ABSTRACT

Title of Dissertation: NEW DIRECTIONS FROM OLD CODES

Nolan J. Coble
Doctor of Philosophy, 2025

Dissertation Directed by: Professor Alexander Barg
Department of Electrical & Computer Engineering
Institute for Systems Research

Professor Matthew Coudron
Department of Computer Science

Reed–Muller (RM) codes form a classic family studied for its interesting algebraic and combinatorial properties as well as from the perspective of information transmission. They achieve Shannon capacity of the basic binary channel models such as channels with independent erasures or flip errors. They have numerous applications to the theory of computational complexity and have well-understood local testability. They also give rise to a family of quantum codes admitting transversal logical operators in increasing levels of the Clifford hierarchy, a property of codes considered necessary for future fault-tolerant quantum computations.

In this dissertation, we show that, despite decades of research surrounding RM codes, new directions sprouting from their simple definition continue to be possible. We will begin by considering an alternate description of RM codes in terms of faces of the Boolean hypercube, and will see that by replacing the hypercube with a more general algebraic object we obtain a large class of previously undiscovered classical error-correcting codes sharing many structural properties with RM codes. These classical codes directly lead to an even larger class of new quantum error-correcting codes with explicitly determined parameters; we will demonstrate that these quantum codes admit many natural transversal logical gates. We finish by specializing to the class of quantum Reed–Muller codes and provide a complete characterization of the logic implemented by these transversal operators, yielding a broad generalization of prior work on the subject.

NEW DIRECTIONS FROM OLD CODES

by

Nolan J. Coble

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2025

Advisory Committee:
Professor Alexander Barg, Chair/Advisor
Professor Matthew Coudron, Co-Advisor
Professor Andrew Childs
Professor Runzhou Tao
Professor Lawrence Washington

Dedication

For my parents.

Acknowledgments

My sincere thanks go first to my advisors, Alexander Barg and Matthew Coudron. To Sasha, thank you for your boundless enthusiasm, support, and love for academic research. You have been immensely helpful at every step and have taught me so much about coding, as well as (perhaps unsuccessfully) the difference between “that” and “which”. I aspire to have as meaningful an impact in my own research areas as you have had in yours. To Matt, thank you for taking me on as your first PhD student at Maryland and for involving me in a project that took me from knowing nothing about quantum computing to feeling confident in my ability to carry out original research in the field. I also thank the remaining members of my committee— Runzhou Tao, Larry Washington, and Andrew Childs (whom I also had the pleasure of TAing for)— for taking time out of their busy schedules to be part of this process. I am grateful to Ann G. Wylie, whose dissertation fellowship supported me during my final semester.

There are many graduate students and postdocs I have relied on throughout my time at Maryland, and without their support I would not have been successful in this endeavor.

To Anna Emenheiser, my best friend and roommate for over four years, thank you for tolerating my endless complaints and rants, for always offering your honest feedback and opinions, and for filling my life outside of school with friendship, laughter, and support. You have been there for me through all the ups and downs over the years, and I will be forever grateful.

To Yusuf Alnawakhtha, from the moment I met you I knew we would be lifelong friends. You are perhaps the kindest person I know, and I cherish the many conversations (and occasional disagreements) we have had about life, quantum computing, and everything in between. I will greatly miss your habitual visits to my office and seeing you wandering the halls of the Atlantic building, lost in thought.

To Srilekha Gandhari, I am deeply grateful for your support and friendship over the years. I could not have asked for a better office mate, and though my frequent interjections may have pulled you away from your research more times than you would have liked, I truly appreciate your willingness to drop everything and lend an ear to my ramblings.

To Christopher Kang, from our first hang in the art galleries of Park City to our entire afternoon roaming the SF Exploratorium, we've always been able to have a great time together. You've become one of the most central friends in my life, and I am excited to see our careers in quantum computing, and our friendship, continue to grow.

To Manasi Shingane, with whom I don't think it's possible to share a dull moment, I will miss interrupting you in your office and arguing about commitments to quantum states from QPCPs. Just know that if you ever need some dal, my freezer is always open.

To Elizabeth Bennewitz, we have already enjoyed many memorable adventures together and I cannot wait for the mischief we will undoubtedly get up to in the years ahead. I only wish we had become friends sooner.

To Dominik Hangleiter, a true espresso connoisseur who taught me the importance of a good afternoon break, thank you for your endless optimism and grounding presence. Time spent with you invariably lifted my spirits, and I will always appreciate how you helped me come out of my shell and feel genuinely more at ease with the social side of conferences.

To Ethan Dudley, the impact of your presence throughout the pandemic and the virtual year of school cannot be measured in any σ-algebra I know. Thank you for being the first friend I made in Maryland.

Many thanks go to Andrea Svedja for her support with numerous administrative matters, and to Daniel Serrano for his career advice and support through both the TREND REU in 2019 and the

MathQuantum fellowship in my last two years at UMD. To everyone else I interacted with at UMD and QuICS, of whom there are far too many to thank individually, I greatly value the roles you have played in my life and in my PhD experience.

I had the great fortune of spending extended time at two workshops during my PhD. For my stay at the Park City Mathematics Institute, where many good times were had at the No Name Saloon, shout outs go to Jon Nelson, Amin Shiraz Gilani, Joel Rajakumar, Benjamin Anker, and Jack Morris. And at the Simons Institute at UC Berkeley, where the foundation for the research in this dissertation was laid, thanks go to William Kretschmer, Justin DuRant, Chris Pattison, and Krystal Maughan. Thank you as well to the many others who made my time at these workshops all the more enjoyable.

I owe a great debt to the faculty members who taught me during my undergraduate education at SUNY Brockport for cultivating the roots of my scientific knowledge. To Eric Monier and Zachary Robinson, I hope you are pleased that, despite my love for abstract mathematics, I remain motivated in research by the physical world around me. To Sanford Miller and Nathan Reff, thank you for showing me the beauty and joy of mathematics, and to Nate in particular for introducing me to algebraic coding theory, the field in which this dissertation is based.

My acknowledgments would not be complete without mentioning the endless support I have received from my family throughout this academic journey, support that has been truly foundational to any success I have had. To my parents, Jason and Lisa, thank you for raising me to be the person I am today and for consistently encouraging me to grow into the best version of myself. Mere words could never express the love and gratitude I have for you. To my older brother, Nathan; my grandparents, Janice, Roberta, Robert, and Joseph; and my many aunts, uncles, cousins, and extended family, thank you for your unwavering belief in me. I hope that I have made all of you proud, and that my accomplishments serve as a reflection of the person I have become because of you.

Table of Contents

Chapter 1: Introduction

The theory of error-correcting codes underpins much of classical and quantum information theory, and forms an integral part of combinatorics and applied algebra. From their inception as a means to reliably transmit information, error-correcting codes have become indispensable tools even in more abstract realms such as computational complexity theory and quantum computation. Reed–Muller (RM) codes, first introduced in 1954 by David E. Muller, are among the oldest infinite families of codes and remain among the most ubiquitous. Though they were first described over 70 years ago, they continue to be a fruitful source of research and insight.

The utility of RM codes arises from their rich algebraic and combinatorial structure [MS77, AK98]. For instance, while it has long been known that the general affine group forms the automorphism group of RM codes [MS77], only recently was the doubly transitive action of this group exploited to prove that RM codes achieve the Shannon capacity of the binary symmetric channel [KKM+15, RP23, AS23]. Regarding more computational properties, RM codes are known to be locally testable [AKK+05], with an optimal local tester constructed via a geometric interpretation of the codes [BKS+10]. This local testability property was crucial in the original proof of the celebrated PCP Theorem in computational complexity theory [AS92, ALM+98]. Even in the relatively young field of quantum error correction, the algebraic structure of RM codes has proven useful in demonstrating that quantum RM codes admit transversal logical gates in increasing levels of the Clifford hierarchy [BCHK25, RCNP20, HLC21, HLC22a, RCNP20]—a property considered crucial for future fault-tolerant quantum computational protocols.

This dissertation is motivated by two main questions:

1. Can the structure of RM codes be extended to new codes that share many of their hallmark properties?

2. Can this structure be exploited when studying quantum versions of these codes?

We are certainly not the first to consider these questions, and many generalizations and variations of RM codes have been studied, e.g., [Sor91, ACLN21, NK23]. Nevertheless, we show that a remarkably simple extension— one that has not been previously explored— gives rise to a broad class of structurally similar codes. Regarding the second question, while quantum RM codes are already known for their role in fault-tolerant quantum computation, this dissertation substantially extends known results on their logic and demonstrates that analogous properties hold for the new quantum codes we construct.

A key insight of this work is that many properties of the RM family can be understood in purely geometric and group-theoretic terms via the Boolean hypercube. In particular, faces of the hypercube can be used to construct the RM codes. Coxeter groups [AB08, BB05], which are generated by reflections and which generalize the symmetric group and $\mathbb{Z}_2^m$, possess a natural combinatorial geometry closely mirroring that of the hypercube. By replacing faces of the hypercube with standard cosets of a Coxeter group, we obtain a direct analog of RM codes in a vastly more general setting. The main technical contributions of this dissertation are as follows:

1. We show that the (binary) order-r Reed–Muller code of length 2^m, $RM(r, m)$, typically defined using m-variate polynomials of degree at most r, can be expressed in terms of indicator functions

of dimension-$(m-r)$ faces of the Boolean hypercube. This geometric reformulation yields a new perspective on their duality, inclusion, and multiplication properties.

2. By replacing the group $\mathbb{Z}_2^m$—the domain of the functions used to define RM codes—by an arbitrary rank-m finite Coxeter group W, we construct a new family of binary linear codes. We prove that these *Coxeter codes*, $C(r,m)$, parameterized by a natural number $r \in \mathbb{N}$, satisfy:

   (Nesting) If $q < r$ then $C(q,m) \subseteq C(r,m)$.

   (Duality) $C(r,m)^{\perp} = C(m-r-1,m)$.

   (Multiplication) $C(r_1,m) \odot C(r_2,m) \subseteq C(r_1+r_2,m)$, where $\odot$ denotes the entrywise (Schur) product of bit strings.

   (Group codes) $C(r,m)$ is a left ideal in the group algebra $\mathbb{F}_2 W$.

   We construct an explicit basis for $C(r,m)$, which yields a basis for the coset $C(r,m)/C(q,m)$ for any $q < r$; we compute the dimension of $C(r,m)$ in terms of so-called "W-Eulerian numbers"; and we study the rate and distance of these codes. The majority of this work was presented in [CB25], which was presented at the 2025 IEEE International Symposium on Information Theory and will appear in an upcoming issue of *Designs, Codes and Cryptography*, contingent on minor revision.

3. Using the CSS construction of quantum codes, we employ pairs of Coxeter codes $C(q,m) \subseteq C(r,m)$ to define *quantum Coxeter codes*, whose spaces of X- and Z-stabilizers and logical operators are all governed by classical Coxeter codes. We derive explicit parameters for all such codes [CB25].

4. We define a natural class of transversal operators for the family of quantum Coxeter codes, which we call *coset operators*, as they act on qubits indexed by standard cosets of the given Coxeter group. We give necessary and sufficient conditions for when such operators either (1) implement nontrivial logical operations, (2) act as the logical identity, or (3) fail to preserve the code space of a quantum Coxeter code. These operators can perform logic in increasing levels of the Clifford hierarchy. These results generalize and unify the work completed in [BCHK25, CB25].

5. In the special case of quantum RM codes, these coset operators act on faces of the Boolean hypercube, with the conditions for logical action depending only on the dimension of the face being acted upon. For quantum RM codes, we prove a full combinatorial description of the logical circuits implemented by these operations. In particular, such *subcube* (or face) operators implement circuits of multi-controlled-Z gates whose control structure can be computed directly from the combinatorial description of the face on which they act. Unlike prior works, which studied only global transversal operators, we demonstrate that quantum RM codes admit a large set of logical operators that act on strict subsets of both the logical and physical qubits of the code. This result forms the bulk of the work [BCHK25], which will appear in an upcoming issue of the *IEEE Transactions on Information Theory*.

The framework of Coxeter codes provides a new lens for constructing and studying error-correcting codes via the geometry of reflection groups. It connects ideas from algebraic coding theory, combinatorial group theory, and quantum information, and suggests natural directions for further generalization. These constructions may also lead to new approaches for implementing fault-tolerant quantum logic that exploit group-theoretic symmetries.

Other works This dissertation expands and combines two works by the author [BCHK25, CB25]. Earlier works for which the author was a main contributor include: a classical algorithm for simulating certain restricted quantum circuits [CC22], appearing in the proceedings of the 2021 IEEE Symposium on Foundations of Computer Science; constructions of local Hamiltonians whose low-energy spaces contains no stabilizer states [CCNN23], appearing in the proceedings of the 2023 Theory of Quantum Computation, Communication and Cryptography conference; and a preprint proving that the local Hamiltonians of the previous work satisfy the much stronger property that their low-energy states require a linear number of T gates [CCNN24].

1.1 Reed–Muller Codes

The standard definition of (binary) RM codes is as the set of truth tables, or *evaluation vectors*, of multi-variate polynomials of a maximum degree:

Definition 1.1.1 (Standard definition of RM codes)**.** Let $r \leq m$ be non-negative integers. The order-r Reed–Muller code of length 2^m is defined as evaluations of all Boolean polynomials in m variables with degree at most r:

$$RM(r,m) := \left\{ \mathrm{eval}(f) \in \mathbb{F}_2^{2^m} \;\middle|\; f(x_1,\ldots,x_m) = \sum_{\substack{K \subseteq \{1,\ldots,m\} \\ |K| \leq r}} c_K x_K,\, c_K \in \{0,1\} \right\},$$

where monomials are denoted by $x_K := \prod_{i \in K} v_i$ for $K \subseteq \{1,\ldots,m\}$, and $\mathrm{eval}(f) \in \mathbb{F}_2^{2^m}$ is the vector with entries given by $(f(v_1,\ldots,v_m))_{v \in \mathbb{Z}_2^m}$.[1]

It should be evident that one basis for RM codes comes from the monomial functions x_K where

[1] By convention, $x_\emptyset = 1$.

$K \subseteq [m] := \{1, \ldots, m\}$ and $|K| \leq r$. RM codes are also generated by another, less obvious, collection of functions which we refer to as signed monomials. A degree-r signed monomial is a product $\prod_{i \in J} w_i$, where $|J| = r$, each $w_i \in \{x_i, \bar{x}_i\}$ and $\bar{x} := 1-x$ denotes the negation of the variable. Clearly any degree-r signed monomial is a polynomial with degree at most r, and it is relatively straightforward to inductively show that any polynomial with degree at most r can be written as a sum of signed monomials with degree *exactly* equal to r. Viewing the domain of m-variate Boolean functions as the m-dimensional (Boolean) hypercube shows that signed monomial functions carry a certain *geometric* structure, which we now detail.

Consider the the group $\mathbb{Z}_2^m$ generated by the set of bit strings of Hamming weight one (the standard basis), denoted below by $S = \{e_i\}_{i=1}^m$, where $e_i = (e_{j,1}, \ldots, e_{j,m})$ with $e_{ji} = \delta_{ji}$ for all $j \in [m]$.[2] The m-dimensional hypercube is a graph with vertices indexed by elements of $\mathbb{Z}_2^m$, and where two vertices are connected by an edge whenever they differ in precisely one coordinate, i.e., when they differ by an element of S. The m-dimensional hypercube is composed of many sub-hypercubes, or simply *subcubes*, with dimensions $\leq m$:

Definition 1.1.2. (Subcubes of the hypercube)

- A *standard subcube* of the m-dimensional hypercube is a subgroup of the form $\langle J \rangle$, where $J \subseteq S$ is a subset of generators. That is, bit strings in $\langle J \rangle$ are precisely those whose support lies entirely within the set J, viewed as a subset of $[m]$.

- A *subcube* is any coset of a standard subcube, i.e., subsets of $\mathbb{Z}_2^m$ of the form $A := z + \langle J \rangle$ for some $z \in \mathbb{Z}_2^m$. The set J is called the *type* of A[3] and the cardinality $|J|$ is called its *dimension*.

[2]We will frequently abuse notation by referring to the sets S and $[m]$ interchangeably. For example, if we write "take $i \in S$", this should be interpreted to mean "take $e_i \in S$ and $i \in [m]$".

[3]Note that the bits appearing outside of J form an invariant of a subcube A of type J: given two bit strings $y, z \in x + \langle J \rangle$, $y_i = z_i$ for every $i \in S \setminus J$.

We write $A \sqsubseteq \mathbb{Z}_2^m$ to indicate that the subset A is a subcube, and by an i-*cube* we mean any $A \sqsubseteq \mathbb{Z}_2^m$ with $\dim A = i$.

It is straightforward to verify that the signed monomial $\bar{x}_K := \prod_{i\in K} \bar{x}_i$ is precisely the indicator function of the standard subcube $\langle S \setminus K\rangle$, and the standard monomial x_K is the indicator function of the subcube $1^m + \langle S \setminus K\rangle$, where 1^m is the all ones bit string. More generally, there is an equivalence between indicator functions of $(m-r)$-cubes and degree-r signed monomials,

$$\mathbb{1}_{z+\langle J\rangle} \leftrightarrow \prod_{i\in S\setminus J} w_i, \quad \text{where } w_i := \begin{cases} x_i & z_i = 1 \\ \\ \bar{x}_i & z_i = 0 \end{cases},$$

where for a subset $U \subseteq \mathbb{Z}_2^m$, $\mathbb{1}_U(z) = 1$ if $z \in U$ and equals 0 otherwise.

In light of the discussion following Definition 1.1.1, we have the following alternate form of RM codes:

Definition 1.1.3 (Alternate definition of RM codes)**.** Let $r \leq m$ be non-negative integers. The order-r Reed–Muller code of length 2^m is defined as the $\mathbb{F}_2$-linear span of evaluations of indicator functions corresponding to $(m-r)$-cubes:

$$RM(r,m) := \mathrm{Span}_{\mathbb{F}_2}\left\{ \mathrm{eval}(\mathbb{1}_A) \in \mathbb{F}_2^{2^m} \;\middle|\; A \sqsubseteq \mathbb{Z}_2^m,\ \dim A = m-r \right\}. \tag{1.1}$$

Equivalently, $RM(r,m)$ is the $\mathbb{F}_2$-linear span of evaluations of degree-$(m-r)$ signed monomials.

We note that Theorem 13.12 in [MS77] states that the set of indicators of $(m-r)$-dimensional flats in the affine geometry $AG(m,2)$ generates the code $RM(r,m)$; Definition 1.1.3 states that $(m-r)$-cubes— a strict subset of $(m-r)$-flats— are sufficient to generate all of $RM(r,m)$.

A simple change to Eq. (1.1) will yield a new family of classical codes, which ultimately share many basic properties with RM codes.

1.2 A New Extension

Many of the basic structural properties of RM codes—containment, duality, multiplication—typically viewed as deriving from the polynomial definition, likewise arise from the alternative definition of RM codes in terms of subcubes given in Definition 1.1.3. For example, $(m-r)$- and $(r+1)$-dimensional subcubes of an m-dimensional hypercube necessarily intersect on an even number of elements, suggestive of the duality $RM(r,m)^{\perp} = RM(m-r-1,m)$. This combinatorial structure is shared by every member of a large family of well-studied groups known as *Coxeter groups*.

Like $\mathbb{Z}_2^m$, a Coxeter group W is generated by a special set of "reflections", $S = \{s_i\}_{i=1}^m$ where each s_i is an involution. The formal definition of a Coxeter group is given in Definition 2.6.1, but for now it will suffice to consider a (finite) group W generated by such an S. Generalizing subcubes of $\mathbb{Z}_2^m$, a *standard coset*[4] is any coset $w\langle J\rangle$ of a subgroup generated by elements of the special generating set, $J \subseteq S$. The *rank* of a standard coset is the number of elements generating it, $\operatorname{rank}(w\langle J\rangle) = |J|$.

Consider now the group algebra $\mathbb{F}_2W := \{f : W \to \mathbb{F}_2\}$ of binary-valued functions on W, and let $\mathbb{1}_U \in \mathbb{F}_2W$ denote the indicator function of a subset $U \subseteq W$. By replacing the group $\mathbb{Z}_2^m$ by an arbitrary Coxeter group W, we obtain our main definition:

Definition 1.2.1 (Coxeter codes)**.** Let $r \leq m$ be non-negative integers. The order-r Coxeter code of type (W,S), denoted by $\mathsf{C}_W(r)$, is the length-$|W|$ defined as the $\mathbb{F}_2$-linear span of evaluations of

[4]The usage of the word "standard" here is not related to its usage in "standard subcubes"; this is to reflect standard terminology in the theory of Coxeter groups.

indicator functions corresponding to standard cosets of rank equal to $(m-r)$:

$$\mathsf{C}_W(r) := \operatorname{Span}_{\mathbb{F}_2}\left\{ \operatorname{eval}(\mathbb{1}_{w\langle J\rangle}) \;\middle|\; w \in W, J \subseteq S, |J| = m-r \right\}.$$

Remark 1.2.2.

- The code $\mathsf{C}_W(r)$ depends on the particular choice of S; we suppress this dependence in the notation for simplicity.
- For $\mathbb{Z}_2^m$ with its standard generating set, the order-r Coxeter code of type $(\mathbb{Z}_2^m, S_m)$ is the code $RM(r,m)$ from Definition 1.1.3.
- The definition allows for the case $r = -1$, yielding the trivial code. For every Coxeter group: $\mathsf{C}_W(-1) = \{0^{|W|}\}$ is a trivial code (given by an empty generating set), $\mathsf{C}_W(0)$ is a repetition code, $\mathsf{C}_W(m-1)$ is a single parity-check code, and $\mathsf{C}_W(m) = \mathbb{F}_2 W$ is the entire vector space. ◁

Several well-known structural results about the RM family extend to *any* Coxeter code. First, Coxeter codes are a nested family of codes:

Theorem 1.2.3. *For integers $q < r \leq m$, the order-q Coxeter code of type (W,S) is strictly contained in the order-r code:*

$$\mathsf{C}_W(q) \subsetneq \mathsf{C}_W(r).$$

Like RM codes, Coxeter codes are also closed under duality:

Theorem 1.2.4. *The dual of the order-r Coxeter code of type (W,S) is the corresponding order-$(m-r-1)$ Coxeter code:*

$$\mathsf{C}_W(r)^{\perp} = \mathsf{C}_W(m-r-1).$$

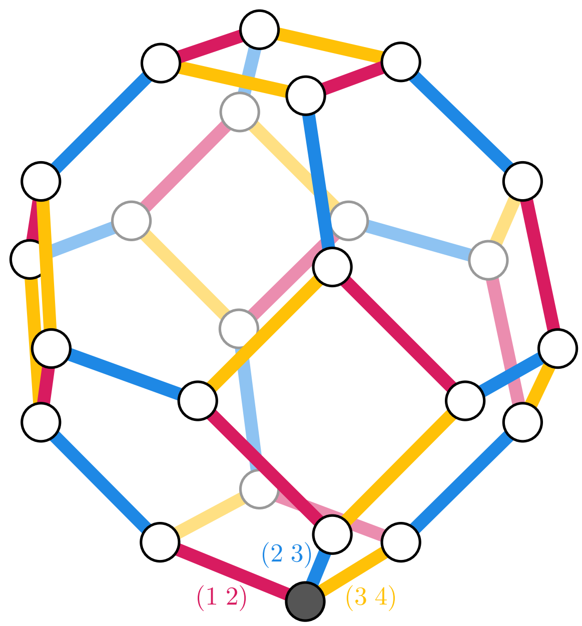


Figure 1.1: A useful way to visualize a Coxeter system (W, S) is a *Cayley graph*, (V, E), where $V = W$ and $(w, w') \in E$ iff there is a generator $s \in S$ such that $w' = ws$. The figure shows the Cayley graph of the 4-letter symmetric group, A_3, with generators given by adjacent transpositions. The shaded vertex represents the identity element. The polytope obtained by embedding this graph in $\mathbb{R}^3$ is called a *permutohedron*.

For two vectors $x, y \in \mathbb{F}_2^n$, their coordinate-wise (Schur) product is a vector $x \odot y = (x_i y_i, i = 1, \dots, n)$, and this definition extends to a product of subsets. RM codes satisfy a multiplication property: for any r_1, r_2,

$$RM(r_1, m) \odot RM(r_2, m) \subseteq RM(r_1 + r_2, m)$$

with $RM(r^*, m) := \mathbb{F}_2^{2^m}$ for all $r^* \geq m$. This follows since the product of two polynomials of degree r_1 and r_2 has degree at most $r_1 + r_2$. This multiplication property is a general feature of all Coxeter codes:

Theorem 1.2.5. *For $r_1, r_2 \in \{-1, \dots, m\}$, the Coxeter codes of type (W, S) and orders r_1 and r_2 satisfy*

$$\mathsf{C}_W(r_1) \odot \mathsf{C}_W(r_2) \subseteq \mathsf{C}_W(r_1 + r_2),$$

where by convention $\mathsf{C}_W(r^*) := \mathbb{F}_2 W$ for all $r^* \geq m$.

Lastly, Coxeter codes are (left) ideals in the group algebra, or *group codes* in the sense of Berman [Ber67].[5] Recall that multiplication in $\mathbb{F}_2 W$ is given by the convolution of functions, denoted by $f * g$.

Theorem 1.2.6. *For every $f \in \mathbb{F}_2 W$, $f * \mathsf{C}_W(r) \subseteq \mathsf{C}_W(r)$.*

While Theorems 1.2.3, 1.2.5 and 1.2.6 can be proved using standard tools from group theory and the definition of Coxeter codes, the route we take here is to construct an explicit basis for every Coxeter code from which these results all follow:

Theorem 1.2.7 (Informal version of Theorems 3.1.6 and 3.2.1)**.** *Let W be an arbitrary Coxeter group generated by the m-element set S. There are (explicitly defined) collections of vectors $\{\mathcal{B}_i\}_{i=0}^m$, $\mathcal{B}_i \subseteq \mathbb{F}^{|W|}$, for which $\bigcup_{i \geq m-r} \mathcal{B}_i$ is a basis for the order-r Coxeter code of type (W, S). The size of each $\mathcal{B}_i$ corresponds to a well-known combinatorial quantity known as the i-*th W-Eulerian number*, $|\mathcal{B}_i| = \left\langle {W \atop i} \right\rangle$, so that $\dim \mathsf{C}_W(r) = \sum_{i=0}^r \left\langle {W \atop i} \right\rangle$ is explicitly computable for every r, W.*

For simplicity, we will delay the definitions of this basis and the W-Eulerian numbers until after we have formally defined Coxeter groups. See Sections 2.6 and 3.1.

1.3 Quantum Codes with Transversal Logic

Designing fault-tolerant quantum logic is central to constructing scalable and reliable quantum computers. While early work has shown that storing quantum information is feasible at reasonably low resource costs [ABO97, KLZ98, Kit97], efficiently performing universal fault-tolerant logic remains a challenge. The need for such techniques is exacerbated by recent experimental progress on stor-

[5] Note a recent paper that extends RM codes [NK23] titled *Berman codes*, which is not related to our construction.

ing information [BEG+24, AABA+24, DSRABR+24] and performing rudimentary logic [BEG+24, RABB+24, RAC+24].

The leading methods for scalable fault tolerance utilize *quantum error-correcting codes*. Similar to their classic counterparts, the premise of quantum error-correcting codes is to embed some small number $\kappa \in \mathbb{N}$ of *logical* qubits into the space of $n > \kappa$ *physical* qubits. This is, in theory, done is a way that the logical space is protected from minor errors on the physical space. To be more precise, recall that the space of n qubits is given by the n-fold tensor product of $\mathbb{C}^2$. A quantum error-correcting code of dimension K and length n is a subspace $\mathcal{C} \subseteq (\mathbb{C}^2)^{\otimes n}$ with $\dim \mathcal{C} = K$. For most codes of interest, $K = 2^\kappa$ is a power of 2 for some $\kappa \in \mathbb{N}$, and we say that $\mathcal{C}$ encodes κ logical qubits into n physical qubits.

A variety of code-theoretic approaches to fault-tolerance have been proposed [BKS21], such as code switching and deformation [PR13, ADP14], and magic state distillation and injection [BK05, BH12, CH17b, YHH+23]. Most relevant to our work is the concept of *transversal logical gates*, tensor products of single-qubit operators which preserve the code space, i.e., $U \coloneqq \bigotimes_{i=1}^n U_i$, $U_i \in \mathrm{U}(2)$, for which $U\mathcal{C} \subseteq \mathcal{C}$. Such operators allow us to manipulate the logical state of a quantum code in a way that minimizes the spread of single-qubit noise affecting physical qubits, and are also useful toward other methods of fault tolerance such as magic state distillation. Studying any of these methods ultimately requires an intimate understanding of quantum codes and their logical operators. For example, the geometric or algebraic structure of specific families of codes is often exploited when constructing transversal logic for the codes [ZCC11, BK13, PY15, JOKY18, YTC16]. Contributing to this line of work, we construct a new family of quantum codes from a pair of classical Coxeter codes and, by leveraging the combinatorial structure of Coxeter groups, we derive a large class of transversal operators that can act non-trivially on these quantum Coxeter codes.

