of the circuit is $O(k + \sqrt{N}/2^{\lceil k/2 \rceil})$. Using these facts and the same analysis of Lemma 6.3.2 yields the result.

From Corollary 6.6.1, on one end of the connectivity spectrum $k = 0$, it recovers the result in Lemma 6.3.2, and for the other extreme $k = \log N$, it yields $O(\log^2 N)$ infidelity scaling which is the main result in [71]. Similarly, if GHZ qubits are allowed, we can replace the first $k$ level of GHZ qubits by long-range swaps to have a modified version of Theorem 6.3.6.
Corollary 6.6.2 For each time step, let \( \varepsilon_G, \varepsilon_I, \varepsilon_s, \varepsilon_{cs} \) be the error of GHZ qubit, router status qubit, SWAP gate, and CSWAP gate, respectively. Let long-distance swap gates connect the first \( k \) level routers. For \( N \) memory locations, the improved fine-grained infidelity of the basic planar layout (Figure 6.6) scales as

\[
O \left( 2^{-\frac{k}{2}} \log N \sqrt{N \varepsilon_G} + \log N \varepsilon_s + \log^2 N \varepsilon_{cs} + \log^2 N \varepsilon_I \right). \tag{6.16}
\]

Proof. To obtain the result, follow the proof of Theorem 6.3.6 and adjust the initial value of \( \ell \) in Equation 6.4 from 1 to \( k \).

It is evident that when \( k \) equals zero, Corollary 6.6.2 yields the same outcome as Theorem 6.3.6. On the other hand, when \( k \) equals \( \log N \), the planar layout achieves the expected \( O(\log^2 N) \) infidelity scaling.

6.6.2 Generic Error Resilient Model

We also can replace the first \( k \) level of GHZ qubits with long-range swaps to have a modified version of Theorem 6.4.5.

Corollary 6.6.3 Consider the QRAM with the high-level scheme in Figure 6.20 with \( N \) memory locations. For each time step, let \( \varepsilon_G, \varepsilon_I, \varepsilon_s, \varepsilon_c, \varepsilon_{cc} \) be the error of GHZ qubit, qubit idling, SWAP gate, CNOT gate, and CCNOT gate respectively. Let \( n = \log N, \lambda = 2^{n-d} \) be the number of intermediate qubits \( q_i \) updated each round in phase II, and \( \gamma = 2^{2-d-d'} \) be the size of a CNOT tree. Let long-distance swap gates connect the first \( k \) level in the router tree. The infidelity of the QRAM is

\[
\tilde{O} \left( \varepsilon_G \left( 2^{-\frac{k}{2}} \sqrt{\lambda} + 2^{-\frac{k}{2}} \frac{N}{\sqrt{\lambda}} + \frac{\gamma N}{\lambda} \right) + \varepsilon_{cc} \frac{N}{\lambda} + \varepsilon_I \frac{\gamma N}{\lambda} + \varepsilon_s \frac{\gamma N}{\lambda} \right), \tag{6.17}
\]

195
for $k \leq d'$, and

$$
\tilde{O} \left( \varepsilon_G \left( 2^{-k} N + 2^{-\frac{k}{2}} \sqrt{\lambda} \right) 
+ \varepsilon_{cc} \frac{N}{\lambda} + \varepsilon_l \frac{\gamma N}{\lambda} + \varepsilon_r \frac{N}{\lambda} \right),
$$

(6.18)

for $d' < k \leq n - d$.

**Proof.** Combine Theorem 6.4.5 and Corollary 6.6.2.

Corollary 6.6.3 illustrates the challenging nature of achieving optimal scaling in various aspects by balancing the parameters $\lambda$ and $\gamma$ with a long-range budget of $2^k$. It becomes apparent that striking the perfect balance is a formidable task, since a trade-off inevitably arises among infidelity, T count, and qubit count, which must be determined based on the specific resource constraints within the given application. We now examine the ranges for $d$, $d'$, and the long-range budget $2^k$ that yield meaningful scalings.