As before, consider a finite Coxeter group W generated by a set of m involutions S. Index a set of $|W|$ qubits by the elements of W. We define a quantum Coxeter code by constructing mutually commuting sets of $|W|$-qubit Pauli X and Z type operators, where $X := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, and $Z := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

Definition 1.3.1 (Quantum Coxeter codes)**.** Let $0 \leq q \leq r \leq m$ be non-negative integers. The order-(q, r) *quantum Coxeter code* of type (W, S), denoted by $\mathsf{QC}_W(q, r)$, is defined as the common $+1$ eigenspace of a Pauli stabilizer group $\langle \mathcal{S}_X, \mathcal{S}_Z \rangle$, with stabilizer generators given by

$$\mathcal{S}_X := \left\{ X_{w\langle J \rangle} \;\middle|\; w \in W, J \subseteq S, |J| = m - q \right\}, \tag{1.2}$$

$$\mathcal{S}_Z := \left\{ Z_{w\langle J \rangle} \;\middle|\; w \in W, J \subseteq S, |J| = r + 1 \right\}. \tag{1.3}$$

That is, $\mathsf{QC}_W(q, r)$ is given by

$$\mathsf{QC}_W(q, r) := \left\{ |\psi\rangle \in (\mathbb{C}^2)^{\otimes |W|} \;\middle|\; P\,|\psi\rangle = |\psi\rangle \text{ for all } P \in \mathcal{S}_X \cup \mathcal{S}_Z \right\}.$$

Showing that elements of $\mathcal{S}_X$ and $\mathcal{S}_Z$ always commute amounts to showing that the intersection of any rank-$(m - q)$ and rank-$(r + 1)$ standard coset always contains an even number of elements, a fact which easily holds for any Coxeter group. Of course, the above definition combined with the fact $X^2 = Z^2 = \mathbb{I}$ implies that the X and Z stabilizer spaces of $\mathsf{QC}_W(q, r)$ are isomorphic to the codes $\mathsf{C}_W(q)$ and $\mathsf{C}_W(m - r - 1)$, respectively. In this way, one also sees via Theorems 1.2.3 and 1.2.4 that the elements of $\mathcal{S}_X$ and $\mathcal{S}_Z$ must commute: the dual space of $\mathsf{C}_W(m - r - 1)$ (corresponding to Pauli X operators that commute with all of $\mathcal{S}_Z$) contains every X stabilizer since $\mathsf{C}_W(m - r - 1)^\perp = \mathsf{C}_W(r) \supseteq \mathsf{C}_W(q)$.

One result of our work on classical Coxeter codes is an explicit formula for the parameters of a quantum Coxeter code.

Theorem (Theorem 4.1.1)**.** *The quantum Coxeter code* $\mathsf{QC}_W(q,r)$ *encodes* $\sum_{i=q+1}^{r} \left\langle {W \atop i} \right\rangle$ *logical qubits into* $|W|$ *physical qubits, and has minimum distance equal to* $2^{\min(q+1,m-r)}$.

While we haven't explicitly defined the minimum distance of a code, it essentially corresponds to the smallest number of non-identity Pauli operators needed to take one $|\psi\rangle \in \mathsf{QC}_W(q,r)$ to a different $|\xi\rangle \in \mathsf{QC}_W(q,r)$, and is thus a measure of the error-resilience of a code.

In the same way that transversal operators on standard cosets of particular ranks generate the Pauli stabilizers for $\mathsf{QC}_W(q,r)$, operators on standard cosets of other ranks generate the groups of *logical* X and Z operators for $\mathsf{QC}_W(q,r)$. Building upon this idea, we will construct transversal logical operators formed of diagonal Z rotations acting on standard cosets. We consider the single-qubit gates

$$Z(k) = |0\rangle\langle 0| + e^{i\frac{\pi}{2^k}} |1\rangle\langle 1|\,, \quad k \geq 0,$$

where $Z(0) = Z$, $Z(1) = S$, $Z(2) = T$, etc. These gates also correspond with increasing levels of the *Clifford hierarchy*.

In Section 4.2, we will construct certain transversal operators $\widetilde{Z}(k)_A$ which act as either $Z(k)$ or $Z(k)^\dagger$ on the qubits in a standard coset A, and as identity elsewhere. Our main result on the transversal logic of quantum Coxeter codes clarifies necessary and sufficient conditions for when these $\widetilde{Z}(k)_A$ operators implement logic on $\mathsf{QC}_W(q,r)$. We delay the explicit definition of $\widetilde{Z}(k)_A$ until after we have given preliminaries on Coxeter groups. We ultimately prove the following:

Theorem (Informal version of Theorem 4.2.3)**.** *Let* $0 \leq q \leq r \leq m$ *be non-negative integers and consider the quantum Coxeter code* $\mathsf{QC}_W(q,r)$*. Suppose* A *is a standard coset of* W*.*

1. *If the rank of A is $\geq (k+1)r+1$, then the operator $\widetilde{Z}(k)_A$ implements a logical identity on the code space, i.e., for every $|\psi\rangle \in \mathsf{QC}_W(q,r)$, $\widetilde{Z}(k)_A|\psi\rangle = |\psi\rangle$.*

2. *If the rank of A is $\geq q+kr+1$ and $\leq (k+1)r$, then the operator $\widetilde{Z}(k)_A$ implements a non-trivial logical operation on the code space, i.e., $\widetilde{Z}(k)_A\mathsf{QC}_W(q,r) = \mathsf{QC}_W(q,r)$, but there is some $|\psi\rangle \in \mathsf{QC}_W(q,r)$ for which $\widetilde{Z}(k)_A|\psi\rangle \neq |\psi\rangle$.*

3. *If the rank of A is $\leq q+kr$, then the operator $\widetilde{Z}(k)_A$ does not preserve the code space, i.e., there is some $|\psi\rangle \in \mathsf{QC}_W(q,r)$ for which $\widetilde{Z}(k)_A|\psi\rangle \notin \mathsf{QC}_W(q,r)$.*

While this result implies the existence of certain logical operators, a priori it says little about what logic they actually implement on the code space. In the next section we return to Reed–Muller codes, where $W = \mathbb{Z}_2^m$, and will demonstrate a relatively simple combinatorial characterization of the implemented logical circuits in this case.

1.4 Logic in Quantum RM Codes

Quantum RM codes have been a popular candidate for implementing universal quantum computation ever since their introduction a quarter century ago in the work of Steane [Ste99]. The standard definition of quantum RM codes uses the Calderbank-Shor-Steane (CSS) construction to design a family of qubit codes with the embedded structure of two classical RM codes, $RM(q,m) \subseteq RM(r,m)$ with the property that $q \leq r \leq m$. For our purposes, we will simply define the quantum RM family directly as an example of a quantum Coxeter code.

Consider the m-dimensional Boolean hypercube with vertices indexed by elements of $\mathbb{Z}_2^m$, which represents a set of 2^m physical qubits. Quantum RM codes are defined by three parameters: m, the dimension of the hypercube of physical qubits, q, the codimension of the X stabilizers, and r, where

$r + 1$ is the dimension of the Z stabilizers:

Definition 1.4.1 (Quantum RM codes)**.** Let $0 \le q \le r \le m$ be non-negative integers. The *quantum Reed–Muller code* of order (q, r) and length 2^m, denoted by $QRM_m(q, r)$, is defined as the common $+1$ eigenspace of a Pauli stabilizer group $\mathcal{S} := \langle \mathcal{S}_X, \mathcal{S}_Z \rangle$, with stabilizer generators given by

$$\mathcal{S}_X := \left\{ X_A \;\middle|\; A \text{ is an } (m-q)\text{-cube} \right\}, \tag{1.4}$$

$$\mathcal{S}_Z := \left\{ Z_A \;\middle|\; A \text{ is an } (r+1)\text{-cube} \right\}, \tag{1.5}$$

These codes encode $\kappa = \sum_{i=q+1}^{r} \binom{m}{i}$ logical qubits into $n = 2^m$ physical qubits and have distance $d = 2^{\min(q+1, m-r)}$. Readers familiar with hypercube codes will recognize them as a particular case of this code family given by $QRM_m(0, 1)$. Stabilizer generators for $QRM_4(0, 2)$ are shown in Fig. 1.2.

Quantum RM codes have many variations, e.g., qudit codes [SK05], entanglement-assisted

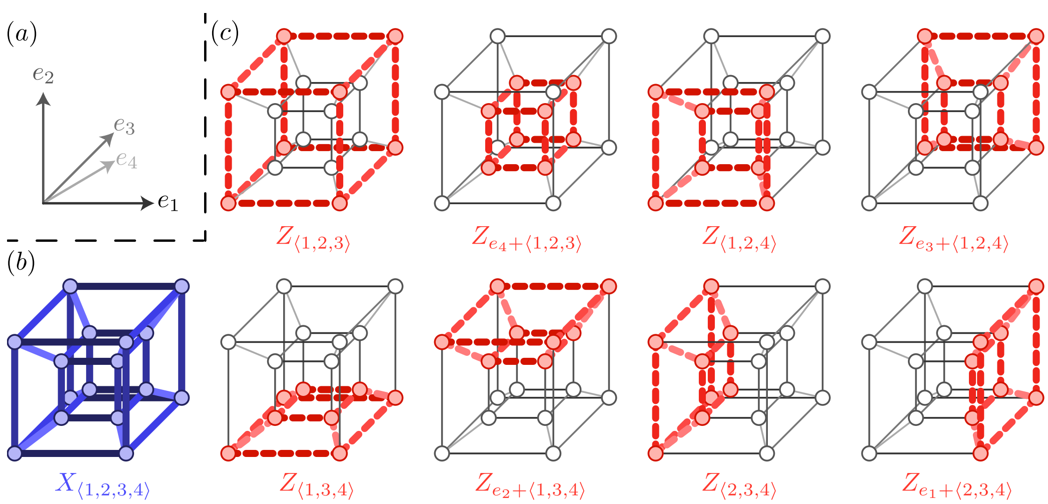


Figure 1.2: Stabilizer generators for the code $QRM_4(0, 2)$. By definition, every $(r + 1) = 3$ cube defines a Z stabilizer and the unique $(m - q) = 4$-cube (i.e., the entire hypercube) defines the only X stabilizer. (a) Orientation of the 4-cube. (b) Global X is the only X stabilizer, by definition, represented here by the (blue) solid cube. (c) The (red) dashed cubes indicate the 8 subcubes in the 4-dimensional hypercube that define the Z stabilizer generators of the code.

RM codes [NJBG24], pin codes [VB22]. Interestingly, quantum RM codes and their descendants can fault-tolerantly realize non-Clifford logic: for example, morphed/punctured codes can realize T gates transversally [BMD07, Ter15, KB15, VK22a]. Much attention has been devoted to meticulously puncturing codes to achieve specific logical operators, for instance, for T state distillation [CAB12, BH12, CH17a, CH17b, HH18].

Despite the proliferation of quantum RM codes and their descendants, a precise characterization of the code's logical operators remains elusive. Recent works [HH18, VB22, SPW24] have studied varying aspects of quantum RM codes and their generalizations, with [HLC21, HLC22a, RCNP20] representing the closest to our work on characterizing their transversal logic. For instance, [HLC21, HLC22a] established necessary and sufficient conditions for when the application of $Z(k)$ to every physical qubit of a quantum RM code will perform logic.

Our Theorem 4.2.3 is phrased in terms of (hitherto undefined) $\widetilde{Z}(k)_A$ operators, but in the case of quantum RM codes the result exactly holds for *subcube* operators — operators acting as $Z(k)$ on the qubits within a subcube A and identity otherwise. For instance, the following is true:

Proposition (Simplified version of Proposition 5.1.2)**.** *If A is an ℓ-cube satisfying $q + kr + 1 \leq \ell \leq (k+1)r$, then the subcube operator $Z(k)_A$ is a non-trivial logical operator for the code $QRM_m(q, r)$. If $\ell \geq (k+1)r + 1$ then $Z(k)_A$ acts as logical identity on the code.*

Proposition 5.1.2 implies and broadly generalizes the mentioned results of [HLC21, HLC22a] by establishing the existence of transversal operators on quantum RM codes that may act non-trivially on strict subsets of both physical and logical qubits. While the authors of [HLC21, HLC22a] determine conditions for when the global $Z(k)$ operation performs logic on $QRM_m(q, r)$, they do not give descriptions of the implemented logical circuits. An earlier work that addresses this question [RCNP20] does detail the logic performed by global $Z(k)$ in the particular case of $QRM_m(r-1,r)$ codes, i.e., when $q = r-1$. Extending these results, we give a complete description of the logical circuit implemented by the transversal $Z(k)$ operation applied to *any* subcube, and for an arbitrary $QRM_m(q,r)$. We will go into the details of the implemented logical circuits later; for now we give some intuition for their structure.

As the $Z(k)$ operators are diagonal operators in the Clifford Hierarchy, they should likewise implement diagonal logical operators in the Clifford Hierarchy. Diagonal operators in the Clifford Hierarchy are fully classified as circuits composed of multi-qubit controlled versions of $Z(k)$ operators [CGK17]. Proposition 5.1.2 is enough, already, to infer the particular type of circuit implemented by transversal $Z(k)$ applied to a subcube. First, note that the square of $Z(k)$ is precisely $Z(k)^2 = Z(k-1)$. Now, suppose that $Z(k)$ operators are applied to a subcube whose dimension is at least $q + kr + 1$. Then Theorem 4.2.3 implies this operation preserves $QRM_m(q,r)$. In fact, it implies something much stronger: since $q + kr + 1 \geq (k-1+1)r + 1$, it must be that $Z(k-1)$—the *square* of $Z(k)$—applied to the same subcube acts as *logical identity* on $QRM_m(q,r)$. In other words, Theorem 4.2.3 implies that such subcube operators are necessarily logically Hermitian.

Now, the classification from [CGK17] implies that the *only* diagonal and Hermitian operators in the Clifford Hierarchy are circuits composed of multi-qubit controlled-Z operators. The *ℓ-qubit controlled-Z gate* is a diagonal gate acting on ℓ qubits that applies a -1 phase to the all ones computational basis state, and leaves all other computational basis states fixed. Our main result for quantum RM codes is to determine precisely what logical multi-controlled-Z circuit is implemented by a subcube operator:

Theorem (Informal version of Theorem 5.3.3)**.** *Consider the quantum RM code $QRM_m(q,r)$ and* *suppose A is a subcube of the m-dimensional hypercube. If $Z(k)_A$ is a non-trivially operator for $QRM_m(q, r)$ then it implements an explicitly determined circuit composed of multi-controlled-Z gates each acting on at most k qubits.*

Theorem 5.3.3 is proven by relating the $Z(k)_A$ subcube operators to the aforementioned $\widetilde{Z}(k)_A$ operators; the bulk of Chapter 5 is spent characterizing the logic of these so-called signed subcube operators.

Chapter 2: Preliminaries

2.1 Notation and Conventions

The following will be used throughout: Positive integers are denoted by $\mathbb{N}$; non-negative integers will always be denoted by $\mathbb{Z}_{\geq 0}$. For $n \in \mathbb{N}$, $[n]$ denotes the set $[n] \coloneqq \{1, \ldots, n\}$. By convention, $\sum_{\emptyset} = 0$ and $\prod_{\emptyset} = 1$. A script $\mathscr{P}(\cdot)$ refers to the power set of the input. Both the cardinality of a set and the Hamming weight of a bit string are denoted by $|\cdot|$; the usage should be clear from context. The i-th entry of a bit string $z \in \{0, 1\}^n$ will be denoted z_i; in the case where $n = 2^m$ for some $m \in NN$ we will index the entries via elements of the group $\mathbb{Z}_2^m$.

For a group G and a subset $S \subseteq G$, $\langle S \rangle \leq G$ denotes the subgroup of G generated by elements of S. For a field $\mathbb{F}$ and $n \in \mathbb{N}$, $\mathbb{F}^n$ denotes the n-dimensional vector space over $\mathbb{F}$. For a group G or a set S, G^n and S^n denote the n-fold Cartesian product of G and S, respectively. For the remainder of the document we reserve the letter $\mathbb{F}$ for the binary field, $\mathbb{F} \coloneqq \mathbb{F}_2$. The additive group of $\mathbb{F}$, i.e., the cyclic group of order two, is denoted by $\mathbb{Z}_2$; the underlying set of bit strings (with no particular group structure) is denoted by $\{0, 1\}$.

The n-qubit unitary group is denoted $\mathrm{U}(2^n)$. For a subset of n total qubits $Q \subseteq [n]$ and any single-qubit operator, U, the operator U_A denotes the n-qubit gate acting as U on the qubits indexed by Q, and identity elsewhere, $U_A \coloneqq \bigotimes_{i \in Q} U_i \bigotimes_{i \in Q^c} I_i$. A bar over an operator indicates a logical gate performed on a given quantum code; for instance, $\overline{\mathbb{I}}$ is the logical identity operator.

2.2 Classical Codes

We now present requisite preliminaries on classical codes. For comprehensive references on coding theory, see [MS77, RGS23]. Consider the n-dimensional binary vector space $\mathbb{F}^n$ under addition modulo 2, denoted simply by $+$.

Definition 2.2.1 (Binary linear code)**.** A *(binary linear) code*, denoted $C \subseteq \mathbb{F}^n$, is a linear subspace of $\mathbb{F}^n$. The *length* of C is the value of n. The dimension of a code is denoted by $\dim C$. The elements of C are referred to as *codewords*.

Definition 2.2.2 (Distance)**.** The *minimum distance*, or simply the *distance*, of a (binary) code $C \subseteq \mathbb{F}^n$ is the shortest distance between two codewords, $\operatorname{dist} C := \min_{c,c' \in C} |c + c'|$.

Given that a code is closed under addition, the minimum distance is equivalently defined as the minimum Hamming weight of any codeword.

Fact 2.2.3. For a code $C \subseteq \mathbb{F}^n$, it holds that $\operatorname{dist} C = \min_{c \in C} |c|$.

A (linear) code with length n, dimension k, and minimum distance d is denoted by $[n, k, d]$.

For two vectors $c, c' \in \mathbb{F}^n$, let $c \cdot c'$ denote their dot product.

Definition 2.2.4 (Dual code)**.** Let $C \subseteq \mathbb{F}^n$ be a code. The *dual code* of C, denoted $C^\perp$, is the set of vectors in $\mathbb{F}^n$ that are orthogonal to every codeword of C:

$$C^\perp := \left\{ c' \in \mathbb{F}^2 \mid c \cdot c' = 0 \text{ for all } c \in C \right\}.$$

The dual code is clearly a binary linear code, and a simple application of the well-known Rank-Nullity Theorem in linear algebra shows that the dimensions of a code and its dual sum to the dimension of the ambient vector space:

Fact 2.2.5. For a code $C \subseteq \mathbb{F}^n$, it holds that $\dim C + \dim C^{\perp} = n$.

Definition 2.2.6 (Group algebra)**.** Let G be a (finite) group. The (binary) *group algebra*, denoted by $\mathbb{F}G$, is the space of all binary-valued functions on G. That is $\mathbb{F}G \coloneqq \{f \colon G \to \mathbb{F}\}$.

For two functions $f, f' \in \mathbb{F}G$, we have the following:

- The sum of two functions, $(f + f')(g) \coloneqq f(g) + f'(g)$ for $g \in G$, gives $\mathbb{F}G$ the structure of a binary vector space.
- Consider their convolution $f * f'$, defined via

$$(f * f')(g) = \sum_{h \in G} f(h) f'(h^{-1}g).$$

  Since $*$ is bilinear in the two arguments, this gives $\mathbb{F}G$ the structure of an algebra over the Boolean field.

We will mostly be interested in the structure of $\mathbb{F}G$ as a vector space. For a function $f \in \mathbb{F}G$, we can consider the length-$|G|$ bit string corresponding to the truth-table, or *evaluation* of f, $\operatorname{eval} f \in \mathbb{F}^{|G|}$, whose entries are given by

$$(\operatorname{eval} f)_g \coloneqq f(g)$$

for each $g \in G$. The ordering of the bit string can be take to be arbitrary. This map $\operatorname{eval} \colon \mathbb{F}G \to \mathbb{F}^{|G|}$

yields the vector space isomorphism:

$$\mathbb{F}G \cong \mathbb{F}^{|G|},$$

so that one can treat linear subspaces of $\mathbb{F}G$ as linear codes of length $|G|$. We will often conflate these two. That is, for a subspace $C \subseteq \mathbb{F}G$, the dimension of C is taken to be $\dim(\mathrm{eval}\, C)$ and the distance of C is taken to be $\mathrm{dist}(\mathrm{eval}\, C)$.

2.3 The Clifford Hierarchy

Definition 2.3.1 (Pauli group)**.** The identity, and Pauli X, Y, and Z operators are the following four single-qubit gates:

$$\mathbb{I} := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y := \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

These matrices satisfy the following:

- $X^2 = Y^2 = Z^2 = \mathbb{I}$;
- $XY = iZ$, $YZ = iX$, and $ZX = iY$;
- $XY = -YX$, $XZ = -ZX$, and $YZ = -ZY$.

The *single-qubit Pauli group* is the group $\mathcal{P}_1 := \{\varpi\,\mathbb{I}, \varpi X, \varpi Y, \varpi Z \mid \varpi \in \{\pm 1, \pm i\}\}$. The n*-qubit Pauli group* is the n-fold tensor power of the single-qubit group, $\mathcal{P}_n := (\mathcal{P}_1)^{\otimes n}$. Elements of $\mathcal{P}_n$ will typically be referred to as *Pauli operators*. By abuse of notation $\mathbb{I}$ may refer to either the single-qubit identity operator or the n-qubit identity operator.

Consider a Pauli operator $P := \varpi P_1 \otimes \cdots \otimes P_n \in \mathcal{P}_n$ If every non-identity term of P is the matrix X then P is called an X type operator, and similarly for Y and Z. The *support* of P is set of indices for which $P_i \neq \mathbb{I}$, and the *weight* of P is the cardinality of its support. From the commutation relations of single-qubit Pauli operators, two Pauli operators $P, Q \in \mathcal{P}^n$ commute if and only if their supports have even overlap.

Definition 2.3.2 (Clifford hierarchy)**.** The 0-th level of the n-qubit Clifford hierarchy[1] is defined to be the Pauli group, $\mathrm{Cl}^{(0)} := \mathcal{P}_n$. For $k \in \mathbb{N}$, the k-th level of the Clifford hierarchy is defined recursively as the set

$$\mathrm{Cl}^{(k)} := \left\{ U \in \mathrm{U}(2^n) \mid U\,\mathrm{Cl}^{(0)}\,U^\dagger \subseteq \mathrm{Cl}^{(k-1)} \right\}.$$

In other words, elements of level k conjugate Pauli operators to elements of level $(k-1)$.

We note that aside from $\mathrm{Cl}^{(0)}$, the Pauli group, and $\mathrm{Cl}^{(1)}$, the well-known *Clifford group*, $\mathrm{Cl}^{(k)}$ is not a subgroup of the unitary group. It is, however, closed under left and right multiplication by Pauli operators and arbitrary phases, i.e., $\mathrm{Cl}^{(k)} = e^{i\theta}\mathcal{P}_n\,\mathrm{Cl}^{(k)}\,\mathcal{P}_n$ for all $\theta \in \mathbb{R}$.

Definition 2.3.3 (Single-qubit rotations)**.** For $k \in \mathbb{Z}$ define the single-qubit Z and X basis rotation gates $Z(k)$ and $X(k)$ via

$$Z(k) := |0\rangle\langle 0| + e^{i\frac{\pi}{2^k}}\,|1\rangle\langle 1|\,,$$

$$X(k) := |+\rangle\langle +| + e^{i\frac{\pi}{2^k}}\,|-\rangle\langle -|\,.$$

Note that the $Z(k)$ operators product several well-known gates, $Z = Z(0)$, $S = Z(1)$, i.e., the phase gate, and $T = Z(2)$. Note that $Z(k) = \mathbb{I}$ for all $k < 0$ and that $Z(k)^2 = Z(k-1)$. The same hold for $X(k)$ operators.

[1] Our indexing differs from the standard choice where the first level of the Clifford hierarchy is the Pauli group.

Denoting $\omega_k := e^{-i\frac{\pi}{2^k}}$, one can easily compute that for all $k \geq 0$,

$$Z(k)XZ(k)^\dagger = \omega_k Z(k-1)X.$$

Lemma 2.3.4. *The operators $Z(k)$ and $X(k)$ are in the k-th level of the Clifford hierarchy.*

Proof. We only prove the Z basis case as the other is similar. Clearly the result holds for $k = 0$; suppose for induction the result holds for $k \geq 0$ and consider $Z(k+1)$. The conjugation identity above implies $Z(k+1) = \omega_{k+1} Z(k)X$, and since the Clifford hierarchy is closed under arbitrary phases and Paulis the result holds by induction. $\square$

Definition 2.3.5. For $\ell \in \mathbb{N}$, the *multi-controlled-Z* gate is defined recursively as the $(\ell+1)$-qubit unitary operator $C^{(\ell)}Z := |0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes C^{(\ell-1)}Z$, where $C^{(0)}Z := Z$.

$C^{(\ell)}Z$ is symmetric in the $\ell+1$ qubits; in particular, $C^{(\ell)}Z$ is a diagonal gate that introduces a -1 phase to the all ones computational basis state, $\left|1^{\ell+1}\right\rangle$, and acts as identity on all other computational basis states.

Definition 2.3.6. Given a subset of n qubits, $I \subset [n]$, define the *I-controlled-Z*, $C^I Z$, as the n qubit unitary that acts as $C^{(|I|-1)}Z$ on the qubits in I and identity elsewhere, $C^I Z := C^{(|I|-1)}Z|_I \otimes \mathbb{I}\,|_{[n]\setminus I}$.

Lemma 2.3.7 (Action of $C^I Z$ on $\mathcal{P}_n$)**.**

1. *For every $i \in [n]$, $(C^I Z)Z_i(C^I Z) = Z_i$.*

2. *For every $i \in [n] \setminus I$, $(C^I Z)X_i(C^I Z) = X_i$.*

3. *For every $i \in I$, $(C^I Z)X_i(C^I Z) = X_i C^{I\setminus\{i\}}Z$.*

Proof. 1 and 2 are trivial. For 3, consider without loss of generality $(C^{(\ell)}Z)X_1(C^{(\ell)}Z)$. We compute

$$\begin{aligned}
(C^{(\ell)}Z)X_1(C^{(\ell)}Z) &= \left(|0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes C^{(\ell-1)}Z\right) X_1 \left(|0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes C^{(\ell-1)}Z\right), \\
&= |0\rangle\langle 1| \otimes C^{(\ell-1)}Z + |1\rangle\langle 0| \otimes C^{(\ell-1)}Z, \\
&= X \otimes C^{(\ell-1)}Z, \\
&= X_1 C^{(\ell-1)}Z|_{[\ell]\setminus\{1\}}.
\end{aligned}$$

□

Definition 2.3.8. Given a collection of subsets of n qubits, $\mathcal{F} \subseteq \mathscr{P}([n])$, define the *$\mathcal{F}$-controlled-$Z$* operator as the circuit consisting of $C^I Z$ operators for each $I \in \mathcal{F}$, $C^{\mathcal{F}}Z := \prod_{I\in\mathcal{F}} C^I Z$.

Note that $C^{\mathcal{F}}Z$ is well-defined as each of the $C^I Z$ operators commute with each other. Further, as $(C^I Z)^2 = \mathbb{I}$ for each $I \subseteq [n]$, $(C^{\mathcal{F}}Z)^2 = \mathbb{I}$, as well. In particular, $C^{\mathcal{F}}Z^\dagger = C^{\mathcal{F}}Z$.

Let $\mathcal{F} \subseteq \mathscr{P}([n])$ be a collection of subsets of qubits. Given a qubit $i \in [n]$, the collection $\mathcal{F}_{\sim i} \subseteq \mathscr{P}([n])$ is defined as

$$\mathcal{F}_{\sim i} := \left\{ I \setminus \{i\} \;\middle|\; I \in \mathcal{F}, i \in I \right\}. \tag{2.1}$$

That is, $\mathcal{F}_{\sim i}$ consists of the sets in $\mathcal{F}$ that contain i, but with i removed. Note that for a single subset, $I \subseteq [n]$, $\{I\}_{\sim i}$ is equal to $I \setminus \{i\}$ if $i \in I$ and empty otherwise.

Lemma 2.3.9 (Action of $C^{\mathcal{F}}Z$ on $\mathcal{P}_n$)**.**

1. *For every $i \in [n]$, $(C^{\mathcal{F}}Z)Z_i(C^{\mathcal{F}}Z) = Z_i$.*

2. *For every $i \in [n]$, $(C^{\mathcal{F}}Z)X_i(C^{\mathcal{F}}Z) = X_i C^{\mathcal{F}_{\sim i}}Z$.*

Proof. 1 is trivial. Let $i \in [n]$. We prove the identity in 2 by induction on $|\mathcal{F}|$. Clearly if $\mathcal{F} = \emptyset$ then $\mathcal{F}_{\sim i} = \emptyset$ and the identity is true. Suppose now the identity holds for all $\mathcal{G}$ with $|G| = m \geq 0$, and consider $\mathcal{F} \subseteq \mathscr{P}([n])$ with $|\mathcal{F}| = m + 1$. Pick an arbitrary $I \in \mathcal{F}$.

$$
\begin{aligned}
(C^{\mathcal{F}} Z) X_i (C^{\mathcal{F}} Z) &= (C^{\mathcal{F}\setminus I} Z)(C^I Z) X_i (C^I Z)(C^{\mathcal{F}\setminus I} Z), \\
\text{(Lemma 2.3.7)} \qquad &= \begin{cases} (C^{\mathcal{F}\setminus I} Z) X_i (C^{I\setminus\{i\}} Z)(C^{\mathcal{F}\setminus I} Z), & \text{if } i \in I \\ (C^{\mathcal{F}\setminus I} Z) X_i (C^{\mathcal{F}\setminus I} Z), & \text{otherwise} \end{cases}, \\
\text{(Def. of } \{I\}_{\sim i} \text{ and commuting operators)} \qquad &= (C^{\mathcal{F}\setminus I} Z) X_i (C^{\mathcal{F}\setminus I} Z)(C^{\{I\}_{\sim i}} Z), \\
\text{(I.H.)} \qquad &= X_i (C^{(\mathcal{F}\setminus I)_{\sim i}} Z) C^{\{I\}_{\sim i}} Z, \\
&= X_i (C^{\mathcal{F}_{\sim i}} Z).
\end{aligned}
$$

□

By induction this also implies the following:

Corollary 2.3.10. *For $k_{\mathcal{F}} \coloneqq \max_{I\in\mathcal{F}} |I|$, $C^{\mathcal{F}} Z \in \mathrm{Cl}^{(k_{\mathcal{F}}-1)}$.*

2.4 Quantum Codes

Definition 2.4.1 (Quantum code)**.** A *quantum code* $\mathcal{C}$ of dimension K and length n is a K-dimensional subspace of the space of n qubits, $\mathcal{C} \subseteq (\mathbb{C}^2)^{\otimes n}$. If $K = 2^\kappa$ for some $\kappa \in \mathbb{N}$ then we say that $\mathcal{C}$ encodes κ logical qubits into n physical qubits.