<table>
<thead>
<tr>
<th>$d'$</th>
<th>0</th>
<th>$n/8$</th>
<th>$2n/8$</th>
<th>$3n/8$</th>
<th>$4n/8$</th>
<th>$5n/8$</th>
<th>$6n/8$</th>
<th>$7n/8$</th>
<th>$n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$n$</td>
<td>$7n/8$</td>
<td>$3n/4$</td>
<td>$5n/8$</td>
<td>$n/2$</td>
<td>$n/2$</td>
<td>$n/2$</td>
<td>$n/2$</td>
<td>$n/2$</td>
</tr>
<tr>
<td>$n/8$</td>
<td>$n$</td>
<td>$7n/8$</td>
<td>$3n/4$</td>
<td>$5n/8$</td>
<td>$9n/16$</td>
<td>$9n/16$</td>
<td>$9n/16$</td>
<td>$9n/16$</td>
<td>$9n/16$</td>
</tr>
<tr>
<td>$2n/8$</td>
<td>$n$</td>
<td>$7n/8$</td>
<td>$3n/4$</td>
<td>$5n/8$</td>
<td>$5n/8$</td>
<td>$5n/8$</td>
<td>$5n/8$</td>
<td>$5n/8$</td>
<td>$5n/8$</td>
</tr>
<tr>
<td>$3n/8$</td>
<td>$n$</td>
<td>$7n/8$</td>
<td>$3n/4$</td>
<td>$11n/16$</td>
<td>$11n/16$</td>
<td>$11n/16$</td>
<td>$11n/16$</td>
<td>$11n/16$</td>
<td>$11n/16$</td>
</tr>
<tr>
<td>$4n/8$</td>
<td>$n$</td>
<td>$7n/8$</td>
<td>$3n/4$</td>
<td>$3n/4$</td>
<td>$3n/4$</td>
<td>$3n/4$</td>
<td>$3n/4$</td>
<td>$3n/4$</td>
<td>$3n/4$</td>
</tr>
<tr>
<td>$5n/8$</td>
<td>$n$</td>
<td>$7n/8$</td>
<td>$13n/16$</td>
<td>$13n/16$</td>
<td>$13n/16$</td>
<td>$13n/16$</td>
<td>$13n/16$</td>
<td>$13n/16$</td>
<td>$13n/16$</td>
</tr>
<tr>
<td>$6n/8$</td>
<td>$n$</td>
<td>$7n/8$</td>
<td>$7n/8$</td>
<td>$7n/8$</td>
<td>$7n/8$</td>
<td>$7n/8$</td>
<td>$7n/8$</td>
<td>$7n/8$</td>
<td>$7n/8$</td>
</tr>
<tr>
<td>$7n/8$</td>
<td>$n$</td>
<td>$15n/16$</td>
<td>$15n/16$</td>
<td>$15n/16$</td>
<td>$15n/16$</td>
<td>$15n/16$</td>
<td>$15n/16$</td>
<td>$15n/16$</td>
<td>$15n/16$</td>
</tr>
<tr>
<td>$n$</td>
<td>$n$</td>
<td>$n$</td>
<td>$n$</td>
<td>$n$</td>
<td>$n$</td>
<td>$n$</td>
<td>$n$</td>
<td>$n$</td>
<td>$n$</td>
</tr>
</tbody>
</table>

**Table 6.3:** Infidelity scaling for $N = 2^n$ with $k = 0$. $d$ and $d'$ subject to the constraint $d + d' \leq n$. In this context, the green region corresponds to the parameter values of $d$ and $d'$, resulting in an $O(N^{3/4})$ T count. The red region corresponds to the regime associated with the basic planar case as elucidated in Figure 6.6.

We investigate infidelity scaling from Table 6.3 to Table 6.7 by examining the equilibrium between $d$ and $d'$ while incrementally increasing the long-range budget.
from 0 to $2^{d'}$. This approach allows us to retrieve the infidelity results for the fundamental planar layout case (Figure 6.6), as demonstrated in Table 6.3, where only nearest neighbor connectivity is permitted, and to obtain infidelity scalings reported in previous studies [71, 100], as depicted in Table 6.7, where all-to-all connectivity is fully established. We found that within the realm of $\tilde{O}(N^{3/4})$ T count, represented by the green region in Table 6.3 to 6.7:

1. When $d'$ is relatively small, specifically when $d' \leq n/4$, the presence of long-range connectivity does not enhance infidelity. This is because the primary source of error originates from the CNOT tree section of the circuit.

2. Any further improvement in infidelity becomes unattainable when $k$ exceeds $d'/2$. This is because, when $k > d'/2$, the predominant factor contributing to the error is the idling error by Eqn. 6.17.

3. The greater the value of $d'$ that can be accommodated, the more favorable the infidelity scaling becomes. This is because larger values of $d'$ serve to diminish both the GHZ error and the idling error for the CNOT tree.

4. Increasing the value of $d$ leads to a more favorable qubit count, as the qubit count scales as $O(2^{n-d})$. However, this sets up a trade-off between selecting a larger value of $d$ for improved qubit count or a larger value of $d'$ for reduced infidelity within the $O(N^{3/4})$ T-count regime.

Extending the analysis naturally allows the initial $k$ levels in the route-in procedure to access the long-range gate, while permitting the final $k'$ levels in the route-out procedure to also utilize the long-range gate. In a practical context, this can be likened to having a long-range budget of $2^{d+k}$ for the route-in and a long-range budget of $2^{k'}$
for the route-out process. The objective is to strike a balance between the values of \( k \) and \( k' \) in order to attain the most favorable scaling of infidelity.

We can briefly argue that it is not useful to separately consider \( k \) vs. \( k' \) in the regime that yields sublinear infidelity and T count. This is because the GHZ error from route-out only dominates that of route-in when \( k > 2d \), at which point a non-zero \( k' \) is required to suppress the GHZ error from the route-out procedure. However, we observed that \( k \) is only meaningful for \( k \leq \frac{d'}{2} \), and it only improves the infidelity for cases where \( d \leq \frac{d'}{2} \), a scenario where it is impossible to have \( k > 2d \).

<table>
<thead>
<tr>
<th>( d )</th>
<th>( d' )</th>
<th>0</th>
<th>n/8</th>
<th>2n/8</th>
<th>3n/8</th>
<th>4n/8</th>
<th>5n/8</th>
<th>6n/8</th>
<th>7n/8</th>
<th>n</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>n</td>
<td>n</td>
<td>7n/8</td>
<td>3n/4</td>
<td>5n/8</td>
<td>n/2</td>
<td>27n/64</td>
<td>13n/32</td>
<td>25n/64</td>
<td>3n/8</td>
</tr>
<tr>
<td>n/8</td>
<td>n</td>
<td>7n/8</td>
<td>3n/4</td>
<td>5n/8</td>
<td>n/2</td>
<td>31n/64</td>
<td>15n/32</td>
<td>29n/64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2n/8</td>
<td>n</td>
<td>7n/8</td>
<td>3n/4</td>
<td>5n/8</td>
<td>n/2</td>
<td>35n/64</td>
<td>17n/32</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3n/8</td>
<td>n</td>
<td>7n/8</td>
<td>3n/4</td>
<td>41n/64</td>
<td>5n/8</td>
<td>39n/64</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4n/8</td>
<td>n</td>
<td>7n/8</td>
<td>3n/4</td>
<td>45n/64</td>
<td>11n/16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5n/8</td>
<td>n</td>
<td>7n/8</td>
<td>25n/32</td>
<td>49n/64</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6n/8</td>
<td>n</td>
<td>7n/8</td>
<td>27n/32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7n/8</td>
<td>n</td>
<td>59n/64</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>n</td>
<td>n</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 6.4:** Infidelity scaling for \( N = 2^n \) with \( k = 1/4d' \).