Definition 2.4.2 (Codespace projector)**.** For a code $\mathcal{C}$ let $\Pi_{\mathcal{C}}$ denote the orthogonal projection onto $\mathcal{C}$. That is $\operatorname{im} \Pi_{\mathcal{C}} = \mathcal{C}$. Given that the eigenvalues of $\Pi_{\mathcal{C}}$ are either $+1$ or 0 (with the former eigenspace equaling $\mathcal{C}$), the dimension of $\mathcal{C}$ is given by $\dim \mathcal{C} = \mathrm{Tr}[\Pi_{\mathcal{C}}]$.

Perhaps the most common way to devise quantum codes is through the so-called "stabilizer formalism", which we now detail.

Definition 2.4.3 (Stabilizer codes [Got96, CRSS97, CRSS98])**.** Let $\mathcal{S} \subseteq \mathcal{P}_n$ be a collection of Pauli operators such that $PQ = QP$ for all $P, Q \in \mathcal{S}$, and $-\mathbb{I} \notin \langle \mathcal{S} \rangle$. In this case, the (Abelian) group generated by $\mathcal{S}$, $\langle \mathcal{S} \rangle \leq \mathcal{P}_n$ is called a *stabilizer group*. The *stabilizer code* associated with $\mathcal{S}$ is defined as the joint $+1$ eigenspace of the elements in $\mathcal{S}$, i.e.,

$$\mathcal{C}_{\mathcal{S}} \equiv \left\{ |\psi\rangle \mid P\,|\psi\rangle = |\psi\rangle \text{ for all } P \in \langle \mathcal{S} \rangle \right\} \subseteq (\mathbb{C}^2)^{\otimes n}.$$

To be accurate, we should denote $\mathcal{C}_{\mathcal{S}}$ by $\mathcal{C}_{\langle \mathcal{S} \rangle}$ as the definition is independent of a particular generating set. By further abuse of notation, the codespace projector of $\mathcal{C}_{\mathcal{S}}$ may be denoted by $\Pi_{\mathcal{S}} \coloneqq \Pi_{\mathcal{C}_{\mathcal{S}}}$ when such a generating set $\mathcal{S}$ is given. Of course, this $\Pi_{\mathcal{S}}$ is also independent of a generating set for the group $\langle \mathcal{S} \rangle$. We may abuse terminology by simply referring to $\langle \mathcal{S} \rangle$ as the stabilizer code, though it should be clear that we are always referring to the subspace $\mathcal{C}_{\mathcal{S}}$

For the following, suppose that $\mathcal{S}$ is the generating set for a stabilizer group. By the classification of finite Abelian groups, there is some subset $\hat{\mathcal{S}} \subseteq \mathcal{S}$ of independent generators for which $\langle \hat{\mathcal{S}} \rangle = \langle \mathcal{S} \rangle$. Let τ denote the number of generators in such a $\hat{\mathcal{S}}$, which is also unique by the classification. In particular, the number of elements of $\langle \mathcal{S} \rangle$ is necessarily 2^τ.

Lemma 2.4.4. *The code space projector of a stabilizer code $\mathcal{C}_{\mathcal{S}}$ is equal to $\Pi_{\mathcal{S}} = \frac{1}{2^\tau} \sum_{P \in \langle \mathcal{S} \rangle} P$.*

Proof. Let $\Pi \coloneqq \frac{1}{2^\tau} \sum_{P \in \langle \mathcal{S} \rangle} P$ denote the operator on the right-hand side.

($\operatorname{im} \Pi \subseteq \mathcal{C}_{\mathcal{S}}$) Left multiplication by an element of a group is a transitive action on the group, so clearly $P\Pi = \Pi$ for all $P \in \langle \mathcal{S} \rangle$. This proves the inclusion.

($\mathcal{C}_{\mathcal{S}} \subseteq \operatorname{im} \Pi$) Take $|\psi\rangle \in \mathcal{C}_{\mathcal{S}}$. Since every element of $\langle \mathcal{S} \rangle$ fixes $|\psi\rangle$, we have $\Pi |\psi\rangle = \frac{|\langle \mathcal{S} \rangle|}{2^\tau} |\psi\rangle = \frac{2^\tau}{2^\tau} |\psi\rangle = |\psi\rangle$, so clearly the inclusion holds.

Now, the desired claim will hold once we prove that Π is, in fact, an orthogonal projection. Clearly $\Pi = \Pi^\dagger$ since every Pauli operator is self-adjoint. Thus, we show that $\Pi^2 = \Pi$:

$$
\begin{aligned}
\Pi^2 &= \frac{1}{2^{2\tau}} \sum_{P, P' \in \langle \mathcal{S} \rangle} \sum_{P' \in \langle \mathcal{S} \rangle} PQ, \\
&= \frac{1}{2^{2\tau}} \sum_{Q \in \langle \mathcal{S} \rangle} Q \cdot |\{(P, P') \mid P, P' \in \langle \mathcal{S} \rangle, PP' = Q\}|, \\
\text{(Left action is transitive)} \qquad &= \frac{2^\tau}{2^{2\tau}} \sum_{Q \in \langle \mathcal{S} \rangle} Q, \\
&= \Pi.
\end{aligned}
$$

$\square$

Corollary 2.4.5. *The code $\mathcal{C}_{\mathcal{S}}$ encodes $n - \tau$ logical qubits into n physical qubits.*

Proof.

$$
\begin{aligned}
& \dim \mathcal{C}_{\mathcal{S}} = \mathrm{Tr}\{\Pi_{\mathcal{S}}\}, \\
\text{(Lemma 2.4.4)} \qquad & = \mathrm{Tr}\left[\frac{1}{2^{\tau}} \sum_{P \in \langle \mathcal{S} \rangle} P\right], \\
\text{(Linearity of trace)} \qquad & = \frac{1}{2^{\tau}} \sum_{P \in \langle \mathcal{S} \rangle \, \mathrm{Tr}[P]}, \\
(\mathrm{Tr}[Q] = 2^{n} \text{ for every } Q \in \mathcal{P}_{n}) \qquad & = \frac{2^{n}}{2^{\tau}}, \\
& = 2^{n-\tau}.
\end{aligned}
$$

□

We now show how the theory of classical error-correcting codes can aid in the construction of quantum codes through the notion of Calderbank-Shor-Steane Codes, or simply CSS codes.

One way to construct a stabilizer group is to only consider operators of a single type: clearly any set of Z type operators will be mutually commuting and will not contain $-\mathbb{I}$. We directly connect such quantum codes to classical binary codes.

Recall that the support of $v \in \mathbb{F}^{n}$ is the set $\operatorname{supp} v := \{i \in [n] \mid v_i \neq 0\}$.

Let $C \subseteq \mathbb{F}^{n}$ be a binary $[n, k, d]$ code and for each codeword $c \in C$ define a Z type operator $Z_{\operatorname{supp} c}$ acting as Z on the qubits in $\operatorname{supp} c$ and identity elsewhere. Thus, the group $\{Z_{\operatorname{supp} c} \mid c \in C\}$, which is isomorphic to C, is naturally a stabilizer group that encodes $n-k$ logical qubits into n physical qubits. Such codes perform poorly as they provide no protection against phase errors. We will need *two* classical codes to yield quantum codes protecting against both bit and phase errors.

Definition 2.4.6 (CSS Code)**.** Let C_1 and C_2 be binary $[n, k_1, d_1]$ and $[n, k_2, d_2]$ codes generated by (possibly over-complete) sets B_1 and B_2, respectively. Consider two sets of Pauli operators $\mathcal{S}_X$ and $\mathcal{S}_Z$ defined by

$$\mathcal{S}_X \coloneqq \{X_{\operatorname{supp} c} \mid c \in B_1\}\,, \tag{2.2}$$

$$\mathcal{S}_Z \coloneqq \{Z_{\operatorname{supp} c} \mid c \in B_2\}\,, \tag{2.3}$$

where $X_{\operatorname{supp} c}$ is defined analogously to $Z_{\operatorname{supp} c}$.

If $C_1 \subseteq C_2^\perp$, then the *CSS code corresponding to C_1 and C_2* is defined as the stabilizer code $\mathrm{CSS}(C_1, C_2) \coloneqq \mathcal{C}_{\mathcal{S}_X \cup \mathcal{S}_Z}$. The groups $\langle \mathcal{S}_X \rangle$ and $\langle \mathcal{S}_Z \rangle$ are called the X and Z stabilizer spaces, and their elements X and Z type stabilizers, respectively.

Lemma 2.4.7. $\mathrm{CSS}(C_1, C_2)$ *is a valid stabilizer code that encodes $n - k_1 - k_2$ logical qubits into n physical qubits.*

Proof. For the first claim we must show that any $X_{\operatorname{supp} c_1} \in B_1$ and $Z_{\operatorname{supp} c_2} \in B_2$ commute, which is equivalent to the statement that $c_1 \cdot c_2 = 0$. Since $C_1 \subseteq C_2^\perp$ this is trivial.

Since X and Z operators are necessarily independent, the number of independent operators in the set $\mathcal{S}_X \cup \mathcal{S}_Z$ is equal to the sum of the number of independent operators in $\mathcal{S}_X$ and $\mathcal{S}_Z$, respectively. This is, of course, equal to the sum of the dimensions of the two classical codes, $\dim C_1 + \dim C_2 = k_1 + k_2$, so second claim follows by Lemma 2.4.4. $\square$

Definition 2.4.8. For $P \in \{X, Z\}$, *undetectable P type error* for a CSS code $\mathrm{CSS}(C_1, C_2)$ is any P type operator which leaves the code space invariant. That is, it is a $P_{\operatorname{supp} v}$ for $v \in \mathbb{F}^n$ such that $P_{\operatorname{supp} v}\, \mathrm{CSS}(C_1, C_2) = \mathrm{CSS}(C_1, C_2)$. The space of all undetectable P errors forms a group under multiplication.

Lemma 2.4.9. *Let* $\mathrm{CSS}(C_1, C_2)$ *be a CSS code. The space of undetectable* X *errors is isomorphic to* $C_2^\perp$*, and the space of undetectable* Z *errors is isomorphic to* $C_1^\perp$*.*

Proof. We only prove the claim for X type operators as the proof for Z is identical. Let $v \in \mathbb{F}^n$ be such that $X_{\mathrm{supp}\, v}$ is an X error. We first establish that $X_{\mathrm{supp}\, v}$ commutes with all Z stabilizers of $\mathrm{CSS}(C_1, C_2)$.

Let $|\psi\rangle \in \mathrm{CSS}(C_1, C_2)$ be arbitrary, so that $|\psi\rangle = Z_{\mathrm{supp}\, c} |\psi\rangle$ for all $c \in C_2$. By assumption, $X_{\mathrm{supp}\, v} |\psi\rangle \in \mathrm{CSS}(C_1, C_2)$, and so $Z_{\mathrm{supp}\, c} X_{\mathrm{supp}\, v} |\psi\rangle = |\psi\rangle$, as well. Together, we have that $X_{\mathrm{supp}\, v} Z_{\mathrm{supp}\, c} |\psi\rangle = Z_{\mathrm{supp}\, c} X_{\mathrm{supp}\, v} |\psi\rangle$ for all $c \in C_2$ and all $|\psi\rangle \in \mathrm{CSS}(C_1, C_2)$, implying that $X_{\mathrm{supp}\, v} Z_{\mathrm{supp}\, c} = Z_{\mathrm{supp}\, c} X_{\mathrm{supp}\, v}$.

Now, a Pauli X and Z operator only commute is the intersection of their supports has an even number of elements. This parity corresponds precisely to the value of $c \cdot v$, to $c \cdot v = 0$ for all $c \in C_2$. By definition, $v \in C_2^\perp$, as required by the claim. □

Definition 2.4.10. Let $\mathrm{CSS}(C_1, C_2)$ be a CSS code. The *X and Z distances* of $\mathrm{CSS}(C_1, C_2)$ are defined as:

$$d_X := \min_{c \in C_2^\perp \setminus C_1} |c|, \tag{2.4}$$

$$d_Z := \min_{c \in C_1^\perp \setminus C_2} |c|, \tag{2.5}$$

respectively. The *distance* of $\mathrm{CSS}(C_1, C_2)$ is $d := \min(d_X, d_Z)$, and we say that $\mathrm{CSS}(C_1, C_2)$ is an $[[n, \kappa, d]]$ code, where n is the number of physical qubits, $\kappa := n - k_1 - k_2$ is the number of logical qubits, and d is the distance. If the distance is unknown we simply say it is an $[[n, \kappa]]$ code.

The distance of a code essentially captures the error correcting and detecting capabilities of the code; as the goal of our results on quantum codes is to construct logical operators we will not discuss these capabilities in any meaningful way.

2.4.1 A note on conventions

When it comes to constructing and working with CSS codes, there are several equivalent definitions that nevertheless have conflicting notation. Here, we have taken the convention that the spaces of X and Z stabilizers are isomorphic to the classical codes C_1 and C_2, and so the commutativity condition is equivalent to the containment $C_1 \subseteq C_2^{\perp}$. We made this choice to reflect the method by which we construct quantum Coxeter codes: by defining X and Z stabilizer generators corresponding to the definition of classical Coxeter codes.

Our choice, however, differs from the more common convention taken in [Got24b]. There, and in arguably most other sources, a CSS code is defined by taking two classical codes C_1', C_2', for which ${C'}_1^{\perp} \subseteq C_2'$. By setting $C_1 = {C'}_1^{\perp}$ and $C_2 = {C'}_2^{\perp}$ this becomes equivalent to our definition, as $(C^{\perp})^{\perp} = C$ for any binary linear code C. Thus, in [Got24b] the X and Z stabilizers are given by elements of ${C'}_1^{\perp}$ and ${C'}_1^{\perp}$, respectively.

This second convention arises when one defines X and Z stabilizers from two parity-check matrices, H_1 and H_2. That is, one takes two binary matrices H_1 and H_2, and defines X stabilizer generators via the rows of H_1 and Z stabilizer generators via the rows of H_2. The X and Z stabilizer spaces are then isomorphic to the codes $\mathrm{im}(H_1^T) = (\ker H_1)^{\perp}$ and $\mathrm{im}(H_2^T) = (\ker H_2)^{\perp}$, respectively. In other words, the fundamental classical codes in the construction are $C_1' := \ker H_1$ and $C_2' := \ker H_2$, representing the spaces of undetectable Z and X errors, respectively. The commutativity condition is equivalent, in this case, to the equality $H_2 H_1^T = 0 \pmod 2$.

Yet a third convention is in use, e.g., [CMLM+24]. A priori, the conditions $C_1 \subseteq C_2^{\perp}$ and ${C'}_1^{\perp} \subseteq C'_2$ both look quite strange; they require specific knowledge of the dual of a code. It would be equivalent to simply consider two nested codes $C_1^* \subseteq C_2^*$. In our convention, this amounts to setting $C_1^* = C_1$ and $C_2^* = C_2^{\perp}$. In addition to being a simpler condition to look for in practice, this convention has the benefit of explicitly specifying the X stabilizer and logical spaces as C_1^* and C_2^*, respectively, at the cost of not having immediate knowledge of the corresponding Z spaces. In the context of both quantum RM and quantum Coxeter codes, which naturally satisfy the nesting property, this convention is perhaps the most natural; we chose to stick with the first convention as it more readily elucidates the structure of the stabilizer groups.

		Stabilizers		**Logicals**		
Convention	Examples	X	Z	X	Z	κ
$C_1 \subseteq C_2^{\perp}$	(Used here), [BH13]	C_1	C_2	$C_2^{\perp}$	$C_1^{\perp}$	$n - k_1 - k_2$
${C'}_1^{\perp} \subseteq C'_2$	[Got24b, LTZ15]	${C'}_1^{\perp}$	${C'}_2^{\perp}$	C'_2	C'_1	$k'_1 + k'_2 - n$
$C_1^* \subseteq C_2^*$	[CS96, CMLM+24]	C_1^*	${C^*}_2^{\perp}$	C_2^*	${C^*}_1^{\perp}$	$k_2^* - k_1^*$

Table 2.1: Conventions for $[[n, \kappa]]$ CSS codes. The classical codes C_i, C'_i, and C_i^* for $i \in \{1, 2\}$ have parameters $[n, k_i]$, $[n, k'_i]$, and $[n, k_i^*]$, respectively.

2.5 Logical Operations

Consider a stabilizer group $\langle \mathcal{S} \rangle$ given by the generating set $\mathcal{S}$, along with the corresponding stabilizer code $\mathcal{C}_{\mathcal{S}} \subseteq (\mathbb{C}^2)^{\otimes n}$. This Pauli stabilizer group can likewise be defined as the group:

$$\mathcal{S}^{(0)} := \left\{ U \in \mathrm{Cl}^{(0)} \mid U \left|\psi\right\rangle = \left|\psi\right\rangle \quad \forall \left|\psi\right\rangle \in \mathcal{C} \right\},$$

$\mathcal{S}^{(0)} = \langle \mathcal{S} \rangle$, i.e., as a subset of the 0-th level of the Clifford hierarchy that leaves the codespace invariant. This definition motivates the following extension to higher levels of the Clifford hierarchy:

Definition 2.5.1. The level-k Clifford stabilizers of $\mathcal{C}$ are the operators in the k-th level of the Clifford hierarchy that leave states in $\mathcal{C}$ invariant:

$$\mathcal{S}^{(k)} := \left\{ U \in \mathrm{Cl}^{(k)} \mid U \left|\psi\right\rangle = \left|\psi\right\rangle \quad \forall \left|\psi\right\rangle \in \mathcal{C} \right\}.$$

Elements of $\mathcal{S}^{(k)}$ perform the *logical identity operator*, $\bar{\mathbb{I}}$, on $\mathcal{C}$.

Likewise, we can define the so-called *undetectable Clifford hierarchy errors* in the following way.

Definition 2.5.2. The level-k undetectable Clifford errors of $\mathcal{C}$ are the operators in the k-th level of the Clifford hierarchy that conjugate Pauli stabilizers of $\mathcal{C}$ to logical identity operators in the $(k-1)$-st level of the Clifford hierarchy:

$$\mathcal{N}^{(k)} := \left\{ U \in \mathrm{Cl}^{(k)} \mid U \mathcal{S}^{(0)} U^{\dagger} \subseteq \mathcal{S}^{(k-1)} \right\}, \tag{2.6}$$

where by convention we set $\mathcal{S}^{(-1)} := \mathcal{S}^{(0)}$.

Note that the set of level-0 errors, $\mathcal{N}^{(0)}$, is the usual space of undetectable *Pauli* errors, and $\mathcal{N}^{(k)}$ corresponds to the intuitive notion of an *undetectable error* on a code:

Lemma 2.5.3. *For a stabilizer code $\mathcal{C}$, let $\Pi_{\mathcal{C}} := \frac{1}{\left|\mathcal{S}^{(0)}\right|} \sum_{S \in \mathcal{S}^{(0)}} S$ denote the code space projector. Suppose $U \in \mathrm{Cl}^{(k)}$ is a k-th level Clifford operator. The following are equivalent:*

1. U is an undetectable Clifford error: $U \in \mathcal{N}^{(k)}$,

2. *U preserves the code space: for every $|\psi\rangle \in \mathcal{C}$, $U|\psi\rangle \in \mathcal{C}$, and*

3. *U commutes with the codespace projector: $U\Pi_{\mathcal{C}}U^\dagger = \Pi_{\mathcal{C}}$.*

Proof. $(2 \Leftrightarrow 3)$ This is equivalent to the statement that U and $\Pi_{\mathcal{C}}$ preserve each other's eigenspaces if and only if they commute with each other.

$(1 \Rightarrow 3)$ Consider $U\Pi_{\mathcal{C}}U^\dagger = \frac{1}{|\mathcal{S}^{(0)}|}\sum_{S\in\mathcal{S}^{(0)}} USU^\dagger$. By definition of $\mathcal{N}^{(k)}$, each $USU^\dagger$ acts as logical identity on $\mathcal{C}$, and so for any $|\psi\rangle \in \mathcal{C}$ we have that $U\Pi_{\mathcal{C}}U^\dagger|\psi\rangle = \frac{1}{|\mathcal{S}^{(0)}|}\sum_{S\in\mathcal{S}^{(0)}}|\psi\rangle = |\psi\rangle$. This implies that $U\Pi_{\mathcal{C}}U^\dagger$ and $\Pi_{\mathcal{C}}$ have the same eigenspaces. Since U is unitary, it preserves the rank of $\Pi_{\mathcal{C}}$, and so $U\Pi_{\mathcal{C}}U^\dagger$ must be equal to the code space projector of $\mathcal{C}$.

$(2 \Rightarrow 1)$ Let $S \in \mathcal{S}^{(0)}$. As $U|\psi\rangle$ can be an arbitrary element of the code space and $U|\psi\rangle = US|\psi\rangle = (USU^\dagger)U|\psi\rangle$, $USU^\dagger$ acts as a logical identity on the code space. $\square$

We note that the above equivalence does not rely on the Clifford hierarchy in any way; the property of being a logical operation is equivalent to conjugating Pauli stabilizers of $\mathcal{C}$ to logical identity operators of the code space. We restricted our attention to Clifford hierarchy operators simply because the goal of the present work is to give transversal operators that are in the Clifford hierarchy.

An important class of undetectable Clifford hierarchy operators are those that act non-trivially on the code space.

Definition 2.5.4. The level-k (non-trivial) Clifford logicals of $\mathcal{C}$ are the operators in the k-th level of the Clifford hierarchy that conjugate Pauli stabilizers of $\mathcal{C}$ to logical identity operators in the $(k-1)$-st level of the Clifford hierarchy, but which are not, themselves, level-k Clifford stabilizers:

$$\mathcal{E}^{(k)} := \mathcal{N}^{(k)} \setminus \mathcal{S}^{(k)}.$$

Definition 2.5.5. Two operators, U and V, are said to be *logically equivalent* on a stabilizer code $\mathcal{C}$, denoted $U \equiv_{\mathcal{C}} V$ or simply $U \equiv V$, if $USU^\dagger = VSV^\dagger$ for every $S \in \mathcal{N}^{(0)}$. This implies that, up to a global phase $e^{i\theta}$, $U|\psi\rangle = e^{i\theta}V|\psi\rangle$ for every $|\psi\rangle \in \mathcal{C}$.

Thus, Clifford stabilizers are the operators that are logically equivalent to identity. We have the following characterization of Clifford stabilizers.

Fact 2.5.6. Let $\mathcal{C}$ be a stabilizer code and suppose that $U \in \mathrm{Cl}^{(k)}$ is a k-th level Clifford operator. $U \in \mathcal{S}^{(k)}$ if and only if $UPU^\dagger \equiv P$ for every $P \in \mathcal{N}^{(0)}$.

Note that since $\mathcal{S}^{(k)} \subseteq \mathcal{N}^{(k)}$, Fact 2.5.6 is stricter than Lemma 2.5.3. Indeed, one recovers Lemma 2.5.3 by requiring only $P \in \mathcal{S}^{(0)}$ in the second condition, instead of $P \in \mathcal{N}^{(0)}$.

While we have given here a definition of logical operators for a code, perhaps more desirable is a way to determine precisely *what* logic a valid logical operator performs. Since operators are uniquely characterized by how they conjugate Pauli operators, we will utilize the following definition. We will only state it explicitly for CSS codes, though it can equivalently be defined for stabilizer codes. To better reflect how we will define a symplectic basis later, let

Definition 2.5.7 (Symplectic basis)**.** Let $\mathrm{CSS}(C_1, C_2)$ be an $[[n, \kappa]]$ CSS code with X and Z stabilizer spaces $\langle \mathcal{S}_X \rangle$ and $\langle \mathcal{S}_Z \rangle$, respectively. A *symplectic basis* for $\mathrm{CSS}(C_1, C_2)$ is any collection of 2κ Pauli operators $\{X_{A_i}, Z_{B_i} \mid A_i, B_j \subseteq [n]\}_{i \in [\kappa]}$, satisfying the following:

- The X_{A_i} operators generate the logical X errors of the code, i.e., $\langle \mathcal{S}_X \cup \{X_{A_i} \mid i \in [\kappa]\} \rangle \cong C_2^\perp$.
- The Z_{B_j} operators generate the logical Z errors of the code, i.e., $\left\langle \mathcal{S}_Z \cup \left\{ Z_{B_j} \mid j \in [\kappa] \right\} \right\rangle \cong C_1^\perp$.
- For $i \in [\kappa]$, the sets A_i and B_i have odd intersection, i.e., $X_{A_i} Z_{B_i} = -Z_{B_i} X_{A_i}$.

- For $i \neq j$, the sets A_i and B_j have even intersection, i.e., $X_{A_i} Z_{B_j} = Z_{B_j} X_{A_i}$ if $i \neq j$.

In short, this property guarantees that the logical qubits of a code can be controlled independently of each other. Fact 2.5.6 can thus be equivalently be stated as: $U \equiv V$ if and only if they conjugate the symplectic basis in the same way. We will not prove it here, but a simple modification to Gaussian elimination can be used to prove that every CSS code has a symplectic basis.

2.6 Coxeter Groups

Definition 2.6.1. Let $S := \{s_1, \ldots, s_m\}$ be a set of m generators. A *Coxeter group* W is given by a presentation

$$W := \left\langle S \mid (s_i s_j)^{M(i,j)} = 1 \right\rangle,$$

where $M(i,i) = 1$ (i.e., $s_i^2 = 1$) and $M(i,j) = M(j,i) \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$. By convention, $M(i,j) = \infty$ means that there is no relation between between s_i and s_j. The pair (W, S) is called a *Coxeter system* of rank m and the matrix $(M(i,j))_{i,j=1}^m$ is called the *defining matrix* of the system.

Clearly, $(\mathbb{Z}_2^m, S_m)$ is a Coxeter system with $M(i,j) = 2$ for all i, j. A classic example of a Coxeter system is the symmetric group on $m+1$ letters, $A_m := (\mathrm{Sym}(m+1), T)$,[2] where $T = \{(i \;\; i+1) \mid i \in [m]\}$ is the set of adjacent transpositions. In this case, $M(i, i+j) = 2$ for all $j \geq 0$ except $j = 1$ when $M(i, i+1) = 3$. A classic visualization of this system is shown in Fig. 1.1, and other examples are given later in Figs. 3.2 and 3.3.

A Coxeter system is called *irreducible* if for any partition of the generators $S = S_1 \sqcup S_2$ there are $s \in S_1$ and $t \in S_2$ that do not commute, and is called *reducible* otherwise. This definition provides no

[2] Not to be confused with the $(m+1)$-letter *alternating group*; in the theory of Coxeter groups, the letter A refers to the full symmetric group.

visual interpretation of irreducibility; a more standard definition relies on Coxeter-Dynkin diagrams [BB05], which we do not use in this paper (except in the proof of Corollary 3.2.8). Finite Coxeter groups have a succinct classification, e.g., [BB05, App.A.1], and we will assume throughout that W is a finite group.

To define Coxeter codes, we need a suitable generalization of a subcube to an arbitrary Coxeter system, where, as before, $\langle J\rangle$ denotes the subgroup generated by a subset $J \subset S$.

Definition 2.6.2. Fix a Coxeter system, (W, S). A *standard subgroup of* W is a subgroup $\langle J\rangle \leq W$ where $J \subseteq S$. A *standard (left) coset* of W is any coset of the form $R \coloneqq \sigma\langle J\rangle$ for $\sigma \in W$, $J \subseteq S$. The *rank* of $R = \sigma\langle J\rangle$ is $\operatorname{rank}(R) \coloneqq |J|$.

Lemma 2.6.3. *A nontrivial finite Coxeter group has even order.*

Proof. If $s \in S \neq \emptyset$, then $\operatorname{ord}(s) = 2$, so $\{1, s\}$ is a subgroup of W, and the result holds by Lagrange's theorem. □

Lemma 2.6.4 ([BB05], Prop. 2.4.1)**.** *Let* $\langle J_1\rangle$ *and* $\langle J_2\rangle$ *be standard subgroups, then*

$$\langle J_1\rangle \cap \langle J_2\rangle = \langle J_1 \cap J_2\rangle.$$

Lemma 2.6.5. *Let* $\sigma_1\langle J_1\rangle$ *and* $\sigma_2\langle J_2\rangle$ *be two standard cosets. If* $|J_1|+|J_2| > m$ *then* $|\sigma_1\langle J_1\rangle \cap \sigma_2\langle J_2\rangle|$ *is even.*

Proof. The result is true if the cosets have trivial overlap. Otherwise, there is a $\sigma \in W$ such that

$$\sigma_1\langle J_1\rangle \cap \sigma_2\langle J_2\rangle = \sigma(\langle J_1\rangle \cap \langle J_2\rangle) = \sigma\langle J_1 \cap J_2\rangle.$$

As $|J_1| + |J_2| > m$ and $|J_1|, |J_2| \leq m$, the intersection $J_1 \cap J_2$ is non-empty and the result holds by Lemma 2.6.3. $\square$

Coxeter systems carry a natural *length function*, $\ell \colon W \to \mathbb{Z}_{\geq 0}$, where the length of an element w is the smallest number of elements from S needed to generate w. That is, $\ell(w) = \ell'$ if there is a decomposition $w = \sigma_1 \sigma_2 \cdots \sigma_{\ell'}$ with $\sigma_i \in S$ for all $i \in [\ell']$, and *any* decomposition of w using elements of S contains at least ℓ' terms. We will make use of two well-known facts:

Lemma 2.6.6 ([BB05], Lem. 1.4.1)**.** *Right multiplication by a generator changes the length of an element, i.e.,* $\ell(ws) = \ell(w) \pm 1$ *for all* $w \in W$ *and* $s \in S$*.*

Lemma 2.6.7 ([AB08], Prop. 2.20)**.** *A standard coset* $w\langle J \rangle$ *has a unique element of minimal length, i.e., there is a unique* $w_1 \in w\langle J \rangle$ *such that* $\ell(w_1) < \ell(u)$ *for every* $u \in w\langle J \rangle$*. This element is characterized by the property that* $\ell(w_1 s) = \ell(w_1) + 1$ *for every* $s \in J$*.*

Given $w \in W$, these statements suggest a way to construct standard cosets for which w is the minimal element: take $w\langle J \rangle$ where J is any set of generators that *increase* the length of w via right multiplication. The following standard definition is phrased in terms of elements that *decrease* the length.

Definition 2.6.8. For $w \in W$, the subset of generators $D(w) \subseteq S$ that reduce the length of w after multiplication on the right is the (right) *descent set* of w:

$$D(w) \coloneqq \left\{ s \in S \;\middle|\; \ell(ws) < \ell(w) \right\}.$$

The value $d(w) \coloneqq |D(w)|$ is the (right) *descent number* of w.

Lemma 2.6.9. *For every* $w \in W$*,* w *is the unique shortest element of the standard coset* $w\langle S \setminus D(w) \rangle$*.*

Proof. By Lemma 2.6.6, $\ell(ws) = \ell(w)+1$ for every $s \in S \setminus D(w)$, so the result holds by Lemma 2.6.7.

□

The following combinatorial quantity will be useful in specifying the dimension of a Coxeter code.

Definition 2.6.10. ([BB05, Sec.7.2],[Pet15]) For $i \in \{0, \ldots, m\}$, the W-Eulerian number $\left\langle {W \atop i} \right\rangle$ is the count of elements in W with descent number equal to i,

$$\left\langle {W \atop i} \right\rangle := \big|\{w \in W \mid d(w) = i\}\big|.$$

Eulerian numbers satisfy the *Dehn–Sommerville equations*

$$\left\langle {W \atop i} \right\rangle = \left\langle {W \atop m-i} \right\rangle. \tag{2.7}$$

From Definition 2.6.10 we also immediately observe that

$$\sum_{i=1}^{m} \left\langle {W \atop i} \right\rangle = |W|. \tag{2.8}$$

Definitions 2.6.8 and 2.6.10 depend on the choice of generating set S, but we suppress this dependence in the notations for simplicity, as is standard.

Remark 2.6.11. If $W = \mathbb{Z}_2^m$ then $\left\langle {W \atop i} \right\rangle = \binom{m}{i}$. If $(W, S) = A_m$ is the symmetric group, then $\left\langle {W \atop i} \right\rangle$ is the classic Eulerian number, i.e., the count of permutations in W with i descents [Pet15, p.6]. See Section 3.3 for expressions computing W-Eulerian numbers for reducible and irreducible Coxeter systems. ◁

We conclude this section with a remark on reducible systems. Suppose that (W_1, S_1) and (W_2, S_2) are finite Coxeter systems of ranks m_1 and m_2, respectively. Their direct product $(W, S) \coloneqq (W_1, S) \times (W_2, T)$ is a finite Coxeter system of rank $m_1 + m_2$ where $S \coloneqq S \sqcup T$ and $(st)^2 = 1$ for every $s \in S$ and $t \in T$. Define the *Eulerian polynomial* of the system W_1 as

$$W_1(t) \coloneqq \sum_{i=0}^{m} \left\langle {W_1 \atop i} \right\rangle t^i,$$

and similarly for W_2. It is a classic fact [BB05, p.202] that for the direct product we have

$$W(t) = W_1(t)W_2(t) \tag{2.9}$$

and thus,

$$\left\langle {W \atop k} \right\rangle = \sum_{i+j=k} \left\langle {W_1 \atop i} \right\rangle \left\langle {W_2 \atop j} \right\rangle, \quad k = 1, \dots, s.$$

We will use this property to compute the dimension of codes on products of dihedral groups.

Chapter 3: Coxeter Codes

3.1 Code Structure

In this section, we construct an explicit basis of Coxeter codes, establish their structural properties, and prove the claims stated in Theorems 1.2.3 to 1.2.6.

Definition 3.1.1. For $w \in W$, the *extension* of w in $\mathbb{F}W$, denoted $\mathcal{E}_w \in \mathbb{F}W$, is the indicator function corresponding to the coset $w\langle S \setminus D(w)\rangle$, $\mathcal{E}_w := \mathbb{1}_{w\langle S \setminus D(w)\rangle}$. The *rank* of $\mathcal{E}_w$ is

$$\operatorname{rank}(\mathcal{E}_w) := m - d(w) = \operatorname{rank}(w\langle S \setminus D(w)\rangle).$$

Definition 3.1.2. Let $\mathcal{B}$ denote the set of all extensions. For $i \in \{0, \ldots, m\}$, let

$$\begin{aligned} \mathcal{B}_i &:= \left\{\mathcal{E}_w \in \mathbb{F}W \;\middle|\; \operatorname{rank}(\mathcal{E}_w) = i\right\} \\ &= \left\{\mathcal{E}_w \in \mathbb{F}W \;\middle|\; w \in W,\ d(w) = m - i\right\}. \end{aligned}$$

Note that by the Dehn–Sommerville equations, Eq. (2.7), we have

$$|\mathcal{B}_i| = |\mathcal{B}_{m-i}| = \left\langle {W \atop i} \right\rangle.$$

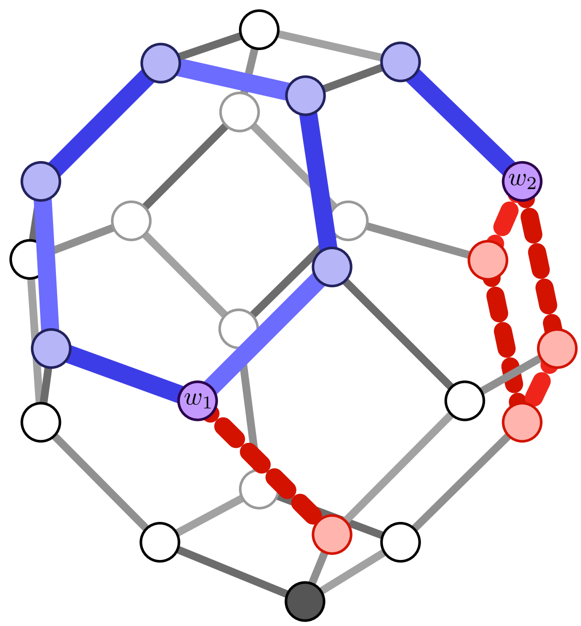


Figure 3.1: This figure shows extensions (blue) and reverse extensions (red) of the elements w_1 and w_2 in A_3. The identity element is shown as the shaded vertex of the graph.

For $r \in \{-1, \ldots, m\}$ consider the collection of extensions with rank at least $m - r$,

$$\mathcal{B}_{\geq m-r} := \bigcup_{i \geq m-r} \mathcal{B}_i.$$

Example 1. For the RM case when $W = \mathbb{Z}_2^m$, this collection is precisely the standard basis of monomials in m variables with degree at most r: if $z \in \mathbb{Z}_2^m$ then $\mathcal{E}_z = \prod_{i \in \mathrm{supp}(z)} x_i$. For instance, take $m = 4$ and let $z = [1001]$. Writing vectors as columns, we have

$$z = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \ S \backslash D(z) = \{e_2, e_3\}, \ z + \langle S \backslash D(z) \rangle = \begin{bmatrix} 1111 \\ 0011 \\ 0101 \\ 1111 \end{bmatrix}, \ \mathcal{E}_z = \mathbb{1}_{z + \langle e_1, e_4 \rangle} = x_1 x_4,$$

and thus $\mathcal{B}_{\geq m-r}$ is equivalently written as the set of monomials of $x_1, \dots, x_4$ of degree r or less. $\triangleleft$

We will prove that $\mathcal{B}_{\geq m-r}$ is always a basis for the order-r Coxeter code of type (W, S). First, proving that $\mathcal{B}$ is linearly independent will rely on the following simple lemma, which says that $w \notin \operatorname{supp}(\mathcal{E}_u)$ for any u of length at least w. Recall again that we do not make a difference between functions and their evaluations, so for $u, w \in W$, $\mathcal{E}_u(w) = 1$ is equivalent to $w \in \operatorname{supp}(\mathcal{E}_u)$.

Lemma 3.1.3. *Let $w \in W$ and $U \subseteq W$. If $\ell(w) \leq \ell(u)$ for all $u \in U$ then $\mathcal{E}_u(w) = 0$ for every $u \in U \setminus \{w\}$.*

Proof. Suppose for contradiction that $\mathcal{E}_u(w) = 1$ for some $u \in U$, so $w \in u\langle S \setminus D(u)\rangle$. As $w \neq u$, Lemma 2.6.9 implies that $\ell(w) > \ell(u)$, contradicting the assumption on U. □

Lemma 3.1.4. *The collection $\mathcal{B}$ is linearly independent.*

Proof. Suppose for contradiction that there is a nonempty subset $U \subseteq W$ for which the function $\sum_{u \in U} \mathcal{E}_u$ is identically zero. Since W is finite, there must exist a $w \in U$ (not necessarily unique) whose length is minimal among the elements in U, i.e., $\ell(w) \leq \ell(u)$ for all $u \in U$. By Lemma 3.1.3 we have $\mathcal{E}_u(w) = 0$ for all $u \in U \setminus \{w\}$. This, however, is impossible, as it implies $\sum_{u \in U} \mathcal{E}_u(w) = \mathcal{E}_w(w) = 1$. □

We now show that the span of $\mathcal{B}_{\geq m-r}$ satisfies a duality structure. Recall that for two functions $f, g \in \mathbb{F}W$, their dot product is given by $f \cdot g = |\operatorname{supp} f \cap \operatorname{supp} g| \pmod 2$.

Lemma 3.1.5. *For each $r \in \{-1, \dots, m\}$ we have*

$$\operatorname{Span} \mathcal{B}_{\geq m-r} = (\operatorname{Span} \mathcal{B}_{\geq r+1})^{\perp}.$$

Proof. We first show that $\operatorname{Span}\mathcal{B}_{\geq m-r} \subseteq (\operatorname{Span}\mathcal{B}_{\geq r+1})^{\perp}$, which is equivalent to the statement that each $\mathcal{E}_{w_1} \in \mathcal{B}_{\geq m-r}$ has even overlap with each $\mathcal{E}_{w_2} \in \mathcal{B}_{\geq r+1}$. The supports of such $\mathcal{E}_{w_1}$ and $\mathcal{E}_{w_2}$ are standard cosets with ranks $r_1 \geq m-r$ and $r_2 \geq r+1$, respectively. Since $r_1 + r_2 > m$, Lemma 2.6.5 implies that the cardinality of their intersection is even. Thus $\mathcal{E}_{w_1} \cdot \mathcal{E}_{w_2} = 0$, as desired.

We now show $\dim(\operatorname{Span}\mathcal{B}_{\geq m-r}) = \dim((\operatorname{Span}\mathcal{B}_{\geq r+1})^{\perp})$, which implies that the two spaces are, in fact, equal. Using Eq. (2.7) and the linear independence of $\mathcal{B}_{\geq m-r}$, we compute

$$\dim(\operatorname{Span}\mathcal{B}_{\geq m-r}) = \sum_{i=m-r}^{m} \left\langle {W \atop i} \right\rangle = \sum_{i=0}^{r} \left\langle {W \atop i} \right\rangle$$

Since the dimensions of a code and its dual code sum to the dimension of the entire vector space, we have

$$\begin{aligned} \dim((\operatorname{Span}\mathcal{B}_{\geq r+1})^{\perp}) &= |W| - \dim(\operatorname{Span}\mathcal{B}_{\geq r+1}) \\ &= \sum_{i=0}^{r} \left\langle {W \atop i} \right\rangle, \end{aligned}$$

where we have used Eqs. (2.7) and (2.8). □

Theorem 3.1.6. *For $r \in \{-1, \ldots, m\}$, the collection of evaluations of functions in $\mathcal{B}_{\geq m-r}$ is a basis for the order-r Coxeter code of type (W, S) and rank m:*

$$\mathsf{C}_W(r) = \operatorname{Span}\operatorname{eval}(\mathcal{B}_{\geq m-r}),$$

or, alternatively,

$$\mathsf{C}_W(r) = \operatorname{Span}\left\{\operatorname{eval}(\mathcal{E}_w) \,\middle|\, w \in W,\ d(w) \leq r\right\}. \tag{3.1}$$

Proof. Recall that $\mathsf{C}_W(r)$ is the span of (evaluations of) indicator functions of standard cosets with rank *exactly* equal to $m - r$.

($\supseteq$) Consider an $\mathcal{E}_w \in \mathcal{B}_{\geq m-r}$, which by definition is the indicator function of $w\langle S \setminus D(w)\rangle$. Let $J \subseteq S \setminus D(w)$ be any subset of $|J| = m - r$ elements of $S \setminus D(w)$, which must exist since $\operatorname{rank}(\mathcal{E}_w) \geq m - r$. The set of cosets of $\langle J\rangle$ in $\langle S \setminus D(w)\rangle$, denoted by $\langle S \setminus D(w)\rangle/\langle J\rangle$, forms a partition of $\langle S \setminus D(w)\rangle$, so their supports are disjoint, and

$$\mathcal{E}_w = \sum_{R \in \langle S \setminus D(w)\rangle/\langle J\rangle} \mathbb{1}_{wR}.$$

This shows that $\mathcal{E}_w$ is a sum of standard coset indicators of rank $m - r$, so its evaluation is a vector in $\mathsf{C}_W(r)$.

($\subseteq$) Let R be a standard coset of rank $m-r$ and let $\mathcal{E}_w \in \mathcal{B}_{\geq r+1}$. By definition, $\operatorname{rank}(\mathcal{E}_w) \geq r+1$, and thus $\operatorname{rank}(R) + \operatorname{rank}(\mathcal{E}_w) > m$. With this, Lemma 2.6.5 implies that R satisfies $\mathbb{1}_R \cdot \mathcal{E}_w = 0$ for every $\mathcal{E}_w \in \mathcal{B}_{r+1}$. Thus, $R \in (\operatorname{Span} \mathcal{B}_{\geq r+1})^{\perp}$, which equals $\operatorname{Span} \mathcal{B}_{\geq m-r}$ by Lemma 3.1.5. $\square$

Example 2 (Example 1 continued). If $W = \mathbb{Z}_2^m$, then extensions are functions $\mathcal{E}_z \colon \mathbb{Z}_2^m \to \mathbb{F}$ given by $\mathcal{E}_z = \prod_{i \in \operatorname{supp} z} x_i$, and descent numbers are given by $d(z) = |z|$. Thus, Eq. (3.1) implies that

$$\mathsf{C}_{\mathbb{Z}_2^m}(r) = \operatorname{Span}\left\{ \operatorname{eval}\Big(\prod_{i \in \operatorname{supp} z} x_i\Big) \;\Big|\; z \in \mathbb{Z}_2^m,\ |z| \leq r \right\},$$

proving that $\mathsf{C}_{\mathbb{Z}_2^m}(r) = RM(r, m)$ and recovering the formula $\dim RM(r, m) = \sum_{i=0}^{r} \binom{m}{i}$. $\triangleleft$

Proposition 3.1.7. *The following hold for all $q < r$ and r_1, r_2:*

(1) (Theorem 1.2.3) $\mathsf{C}_W(q) \subsetneq \mathsf{C}_W(r)$,

(2) (Theorem 1.2.4) $\mathsf{C}_W(r)^{\perp} = \mathsf{C}_W(m-r-1)$,

(3) (Theorem 1.2.5) $\mathsf{C}_W(r_1) \odot \mathsf{C}_W(r_2) \subseteq \mathsf{C}_W(r_1+r_2)$, *and*

(4) (Theorem 1.2.6) $f * \mathsf{C}_W(r) \subseteq \mathsf{C}_W(r)$ *for any* $f \in \mathbb{F}W$.

Proof. (1) This follows from Theorem 3.1.6.

(2) This follows from Lemma 3.1.5 and Theorem 3.1.6.

(3) Let $R_1 := \sigma_1\langle J_1\rangle$ and $R_2 := \sigma_2\langle J_2\rangle$ be standard cosets of ranks $(m-r_1)$ and $(m-r_2)$, respectively, so that $\mathbb{1}_{R_1}$ and $\mathbb{1}_{R_2}$ are arbitrary generators of $\mathsf{C}_W(r_1)$ and $\mathsf{C}_W(r_2)$, respectively. Their intersection, if non-empty, is a standard coset $R_1 \cap R_2 = \sigma\langle J_1 \cap J_2\rangle$ of rank

$$
\begin{aligned}
|J_1 \cap J_2| &= |J_1| + |J_2| - |J_1 \cup J_2| \\
&\geq 2m - (r_1+r_2) - m \\
&= m - (r_1+r_2).
\end{aligned}
$$

By definition, $\mathbb{1}_{R_1} \odot \mathbb{1}_{R_2} = \mathbb{1}_{R_1\cap R_2}$, and since $R_1 \cap R_2$ is a standard coset of rank $\geq m-(r_1+r_2)$, we have $\mathbb{1}_{R_1\cap R_2} \in \mathsf{C}_W(q)$ for some $q \leq r_1+r_2$. The result holds by Theorem 1.2.3.

(4) Suppose that $f = \mathbb{1}_w$ is the indicator function for a single $w \in W$, and that $\mathbb{1}_{\sigma\langle J\rangle}$ is the indicator function of an arbitrary rank-$(m-r)$ standard coset. We compute the value of $\mathbb{1}_w * \mathbb{1}_{\sigma\langle J\rangle}$ on

an arbitrary $u \in W$:

$$\begin{aligned}(\mathbb{1}_w * \mathbb{1}_{\sigma\langle J\rangle})(u) &= \sum_{g\in W} \mathbb{1}_w(g)\mathbb{1}_{\sigma\langle J\rangle}(g^{-1}u) \\ &= \mathbb{1}_{\sigma\langle J\rangle}(w^{-1}u) \\ &= \mathbb{1}_{(w\sigma)\langle J\rangle}(u),\end{aligned}$$

where the last line follows since $w^{-1}u \in \sigma\langle J\rangle$ if and only if $u \in (w\sigma)\langle J\rangle$. As $(w\sigma)\langle J\rangle$ is also a rank-$(m-r)$ standard coset, we have that $\mathbb{1}_w * \mathbb{1}_{\sigma\langle J\rangle} \in \mathsf{C}_W(r)$. Since any function can be written in terms of single-point indicators, the full result follows by the linearity of convolution. □

3.1.1 Reverse extensions

We conclude this section with a remark on extensions, which we have chosen to define as indicators corresponding to the cosets $w\langle S \setminus D(w)\rangle$. Perhaps a more straightforward choice would have been the cosets corresponding directly to descents, $w\langle D(w)\rangle$. Indeed, the results of this chapter hold equally well by using the *reverse extension*, $\mathcal{R}_w \coloneqq \mathbb{1}_{w\langle D(w)\rangle}$, e.g.,

$$\mathsf{C}_W(r) = \operatorname{Span}\left\{\operatorname{eval}(\mathcal{R}_w) \;\middle|\; w \in W,\, d(w) \geq m - r\right\}.$$

In the case of RM codes, this basis corresponds to signed monomials of degree at most r,

$$\left\{\prod_{i\in A} \bar{x}_i \;\middle|\; A \subseteq [m],\, |A| \leq r\right\},$$

or equivalently, the evaluation vectors of (unsigned) monomials after string reversal. Thus, while reverse extensions may appear better suited for the context of Coxeter codes, they do not explicitly generalize the standard basis of RM codes.

3.2 Code Parameters

3.2.1 Dimension and rate

Lemma 3.1.5 and Theorem 3.1.6 immediately imply the following result:

Theorem 3.2.1. *The dimension of the order-r Coxeter code of type (W, S) is given by*

$$\dim \mathsf{C}_W(r) = \sum_{i=0}^{r} \left\langle {W \atop i} \right\rangle. \tag{3.2}$$

The rate of the Reed–Muller code $RM(r,m)$ equals $2^{-m}\sum_{k=0}^{r}\binom{m}{i}$. By standard asymptotic arguments, for large m it changes from near zero to near one when r crosses $m/2$, and is about $1/2$ if $r = \lfloor m/2 \rfloor$, with more precise information derived from the standard Gaussian distribution. This behavior largely extends to many Coxeter codes.

In particular, consider the three infinite series of Coxeter groups in the Coxeter-Dynkin classification: A_m (the symmetric group on $m+1$ elements), B_m (the hyperoctahedral group of order $2^m m!$), and D_m (the generalized dihedral group of order $2^{m-1}m!$). The rate $\kappa(\mathsf{C}_W(r))$ has no closed-form expression for any of these cases (for that matter, there is no such expression even for RM codes), but asymptotic normality of Eulerian numbers of types A, B, D has been addressed in many places in the literature [Ben73], [CTZ09], with [HCD20] being the most comprehensive source. As implied by these references, for each of the infinite series of groups, the random variable X_m with

$P(X_m = k) = \left\langle {W \atop k} \right\rangle / |W|$ is asymptotically normal with mean $\frac{m}{2}$ and variance $\frac{m}{12}$. Following the proof of the De Moivre–Laplace theorem for the binomial distribution, we obtain the following statement about the asymptotics of the code rate.

Theorem 3.2.2 (Code rate)**.** *Suppose that $(W, S)_m$ is one of the irreducible Coxeter families A_m, B_m, or D_m. Let $\Phi(x) = \int_{-\infty}^{x} e^{-t^2/2} dt/\sqrt{2\pi}$ and let $m \to \infty$.*

(i) Let $r_m = \frac{m}{2} + \rho_m \sqrt{\frac{m}{12}}$. If $\rho_m \to \rho \in \mathbb{R}$, then the code rate $\kappa(C_W(r_m)) \to \Phi(\rho)$.

(ii) For a fixed $\kappa \in (0, 1)$, define the sequence of order values

$$r_m^* := \left\lfloor \frac{m}{2} + \sqrt{\frac{m}{12}} \Phi^{-1}(\kappa) \right\rfloor, m = 1, 2, \ldots.$$

Assuming that $r_m^* \geq 0$, $\kappa(\mathsf{C}_W(r_m^*)) \to \kappa$.

(iii) Consider a sequence of order values $r_m, m = 1, 2, \ldots$. If $|\frac{m}{2} - r_m| \gg \sqrt{m}$ and for all m, (a) $r < m/2$, then $\kappa(\mathsf{C}_W(r_m)) \to 0$; (b) $r > m/2$, then $\kappa(\mathsf{C}_W(r_m)) \to 1$.

The rate of any infinite family of Coxeter codes, including the ones constructed from reducible systems (Section 3.3), exhibits a behavior similar to Theorem 3.2.2. This follows from the product structure of the W-polynomials of Coxeter groups, Eq. (2.9), although the corresponding fact involves convergence to a multivariate Gaussian distribution, as is apparent, for instance, from Eq. (3.3) below.

3.2.2 Distance

Given that $\mathsf{C}_W(r)$ is generated by standard cosets of rank $m - r$, there is a trivial upper bound on the code distance given by the *smallest* such coset. We conjecture that this bound is, in fact, tight:

Conjecture 3.2.3. *Let (W, S) be a Coxeter system of rank m. The distance of the code $\mathsf{C}_W(r)$ is given* *by*

$$\mathrm{dist}(\mathsf{C}_W(r)) = \min_{J \subseteq S, |J| = m-r} |\langle J \rangle|.$$

This conjecture is true for RM codes and the family of Coxeter codes given by the dihedral groups, $I_2(n)$. We have further verified it by computer for all nontrivial Coxeter codes of length at most 120 (some of them are listed in Tables 3.2 to 3.4, where the distance values shown in italic rely on the validity of Conjecture 3.2.3). We can also prove that the conjecture is true whenever $r \geq \lfloor \frac{m}{2} \rfloor$, see Corollary 3.2.8 below.

To continue the discussion of the distance, we prove the following lower bound for any r:

Theorem 3.2.4. *Let (W, S) be a Coxeter system of rank m. The distance of any order-r Coxeter code satisfies* $\mathrm{dist}(\mathsf{C}_W(r)) \geq 2^{m-r}$.

This bound is tight for RM codes but not for the codes arising from the symmetric group: the bound in Conjecture 3.2.3 is strictly larger whenever $r > \lceil \frac{m}{2} \rceil$ in the case of A_m.

Lemma 3.2.5. *If $r < m$, then for every $c \in \mathsf{C}_W(r)$ the Hamming weight of c is even.*

Proof. We know $m - r - 1 \geq 0$ since $r \leq m - 1$, so

$$\begin{aligned} \mathsf{C}_W(r) &\overset{\text{(duality)}}{=} \mathsf{C}_W(m-r-1)^{\perp} \\ &\overset{\text{(nesting)}}{\subseteq} \mathsf{C}_W(0)^{\perp} \\ &= \left\{0^{|W|}, 1^{|W|}\right\}^{\perp}, \end{aligned}$$

i.e., every $c \in \mathsf{C}_W(r)$ is orthogonal to the all 1's vector and thus has even weight. $\square$

Lemma 3.2.6. *If $w_1, w_2 \in W$ are not equal, then there is a $K \subseteq S$, $|K| = m - 1$, for which* $w_1\langle K \rangle \neq w_2\langle K \rangle$.

Proof. Let $J_1, \ldots, J_m$ be the distinct $(m-1)$-subsets of S. Note that $\cap_{i=1}^m \langle J_i \rangle = 1$. Since $w_1 \neq w_2$, there is an $i \in [m]$ such that $w_2^{-1} w_1 \notin \langle J_i \rangle$. Put $K = J_i$ and observe that $w_1 \langle K \rangle = w_2 \langle K \rangle$ would yield a contradiction. $\square$

Lemma 3.2.7. *Consider a standard coset $w\langle K \rangle$. If $c \in \mathsf{C}_W(r)$ then the punctured code $c|_{w\langle K \rangle} \in \mathsf{C}_{\langle K \rangle}(r)$.*

Proof. By definition there exist $\{\sigma_i \langle J_i \rangle\}_{i \in I}$, $|J_i| = m - r$, for which $c = \sum_{i \in I} \mathbb{1}_{\sigma_i \langle J_i \rangle}$. The function restricted to $w\langle K \rangle$ equals the product $c\mathbb{1}_{w\langle K \rangle}$, and

$$
\begin{aligned}
c\mathbb{1}_{w\langle K \rangle} &= \sum_{i \in I} \mathbb{1}_{\sigma_i \langle J_i \rangle} \mathbb{1}_{w\langle K \rangle}, \\
&= \sum_{i \in I'} \mathbb{1}_{\sigma_i' \langle J_i \cap K \rangle},
\end{aligned}
$$

where $I' \subseteq I$ indexes the standard cosets that have nontrivial intersection with $w\langle K \rangle$. We lower bound

$$
\begin{aligned}
|J_i \cap K| &= |J_i| + |K| - |J_i \cup K|, \\
&\geq m - r + |K| - m, \\
&= |K| - r.
\end{aligned}
$$

Now note that $\mathsf{C}_{\langle K \rangle}(r)$ is spanned by standard cosets of rank $|K| - r$. By an argument similar to the proof of the first part of Theorem 3.1.6, $c|_{w\langle K \rangle} = c\mathbb{1}_{w\langle K \rangle}$ is a codeword in $\mathsf{C}_{\langle K \rangle}(r)$. $\square$

Proof of Theorem 3.2.4. The result holds for all $m \geq 1$ when $r = 0$: $\mathsf{C}_W(0)$ is a repetition code with $\mathrm{dist}(\mathsf{C}_W(0)) = |W| \geq 2^m$. Fix $r \geq 1$. We proceed by induction on m. The result is true when $m = r$, as $\mathsf{C}_W(m) = \mathbb{F}W$ has distance $2^0 = 1$. Supposing that the result holds whenever (W, S) has rank

$k \geq r$, consider a system (W', S') with rank $k+1$ and the code $\mathsf{C}_{W'}(r)$.

By Lemma 3.2.5, if $c \in \mathsf{C}_{W'}(r)$ is a nonzero vector, then $|c| \geq 2$. Let $w_1, w_2 \in \mathrm{supp}(c)$. By Lemma 3.2.6 there is a subset $K \subseteq S'$, $|K| = k$ such that $w_1\langle K \rangle \neq w_2\langle K \rangle$ (and thus $w_1\langle K \rangle \cap w_2\langle K \rangle = \emptyset$). Let c_1 and c_2 denote the restrictions of c to $w_1\langle K \rangle$ and $w_2\langle K \rangle$, respectively. Note the following:

1. By Lemma 3.2.7 we are guaranteed that $c_1, c_2 \in \mathsf{C}_{\langle K \rangle}(r)$.

2. Since $c(w_1) = c(w_2) = 1$, these restrictions are nonzero codewords of $\mathsf{C}_{\langle K \rangle}(r)$.

3. Since $w_1\langle K \rangle \neq w_2\langle K \rangle$, their intersection is empty, and we obtain $|c| \geq |c_1| + |c_2|$.