<table>
<thead>
<tr>
<th>( d )</th>
<th>( d' )</th>
<th>0</th>
<th>n/8</th>
<th>2n/8</th>
<th>3n/8</th>
<th>4n/8</th>
<th>5n/8</th>
<th>6n/8</th>
<th>7n/8</th>
<th>n</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>n</td>
<td>n</td>
<td>7n/8</td>
<td>3n/4</td>
<td>5n/8</td>
<td>n/2</td>
<td>3n/8</td>
<td>5n/16</td>
<td>3n/8</td>
<td>n/4</td>
</tr>
<tr>
<td>n/8</td>
<td>n</td>
<td>7n/8</td>
<td>3n/4</td>
<td>5n/8</td>
<td>n/2</td>
<td>13n/32</td>
<td>3n/8</td>
<td>11n/32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2n/8</td>
<td>n</td>
<td>7n/8</td>
<td>3n/4</td>
<td>5n/8</td>
<td>n/2</td>
<td>15n/32</td>
<td>7n/16</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3n/8</td>
<td>n</td>
<td>7n/8</td>
<td>3n/4</td>
<td>5n/8</td>
<td>9n/16</td>
<td>17n/32</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4n/8</td>
<td>n</td>
<td>7n/8</td>
<td>3n/4</td>
<td></td>
<td></td>
<td>21n/32</td>
<td>5n/8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5n/8</td>
<td>n</td>
<td>7n/8</td>
<td>3n/4</td>
<td></td>
<td></td>
<td>23n/32</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6n/8</td>
<td>n</td>
<td>7n/8</td>
<td></td>
<td></td>
<td></td>
<td>13n/16</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7n/8</td>
<td>n</td>
<td>29n/32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>n</td>
<td>n</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 6.5:** Infidelity scaling for \( N = 2^n \) with \( k = 1/2d' \).
Table 6.6: Infidelity scaling for $N = 2^n$ with $k = 3/4d'$. 

<table>
<thead>
<tr>
<th>$d$</th>
<th>$d'$</th>
<th>0</th>
<th>$n/8$</th>
<th>2$n/8$</th>
<th>3$n/8$</th>
<th>4$n/8$</th>
<th>5$n/8$</th>
<th>6$n/8$</th>
<th>7$n/8$</th>
<th>$n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$n$</td>
<td>7$n/8$</td>
<td>3$n/4$</td>
<td>5$n/8$</td>
<td>$n/2$</td>
<td>3$n/8$</td>
<td>$n/4$</td>
<td>11$n/64$</td>
<td>$n/8$</td>
<td></td>
</tr>
<tr>
<td>$n/8$</td>
<td>$n$</td>
<td>7$n/8$</td>
<td>3$n/4$</td>
<td>5$n/8$</td>
<td>$n/2$</td>
<td>3$n/8$</td>
<td>9$n/32$</td>
<td>15$n/64$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2$n/8$</td>
<td>$n$</td>
<td>7$n/8$</td>
<td>3$n/4$</td>
<td>5$n/8$</td>
<td>$n/2$</td>
<td>25$n/64$</td>
<td>11$n/32$</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3$n/8$</td>
<td>$n$</td>
<td>7$n/8$</td>
<td>3$n/4$</td>
<td>5$n/8$</td>
<td>$n/2$</td>
<td>29$n/64$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4$n/8$</td>
<td>$n$</td>
<td>7$n/8$</td>
<td>3$n/4$</td>
<td>5$n/8$</td>
<td>9$n/16$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5$n/8$</td>
<td>$n$</td>
<td>7$n/8$</td>
<td>3$n/4$</td>
<td>43$n/64$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6$n/8$</td>
<td>$n$</td>
<td>7$n/8$</td>
<td>25$n/32$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7$n/8$</td>
<td>$n$</td>
<td>57$n/64$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$n$</td>
<td>$n$</td>
<td>$n$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 6.7: Infidelity scaling for $N = 2^n$ with $k = d'$. The orange cell represents the domain linked to the all-to-all connectivity QRAM case explored in Ref. [17], while the blue cells pertain to the look-up table as detailed in Ref. [100].
Figure 6.16: The conditional optimal layout. The conditional optimal layout for the high-level router arrangement uses linear routers ($R$), CSWAP routers ($R'$), and CNOT routers (+) for $N = 16$ and $i \in \{0, 1, 2, 3\}$. 
Figure 6.17: Linear router layout. (a) A high-level scheme for two linear routers. (b) Circuit for routing in the address bit into linear routers. (c) A planar layout of linear routers.

Figure 6.18: Linear router circuit. (a) The linear routers $R_0$ and $R_1$ are configured based on the value of address bits which are set to $|00\rangle$. (b) In round 0, a specific set of multi-control CNOT gates is applied to ensure that the control qubit $q_0$ is set to $|1\rangle$. A detailed implementation of the multi-control CNOT gate can be found in Ref. [17, Section 3A]. (c) The circuit outputs $q_i = |0\rangle$ for all $i \neq |00\rangle$. 

201
Figure 6.19: Pauli error propagation. (a) Pauli $X$ error does not propagate from the bad branch (red) to the good branch (blue) in the CNOT router. (b) Pauli $Z$ error does propagate into the parent register from a child branch in the CNOT router.
**Algorithm 3** Pseudocode for data lookup on memory of size $N$ with partition size $\lambda$, CNOT tree size $\gamma$

**Setup:** classical database data of size $N$ with $n = \log_2 N$, memory partition $\lambda \leq N$ with $d = \log_2 \left( \frac{N}{\lambda} \right)$ and CNOT tree size $\gamma \leq \lambda$ with $d' = \log_2 \left( \frac{\lambda}{\gamma} \right)$.

**Input:** state $|a\rangle$ where $a = a_0 \ldots a_{n-1}$ is an address of length $n$.

**Output:** state $|a\rangle|\text{data}[a]\rangle$ where $\text{data}[a]$ refers to the data at address $a$.

**Stage I:**
1: Initialize all qubits of the quantum lookup table to 0.
2: for $k$ in $0 \ldots d - 1$ do
3: \hspace{1em} Set $a_k$ as the status of the linear router $R_k$.

**Stage II:**
4: for $i$ in $0 \ldots 2^d - 1$ do
5: \hspace{1em} if $i = a_0 \ldots a_{d-1}$ then
6: \hspace{2em} Set $q_i \leftarrow |1\rangle$
7: \hspace{1em} else
8: \hspace{2em} Set $q_i \leftarrow |0\rangle$
9: \hspace{1em} Set the status of the CSWAP routers based on address bits $a_d \ldots a_{d+d'-1}$
10: Route $q_i$ along the query path determined by the CSWAP routers.
11: Propagate $q_i$'s signal to the $\gamma$ leaves $c_0, \ldots, c_{\gamma-1}$ of the CNOT tree attached to the last CSWAP router.
12: for $j$ in $0 \ldots \lambda - 1$ do
13: \hspace{1em} Apply unitary $U_{\lambda' + j}$ where $U_{\lambda' + j} = \text{CNOT}|c_j\rangle|y_j\rangle$ if $\text{data}[\lambda' i + j] = 1$ and $I$ otherwise.
14: \hspace{1em} Apply CNOT$|y_j\rangle|q'_j\rangle$.
15: \hspace{1em} Reset all qubits $c_j$, $y_j$, and those in the CNOT tree to 0.
16: Route $q_i$ back up the CSWAP routers to its original location.
17: Reset the status of CSWAP routers and $q_i$ to 0.