Since the rank of $(\langle K \rangle, K)$ is k, we can use the induction hypothesis for c_1 and c_2, which are nonzero codewords of $\mathsf{C}_{\langle K \rangle}(r)$, to obtain

$$|c| \geq |c_1| + |c_2| \geq 2^{k-r} + 2^{k-r} = 2^{k+1-r},$$

completing the proof. $\square$

Corollary 3.2.8. *If* $r \geq \lfloor \frac{m}{2} \rfloor$ *then* $\mathrm{dist}(\mathsf{C}_W(r)) = 2^{m-r}$.

Proof. Let $\mathsf{C}_W(r)$ be a code of order r constructed from a Coxeter system (W, S). If there is a standard subgroup $\langle J \rangle$ of rank $m - r$, all of whose generators are pairwise commuting, this yields a codeword of weight 2^{m-r}, matching the lower bound from Theorem 3.2.4. By assumption, $m - r \leq \lceil \frac{m}{2} \rceil$, so our claim will follow if we show that any Coxeter system contains at least $\lceil \frac{m}{2} \rceil$ commuting generators.

First, suppose that (W, S) is irreducible. As mentioned above, irreducible systems are completely classified in terms of their Coxeter-Dynkin diagrams [BB05]. Any such diagram is connected and, by inspection, has no cycles. In other words, it is a bipartite graph, which therefore contains a part of size $\geq \lceil \frac{m}{2} \rceil$. This subset of vertices forms an independent set, giving the desired collection of commuting generators.

Now suppose that $(W, S) = \prod_i (W_i, S_i)$, where each factor is irreducible, and let $m_i := |S_i|$ for all i, so that $|S| = \sum_i m_i$. Generators from different sets S_i commute, and each S_i contains $\geq \lceil \frac{m_i}{2} \rceil$ commuting generators by the above. Since

$$\sum_i \left\lceil \frac{m_i}{2} \right\rceil \geq \left\lceil \frac{\sum_i m_i}{2} \right\rceil,$$

this again proves our claim. $\square$

Supposing that Conjecture 3.2.3 is true, we will compute the distances for the families of codes corresponding to A_m and $I_2(n)^\mu$.

3.2.2.1 Codes of type A_m

For $m \geq 1$, A_m is a rank-m Coxeter system with defining matrix

$$M(i,j) = \begin{cases} 1, & i = j, \\ 3, & |j-i| = 1, \\ 2, & \text{otherwise.} \end{cases}$$

For $r \in \{1, \ldots, m\}$ let

$$T(m,r) := \left(\left\lceil \frac{m}{r} \right\rceil ! \right)^{m \bmod r} \left(\left\lfloor \frac{m}{r} \right\rfloor ! \right)^{r - m \bmod r}.$$

Note that

$$\left\lceil\frac{m}{r}\right\rceil(m \bmod r) + \left\lfloor\frac{m}{r}\right\rfloor(r - m \bmod r) = m$$

and that this relation describes a partition of m into r close-to-equal parts with the largest possible number of parts of size $\lfloor\frac{m}{r}\rfloor$.

Theorem 3.2.9. *For all $r \in \{0, 1, \ldots, m\}$, the parameters of the codes $\mathsf{C}_{A_m}(r)$ are given by*

$$\left[(m+1)!,\ \sum_{i=0}^{r}\left\langle {A_m \atop i} \right\rangle,\ T(m+1, r+1)\right]$$

assuming Conjecture 3.2.3 when $r < \lfloor\frac{m}{2}\rfloor$.

Proof. The length and dimension are immediate from the construction. To find the code distance, first let $r \geq \lfloor\frac{m}{2}\rfloor$. In this case, Corollary 3.2.8 implies that $\mathrm{dist}_{A_m}(r) = 2^{m-r}$. We will show that $T(m+1, r+1) = 2^{m-r}$. To see this, we consider the following two possibilities:

(a) If $r \geq \lfloor\frac{m}{2}\rfloor + 1$, then $\lceil\frac{m+1}{r+1}\rceil = 2$, $\lfloor\frac{m+1}{r+1}\rfloor = 1$, and $(m+1) \bmod (r+1) = m - r$.

(b) If $r = \lfloor\frac{m}{2}\rfloor$, then

(b1) if m is odd, then $\lceil\frac{m+1}{r+1}\rceil = \lfloor\frac{m+1}{r+1}\rfloor = 2$, and their exponents in the expression for $T(m+1, r+1)$ are 0 and $m-r$, respectively;

(b2) if m is even, then $\lceil\frac{m+1}{r+1}\rceil = 2$, $(m+1) \bmod (r+1) = m - r$, and $\lfloor\frac{m+1}{r+1}\rfloor = 1$, confirming again the value of 2^{m-r}.

Altogether, this shows our claim.

Now let $r \leq \lfloor\frac{m}{2}\rfloor - 1$ or $m - r \geq \lfloor\frac{m+1}{2}\rfloor + 1$. In this case, some of the generators of any rank-$(m-r)$ subgroup necessarily do not commute since the transpositions overlap. Suppose that disjoint sets $S_1, S_2, \ldots, S_{r+1}$ form a partition of $[m+1]$ into $r+1$ segments, wherein the junction points of the segments correspond to the r missing generators in the set of $m-r$ generators. Each set S_i generates a permutation group of order $|S_i|!$, and the order of H equals the product of their orders. This product is minimized if its terms are equal, or as close as possible to being equal, i.e., $S_i \in \{\lfloor \frac{m+1}{r+1} \rfloor, \lceil \frac{m+1}{r+1} \rceil\}$ with as many smaller-size subsets S_i as possible. According to the remark before the theorem, the size of H is exactly $T(m+1, r+1)$, and Conjecture 3.2.3 implies that this is the value of the code distance. $\square$

Note that in the $r \geq \lfloor \frac{m}{s} \rfloor$ case of this theorem, the subgroup H is generated by commuting transpositions and therefore forms an $(m-r)$-dimensional cube in the Cayley graph, giving rise to a minimum-weight codeword in $C_{A_m}(r)$. In the Reed-Muller case, since all the generators commute, the distance of the code is exactly 2^{m-r} for all r.

Remark 3.2.10. The sequence $T(1,1), T(2,1), T(2,2), T(3,1), T(3,2), \ldots$ appears in OEIS [OEI25] as entry A335109. According to the OEIS description, the number $T(m,r)$ gives the count of permutations $\pi : [m] \to [m]$ such that $\pi(i) \equiv i (\operatorname{mod} r)$ for all $i \in [m]$. It is not clear to us if the two descriptions are connected.

The code $\mathsf{C}_{A_m}(0)$ of order $r = 0$ is simply a repetition code. The parameters of the first-order code can be written explicitly as follows.

Proposition 3.2.11. *For $m \geq 1$, the parameters of the binary linear code $\mathsf{C}_{A_m}(1)$ (assuming Conjecture 3.2.3) are given by:*

$$\Big[(m+1)!, 2^{m+1} - m - 1, (m+1)! \Big/ \binom{m+1}{\lfloor \frac{m+1}{2} \rfloor}\Big].$$

Proof. The dimension $\dim(\mathsf{C}_{A_m}(1)) = 1 + \left\langle {A_m \atop 1} \right\rangle$. The Eulerian number $\left\langle {A_m \atop 1} \right\rangle$ can be found using

Eq. (3.4) below:

$$\left\langle {A_m \atop 1} \right\rangle = \sum_{i=0}^{m-1} (m-i)2^i = 2^{m+1} - m - 2,$$

giving the value of the dimension. The sequence of distances $\operatorname{dist}(\mathsf{C}_{A_m}(1)) = T(m+1,2)$ appears as entry A010551 in OEIS [OEI25], and has explicit formula $T(m,2) = m!/\binom{m}{\lfloor \frac{m}{2} \rfloor}$. $\square$

3.2.2.2 Codes of type $I_2(n)^\mu$.

For $n \in \mathbb{Z}_{\geq 2}$ and $m \geq 1$, $I_2(n)^\mu$ is a Coxeter system of rank $m = 2\mu$ with $|I_2(n)^\mu| = (2n)^\mu$ and defining matrix

$$M(i,j) = \begin{cases} 1, & i = j, \\ n, & j = i+1 \text{ and } j \equiv 0 \pmod 2, \\ n, & i = j+1 \text{ and } i \equiv 0 \pmod 2, \\ 2, & \text{otherwise.} \end{cases}$$

Proposition 3.2.12. *The binary linear code $\mathsf{C}_{I_2(n)^\mu}(r)$ has parameters $[(2n)^\mu, k, d]$, where the dimension k is given by*

$$k = \sum_{\substack{i,j \in \mathbb{N} \\ i+j \leq \mu \\ 2i+j \leq r}} \frac{\mu!}{i!j!(\mu-i-j)!}(2n-2)^j \tag{3.3}$$

and the distance d (assuming Conjecture 3.2.3 when $r < \mu$) is given by

$$d = \begin{cases} 2^{2\mu - r}, & \mu \leq r \leq 2\mu, \\ 2^\mu n^{\mu - r}, & 0 \leq r < \mu. \end{cases}$$

Proof. For the dimension, we note that the Eulerian numbers of $I_2(n)$ are $\left\langle {W \atop i} \right\rangle = 1, 2n-2, 1$ for $i = 0, 1, 2$, so using Eq. (2.9), we obtain $W(t) = (t^2 + (2n-2)t + 1)^\mu$ Computing the dimension of the code $\mathsf{C}_{I_2(n)^\mu}(r)$ by Eq. (3.2), we obtain the expression in Eq. (3.3).

Turning to the distance, the $r \geq \mu$ case holds by Corollary 3.2.8 (note that the rank of this Coxeter system is 2μ), so we only rely on Conjecture 3.2.3 when $r < \mu$. We need to minimize the size of $|\langle J \rangle|$ where $J \subset S, |J| = 2\mu - r \geq \mu$. It is straightforward to verify that, without loss of generality, such a collection necessarily contains the even index generators, $J_{\text{even}} = \{2i\}_{i=1}^{\mu} \subseteq J$. For each additional generator s_{2j-1} added to J_{even}, we replace a factor of 2 in $|\langle J \rangle|$ with a factor of $2n$, the order of the subgroup $\langle s_{2j-1}, s_{2j} \rangle$. $\square$

Corollary 3.2.13. *For fixed r, n and $\mu \to \infty$, the distance of $\mathsf{C}_{I_2(n)^\mu}(r)$ is $(2n)^\mu n^{-r}$, i.e., it forms a constant proportion of the code length.*

Codes $\mathsf{C}_{I_2(n)^\mu}(r)$ are perhaps the closest to RM codes in the Coxeter family: for instance, $\mathsf{C}_{I_2(2)^\mu}(r)$ is simply $RM(r, 2\mu)$, so it is of interest to further study such codes for small n. In Section 3.4.2 we give a table of parameters of the codes $\mathsf{C}_{I_2(n)^\mu}(r)$ for $n = 3, 4$ and several values of μ.

3.3 Computing W-Eulerian Numbers

To find the code dimension via Eq. (3.2), it is useful to have explicit expressions for the W-Eulerian numbers. For the irreducible families of Coxeter groups, they appear in many references, e.g., [Pet15, Hya16, Bre94]. We give these expressions in our notation, along with an expression to compute the W-Eulerian numbers for direct products of Coxeter groups.

For every finite Coxeter system (W, S) of rank m, the 0-th and m-th W-Eulerian numbers equal 1, $\left\langle {W \atop 0} \right\rangle = \left\langle {W \atop m} \right\rangle = 1$.

Type A. [OEI25, A008292] The A_m-*Eulerian numbers* can be computed via the recurrence relation

$$\left\langle {A_m \atop i} \right\rangle = (m - i + 1)\left\langle {A_{m-1} \atop i-1} \right\rangle + (i+1)\left\langle {A_{m-1} \atop i} \right\rangle. \tag{3.4}$$

Type B. [OEI25, A060187] The B_m-Eulerian numbers can be computed via the recurrence relation

$$\left\langle {B_m \atop i} \right\rangle = (2m - 2i + 1)\left\langle {B_{m-1} \atop i-1} \right\rangle + (2i+1)\left\langle {B_{m-1} \atop i} \right\rangle.$$

Type D. [OEI25, A066094] The D_m-Eulerian numbers can be computed from the A_m- and B_m-Eulerian numbers via

$$\left\langle {D_m \atop i} \right\rangle = \left\langle {B_m \atop i} \right\rangle - m2^{m-1}\left\langle {A_{m-2} \atop i-1} \right\rangle.$$

Dihedral group. Since $I_2(n)$ has two generators, the only possible descent numbers are 0, 1, and 2, so $\left\langle {I_2(n) \atop 1} \right\rangle = 2n - 2$.

Exceptional types. See Table 3.1.

	r						
W	1	2	3	4	5	6	7
E_6	1272	12183	24928	12183	1272	1	
E_7	17635	309969	1123915	1123915	309969	17635	1
E_8	881752	28336348	169022824	300247750	169022824	28336348	881752
F_4	236	678	236	1			
H_3	59	59	1				
H_4	2636	9126	2636	1			

Table 3.1: W-Eulerian numbers for groups of exceptional type [Pet15, p.248].

3.4 Examples

One particularly useful way to visualize Coxeter groups and codes is via the following:

Definition 3.4.1. The *Cayley graph* of a Coxeter system (W, S) is a graph $G = (V, E)$ with vertices given by elements of the group $V := W$, and with edges given by

$$E := \left\{(w, v) \mid w^{-1}v \in S\right\}.$$

The Cayley graph of a Coxeter group is undirected since each generator squares to identity, and it also has a natural edge-coloring given by $\mathrm{color}((w, v)) := w^{-1}v$.

Below we consider some Coxeter codes arising from the families A_m, $I_2(3)^\mu$, and $I_2(4)^\mu$. In addition to showing Cayley graphs for some of these groups, we also list some explicit code parameters. Italics indicate distances that rely on Conjecture 3.2.3 and regular font indicates a proven value. In particular, Corollary 3.2.8 guarantees that $\mathrm{dist}(\mathsf{C}_W(r)) = 2^{m-r}$ whenever $r \geq \lfloor \frac{m}{2} \rfloor$; the distances of some order-1 codes were computed by brute force.

3.4.1 Codes of type A_m

Consider Coxeter codes corresponding to the infinite family A_m, the symmetric group on $m+1$ letters.

The Cayley graphs for A_3 and A_4 are shown in Figs. 1.1 and 3.2, respectively.

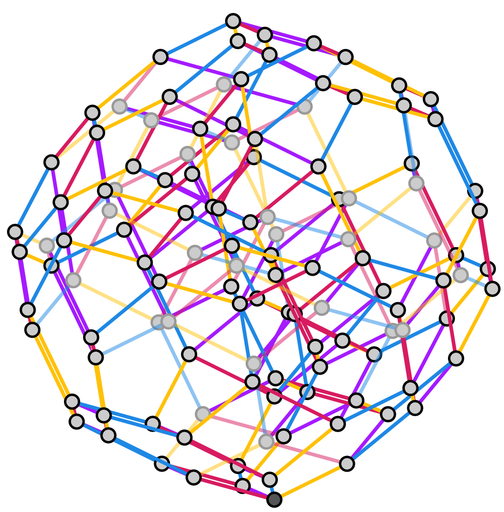


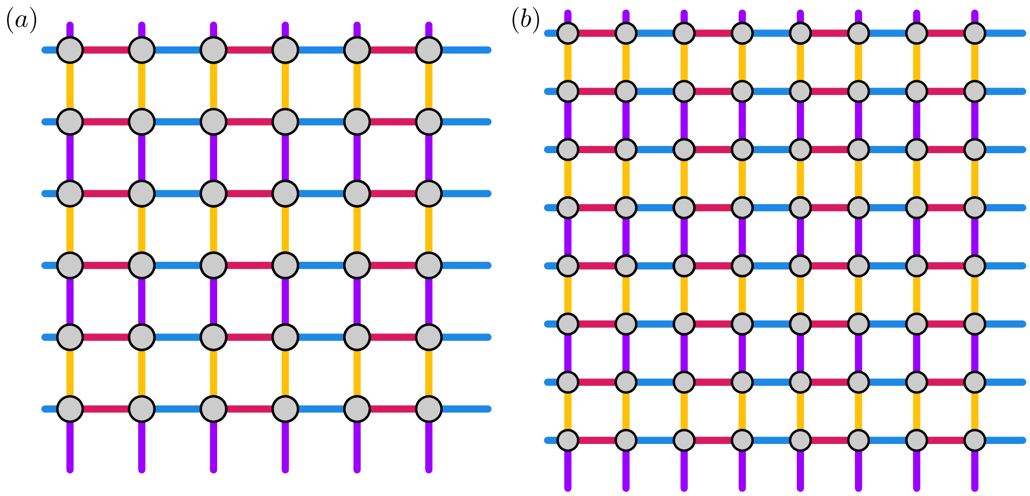
Figure 3.2: Cayley graph for the symmetric groups A_4

r	m = 2	3	4	5	6
1	[6, 5, 2]	[24, 12, 4]	[120, 27, 12]	[720, 58, *36*]	[5040, 121, *144*]
2	[6, 6, 1]	[24, 23, 2]	[120, 93, 4]	[720, 360, 8]	[5040, 1312, *24*]
3		[24, 24, 1]	[120, 119, 2]	[720, 662, 4]	[5040, 3728, 8]
4			[120, 120, 1]	[720, 719, 2]	[5040, 4919, 4]
5				[720, 720, 1]	[5040, 5039, 2]
6					[5040, 5040, 1]

Table 3.2: Parameters of the codes $\mathsf{C}_{A_m}(r)$. Here and below, the distance values shown in italic rely on the validity of Conjecture 3.2.3.

3.4.2 Codes of type $I_2(3)^\mu$

Consider Coxeter codes corresponding to the infinite family $I_2(3)^\mu$, μ copies of the order-6 dihedral group. Note that the rank of $I_2(3)^\mu$ is $m = 2\mu$.



$$\left\langle r, b, y, p \;\middle|\; \begin{matrix} r^2=b^2=y^2=p^2=1 \\ (rb)^3=(br)^3=(yp)^3=(py)^3=1 \\ (ry)^2=(rp)^2=(by)^2=(bp)^2=1 \end{matrix} \right\rangle \qquad \left\langle r, b, y, p \;\middle|\; \begin{matrix} r^2=b^2=y^2=p^2=1 \\ (rb)^4=(br)^4=(yp)^4=(py)^4=1 \\ (ry)^2=(rp)^2=(by)^2=(bp)^2=1 \end{matrix} \right\rangle$$

Figure 3.3: Cayley graphs for Cartesian products of two dihedral groups: (a) $I_2(3)$— note that $I_2(3) \cong A_2$, the symmetric group on 3 letters— and (b) $I_2(4)$. The Coxeter system $I_2(4) \cong B_2$, the hyperoctahedral group, or *signed symmetric group*, on 3 letters.

	μ				
r	1	2	3	4	5
1	[6, 5, 2]	[36, 9, 12]	[216, 13, 72]	[1296, 17, 432]	[7776, 21, 2592]
2	[6, 6, 1]	[36, 27, 4]	[216, 64, *24*]	[1296, 117, *144*]	[7776, 186, *864*]
3		[36, 35, 2]	[216, 152, 8]	[1296, 421, *48*]	[7776, 906, *288*]
4		[36, 36, 1]	[216, 203, 4]	[1296, 875, 16]	[7776, 2676, *96*]
5			[216, 215, 2]	[1296, 1179, 8]	[7776, 5100, 32]
6			[216, 216, 1]	[1296, 1279, 4]	[7776, 6870, 16]
7				[1296, 1295, 2]	[7776, 7590, 8]
8				[1296, 1296, 1]	[7776, 7755, 4]
9					[7776, 7775, 2]
10					[7776, 7776, 1]

Table 3.3: Parameters of the codes $\mathsf{C}_{I_2(3)^\mu}(r)$.

3.4.3 Codes of type $I_2(4)^\mu$

Consider Coxeter codes corresponding to the infinite family $I_2(4)^\mu$, m copies of the order-8 dihedral group. Note that the rank of $I_2(4)^\mu$ is 2μ.

	μ			
r	1	2	3	4
1	[8, 7, 2]	[64, 13, 16]	[512, 19, 128]	[4096, 25, 1024]
2	[8, 8, 1]	[64, 51, 4]	[512, 130, *32*]	[4096, 245, *256*]
3		[64, 63, 2]	[512, 382, 8]	[4096, 1181, *64*]
4		[64, 64, 1]	[512, 493, 4]	[4096, 2915, 16]
5			[512, 511, 2]	[4096, 3851, 8]
6			[512, 512, 1]	[4096, 4071, 4]
7				[4096, 4095, 2]
8				[4096, 4096, 1]

Table 3.4: Parameters of the codes $\mathsf{C}_{I_2(4)^\mu}(r)$.

Chapter 4: Quantum Coxeter Codes and Transversal Logic

4.1 A New Family of CSS Codes

Recall the definition of quantum Coxeter codes from Chapter 1:

Definition 1.3.1 (Quantum Coxeter codes)**.** Let $0 \leq q \leq r \leq m$ be non-negative integers. The order-(q, r) *quantum Coxeter code* of type (W, S), denoted by $\mathsf{QC}_W(q, r)$, is defined as the common $+1$ eigenspace of a Pauli stabilizer group $\langle \mathcal{S}_X, \mathcal{S}_Z \rangle$, with stabilizer generators given by

$$\mathcal{S}_X \coloneqq \left\{ X_{w\langle J \rangle} \;\middle|\; w \in W, J \subseteq S, |J| = m - q \right\}, \tag{1.2}$$

$$\mathcal{S}_Z \coloneqq \left\{ Z_{w\langle J \rangle} \;\middle|\; w \in W, J \subseteq S, |J| = r + 1 \right\}. \tag{1.3}$$

That is, $\mathsf{QC}_W(q, r)$ is given by

$$\mathsf{QC}_W(q, r) \coloneqq \left\{ |\psi\rangle \in (\mathbb{C}^2)^{\otimes |W|} \;\middle|\; P\,|\psi\rangle = |\psi\rangle \text{ for all } P \in \mathcal{S}_X \cup \mathcal{S}_Z \right\}.$$

Thus, the X and Z stabilizer spaces of $\mathsf{QC}_W(q, r)$ are isomorphic to the classical codes $\mathsf{C}_W(q)$ and $\mathsf{C}_W(m - r - 1)$, respectively. Following Section 2.4 on CSS codes, we have the following:

Theorem 4.1.1. *The order-(q, r) quantum Coxeter code of type (W, S) is the CSS code* $\mathsf{QC}_W(q, r) =$

$\mathrm{CSS}(\mathsf{C}_W(q), \mathsf{C}_W(m-r-1))$. *The parameters of* $\mathsf{QC}_W(q,r)$ *are*

$$[[n = |W|, k = \sum_{i=q+1}^{r} \left\langle {W \atop i} \right\rangle, d = 2^{\min(q+1, m-r)}]].$$

Proof. The length and number of logical qubits are clear by construction. Denote the X and Z stabilizer spaces by $C_1 = \mathsf{C}_W(q)$ and $C_2 = \mathsf{C}_W(m-r-1)$, respectively. The distance is given by $\mathrm{dist}(\mathsf{QC}_W(q,r)) = \min(d_X, d_Z)$, where $d_X := w_H(C_2^\perp \backslash C_1)$ is the minimum Hamming weight of the binary code $C_2^\perp \backslash C_1$ and similarly for $d_Z := w_H(C_1^\perp \backslash C_2)$. Below we assume that $q < r$ because if $q = r$, then the code has no logical qubits, and the distance is not well defined. The argument depends on whether $r \le \lfloor \frac{m}{2} \rfloor$ or not.

1. $q < r \le \lfloor \frac{m}{2} \rfloor$. In this case, $m - q - 1 \ge m - \lfloor \frac{m}{2} \rfloor \ge \lfloor \frac{m}{2} \rfloor$, and thus $\mathrm{dist}(C_1^\perp) = 2^{q+1}$ by Corollary 3.2.8, and $\mathrm{dist}(C_2) = 2^{m-r}$ for the same reason. Since $C_1 \subseteq C_2^\perp$, we conclude that $d_X = 2^{\min(q+1,m-r)}$. The argument for d_Z is fully analogous, which proves the claim of the theorem.

2. $q \le \lfloor \frac{m}{2} \rfloor < r$. As above, we have $\mathrm{dist}(C_1^\perp) = 2^{q+1}$. By Theorem 3.2.4, $\mathrm{dist}(C_2) \ge 2^{r+1} \ge \mathrm{dist}(C_1^\perp)$, so clearly $d_X = 2^{q+1}$. The argument for d_Z is again fully symmetric, yielding the estimate $d_Z = 2^{m-r}$ and concluding the proof. □

Remark 4.1.2. A related construction of quantum stabilizer codes was earlier outlined in [VB22]. Its authors start with an abstract combinatorial generalization of RM codes wherein the group $\mathbb{Z}_2^m$ is replaced with a Cartesian product $\mathcal{L}_m = L_1 \times \cdots \times L_m$ of finite sets of varying size. Fixing a subset $\mathcal{F} \subset \mathcal{L}_m$ defines the support set of qubits of the quantum code, and the stabilizers act on specially chosen subsets of $\mathcal{F}$ that sustain the commutation relations. As the authors of [VB22] observe, one way of choosing the collection $\mathcal{L}_m$ is by taking the sets L_i as rank-$(m-1)$ standard subgroups of a Coxeter group W of rank m. They further construct the stabilizer group by taking X- and Z-stabilizers that act on subsets corresponding to the standard cosets of W. At the same time, [VB22] does not link this construction to CSS codes or identify the properties of the obtained quantum codes, suggesting that knowing the group presentation is not sufficient for that purpose. Our approach advances this understanding, showing that it is possible to pinpoint code's properties starting from the structure of the underlying Coxeter group.

Finally, the logical X and Z spaces of $\mathsf{QC}_W(q, r)$ are fully characterized:

Lemma 4.1.3. *For $\mathsf{QC}_W(q, r)$, spaces of logical X and Z operators are isomorphic to the classical Coxeter codes $\mathsf{C}_W(r)$ and $\mathsf{C}_W(m - q - 1)$, respectively.*

Proof. This follows directly from Theorem 1.2.4 and Lemma 2.4.9. □

In Section 4.3 we give a few examples of quantum Coxeter codes.

4.2 Transversal Logic on Quantum Coxeter Codes

We will now demonstrate how the simple combinatorial structure of Coxeter groups leads to a large class of transversal logical operators acting on the code space of a quantum Coxeter code. Throughout, we suppose that (W, S) is a fixed (spherical) Coxeter system of rank m, $q, r \in \mathbb{Z}_{\geq 0}$ satisfy $0 \leq q < r \leq m$. Consider the quantum code $\mathsf{QC}_W(q, r)$.

The duality of Coxeter codes combined with Lemma 2.4.9 implies that the logical X and Z spaces for $\mathsf{QC}_W(q, r)$ are given by the classical codes $\mathsf{C}_W(r)$ and $\mathsf{C}_W(m - q - 1)$. That is, a vector $x \in \mathbb{F}_2^{|W|}$ gives rise to a *logical* X, $X_{\operatorname{supp} x}$, if and only if $x \in \mathsf{C}_W(r)$ (and similarly for Z). Building upon this fact, we construct transversal logical operators formed of diagonal Z rotations acting on standard cosets. We consider the single-qubit gates

$$Z(k) = |0\rangle\langle 0| + e^{i\frac{\pi}{2^k}} |1\rangle\langle 1|, \quad k \geq 0.$$

The $Z(k)$ operators are defined so that they reproduce the natural k-th level Clifford hierarchy single-qubit Z basis gates: $Z(-1) = \mathbb{I}$, the identity, $Z(0) = Z$, the Pauli Z operator, $Z(1) = \mathrm{S} = \sqrt{Z}$, the phase gate, $Z(2) = T = \sqrt{\mathrm{S}}$, the T gate, etc. Note that $Z(k)^{2^\ell} = Z(k-\ell)$ for $\ell \in \{0, \ldots, k+1\}$, so $Z(k)$ has order 2^{k+1}.

We will now define a set of natural transversal operators acting on physical qubits indexed by the elements of W. For an arbitrary subset $A \subseteq W$, let $\widetilde{Z}(k)_A$ be the $|W|$-qubit operator implementing the following gate on the qubit corresponding to $w \in W$:

$$\left(\widetilde{Z}(k)_A\right)_w \coloneqq \begin{cases} Z(k), & \text{if } w \in A \text{ and } \ell(w) \text{ is even} \\ Z(k)^\dagger, & \text{if } w \in A \text{ and } \ell(w) \text{ is odd} \\ \mathbb{I}, & \text{otherwise,} \end{cases}$$

where ℓ is the length function on W (see Section 2.6).

Definition 4.2.1. When $A \coloneqq \sigma\langle K\rangle$ is a standard coset, we say that $\widetilde{Z}(k)_{\sigma\langle K\rangle}$ is a signed standard coset operator, or simply *coset operator*.

Thus, when $k = 0$ and $\widetilde{Z}(0)_{\sigma\langle K\rangle} = Z_{\sigma\langle K\rangle}$ is a Z operator acting on $\sigma\langle K\rangle$, the following is a consequence of Lemma 2.4.9:

Lemma 4.2.2. *Consider $\mathsf{QC}_W(q,r)$ and let $A \leq W$ be a standard coset. The following are true:*

- $Z_A \in \mathcal{S}^{(0)}$ *if and only* $\operatorname{rank} A \geq r+1$, *and* $X_A \in \mathcal{S}^{(0)}$ *if and only if* $\operatorname{rank} A \geq m-q$.

- $Z_A \in \mathcal{E}^{(0)}$ *if and only if* $\operatorname{rank} A \geq q+1$*, and* $X_A \in \mathcal{E}^{(0)}$ *if and only if* $\operatorname{rank} A \geq m-r$*.*

The aim of the present section is to prove the following generalization of Lemma 4.2.2 to $Z(k)_A$ and $\widetilde{Z}(k)_A$ operators for arbitrary values of $k \geq 0$, previously called the Validity Theorem:

Theorem 4.2.3. *Consider* $\mathsf{QC}_W(q,r)$*,* $k \in \mathbb{Z}_{\geq 0}$*, and* $A \leq W$ *be a standard coset. The following are true:*

1. $\widetilde{Z}(k)_A \in \mathcal{S}^{(k)}$ *if and only if* $\operatorname{rank} A \geq (k+1)r+1$*.*

2. $\widetilde{Z}(k)_A \in \mathcal{E}^{(k)}$ *if and only if* $q+kr+1 \leq \operatorname{rank} A \leq (k+1)r$*.*

The two parts of this statement are proved as Claims 4.2.8 and 4.2.9 below, by examining how the coset operators conjugate the logical X operators for $\mathsf{QC}_W(q,r)$. We also mention that one can consider *unsigned* $Z(k)$ operators, i.e., without locally inverting based on the parity of $\ell(w)$; Theorem 4.2.3 is only applicable for such operators when $W = \mathbb{Z}_2^m$ and $\mathsf{QC}_W(q,r) = QRM_m(q,r)$, which will be discussed in Section 5.1.

Denoting $\omega_k := e^{-i\frac{\pi}{2^k}}$, one can easily compute that for all $k \geq 0$,

$$Z(k)XZ(k)^\dagger = \omega_k Z(k-1)X.$$

It immediately follows that for any two subsets of qubits, $A, B \subseteq W$,

$$\widetilde{Z}(k)_A X_B \widetilde{Z}(k)_A^\dagger = \alpha \widetilde{Z}(k-1)_{A\cap B} X_B \tag{4.1}$$

for some unit-norm $\alpha \in \mathbb{C}$. By definition, the X and Z stabilizers of $\mathsf{QC}_W(q,r)$ have positive signs; in order to preserve the code space it will be crucial that this α is *precisely* $\alpha = 1$. This motivates the

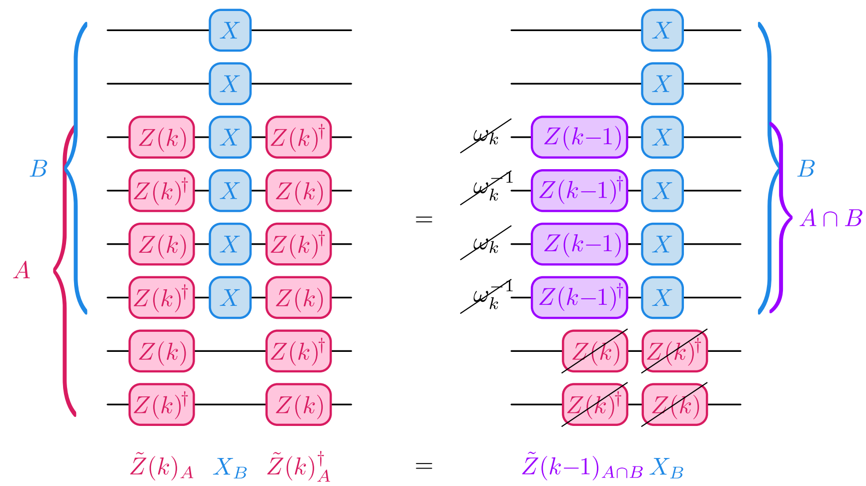


Figure 4.1: A visual "proof" of Lemma 4.2.5

following:

Definition 4.2.4. For subsets $A, B \subseteq W$ and $k \geq 0$, the operator $\widetilde{Z}(k)_A X_B \widetilde{Z}(k)_A^\dagger$ is said to be *phase-free* if $\widetilde{Z}(k)_A X_B \widetilde{Z}(k)_A^\dagger = \widetilde{Z}(k-1)_{A\cap B} X_B$.

We will always take A and B to be standard cosets, and since any standard coset with strictly positive rank has an even number of vertices via Lemma 2.6.3, the following is true:

Lemma 4.2.5. *For standard cosets $A, B \leq W$ with non-trivial intersection, $\widetilde{Z}(k)_A X_B \widetilde{Z}(k)_A^\dagger$ is phase-free if and only if* $\operatorname{rank} A \cap B \geq 1$.

See Section 4.2 for a proof by illustration.

To prove Claims 4.2.8 and 4.2.9 we will make frequent use of the following statement detailing intersections of various standard cosets in W.

Lemma 4.2.6. *For $\ell \in \{0, \ldots, m\}$, let $\mathcal{B}_{A,\ell}$ denote the collection of rank $\geq \ell$ standard cosets that have a non-trivial overlap with a given standard coset $A \leq W$:*

$$\mathcal{B}_{A,\ell} := \left\{ B \;\middle|\; B \text{ is a standard coset with } \operatorname{rank} B \geq \ell \text{ and } A \cap B \neq \emptyset \right\}.$$

For $p \in \mathbb{N}$, $\operatorname{rank} A \cap B \geq p$ for every $B \in \mathcal{B}_{A,\ell}$ if and only if $\operatorname{rank} A \geq m - \ell + p$.

Proof. Without loss of generality, we can assume that $A = \langle J \rangle$ for some $J \subseteq S$.

($\Rightarrow$) By assumption, $\operatorname{rank} A \cap B \geq p$, so $|J| = \operatorname{rank} A \geq p$. Suppose for contradiction that $p \leq |J| < m - \ell + p$. Define $K \subseteq S$ to be the union of $[m] \setminus J$ and any $p-1$ elements of J, so that $|K| > m - (m - \ell + p) + p - 1 = \ell - 1$. But then $\langle K \rangle$ is has rank $\geq \ell$ and $\operatorname{rank} A \cap B = |J \cap K| = p - 1 < p$.

($\Leftarrow$) For arbitrary $B \in \mathcal{B}_{A,\ell}$ there exists a $K \subseteq S$, $|K| \geq \ell$, and a $\sigma \in W$ such that $B = \sigma\langle K \rangle$. As $A \cap B \neq \emptyset$ by definition of $B \in \mathcal{B}_{A,\ell}$, there is a $\rho \in W$ such that $A \cap B = \rho\langle J \cap K \rangle$ and $\operatorname{rank} A \cap B = |J \cap K|$. Since J and K are both subsets of S, which has m elements, a simple counting argument combined with $|J| \geq m - \ell + p$ and $|K| \geq \ell$ implies that $|J \cap K| \geq p$. $\square$

One simple consequence of this structural result is that as long as the rank of A is large enough, conjugating a stabilizer with $\widetilde{Z}(k)_A$ will not introduce any unwanted phases.

Lemma 4.2.7. *For an arbitrary standard coset $A \leq W$, $\widetilde{Z}(k)_A X_B \widetilde{Z}(k)_A^\dagger$ is phase-free for every X stabilizer generator X_B of $\mathsf{QC}_W(q, r)$ if and only if $\operatorname{rank} A \geq q + 1$.*

Proof. By definition of $\mathsf{QC}_W(q, r)$, the X_B's that are stabilizer generators are precisely those where $\operatorname{rank} B = m - q$. By Lemma 4.2.5, the statement of the lemma can be rephrased as follows: $\widetilde{Z}(k)_A X_B \widetilde{Z}(k)_A^\dagger$ is phase-free if and only if $\operatorname{rank} A \cap B \geq 1$ for every standard coset B that has non-trivial intersection with A and satisfies $\operatorname{rank} B \geq m - q$. The desired result therefore holds by applying Lemma 4.2.6 with $\ell = m - q$ and $p = 1$. $\square$

Claim 4.2.8. For $k \geq 0$ and a standard coset A, $\widetilde{Z}(k)_A$ is a level-k Clifford stabilizer for $\mathsf{QC}_W(q, r)$ if and only if $\operatorname{rank} A \geq (k + 1)r + 1$.

Proof. We will prove both the direct and converse parts of the claim by induction on k. When $k = 0$, $\widetilde{Z}(0)_A = Z_A$ and the statement is true by Lemma 4.2.2. Let us suppose that the statement is true for $k \geq 0$ and consider the statement for $k + 1$.

($\Rightarrow$) Suppose for contradiction that there exists a standard coset A such that (1) $\widetilde{Z}(k+1)_A \in \mathcal{S}^{(k+1)}$, but (2) $\operatorname{rank} A \leq (k+2)r$. As A is a standard coset, there exist $\sigma \in W$ and $K \subseteq S$ ($|K| = \operatorname{rank} A$), such that $A = \sigma\langle K \rangle$.

Now, by assumption of $\widetilde{Z}(k)_A \in \mathcal{S}^{(k+1)}$, it must be true that for every logical X coset operator X_B, the operators $\widetilde{Z}(k)_A X_B \widetilde{Z}(k)^\dagger_A$ and X_B are equivalent. Given our assumption for the rank of A, we will obtain a contradiction by constructing a logical X_B for which $\widetilde{Z}(k)_A X_B \widetilde{Z}(k)^\dagger_A \not\equiv X_B$.

Let $K^* \subseteq S$ be any subset of S with $|K^*| = m - r$ elements such that $S \setminus K \subseteq K^*$. Define the standard coset $B := \sigma\langle K^* \rangle$, so that $A \cap B = \sigma\langle K \cap K^* \rangle \neq \emptyset$. Using Eq. (4.1) for $Z(k)$ and $Z(k)^\dagger$ we have that $\widetilde{Z}(k+1)_A X_B \widetilde{Z}(k+1)^\dagger_A = \alpha \widetilde{Z}(k)_{A\cap B} X_B$, where α is some global phase factor dependent on k, A, and B. This implies that for $\widetilde{Z}(k+1)_A X_B \widetilde{Z}(k+1)^\dagger_A \in \mathcal{S}^{(k)}$ to be true it must be that $\widetilde{Z}(k)_{A\cap B} \in \mathcal{S}^{(k)}$, as otherwise $\alpha \widetilde{Z}(k)_{A\cap B} X_B |\psi\rangle$ cannot equal $X_B |\psi\rangle$ for every state $|\psi\rangle$ in the code space of $\mathsf{QC}_W(q, r)$. As it turns out, $\widetilde{Z}(k)_{A\cap B} \in \mathcal{S}^{(k)}$ contradicts our induction hypothesis that

$\operatorname{rank} A \cap B \geq (k+1)r + 1$. Indeed, we can upper-bound this rank as

$$\begin{aligned}
\operatorname{rank} A \cap B &= |K \cap K^*|, \\
&= |K^* \setminus (S \setminus K)|, \\
(S \setminus K \subseteq K^*) \qquad &= |K^*| - |S \setminus K|, \\
&= (m-r) - (m - |K|), \\
&= |K| - r, \\
(\operatorname{rank} A \leq (k+2)r \text{ by assumption (2)}) \qquad &\leq (k+1)r,
\end{aligned}$$

Thus, $\widetilde{Z}(k)_{A\cap B} \notin \mathcal{S}^{(k)}$, implying that $\widetilde{Z}(k+1)_A \notin \mathcal{S}^{(k+1)}$.

($\Leftarrow$) Assume that $\widetilde{Z}(k)_A$ is a level-k Clifford stabilizer for all A satisfying $\operatorname{rank} A \leq (k+1)r+1$. Now suppose that A is a standard coset with $\operatorname{rank} A \geq (k+2)r+1$. Let B be an arbitrary standard coset for which X_B is an undetectable X error, which by Lemma 4.2.2 occurs if and only if $\operatorname{rank} B \geq m-r$. By Fact 2.5.6, the desired result, $\widetilde{Z}(k+1)_A \in \mathcal{S}^{(k+1)}$, holds if and only if $\widetilde{Z}(k+1)_A X_B \widetilde{Z}(k+1)_A^\dagger \equiv X_B$. Thus, we consider the operator $\widetilde{Z}(k+1)_A X_B \widetilde{Z}(k+1)_A^\dagger$.

As $\operatorname{rank} A \geq r+1 \geq q+1$, Lemma 4.2.7 implies that the operator is phase-free, and so

$$\widetilde{Z}(k+1)_A X_B \widetilde{Z}(k+1)_A^\dagger = \widetilde{Z}(k)_{A\cap B} X_B.$$

Now notice that, since $\operatorname{rank} A \geq (k+2)r+1 = m-(m-r)+(k+1)r+1$, by Lemma 4.2.6 we have that $\operatorname{rank} A \cap B \geq (k+1)r+1$, so $\widetilde{Z}(k)_{A\cap B}$ is a level-k Clifford stabilizer for the code and the desired result holds by the induction hypothesis. $\square$

Claim 4.2.9. For $k \in \mathbb{Z}_{\geq 0}$ and a standard coset A, $\widetilde{Z}(k)_A$ is a level-k undetectable Clifford error for

$\mathsf{QC}_W(q,r)$ if and only if $\operatorname{rank} A \geq q + kr + 1$.

Proof. Let X_B be an arbitrary stabilizer generator. By definition (2.6), $\widetilde{Z}(k)_A \in \mathcal{N}^{(k)}$ if and only if $\widetilde{Z}(k)_A X_B \widetilde{Z}(k)_A^\dagger \in \mathcal{S}^{(k-1)}$ for every X_B acting on a standard coset B with $\operatorname{rank} B = m - q$. Using (4.1) for $Z(k)$ and $Z(k)^\dagger$, we have that $\widetilde{Z}(k)_A X_B \widetilde{Z}(k)_A^\dagger = \alpha \widetilde{Z}(k-1)_{A\cap B} X_B$, where α is some global phase factor dependent on k, A, and B. Since X_B is a stabilizer, we have that $\widetilde{Z}(k)_A X_B \widetilde{Z}(k)_A^\dagger \in \mathcal{S}^{(k)}$ if and only if $\alpha \widetilde{Z}(k-1)_{A\cap B} \in \mathcal{S}^{(k-1)}$ for every B with $\operatorname{rank} B = m - q$.

($\Rightarrow$) We assume that $\alpha \widetilde{Z}(k-1)_{A\cap B} \in \mathcal{S}^{(k-1)}$ for every standard coset B with $\operatorname{rank} B = m - q$, and we seek to show that $\operatorname{rank} A \geq q + kr + 1$. If the global phase factor $\alpha_k \neq 1$, then $\alpha \widetilde{Z}(k-1)_{A\cap B}$ cannot fix the code space, so by Lemma 4.2.7 we have that $\operatorname{rank} A \geq q+1$ in order for $\widetilde{Z}(k)_A X_B \widetilde{Z}(k)_A^\dagger$ to be phase-free. Now, we must show that $\widetilde{Z}(k-1)_{A\cap B} \in \mathcal{S}^{(k-1)}$ for every B such that $\operatorname{rank} B = m-q$. Using Claim 4.2.8, $\widetilde{Z}(k-1)_{A\cap B} \in \mathcal{S}^{(k-1)}$ if and only if $\operatorname{rank} A\cap B \geq kr+1$. By Lemma 4.2.6 we have that $\operatorname{rank} A \cap B \geq kr + 1$ for every B with $\operatorname{rank} B = m - q$ only if $\operatorname{rank} A \geq m - (m - q) + kr + 1 = q + kr + 1$, as desired.

($\Leftarrow$) We assume that $\operatorname{rank} A \geq q + kr + 1$, and we seek to show that $\alpha \widetilde{Z}(k-1)_{A\cap B} \in \mathcal{S}^{(k-1)}$ for every standard coset B with $\operatorname{rank} B = m - q$. As $k \geq 0$, $\operatorname{rank} A \geq q + 1$ and Lemma 4.2.7 implies that $\widetilde{Z}(k)_A X_B \widetilde{Z}(k)_A^\dagger$ is phase-free, and so $\alpha = 1$. By Lemma 4.2.6, since $\operatorname{rank} A \geq q + kr + 1$ we have that $\operatorname{rank} A \cap B \geq kr + 1$ for every B with $\operatorname{rank} B = m - q$. Claim 4.2.8 thus implies that $\widetilde{Z}(k-1)_{A\cap B} \in \mathcal{S}^{(k-1)}$, as desired. $\square$

We have thus completed the proof of Theorem 4.2.3, giving necessary and sufficient conditions for when coset operators performs non-trivial logic on $\mathsf{QC}_W(q,r)$. A simple corollary of Theorem 4.2.3 gives one hint toward the structure of the logical circuits:

Corollary 4.2.10. *If $\widetilde{Z}(k)_A \in \mathcal{N}^{(k)}$, then $\widetilde{Z}(k)_A^2 \in \mathcal{S}^{(k-1)}$ and $\widetilde{Z}(k)_A \equiv \widetilde{Z}(k)_A^\dagger$.*

Proof. The first implication follows by Theorem 4.2.3 since $\dim A \geq q + kr + 1 \geq \big((k-1)+1\big)r + 1$ and $\widetilde{Z}(k)_A^2 = \widetilde{Z}(k-1)_A$. Since $\widetilde{Z}(k)_A$ is unitary, the logical involution property implies that $\widetilde{Z}(k)_A$ is logically Hermitian. $\square$

One may expect that, as a diagonal operator in the k-th level of the Clifford hierarchy, operator $\widetilde{Z}(k)_A$ discussed in this corollary implements a logical diagonal operator in the k-th level, as well. The only diagonal k-th level Clifford hierarchy operators that are Hermitian are circuits of multi-controlled-Z gates, where the number of controls is at most $k-1$ for any gate [CGK17]. Thus, Corollary 4.2.10 suggests that $\widetilde{Z}(k)_A$ implements logical multi-controlled-Z circuits. In the next section, we will explicitly prove this for the quantum RM case where $W = \mathbb{Z}_2^m$, and fully characterize the implemented circuits.

4.3 Examples

4.3.1 Iceberg codes

Consider the dihedral group $I_2(n)$ whose Cayley graph is a $2n$-cycle. Then $\mathsf{QC}_W(0,1)$ is the *Iceberg code* generated by global $X^{\otimes 2n}$ and $Z^{\otimes 2n}$ stabilizers.

4.3.2 3D ball codes

The Cayley graphs of the Coxeter systems A_3, B_3, and H_3 correspond to the truncated octahedron, truncated cuboctahedron, and truncated icosidodecahedron, respectively. By definition, the quantum Coxeter codes $\mathsf{QC}_W(0,1)$ for these three groups have a single global X stabilizer, and Z stabilizers given by the faces of the corresponding polyhedron. These three codes appear in [VK22b] as examples of *3D ball codes*. The authors of [VK22b] note that a transversal operator consisting of the T operator on a certain half of the qubits, and $T^\dagger$ on the other half, is a non-trivial logical operator for these codes; this result also follows from our Theorem 4.2.3.

4.3.3 The dihedral (quantum) code family

Consider the Coxeter system $W = I_2(n)^\mu$, μ copies of the $2n$-element dihedral group for $\mu \geq 2$, and the quantum code $\mathsf{QC}_{I_2(3)^\mu}(\mu-1,\mu)$. For $n = 3$, the parameters of the particular code $\mathcal{Q}_\mu :=$ $\mathsf{QC}_{I_2(3)^\mu}(\mu-1,\mu)$ are

$$\left[\left[\text{length} = 6^\mu, \kappa_\mu = \left\langle \begin{matrix} I_2(3)^\mu \\ \mu \end{matrix} \right\rangle, d = 2^\mu \right]\right].$$

The number of logical qubits κ can be computed explicitly: recalling the proof of Theorem 4.1.1, this is simply the "central coefficient" in the expansion of the Eulerian polynomial $W(t)$:

$$\kappa_\mu = \text{Coeff}_{[t^\mu]}(t^2+4t+1)^\mu = \sum_{i,j,l} \frac{\mu!}{i!j!l!} 4^j,$$

where $i, j, l \geq 0$ and $i+j+l = \mu, 2i+j = \mu$. Solving for j, l, we obtain $l = i, j = \mu - 2i$. Substitute into the above line and rewrite to obtain the expression

$$\kappa_\mu = \sum_{i=0}^{\lfloor \mu/2 \rfloor} \frac{\mu!}{(i!)^2(\mu-2i)!} 4^{\mu-2i}. \tag{4.2}$$

Let us compare the obtained parameters with existing proposals. A family of codes with similar parameters was considered recently in [Got24a]. The codes in this family, which the authors refer to as *many-hypercube codes*, are obtained as concatenations of μ copies of the $[[6,4,2]]$ Iceberg code, i.e., concatenations of $\mathsf{QC}_{I_2(3)}(0,1)$, resulting in parameters $[[6^\mu, 4^\mu, 2^\mu]]$ for all $\mu \geq 2$.

Clearly, the codes $\mathcal{Q}_\mu$ have the same length and distance as the many-hypercube codes. Isolating the first two terms in Eq. (4.2), we further obtain

$$\kappa_\mu \geq \Big(1 + \frac{\mu(\mu-1)}{16}\Big)4^\mu,$$

where the inequality is strict for all $\mu \geq 4$. For the same values of length and distance, quantum (dihedral) Coxeter codes $\mathcal{Q}_\mu$ encode strictly more logical information than the construction of [Got24a] for all $\mu > 1$.

One may wonder how the information rates of these two code families compare as μ increases. For the many-hypercube codes, the rate declines exponentially as $(2/3)^\mu$. To compute the rate asymptotics of the $\mathcal{Q}_\mu$ family, we have to analyze the behavior of the sum in Eq. (4.2), relying on the generating function of the "central trinomial coefficients" [Wag12]. As a result, we obtain $\Theta(\mu^{-1/2})$, so the rate of quantum Coxeter codes, while not constant, exhibits a much slower decline.

Let us give a few numerical examples using Table 3.3. It is easier to compute the number of logical qubits once we realize that $\kappa_\mu = \dim(\mathsf{C}_{I_2(3)^\mu}(\mu)) - \dim(\mathsf{C}_{I_2(3)^\mu}(\mu-1))$. For instance, for $\mu = 3, 4$, the codes $\mathcal{Q}_\mu$ have parameters $[[216, 88, 8]]$ and $[[1296, 454, 16]]$. At the same time, the many-hypercube codes for the same μ have parameters $[[216, 64, 8]]$ and $[[1296, 256, 16]]$.

Note that the distance of the code $\mathcal{Q}_3 = \mathsf{QC}_{I_2(3)^3}(2, 3)$ still falls short of the best known quantum code[1] for $n = 216$, $\kappa = 88$, which has distance 21. At the same time, both quantum Coxeter and many-hypercube codes are instances of general code families with clearly described structure, and in the latter case are also equipped with efficient encoding and decoding procedures.

[1] Per codetables.de, the code was constructed by computer. The tables stop at length $n = 256$.

Chapter 5: Characterizing Logic in Quantum RM Codes

5.1 Specializing To The Hypercube

We now restrict our attention to the case where the Coxeter system is $(\mathbb{Z}_2^m, S_m)$, the finite elementary Abelian 2-group $\mathbb{Z}_2^m$ with generating set of weight-1 bit strings $S_m := \{e_i\}_{i=1}^m$. This choice yields the well-known family of quantum Reed–Muller (RM) codes $QRM_m(q,r) := \mathsf{QC}_{\mathbb{Z}_2^m}(q,r)$. In light of Theorem 4.2.3, our goal will be to explicitly characterize the logic implemented by coset operators $Z(k)_A$. To do so, we begin by recasting our terminology to better reflect the particular structure of $\mathbb{Z}_2^m$. Throughout, we let $S := S_m$, as we are only working in the case where $W = \mathbb{Z}_2^m$. We will frequently abuse notation by referring to S and the set $[m]$ interchangeably. For example, when we write "let $i \in S$", this should be interpreted to mean "let $e_i \in S$ for $i \in [m]$".

One common view of the group $\mathbb{Z}_2^m$ is that of the m-dimensional Boolean hypercube graph, where vertices correspond to the elements of $\mathbb{Z}_2^m$ and two vertices are connected by an edge whenever their labels differ in a single coordinate, i.e., $x, y \in \mathbb{Z}_2^m$ are connected by an edge if $x = y + e_i$ for some $i \in [m]$. In this view, a standard coset $x + \langle J \rangle$ for $x \in \mathbb{Z}_2^m$ and $J \subseteq S_m$ geometrically appears like a $|J|$-dimensional subcube of the Boolean hypercube. Thus, for the remainder of this chapter we will use the subcube terminology from the introduction:

Definition 1.1.2. (Subcubes of the hypercube)

- A *standard subcube* of the m-dimensional hypercube is a subgroup of the form $\langle J \rangle$, where $J \subseteq S$ is a subset of generators. That is, bit strings in $\langle J \rangle$ are precisely those whose support lies entirely within the set J, viewed as a subset of $[m]$.

- A *subcube* is any coset of a standard subcube, i.e., subsets of $\mathbb{Z}_2^m$ of the form $A := z + \langle J \rangle$ for some $z \in \mathbb{Z}_2^m$. The set J is called the *type* of A[1] and the cardinality $|J|$ is called its *dimension*.

Recall that we write $A \sqsubseteq \mathbb{Z}_2^m$ to indicate that the subset A is a subcube. Note that the bits appearing outside of J form an invariant of a subcube A of type J: given two bit strings $x, y \in x + \langle J \rangle$, $x_i = y_i$ for every $i \in S \setminus J$. An i-cube is a subcube with dimension equal to $i \geq 0$.

Remark 5.1.1. We are now using the term "standard" in a different way than before: With Coxeter groups and codes, "standard" referred to cosets of subgroups generated by subsets S. Here, "standard" subcubes refers to standard subgroups in the Coxeter system $(\mathbb{Z}_2^m, S_m)$, and subcubes (without the adjective "standard") are more general standard *cosets*.

We now recall the definition of a quantum Reed–Muller code:

Definition 1.4.1 (Quantum RM codes)**.** Let $0 \leq q \leq r \leq m$ be non-negative integers. The *quantum Reed–Muller code* of order (q, r) and length 2^m, denoted by $QRM_m(q, r)$, is defined as the common $+1$ eigenspace of a Pauli stabilizer group $\mathcal{S} := \langle \mathcal{S}_X, \mathcal{S}_Z \rangle$, with stabilizer generators given by

$$\mathcal{S}_X := \left\{ X_A \;\middle|\; A \text{ is an } (m-q)\text{-cube} \right\}, \tag{1.4}$$

$$\mathcal{S}_Z := \left\{ Z_A \;\middle|\; A \text{ is an } (r+1)\text{-cube} \right\}, \tag{1.5}$$

Our main goal will be to study *signed subcube operators*, $\widetilde{Z}(k)_A$, which implement the following

[1] Note that the bits appearing outside of J form an invariant of a subcube A of type J: given two bit strings $y, z \in x + \langle J \rangle$, $y_i = z_i$ for every $i \in S \setminus J$.

gate on the physical qubit index by an $x \in \mathbb{Z}_2^m$:

$$\left(\widetilde{Z}(k)_A\right)_x \coloneqq \begin{cases} Z(k), & \text{if } x \in A \text{ and } |x| \text{ is even} \\ Z(k)^\dagger, & \text{if } x \in A \text{ and } |x| \text{ is odd} \\ \mathbb{I}, & \text{otherwise.} \end{cases}$$

That is, a signed subcube operator is precisely a signed coset operator from the previous section, specialized to the case of the Boolean hypercube $W = \mathbb{Z}_2^m$. One could also consider *unsigned* subcube operators $Z(k)_A$ acting as $Z(k)$ on the qubits in A and identity elsewhere. In fact, one can prove the following version of Theorem 4.2.3 for these subcube operators:

Proposition 5.1.2. *Consider $QRM_m(q, r)$, $k \in \mathbb{Z}_{\geq 0}$, and $A \sqsubseteq \mathbb{Z}_2^m$ a subcube of the m-dimensional Boolean hypercube. The following are true:*

1. $Z(k)_A \in \mathcal{S}^{(k)}$ *if and only if* $\dim A \geq (k+1)r + 1$.
2. $Z(k)_A \in \mathcal{E}^{(k)}$ *if and only if* $q + kr + 1 \leq \dim A \leq (k+1)r$.

The main reason that signed coset operators are more natural than unsigned ones is Lemma 4.2.7: no unwanted global phases are introduced when conjugating stabilizers and logicals with signed coset operators of large-enough rank, because the intersection always contains a matching number of $Z(k)$ and $Z(k)^\dagger$ operators. For instance, when conjugating logical X operators with unsigned coset operators (to imply the logical identity property), it is imperative that the total number of $Z(k)$ operators acting on the intersection is congruent to 0 modulo 2^{k+1}; the lower bounds on dimension when considering unsigned *subcube* operators, i.e., specifically for the quantum RM code family, will *still* guarantee unit phases.

To give another example of how the phase considerations manifest for unsigned subcube operators, consider the simple $[[4,2,2]]$ code with two stabilizer generators $X^{\otimes 4}$ and $Z^{\otimes 4}$. This code is the quantum RM code $QRM_2(0,1)$, where the edges of the square give rise to logical X and Z operators for the code. It is simple to show that a global phase gate $Z(1)^{\otimes 4} = \mathrm{S}^{\otimes 4}$ preserves the code space: S conjugates X as $\mathrm{S}\,X\,\mathrm{S}^\dagger = -iZX$, so $(\mathrm{S}\,X\,\mathrm{S}^\dagger)^{\otimes 4} = (-i)^4 Z^{\otimes 4} X^{\otimes 4} = Z^{\otimes 4} X^{\otimes 4}$ is clearly a stabilizer. Its conjugation action on the X edge operator $X \otimes X \otimes I \otimes I$ gives $(-i)^2 (Z \otimes Z \otimes I \otimes I)(X \otimes X \otimes I \otimes I) = -(Z \otimes Z \otimes I \otimes I)(X \otimes X \otimes I \otimes I)$. While the -1 phase is not inherently a problem, it's indicative of the fact $S^{\otimes 4}$ does not simply implement a logical controlled-Z for the code, but rather the slightly more complicated $\overline{CZ}(\overline{Z} \otimes \overline{Z})$ circuit. We can fix this, however, by considering a *signed* version of the global phase gate, $\mathrm{S} \otimes \mathrm{S}^\dagger \otimes \mathrm{S} \otimes \mathrm{S}^\dagger$, acting as S on two opposite corners of the square and as the adjoint on the remaining two vertices. The logical action of this gate is precisely $\overline{CZ}$, and it is well known that the $Z(k)$ generalization of this signed gate implements the m-qubit logical multi-controlled-Z gate in the family of hypercube codes, $QRM_m(0,1)$ [WBB22, Cam].