**Stage III:**
18: Set the status of $\log_2(\gamma)$ CSWAP routers based on address bits $a_{d+d'} \ldots a_{n-1}$.
19: Route $q'_\ell$ along the query path determined by the CSWAP routers to the output register where $\ell \equiv a \pmod{\frac{N}{\lambda}}$. 

---

203
Figure 6.20: **Generic optimal scheme.** The Pauli error resilient layout is an improvement over the scheme in Figure 6.16. In this case, $N = 16$, $n = 4$, $i \in \{0, 1, 2, 3\}$, the linear circuit depth $d = 2$, routing-in CSWAP router is depth $d' = 1$, and the CNOT router depth is $n - d - d' = 1$. Suppose in this example $x_0$ is being queried, then the address bit $|a_3a_2a_1a_0\rangle = |0000\rangle$, $|R_0\rangle = |a_0\rangle$, $|R_1\rangle = |a_1\rangle$, $|R'_0\rangle = |R'_0\rangle = |a_2\rangle$, and $|R'_1\rangle = |a_3\rangle$. The number of repetitions of Stage II is $2^{n-d}$. The colored line is an example of the query branch.
Figure 6.21: Parallel read out. A high-level scheme for parallel readout of word size $b = 2$, an extension to the scheme in Figure 6.20.

Figure 6.22: Planar layout for parallel read out. A planar layout designed for resilience against Pauli errors with a word size of $b = 6$. Each square, labeled by $q''_i$, encompasses the full fractal planar layout as depicted by the tree in Figure 6.21. The red line indicates the alignment of GHZ qubits responsible for diffusing the signal $q_i$ to all $q''$ instances.
Figure 6.23: Sequential read out. A high-level scheme for sequential readout of word size $b = 2$, an extension to the scheme in Figure 6.20.
[1] Scott Aaronson and Yaoyun Shi. Quantum lower bounds for the collision and

Johnson, Sam Morley-Short, Sam Pallister, Alasdair Price, and Stasja Stanisic. 


[4] Andrei Alexandru, Paulo F. Bedaque, Siddhartha Harmalkar, Henry Lamm,
Scott Lawrence, and Neill C. Warrington. Gluon field digitization for quantum
114501.

10.1103/PhysRevLett.123.090501.

of digitized qcd: Glueballs in a s (1080) gauge theory. *Physical Review D*, 105


[14] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell,


[56] Alicja Dutkiewicz, Barbara M Terhal, and Thomas E O’Brien. Heisenberg-
limited quantum phase estimation of multiple eigenvalues with few control


[59] H. Flyvbjerg. CHARACTER TABLE FOR THE 1080 ELEMENT POINT

[60] Henrik Flyvbjerg. Group Space Decimation:: A Way to Simulate QCD by
the 1080 Element Subgroup of SU(3)? *Nucl. Phys.*, B243:350–364, 1984. doi:
10.1016/0550-3213(84)90033-6.


of $\mathbb{Z}(N)$ Lattice Gauge Theory With Generalized Actions in Four Space-time
90217-1.


[93] Tongyang Li and Xiaodi Wu. Quantum query complexity of entropy estimation. 

[94] Lin Lin and Yu Tong. Heisenberg-limited ground-state energy estimation for 

[95] P. Lisboa and Christopher Michael. Discrete Subsets of SU(3) for Lattice Gauge 

[96] Daniel Litinski and Naomi Nickerson. Active volume: An architecture for 
efficient fault-tolerant quantum computers with limited non-local connections. 

Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Con-
ference on the Theory and Applications of Cryptographic Techniques, Darm-
stadt, Germany, May 19-23, 2019, Proceedings, Part III, pages 189–218, 
978-3-030-17659-4_7.

[98] Seth Lloyd, Masoud Mohseni, and Patrick Rebentrost. Quantum algorithms for 
2013.

[99] Guang Hao Low and Isaac L Chuang. Hamiltonian simulation by qubitization. 

for dirty qubits in state preparation and unitary synthesis. arXiv preprint 