We will ultimately see in Section 5.3 that the logical circuit for $Z(k)_A$ can be deduced from that of signed subcube operators $\widetilde{Z}(k)_A$. For now, we will only consider signed operators.

In order to define the action of a logical circuit, we will first need to detail a *symplectic basis* of logical Pauli errors (Definition 2.5.7). For a subset $J \subseteq S$, we use the shorthand $e_J := \sum_{i \in J} e_i \in \mathbb{Z}_2^m$ to denote the indicator bit string of length m corresponding to J.

Lemma 5.1.3. *Consider the following sets of Pauli X and Z operators*

$$
\begin{aligned}
L_X &:= \left\{ X_{e_J + \langle S \setminus J \rangle} \;\middle|\; J \subseteq S,\ q+1 \leq |J| \leq r \right\}, \\
L_Z &:= \left\{ Z_{\langle J \rangle} \;\middle|\; J \subseteq S,\ q+1 \leq |J| \leq r \right\}.
\end{aligned}
$$

$\{L_X, L_Z\}$ *is a symplectic basis for* $QRM_m(q,r)$*. In particular, operators* $Z_{\langle J\rangle} \in L_Z$ *and* $X_{e_K+\langle S\setminus K\rangle} \in L_X$ *commute if and only if* $J \neq K$*.*

Proof. The equivalence between signed monomials and indicator functions of subcubes implies that these X and Z operators generate the corresponding logical spaces. We now prove the symplectic condition:

($\Rightarrow$) Assuming $J = K$, we have that $\langle J\rangle \cap (e_J + \langle S \setminus J\rangle) = \{e_J\}$, implying that $Z_{\langle J\rangle}$ and $X_{\langle S\setminus K\rangle}$ have overlapping support on a single qubit and therefore anti-commute.

($\Leftarrow$) Consider the set of qubits that are acted on by both operators, given by $A \coloneqq \langle J\rangle \cap (e_K + \langle S \setminus K\rangle)$. We proceed in cases:

Case I. ($J \subsetneq K$) Note that this case can only occur when $q < r - 1$. Suppose that $x \in A \neq \emptyset$. Then there exists $J' \subseteq J$ and $M \subseteq (S \setminus K)$ such that $x = e_{J'} = e_K + e_M$, implying that $e_{J'} + e_K = e_M$. Now, since $J \subset K$, we are guaranteed that $J' \cap M = \emptyset$, and for the equality to hold, it must be that $e_{J'} + e_K = e_M = 0$. Thus, we have that $e_{J'} = e_K$. But by assumption, K is strictly larger than J', so this equation cannot be satisfied and no such x can exist. Thus $A = \emptyset$ and the operators commute.

Case II. ($J \setminus K \neq \emptyset$) Recall that either $A = \emptyset$ or else there is an $x \in \mathbb{Z}_2^m$ such that $A = x + \langle J \cap (S \setminus K)\rangle$. We are guaranteed in this case that $J \cap (S \setminus K) \neq \emptyset$, so $|A| \in \left\{0, 2^{|J\cap(S\setminus K)|}\right\}$ is even and the operators commute. □

Lemma 5.1.3 allows us to use the subsets, $J \subseteq S$, with $q + 1 \leq |J| \leq r$ to uniquely index the logical qubits of the $QRM_m(q,r)$ code:

Definition 5.1.4 (Index set for the logical qubits)**.** Consider the quantum code $QRM_m(q,r)$. The collection of subsets $\mathcal{Q} \coloneqq \{J \subseteq S \mid q + 1 \leq |J| \leq r\}$ is called the *index set for logical qubits of*

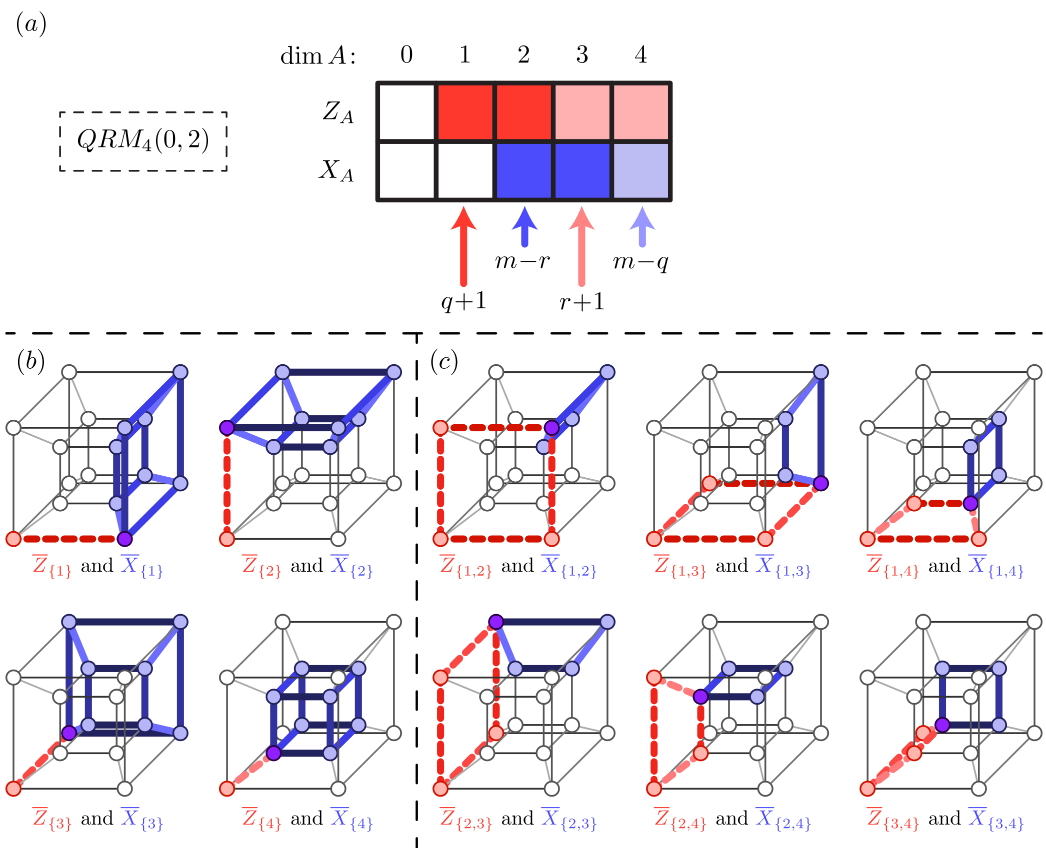


Figure 5.1: Consider the quantum RM code $QRM_4(0,2)$, whose physical qubits are indexed by the vertices of the 4-dimensional hypercube.

(a) By construction, a transversal Z operator applied to a subcube with dimension equal to either 1 or 2 (edges/squares) is necessarily a Z logical operator (represented by dark red boxes). Similarly, a transversal X operator applied to a subcube with dimension equal to either 2 or 3 (squares/cubes) is necessarily an X logical operator (represented by dark blue boxes). The light red and blue boxes indicate dimensions where Z_A and X_A act as stabilizers of the code, respectively. The white boxes indicate dimensions where neither Z_A nor X_A preserve the code space.

(b)–(c) The code has $\binom{4}{1} + \binom{4}{2} = 10$ logical qubits that are indexed by subsets $J \subseteq [m]$ with $|J| = 1$ or 2, and the distance of the code is 2. Thus, there are two classes of logical operators, those whose index set J has size $|J| = 1$, shown in (b), and those whose index set has size $|J| = 2$, shown in (c). Each of the 10 4-cubes shown in (b)–(c) represents a symplectic pair of logical Pauli operators. The (red) dashed edges and squares indicate Z subcube operators and the (blue) solid squares and cubes indicate X subcube operators. A symplectic pair of operators overlap on a single qubit, namely, the qubit with index $e_J := \sum_{i\in J} e_i$. These qubits are represented by (purple) vertices that lie at the intersection of the corresponding dashed and solid subcubes.

(b) The first class of logical operators are the Z operators that act on subcubes of dimension 1 (dashed red edges), together with the X operators that act on subcubes of *codimension* 1 (solid blue cubes).

(c) The second class of logical operators are the Z operators that act on subcubes of dimension 2 (dashed red squares), together with the X operators that act on subcubes of *codimension* 2 (solid blue squares).

$QRM_m(q,r)$. For $J \in \mathcal{Q}$, the *J-th logical qubit*[2] *of* $QRM_m(q,r)$ is defined via the logical Pauli operators $\overline{Z}_J := Z_{\langle J \rangle}$ and $\overline{X}_J := X_{e_J + \langle S \setminus J \rangle}$.

Instead of considering arbitrary subcubes $A \sqsubseteq \mathbb{Z}_2^m$, it turns out that we only need to consider the standard subcube operators; we will prove in Section 5.2.1 that every $\widetilde{Z}(k)_A$ operator can be decomposed as a product of operators $\widetilde{Z}(k')_{\langle K \rangle}$ for various $k' \leq k$ and $K \subseteq S$. This motivates the following generalization of Definition 5.1.4:

Definition 5.1.5 (Index set for the k-th level logicals)**.** For $k \geq 0$, the *index set for the k-th level Clifford logical operators of* $QRM_m(q,r)$, denoted by $\mathcal{Q}_k \subseteq \mathscr{P}(S)$, is given by the following collection of subsets of generators (which implicitly depends on the choices of q and r):

$$\mathcal{Q}_k := \{K \subseteq S \mid q + kr + 1 \leq |K| \leq (k+1)r\} \,. \tag{5.1}$$

That is, $K \in \mathcal{Q}_k$ implies that $\widetilde{Z}(k)_{\langle K \rangle}$ acts on a subcube with dimension large enough to preserve stabilizers but not so large as to realize trivial logic.

As mentioned earlier, Theorem 4.2.3 implies that the logical circuit implemented by $\widetilde{Z}(k)_{\langle K \rangle}$, $K \in \mathcal{Q}_k$, will be a circuit composed of multi-controlled-Z operators (see Section 2.3 for the definition/notation of such circuits). Given a $K \in \mathcal{Q}_k$, we will now define such a collection that will, in many cases, correctly determine the corresponding logical circuit for $\widetilde{Z}(k)_{\langle K \rangle}$. Recall from Definition 5.1.4 that a set of logical qubits $\mathcal{J}$, itself, is a collection of subsets of generators $J \subseteq S$.

Definition 5.1.6 (Minimal covers for logical index sets)**.** Suppose that $K \in \mathcal{Q}_k$. A set of logical qubits $\mathcal{J} \subseteq \mathcal{Q}$ is said to form a *$\mathcal{Q}$-minimal cover for K*, or simply a *minimal cover for K*, if (1) $\mathcal{J}$ is a cover

[2]We emphasize a possible point of confusion: the index set for logical qubits is, itself, a collection of subsets.

of K, i.e., $\bigcup_{J \in \mathcal{J}} J = K$, and (2) the number of logical qubits in $\mathcal{J}$ is $|\mathcal{J}| = k + 1$. Since $|J| \leq r$ for each $J \in \mathcal{Q}$ and $|K| \geq q + kr + 1$ by Definition 5.1.5, $k + 1$ is the smallest possible number of sets from $\mathcal{Q}$ that cover K, hence the "minimal" designation.

Let $\mathcal{F}(K) \subseteq \mathscr{P}(\mathcal{Q})$ denote the collection of all minimal covers for K,

$$\mathcal{F}(K) \coloneqq \{\mathcal{J} \subseteq \mathcal{Q} \mid \mathcal{J} \text{ is a minimal cover for } K\} .$$

Remark 5.1.7. The "minimality" condition implies that a multi-controlled-Z circuit corresponding to $\mathcal{F}(K)$ lies in the k-th level of the Clifford hierarchy (see Section 2.3). We will see that $Z(k)$ subcube operators implement such circuits, matching intuitively with the fact that $Z(k)$ is also in the k-th level. The "cover" property implies a special overlap condition: $\mathcal{J}$ is a cover of K if and only if $Z(k)_{\langle K \rangle}$ jointly overlaps with all of the logical $\overline{X}_J$ operators, $J \in \mathcal{J}$, on a *single* qubit (e.g., see Fig. 5.2). While we won't utilize this property, perhaps an odd overlap on the joint support of X logicals is part of a more general phenomenon related to the classification of the circuits implemented by transversal $Z(k)$ operators; we leave this question, which may be related to the triorthogonality property [BH12], for future work.

When $k = 0$, any $\mathcal{Q}$-minimal cover for $J \in \mathcal{Q}$ necessarily contains a single element from $\mathcal{Q}$, which by definition must be J itself. So, the set of all minimal covers for $J \in \mathcal{J}$ is simply $\mathcal{F}(J) = \{\{J\}\}$. Any theorem describing the logical circuit for $\widetilde{Z}(k)_{\langle K \rangle}$, $K \in \mathcal{Q}_k$ must necessarily reduce to $Z(0)_{\langle J \rangle} = \overline{Z}_J$ in the case that $J \in \mathcal{Q}$. We note that, at least in this simple case of $k = 0$, it is trivial that $Z(0)_{\langle J \rangle} = \overline{C^{\mathcal{F}(J)} Z}$ for $J \in \mathcal{Q}$; this fact will hold for more general $k \geq 0$, at least in the case that $q \geq 1$.

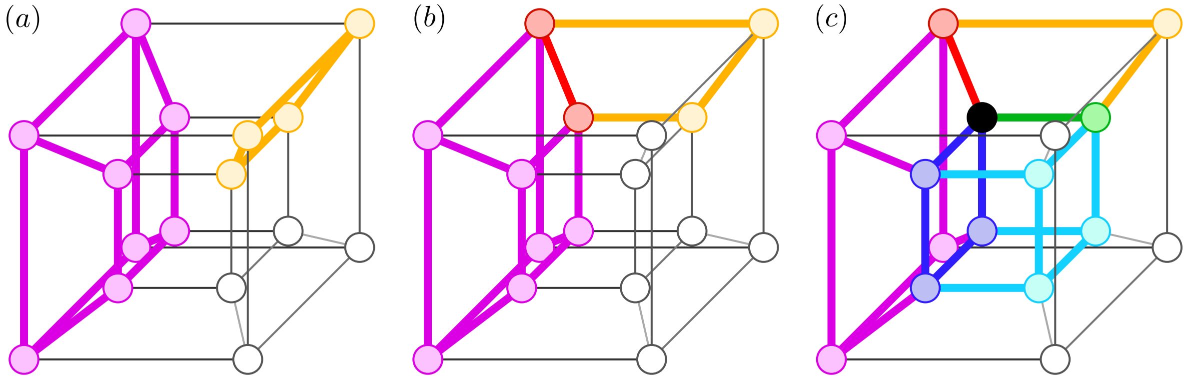


Figure 5.2: Consider the code $QRM_4(0, 2)$ and the standard subcube operator $\mathrm{S}_{\langle 2,3,4\rangle}$. To motivate the utility of the "cover" property for a collection of logical qubits $\mathcal{J} \subseteq \mathcal{Q}$, we consider the intersection of the standard subcube $\langle 2, 3, 4\rangle$ (represented as a magenta cube in each subfigure) with various collections.
(a) In this case $\mathcal{J} = \{\{1, 2\}\}$ is not a cover for $\{2, 3, 4\}$. The logical X operator it corresponds to acts on the *non-standard* subcube $1100 + \langle 3, 4\rangle$ (represented by an orange square). Clearly this subcube does not intersect $\langle 2, 3, 4\rangle$, so subcube operators acting on them commute.
(b) In this case $\mathcal{J} = \{\{2, 3\}\}$ is not a cover for $\{2, 3, 4\}$. The logical X operator it corresponds to acts on the *non-standard* subcube $0110 + \langle 1, 4\rangle$ (represented by an orange square). By construction, this subcube intersects $\langle 2, 3, 4\rangle$ on an even number of qubits (represented as red dots).
(c) In this case $\mathcal{J} = \{\{2, 3\}, \{4\}\}$ *is* a cover for $\{2, 3, 4\}$. It corresponds to two logical X operators acting on *non-standard* subcubes: $0110 + \langle 1, 4\rangle$ (orange square) and $0001 + \langle 1, 2, 3\rangle$ (cyan cube). The joint intersection of these subcubes with the standard subcube $\{2, 3, 4\}$ is a *single* qubit (black vertex), 0111.

5.2 Signed Subcube Operator Logic

We suppose that $q < r$, as otherwise $QRM_m(q, r)$ encodes no logical qubits. Our main theorem is to prove the logical action of signed subcube operators.

Theorem 5.2.1. *For every $K \in \mathcal{Q}_k$, $\widetilde{Z}(k)_{\langle K\rangle}$ implements the logical multi-controlled-Z circuit corresponding to the collection of minimal covers of K:*

$$\widetilde{Z}(k)_{\langle K\rangle} \equiv \overline{C^{\mathcal{F}(K)}Z}.$$

As $Z(k)$ and $\overline{C^{k+1}Z}$ are both diagonal, to characterize the logic of a $Z(k)_{\langle K\rangle}$ operator we will only need to understand how multi-controlled-Z circuits corresponding to $\mathcal{F}(K)$ conjugate logical X operators. The following is the logical version of Lemma 2.3.9 for the X operators.

Lemma 5.2.2. *For every logical qubit $J \in \mathcal{Q}$,*

$$\overline{C^{\mathcal{F}(K)}Z}\ \overline{X}_J\ \overline{C^{\mathcal{F}(K)}Z} = \overline{C^{\mathcal{F}(K)_{\sim J}}Z}\overline{X}_J \tag{5.2}$$

where we define

$$\mathcal{F}(K)_{\sim J} \coloneqq \{\mathcal{J} \setminus \{J\} \mid \mathcal{J} \in \mathcal{F}(K) \textit{ and } J \in \mathcal{J}\}\,.$$

So, our objective is to prove that for every logical qubit $J \in \mathcal{Q}$,

$$\widetilde{Z}(k)_{\langle K\rangle}\overline{X}_J\widetilde{Z}(k)^{\dagger}_{\langle K\rangle} = \overline{C^{\mathcal{F}(K)}Z}\ \overline{X}_J\ \overline{C^{\mathcal{F}(K)}Z}. \tag{5.3}$$

Using conjugation identities for $\widetilde{Z}(k)$ and multi-controlled-Z gates, Eqs. (4.1) and (5.2), we can rewrite this relation as

$$\widetilde{Z}(k-1)_B\overline{X}_J = \overline{C^{\mathcal{F}(K)_{\sim J}}Z}\ \overline{X}_J. \tag{5.4}$$

where $B \coloneqq \langle K\rangle \cap (e_J + \langle S \setminus J\rangle)$ is the common support of $\widetilde{Z}(k)_{\langle K\rangle}$ and X_J.

The proof of Theorem 5.2.1 is presented in Sections 5.2.1 and 5.2.2 and amounts to showing that $\widetilde{Z}(k-1)_B \equiv \overline{C^{\mathcal{F}(K)_{\sim J}}Z}$. Our plan is to use induction on k; however, this does not work directly since B on the left-hand side of Eq. (5.4) is guaranteed to *not* be a standard subcube. Instead, we will proceed using the following sequence of steps:

Step I: We use the decomposition result in Theorem 5.2.5 to rewrite $\widetilde{Z}(k-1)_B$ as a product of standard subcube operators for which induction will apply;

Step II: We show how to compose multi-controlled-Z circuits that arise from this induction;

Step III: Combine these results to complete the proof.

5.2.1 A basis for k-th level subcube logic

A standard cube $\langle J\rangle$ has a unique element of minimum Hamming weight, namely the origin. This property extends to all subcubes, as shown in the next lemma.

Lemma 5.2.3. *Let $A \sqsubseteq \mathbb{Z}_2^m$ be an arbitrary subcube of type $J \subseteq S$. It contains a unique element, x^*, such that $|x^*| < |y|$ for all $y \in A \setminus \{x^*\}$.*

Proof. Let A be a subcube of type J. We claim that A can be constructed as $x + \langle J\rangle$, where x depends on A and satisfies $\mathrm{supp}(x) \cap J = \emptyset$. Indeed, there are $2^{m-|J|}$ such vectors x, and for $x \neq x'$, the subcubes (cosets) $x + \langle J\rangle$ and $x' + \langle J\rangle$ are disjoint. Clearly, x is the unique vector of minimum Hamming weight in its coset, so $x^* = x$. □

To introduce the next lemma, suppose we have nested subcubes $z+\langle J\rangle$ and $z+\langle J\cup\{1\}\rangle$ where $J \subseteq S\setminus\{1\}$ and $z \in \mathbb{Z}_2^m$ is arbitrary. The set difference $\langle J\cup\{1\}\rangle\setminus\langle J\rangle$ is a subcube of type J, namely $e_1 + \langle J\rangle$. Multiplying the subcube operators $\widetilde{Z}(k)$ corresponding to these two nested subcubes, we obtain

$$\widetilde{Z}(k)_{z+\langle J\rangle}\widetilde{Z}(k)_{z+\langle J\cup\{1\}\rangle} = \widetilde{Z}(k)_{z+e_1+\langle J\rangle}\widetilde{Z}(k-1)_{z+\langle J\rangle}, \tag{5.5}$$

as each element of $z + \langle J\rangle$ is acted on twice by $Z(k)$ (or $Z(k)^\dagger$). The following lemma is essentially the inductive application of this relation to the increasing standard subcubes on the left-hand side of Eq. (5.6). Below we abbreviate $\mathrm{supp}(x) \subseteq \mathrm{supp}(x^*)$ as $x \subseteq x^*$.

Lemma 5.2.4. *Let $x^* + \langle J \rangle \sqsubseteq \mathbb{Z}_2^m$ be a subcube with x^* as in the previous lemma. For all $k \geq 0$,*

$$\prod_{x \subseteq x^*} \widetilde{Z}(k)_{\langle \mathrm{supp}(x) \cup J \rangle} = \prod_{x \subseteq x^*} \widetilde{Z}(k - |x|)_{x^* - x + \langle \mathrm{supp}(x) \cup J \rangle}. \tag{5.6}$$

Proof. Induction on the weight of x^*. If $|x^*| = 0$ then there is a single term on each side of Eq. (5.6) corresponding to $x^* = 0^m$, and the two sides are clearly equal. Suppose Eq. (5.6) holds for all $x^* + \langle J \rangle$ where $|x^*| = k \geq 0$, and take an $x^* + \langle J \rangle$ with $|x^*| = k + 1$. We assume without loss of generality that $1 \in \mathrm{supp}(x^*)$. Let us group the terms on the left-hand side of Eq. (5.6) by those that only differ on 1:

$$\begin{aligned}
\prod_{x \subseteq x^*} \widetilde{Z}(k)_{\langle \mathrm{supp}(x) \cup J \rangle} &= \Big(\prod_{x \subseteq (x^* - e_1)} \widetilde{Z}(k)_{\langle \mathrm{supp}(x) \cup J \rangle} \Big) \cdot \Big(\prod_{x \subseteq (x^* - e_1)} \widetilde{Z}(k)_{\langle \mathrm{supp}(x) \cup \{1\} \cup J \rangle} \Big), \\
&= \Big(\prod_{x \subseteq (x^* - e_1)} \widetilde{Z}(k - |x|)_{x^* - e_1 - x + \langle \mathrm{supp}(x) \cup J \rangle} \Big) \cdot \\
&\qquad \Big(\prod_{x \subseteq (x^* - e_1)} \widetilde{Z}(k - |x|)_{x^* - e_1 - x + \langle \mathrm{supp}(x) \cup \{1\} \cup J \rangle} \Big). \\
&= \prod_{x \subseteq (x^* - e_1)} \Big(\widetilde{Z}(k - |x|)_{x^* - e_1 - x + \langle \mathrm{supp}(x) \cup J \rangle} \cdot \\
&\qquad \widetilde{Z}(k - |x|)_{x^* - e_1 - x + \langle \mathrm{supp}(x) \cup \{1\} \cup J \rangle} \Big),
\end{aligned}$$

where the second equality uses the induction hypothesis on each term.

For each $x \subseteq x^* - e_1$ we have a product of two subcube operators, where one subcube contains—

and is one dimension larger—than the other. Now the observation in Eq. (5.5) completes the proof:

$$\prod_{x\subseteq x^*} \widetilde{Z}(k)_{\langle \mathrm{supp}(x)\cup J\rangle} = \Big(\prod_{x\subseteq (x^*-e_1)} \widetilde{Z}(k-|x|)_{x^*-x+\langle \mathrm{supp}(x)\cup J\rangle}\Big)\cdot \widetilde{Z}(k-|x|-1)_{x^*-e_1-x+\langle \mathrm{supp}(x)\cup J\rangle},$$
$$= \prod_{x\subseteq x^*} \widetilde{Z}(k-|x|)_{x^*-x+\langle \mathrm{supp}(x)\cup J\rangle},$$

where the last equality holds because the bit strings $x^*-(e_1+x)$, $x\subseteq(x^*-e_1)$, appearing in the second term, correspond to the substrings of x^* that are supported on the first index. □

Theorem 5.2.5. *Let $k\in\mathbb{Z}_{\geq 0}$, and consider $QRM_m(q,r)$. The standard subcube operators*

$$\{\widetilde{Z}(k)_{\langle K\rangle} \mid K\in\mathcal{Q}_k\}$$

form a basis for the space of logical $\widetilde{Z}(k)_A$ operators on $QRM_m(q,r)$. That is, for $x^*+\langle K\rangle \sqsubseteq \mathbb{Z}_2^m$ with minimum-weight element x^*, if $\widetilde{Z}(k)_{x^*+\langle K\rangle}\in\mathcal{N}^{(k)}$ then

$$\widetilde{Z}(k)_{x^*+\langle K\rangle} \equiv \prod_{x\subseteq x^*:\ |x|+|K|\leq (k+1)r} \widetilde{Z}(k)_{\langle \mathrm{supp}(x)\cup K\rangle}, \tag{5.7}$$

up to Clifford stabilizers, where each $\mathrm{supp}(x)\cup K\in\mathcal{Q}_k$.

Proof. By Lemma 5.2.4 we have the following equality:

$$\prod_{x\subseteq x^*} \widetilde{Z}(k-|x|)_{x^*-x+\langle \mathrm{supp}(x)\cup K\rangle} = \prod_{x\subseteq x^*} \widetilde{Z}(k)_{\langle \mathrm{supp}(x)\cup K\rangle}. \tag{5.8}$$

We will show that, under our assumptions, this identity is precisely Eq. (5.7).

Recall that by Theorem 4.2.3 we necessarily have $K \in \mathcal{Q}_k$, so

$$q + kr + 1 \leq |K| \leq (k+1)r.$$

Consider the right-hand side of Eq. (5.8). Since $x \subseteq x^*$ and $\mathrm{supp}(x^*) \cap K = \emptyset$, we have that $|\mathrm{supp}(x) \cup K| = |x| + |K|$. By Theorem 4.2.3, if this quantity is $\geq (k+1)r + 1$ then the operator $\widetilde{Z}(k)_{\langle \mathrm{supp}(x) \cup K \rangle} \in \mathcal{S}^{(k)}$ is a Clifford stabilizer, so the only terms on the right hand side of Eq. (5.8) that act non-trivially on $QRM_m(q, r)$ are those with $|x| + |K| \leq (k+1)r$. The claim that each $\mathrm{supp}(x) \cup K \in \mathcal{Q}_k$ holds by further using the lower bound on $|K|$.

Now consider the left-hand side of Eq. (5.8). The term corresponding to $0^m \subseteq x^*$ is precisely $\widetilde{Z}(k)_{x^* + \langle K \rangle}$; it turns out that the assumption $K \in \mathcal{Q}_k$ is sufficient to guarantee that every other term is a logical identity. Indeed, $|\mathrm{supp}(x) \cup K| = |x| + |K|$ and $K \in \mathcal{Q}_k$ imply that each such term acts on a subcube with dimension $|\mathrm{supp}(x) \cup K| \geq |x| + q + kr + 1$. For all $|x| \geq 1$, this bound can be improved to $|x| + q + kr + 1 \geq (k - |x| + 1)r + 1$, which by Theorem 4.2.3 is precisely the condition for $\widetilde{Z}(k - |x|)_{x^* - x + \langle \mathrm{supp}(x) \cup K \rangle} \in \mathcal{S}^{(k-|x|)}$. Thus, only the 0^m term is non-identity and thus, (5.8) translates into (5.7). $\square$

5.2.2 Standard subcube logic

We are ready to implement the sequence of steps listed prior to Section 5.2.1. Our ultimate goal will be to show that $\widetilde{Z}(k-1)_B \equiv \overline{C^{\mathcal{F}(K)_{\sim J}} Z}$, so we will give a name to the elements of the collection $\mathcal{F}(K)_{\sim J}$ for $J \in \mathcal{Q}$. We say each $\mathcal{J}' \in \mathcal{F}(K)_{\sim J}$ is a *partial minimal cover for K relative to J*; they are precisely the collections of logical qubit indices for which $\mathcal{J}' \cup \{J\}$ is a minimal cover for K. Note that the logical multi-controlled-Z circuit defined via partial minimal covers, $\overline{C^{\mathcal{F}(K)_{\sim J}} Z}$, necessarily acts as logical identity on the J-th logical qubit.

We will use the following subset of generators, which depends on a fixed logical qubit $J \in \mathcal{Q}$:

Definition 5.2.6 (Dense subsets)**.** Let $K \in \mathcal{Q}_k, K \supseteq J$ be the index of a k-th level logical operator and let $K' \subseteq K$ be an arbitrary subset of K. The set K' is said to be *dense* in K relative to J if

1. K' is an index of a $(k-1)$-st level logical operator, $K' \in \mathcal{Q}_{k-1}$, and
2. the union of K' and J is all of K, $K = K' \cup J$.

The collection of all dense subsets $K' \subset K$ is denoted by $\mathcal{D}_J(K)$:

$$\mathcal{D}_J(K) \coloneqq \left\{K' \subseteq K \mid K' \in \mathcal{Q}_{k-1},\ K = K' \cup J\right\}.$$

The following characterization of dense subsets will be more useful:

Lemma 5.2.7. *The collection $\mathcal{D}_J(K)$ can alternatively be defined as:*

$$\mathcal{D}_J(K) \coloneqq \left\{K' \subset K \mid K' \in \mathcal{Q}_{k-1},\ K' = I \cup (K \setminus J)\ \textit{for some}\ I \subseteq J\right\}. \tag{5.9}$$

Proof. ($\subseteq$) Suppose K' satisfies Definition 5.2.6. For $I \coloneqq K' \cap J \subseteq J$ we have $K' = I \cup (K \setminus J)$.

($\supseteq$) Suppose K' satisfies Eq. (5.9). Clearly $K' \cup J = I \cup (K \setminus J) \cup J = K$. $\square$

(**Step I:** Conjugating logical Pauli operators) Our first task is to understand how $\widetilde{Z}(k)_{\langle K \rangle}$ conjugates the logical Pauli operators of $QRM_m(q,r)$. For this, we will need the decomposition result of Theorem 5.2.5. As usual, we assume $q < r$ as otherwise $QRM_m(q,r)$ encodes no logic.

Claim 5.2.8. Take $J \in \mathcal{Q}$ and $K \in \mathcal{Q}_k$, $k \geq 1$. Consider the operator $\widetilde{Z}(k)_{\langle K \rangle}$ acting on $QRM_m(q,r)$.

1. $\widetilde{Z}(k)_{\langle K\rangle}$ commutes with every logical Z operator.

2. Up to Clifford stabilizers, $\widetilde{Z}(k)_{\langle K\rangle}$ conjugates a logical $\overline{X}_J$ operator as

$$\widetilde{Z}(k)_{\langle K\rangle}\overline{X}_J\widetilde{Z}(k)^{\dagger}_{\langle K\rangle} \equiv \begin{cases} \overline{X}_J, & \text{if } J \not\subseteq K, \\ \left(\prod_{K'\in\mathcal{D}_J(K)} \widetilde{Z}(k-1)_{\langle K'\rangle}\right)\overline{X}_J, & \text{otherwise.} \end{cases}$$

Proof. The first assertion is trivial, so we only prove the second.

As e_J is the minimum Hamming weight element of $e_J+\langle S\setminus J\rangle$, clearly $\langle K\rangle\cap(e_J+\langle S\setminus J\rangle)\neq\emptyset$ if and only if $e_J\in\langle K\rangle$. Thus, $J\not\subseteq K$ is precisely the case that $\widetilde{Z}(k)_{\langle K\rangle}$ and $\overline{X}_J$ have disjoint supports and therefore commute. For the rest of the proof, suppose that $J\subseteq K$, so

$$\begin{aligned}\langle K\rangle\cap(e_J+\langle S\setminus J\rangle) &= e_J+\langle K\cap(S\setminus J)\rangle, \\ &= e_J+\langle K\setminus J\rangle,\end{aligned}$$

and further, e_J is the minimum-weight element of $e_J+\langle K\setminus J\rangle$.

We now apply Theorem 4.2.3 to both K and J to bound

$$\begin{aligned}\dim(e_J+\langle K\setminus J\rangle) &= |K|-|J|, \\ &\geq q+kr+1-|J|, \\ &\geq q+kr+1-r, \\ &= q+(k-1)r+1.\end{aligned}$$

Since $k\geq 1$, also $\dim(e_J+\langle K\setminus J\rangle)\geq 1$ and $\widetilde{Z}(k)_{\langle K\rangle}\overline{X}_J\widetilde{Z}(k)^{\dagger}_{\langle K\rangle}$ is phase-free by Lemma 4.2.7. By definition, this means

$$\widetilde{Z}(k)_{\langle K\rangle}\overline{X}_J\widetilde{Z}(k)^\dagger_{\langle K\rangle} = \left(\widetilde{Z}(k-1)_{e_J+\langle K\setminus J\rangle}\right)\overline{X}_J. \tag{5.10}$$

We would like to use Theorem 5.2.5 on the operator $\widetilde{Z}(k-1)_{e_J+\langle K\setminus J\rangle}$, but doing so requires $K\setminus J \in \mathcal{Q}_{k-1}$. This containment relies on the dimension bounds of Eq. (5.1), and the lower bound has been established above. Unfortunately, the upper bound $|K\setminus J|\leq kr$ may fail, so we will proceed in cases:

Case I. ($|K\setminus J|\leq kr$) In this case we have established $K\setminus J\in\mathcal{Q}_{k-1}$, so we apply Theorem 5.2.5 to rewrite $\widetilde{Z}(k-1)_{e_J+\langle K\setminus J\rangle}$ as a product of standard subcube operators:

$$\begin{aligned}\widetilde{Z}(k)_{\langle K\rangle}\overline{X}_J\widetilde{Z}(k)^\dagger_{\langle K\rangle} &= \Big(\prod_{x\subseteq e_J:\ |x|+|K\setminus J|\leq kr}\widetilde{Z}(k-1)_{\langle \mathrm{supp}(x)\cup K\setminus J\rangle}\Big)\overline{X}_J,\\ &= \Big(\prod_{I\subseteq J:\ |I|+|K|-|J|\leq kr}\widetilde{Z}(k-1)_{\langle I\cup(K\setminus J)\rangle}\Big)\overline{X}_J,\end{aligned} \tag{5.11}$$

where in the last equality we've utilized $\mathrm{supp}(e_J)=J$ and $J\subseteq K$, and let $I\coloneqq\mathrm{supp}(x)\subseteq J$.

Theorem 5.2.5 also guarantees that each $I\cup(K\setminus J)\in\mathcal{Q}_{k-1}$. The statement of the claim now holds by Lemma 5.2.7, which says that the sets appearing in the product in Eq. (5.11) correspond precisely to the collection of dense subsets of K relative to J, $\mathcal{D}_J(K)$.

Case II. ($|K\setminus J|\geq kr+1$). Returning to Eq. (5.10), we examine the operator $\widetilde{Z}(k-1)_{e_J+\langle K\setminus J\rangle}$. Given the assumed lower bound on $|K\setminus J|$, Theorem 4.2.3 implies that $\widetilde{Z}(k-1)_{e_J+\langle K\setminus J\rangle}\in\mathcal{S}^{(k-1)}$ is a Clifford stabilizer. Fortunately, the lower bound on $|K\setminus J|$ guarantees that $\mathcal{D}_J(K)=\emptyset$ is empty, so the operator $\prod_{K'\in\mathcal{D}_J(K)}\widetilde{Z}(k-1)_{\langle K'\rangle}=\mathbb{I}$ acts as identity, as well. To see this, suppose there is some $K'\in\mathcal{D}_J(K)$. Using the definition of dense subsets given in Definition 5.2.6, we see

1. $K' \in \mathcal{Q}_{k-1}$, implying $|K'| \leq kr$, and

2. $K = K' \cup J$, further implying $|K| \leq kr + |J|$.

We have $J \subseteq K$ (otherwise $\widetilde{Z}(k)_{\langle K \rangle}$ and $\overline{X}_J$ commute), so the case we are in implies $|K| - |J| = |K \setminus J| \geq kr + 1$. Combining this with the upper bound we obtained for $|K|$ we must have that $kr + |J| - |J| \geq kr + 1$, which is clearly a contradiction. Thus $\mathcal{D}_J(K) = \emptyset$ and the claim holds. $\square$

(**Step II:** Composition of multi-controlled-Z circuits) For a fixed logical qubit index, $J \in \mathcal{Q}$, and a fixed k-th level operator index, $K \in \mathcal{Q}_k$, our next goal is to relate the collection of partial minimal covers of K to the collection of dense subsets of K. The culmination of this effort will be the following result on the composition of logical multi-controlled-Z circuits defined using these collections:

Claim 5.2.9. Let $J \in \mathcal{Q}$ and $K \in \mathcal{Q}_k$ with $J \subseteq K$. Then

$$\overline{C^{\mathcal{F}(K)_{\sim J}} Z} = \prod_{K' \in \mathcal{D}_J(K)} \overline{C^{\mathcal{F}(K')} Z}. \tag{5.12}$$

That is, given a dense set $K' \in \mathcal{D}_J(K)$, we can consider the collection of sets of logical qubits that it defines via *its own* collection of minimal covers, $\mathcal{F}(K')$. Claim 5.2.9 says that the composition of the multi-controlled-Z circuits defined by the minimal covers of all dense subsets of K is precisely the multi-controlled-Z circuit defined by the collection of partial minimal covers of K.

Claim 5.2.9 follows from the next two lemmas. First, we note that by definition, no set of logical qubits can be a minimal cover for two different $K_1, K_2 \in \mathcal{Q}_k$:

Lemma 5.2.10. *Let $K_1, K_2 \subseteq S$ be disjoint subsets of generators, $K_1 \neq K_2$. The intersection of the collections of their minimal covers is empty, $\mathcal{F}(K_1) \cap \mathcal{F}(K_2) = \emptyset$.*

This is true simply because a minimal cover covers the subset exactly, so $K_1 \neq K_2$ is not possible.

Next, we show that the collection of partial minimal covers of K is given by the union of all minimal covers of dense subsets of K.

Lemma 5.2.11. *Let $J \in \mathcal{Q}$ and $K \in \mathcal{Q}_k$ with $J \subseteq K$. Then $\bigcup_{K' \in \mathcal{D}_J(K)} \mathcal{F}(K') = \mathcal{F}(K)_{\sim J}$.*

Proof. ($\subseteq$) Take $\mathcal{J}' \in \mathcal{F}(K')$ for some $K' \in \mathcal{D}_J(K)$. By definition, $\mathcal{J}' \in \mathcal{F}(K)_{\sim J}$ if and only if $\mathcal{J}' \cup \{J\}$ is a minimal cover for K. We verify the two conditions for $\mathcal{J}'$ to be a minimal cover:

1. $\mathcal{J}' \cup \{J\}$ is a cover for K: We have assumed that $\mathcal{J}'$ is a cover for K' and that K' dense in K relative to J. Thus, by definition, $\left(\bigcup_{J' \in \mathcal{J}'} J'\right) \cup J = K' \cup J = K$.

2. $|\mathcal{J}' \cup \{J\}| = k+1$: First, note that $J \notin \mathcal{J}$; otherwise $K' = K$, which cannot happen as $K' \in \mathcal{Q}_{k-1}$, $K \in \mathcal{Q}_k$, and $\mathcal{Q}_{k-1} \cap \mathcal{Q}_k = \emptyset$. So, $|\mathcal{J}' \cup \{J\}| = |\mathcal{J}'| + 1$. Now, since $\mathcal{J}'$ is a minimal cover for $K' \in \mathcal{Q}_{k-1}$ we know that $|\mathcal{J}'| = (k-1) + 1 = k$, so $|\mathcal{J}' \cup \{J\}| = k+1$.

($\supseteq$) Take $\mathcal{J}' \in \mathcal{F}(K)_{\sim J}$ and define $K' := \bigcup_{J' \in \mathcal{J}'} J'$. We will show (1) $\mathcal{J}'$ is a minimal cover for K' and (2) K' is an almost-covering set for K, which together imply the desired result. We will first show that $K' \in \mathcal{Q}_{k-1}$.

Note that as $\mathcal{J}' \in \mathcal{F}(K)_{\sim J}$, by assumption we know that $J \cup K' = K$ and that $|\mathcal{J}'| = k$. As any set in $\mathcal{Q}$ has at most r elements (Definition 5.1.4), we can upper bound

$$\begin{aligned}|K'| &\leq \sum_{J' \in \mathcal{J}'} |J'|, \\ &\leq kr \\ &< ((k-1)+1)\,r + 1.\end{aligned}$$

As $K' \supseteq (J \cup K') \setminus J = K \setminus J$, so we can lower bound

$$\begin{aligned} & |K'| \geq |K| - |J|, \\ (K \in \mathcal{Q}_k) \qquad & \geq q + kr + 1 - |J| \\ (J \in \mathcal{Q}) \qquad & \geq q + \big(k-1\big)r + 1. \end{aligned}$$

The given bounds on $|K'|$ are precisely the conditions for $K' \in \mathcal{Q}_{k-1}$, cf. Eq. (5.1).

By definition, $\mathcal{J}'$ is a cover of K', and since $|\mathcal{J}'| = k = (k-1)+1$ we have that $\mathcal{J}'$ is a minimal cover for K'. Further, since $K' \cup J = K$ and $K' \in \mathcal{Q}_{k-1}$, K' satisfies the condition for an almost-covering of K. Thus $\mathcal{J}' \in \mathcal{F}(K')$ for some $K' \in \mathcal{D}_J(K)$. □

Now we have everything to prove the desired decomposition result:

Proof of Claim 5.2.9. Consider $\prod_{K' \in \mathcal{D}_J(K)} \overline{C^{\mathcal{F}(K')} Z}$. By Lemma 5.2.10 we are guaranteed that no $\overline{C^{\mathcal{J}_1} Z}$ for $\mathcal{J}_1 \in \mathcal{F}(K_1)$ can cancel with a $\overline{C^{\mathcal{J}_2} Z}$ for $\mathcal{J}_2 \in \mathcal{F}(K_2)$, $K_2 \neq K_1$ for $K_1, K_2 \in \mathcal{D}_J(K)$. Thus

$$\begin{aligned} \prod_{K' \in \mathcal{D}_J(K)} \overline{C^{\mathcal{F}(K')} Z} &= \prod_{K' \in \mathcal{D}_J(K)} \prod_{\mathcal{J}' \in \mathcal{F}(K')} \overline{C^{\mathcal{J}'} Z}, \\ (\text{Lemma 5.2.10}) \qquad &= \prod_{\mathcal{J}' \in \bigcup_{K' \in \mathcal{D}_J(K)} \mathcal{F}(K')} \overline{C^{\mathcal{J}'} Z}, \\ (\text{Lemma 5.2.11}) \qquad &= \prod_{\mathcal{J}' \in \mathcal{F}(K)_{\sim J}} \overline{C^{\mathcal{J}'} Z}. \end{aligned}$$

□

(**Step III:** Implemented logic) We are now prepared to describe the logic performed by standard subcube operators using Claims 5.2.8 and 5.2.9.

Theorem 5.2.1. *For every $K \in \mathcal{Q}_k$, $\widetilde{Z}(k)_{\langle K\rangle}$ implements the logical multi-controlled-Z circuit corresponding to the collection of minimal covers of K:*

$$\widetilde{Z}(k)_{\langle K\rangle} \equiv \overline{C^{\mathcal{F}(K)}Z}.$$

Proof. Induction on k. If $k = 0$ then $\mathcal{F}(K) = \{\{K\}\}$ and $\widetilde{Z}(0)_{\langle K\rangle} = \overline{Z}_K = \overline{C^{\{\{K\}\}}Z}$, so the result holds in the base case. Suppose now that the result holds for all $K' \in \mathcal{Q}_k$, and choose $K \in \mathcal{Q}_{k+1}$. We seek to show that $\widetilde{Z}(k)_{\langle K\rangle}$ and $\overline{C^{\mathcal{F}(K)}Z}$ conjugate logical Pauli operators in the same way.

Consider $J \in \mathcal{Q}$. By Claim 5.2.8, $\widetilde{Z}(k)_{\langle K\rangle}$ commutes with $\overline{Z}_J$ and maps

$$\widetilde{Z}(k)_{\langle K\rangle}\overline{X}_J\widetilde{Z}(k)^{\dagger}_{\langle K\rangle} \equiv \begin{cases} \overline{X}_J, & \text{if } J \not\subseteq K, \\ \left(\prod_{K'\in\mathcal{D}_J(K)} \widetilde{Z}(k-1)_{\langle K'\rangle}\right)\overline{X}_J, & \text{otherwise.} \end{cases}$$

By Lemma 2.3.9, $\overline{C^{\mathcal{F}(K)}Z}$ commutes with $\overline{Z}_J$ and maps

$$\left(\overline{C^{\mathcal{F}(K)}Z}\right)\overline{X}_J\left(\overline{C^{\mathcal{F}(K)}Z}\right) = \left(\overline{C^{\mathcal{F}(K)_{\sim J}}Z}\right)\overline{X}_J.$$

We proceed in cases:

Case I. ($J \not\subseteq K$) $\mathcal{F}(K)_{\sim J} = \emptyset$ in this case, as any union $J \cup \left(\bigcup_{J'\in\mathcal{J}'} J'\right)$ for $\mathcal{J}' \subseteq \mathcal{Q}$ is guaranteed to contain an element outside of K. Thus $\widetilde{Z}(k)_{\langle K\rangle}$ and $\overline{C^{\mathcal{F}(K)}Z}$ each commute with both $\overline{Z}_J$ and $\overline{X}_J$.

Case II. ($J \subseteq K$) In this case,

$$\widetilde{Z}(k)_{\langle K\rangle}\overline{X}_J\widetilde{Z}(k)^{\dagger}_{\langle K\rangle} \equiv \left(\prod_{K'\in\mathcal{D}_J(K)} \widetilde{Z}(k-1)_{\langle K'\rangle}\right)\overline{X}_J. \tag{5.13}$$

By definition of $\mathcal{D}_J(K)$, each subcube, $\langle K' \rangle$, appearing in the product on the right-hand side of Eq. (5.13) satisfies $K' \in \mathcal{Q}_{k-1}$, so we can use the induction hypothesis to compute

$$\equiv \Big(\prod_{K' \in \mathcal{D}_J(K)} \overline{C^{\mathcal{F}(K')} Z} \Big) \overline{X}_J,$$

which by Claim 5.2.9 equals

$$\equiv \big(\overline{C^{\mathcal{F}(K)_{\sim J}} Z} \big) \overline{X}_J.$$

As $\overline{C^{\mathcal{F}(K)} Z}$ and $\widetilde{Z}(k)_{\langle K \rangle}$ conjugate the logical Pauli operators of $QRM_m(q,r)$ in the same way, by definition they are equivalent logical operators for the code. □

5.2.3 Arbitrary subcubes

Consider an arbitrary subcube $A := x + \langle K \rangle \sqsubseteq \mathbb{Z}_2^m$, where $K \subseteq S$ is the type of A. Theorem 4.2.3 tells us that the operator $\widetilde{Z}(k)_A$ will be a logical operator for $QRM_m(q,r)$ if and only if $K \in \mathcal{Q}_k$. Given the decomposition of $\widetilde{Z}(k)_A$ into standard subcube operators (Theorem 5.2.5) as well as the description of logical multi-controlled-Z circuits implemented by these operators (Theorem 5.2.1), it may be natural to wonder if interesting logical circuits can be constructed via $\widetilde{Z}(k)_A$. As as example, it is straightforward to verify from Theorem 5.2.1 and the definition of minimal covers that every $\widetilde{Z}(k)_{\langle K \rangle}$ implements a circuit containing more than one logical gate[3]. Can $\widetilde{Z}(k)_A$ implement single multi-controlled-Z gates when A is no longer a standard subcube? Or perhaps more generally, can some product of $\widetilde{Z}(k)_{\langle K \rangle}$ operators implement a single multi-controlled-Z gate?

Unfortunately, the standard subcube operators are, in some sense, the fundamental logical multi-

[3]Other than the case of $QRM_m(0,1)$, which corresponds to the well-known family of hypercube codes.

controlled-Z circuits that can be implemented on $QRM_m(q, r)$. By this, we mean that the logical circuit defined by a product, $\widetilde{Z}(k_1)_{\langle K_1 \rangle} \cdot \widetilde{Z}(k_2)_{\langle K_2 \rangle}$, can never have cancellations of logical gates. More formally:

Theorem 5.2.12. *Let $\{k_1, \ldots, k_\ell\}$ be a set of non-negative integers, and suppose $\{K_i\}_{i \in [\ell]}$ is a collection of (distinct) subsets $K_i \subseteq S$, such that $K_i \in \mathcal{Q}_{k_i}$ for every $i \in [\ell]$. Then*

$$\prod_{i \in [\ell]} \widetilde{Z}(k_i)_{\langle K_i \rangle} \equiv \overline{C^{\mathcal{F}} Z},$$

where

$$\mathcal{F} := \left\{ \mathcal{J} \subseteq \mathcal{Q} \;\middle|\; \mathcal{J} \text{ is a minimal cover for some } K_i \right\}$$

is simply the union of all collections of minimal covers of the K_i sets.

Proof. A direct application of Theorem 5.2.1 implies that

$$\prod_{i \in [\ell]} \widetilde{Z}(k_i)_{\langle K_i \rangle} \equiv \prod_{i \in [\ell]} \prod_{\mathcal{J} \in \mathcal{F}(K_i)} \overline{C^{\mathcal{J}} Z}. \tag{5.14}$$

The result will hold by proving that any $\overline{C^{\mathcal{J}} Z}$ in the right-hand side of Eq. (5.14) can only appear once. It is trivial that for a *particular* $i \in [\ell]$, $\overline{C^{\mathcal{J}} Z}$ can only appear once in the product $\prod_{\mathcal{J} \in \mathcal{F}(K_i)} \overline{C^{\mathcal{J}} Z}$. The operator $\overline{C^{\mathcal{J}} Z}$ can also only appear for a *single* $i \in [\ell]$, as otherwise the cover property of $\mathcal{J}$ would imply that $K_i = \bigcup_{J \in \mathcal{J}} J = K_j$, but we have assumed that K_i sets are all distinct. □

In conclusion, while the operator $\widetilde{Z}(k)_{x + \langle K \rangle}$ is non-trivial whenever $K \in \mathcal{Q}_k$, Theorem 5.2.12 implies that the circuit it defines necessarily contains more gates than $\widetilde{Z}(k)_{\langle K \rangle}$.

5.3 Unsigned Subcube Operator Logic

We now consider subcube operators $Z(k)_{\langle K\rangle}$ whose individual gates are never inverted. We will see that in many practical cases, these operators are logically equivalent to their signed counterparts. For instance, whenever $q > 0$, we will show that $Z(k)_{\langle K\rangle} \equiv \widetilde{Z}(k)_{\langle K\rangle}$. We begin with a general decomposition result relating unsigned and signed subcube operators. This result is independent of the choice of quantum RM code.

Lemma 5.3.1. *For any standard subcube $\langle K\rangle \sqsubseteq \mathbb{Z}_2^m$ and any $k \in \mathbb{Z}_{\geq 0}$, we have*

$$Z(k)_{\langle K\rangle} = \prod_{i=0}^{|K|} \prod_{J\subseteq K:\, |J|=i} \widetilde{Z}(k-(|K|-i))_{\langle J\rangle}^{(-1)^i}. \tag{5.15}$$

Proof. Recall that the physical qubits are indexed by elements of $\mathbb{Z}_2^m$, and consider the operator on the right hand side of (5.15). We will prove the lemma by showing that this operator acts as $Z(k)$ on any $x \in \langle K\rangle$ and identity otherwise, precisely the definition of $Z(k)_{\langle K\rangle}$. Let $x \in \mathbb{Z}_2^m$ index a physical qubit. We proceed in cases.

Case I. ($x \notin \langle K\rangle$) Every operator in (5.15) acts on a subcube $\langle J\rangle$ for which $J \subseteq K$. Clearly $x \notin \langle J\rangle$ for any $J \subseteq K$, so the x qubit is always acted on by identity.

Case II. ($x \in \langle K\rangle$) In this case $\operatorname{supp}(x) \subseteq K$. For each $i \in \{0, \ldots, |K|\}$ define a collection $\mathcal{K}_i \subseteq \mathscr{P}(K)$ via

$$\mathcal{K}_i \coloneqq \{J \subseteq K \mid J \supseteq \operatorname{supp}(x),\ |J| = i\}.$$

The x-th qubit is therefore acted on by the operator

$$\prod_{i=0}^{|K|} \prod_{J\subseteq K:\, |J|=i} Z(k-(|K|-i))^{(-1)^{i-|x|}|\mathcal{K}_i|} = \prod_{i=0}^{|K|} \prod_{J\subseteq K:\, |J|=i} Z(k)^{2^{|K|-i}(-1)^{i-|x|}|\mathcal{K}_i|},$$

where we recall that $Z(k-\ell) = Z(k)^{2^\ell}$ for all $\ell \geq 0$. The extra factor of $|x|$ in the exponent of (-1) appears since we are considering a product of *signed* subcube operators, so the parity of the Hamming weight of x determines whether or not the operator should be inverted.

This expression is a product of only $Z(k)$ operators, so we can move the products into the exponent of $Z(k)$ to find that the x-th qubit is acted on by $Z(k)^{f(x)}$, where $f(x)$ is defined as

$$f(x) \coloneqq \sum_{i=0}^{|K|} 2^{|K|-i}(-1)^{i-|x|}|\mathcal{K}_i|.$$

With this notation, our goal is to prove that $f(x) = 1$ given $x \in \langle K \rangle$. We now consider the collections $\mathcal{K}_i$, which depend implicitly on the given x.

If $i < |x|$ then $|\mathcal{K}_i| = 0$. Consider now $i \geq |x|$. We seek to determine the number of i-subsets J for which $\mathrm{supp}(x) \subseteq J \subseteq K$. Since J must contain all of $\mathrm{supp}(x)$, we must pick $i - |x|$ additional elements from the set $K \setminus \mathrm{supp}(x)$ to complete a set $J \in \mathcal{K}_i$. The size of this set is $|K \setminus \mathrm{supp}(x)| = |K| - |x|$, so $|\mathcal{K}_i| = \binom{|K|-|x|}{i-|x|}$. With this, we compute:

$$\begin{aligned} f(x) &= \sum_{i=|x|}^{|K|}(-1)^{i-|x|}\binom{|K|-|x|}{i-|x|}2^{|K|-i} \\ &= \sum_{j=0}^{|K|-|x|}(-1)^j\binom{|K|-|x|}{j}2^{(|K|-|x|)-j} \\ &= (2-1)^{|K|-|x|}, \\ &= 1. \end{aligned}$$

□

We now specialize Lemma 5.3.1 to the case of a chosen quantum RM code $QRM_m(q,r)$ with $0 \leq q < r \leq m$.

Theorem 5.3.2. *Consider the code $QRM_m(q,r)$ and let $K \in \mathcal{Q}_k$ for $k \in \mathbb{Z}_{\geq 0}$. The logic implemented by $Z(k)_{\langle K \rangle}$ can be deduced from the logic of signed subcube operators. In particular,*

$$Z(k)_{\langle K \rangle} = \prod_{j=0}^{k} \Big(\prod_{J \subseteq K :\, |J| = |K| - j} \widetilde{Z}(k-j)_{\langle J \rangle} \Big). \tag{5.16}$$

Proof. Since $Z(k-\ell) = \mathbb{I}$ for any $\ell \geq k+1$, the product on the right-hand side of Eq. (5.15) is only non-trivial when $i \geq |K| - k$, so

$$\begin{aligned} Z(k)_{\langle K \rangle} &= \prod_{i=|K|-k}^{|K|} \prod_{J \subseteq K :\, |J| = i} \widetilde{Z}(k - (|K| - i))_{\langle J \rangle}^{(-1)^i}, \\ &= \prod_{j=0}^{k} \prod_{J \subseteq K :\, |J| = |K| - j} \widetilde{Z}(k-j)_{\langle J \rangle}^{(-1)^{|K|-j}}. \end{aligned}$$

This expression is identical to the claim except for the inversions whenever $|K| - j$ is odd. Note that we can lower bound each $|J|$,

$$\begin{aligned} & & |J| &= |K| - j, \\ &(K \in \mathcal{Q}_k) & &\geq q + kr + 1 - j, \\ &(r \geq 1) & &\geq q + (k-j)r + 1, \end{aligned}$$

so Theorem 4.2.3 implies that $\widetilde{Z}(k-j)_{\langle J \rangle} \in \mathcal{N}^{(k-j)}$. Corollary 4.2.10 now guarantees that each $\widetilde{Z}(k-j)_{\langle J \rangle}$ is logically equivalent to its Hermitian, completing the proof. □

In many cases, the operators $\widetilde{Z}(k-j)_{\langle J \rangle}$ appearing in Eq. (5.16) are stabilizers of $QRM_m(q,r)$

and *not* non-trivial logical operators. Recall that the collections $\mathcal{Q}_k$ are defined (5.1) via:

$$\mathcal{Q}_k \coloneqq \{K \subseteq S \mid q + kr + 1 \leq |K| \leq (k+1)r\}\,.$$

The subsets $\{q+kr+1, \ldots, (k+1)r\} \subset \mathbb{N}$ defining the $\mathcal{Q}_k$ are disjoint, and if $q = 0$, they also form a partition of $\mathbb{N}$. They each contain $r - q$ numbers, and any adjacent subsets $\{q + (k-1)r + 1, \ldots, kr\}$ and $\{q + kr + 1, \ldots, (k+1)r\}$ are separated by q numbers.

Each time the index j increases in Eq. (5.16), we decrease the level of the Clifford hierarchy of operators by one while only decreasing the dimension of the subcubes they act on by one. One simple consequence of this is that if $q \geq 1$, then *only* the $j = 0$ term can act non-trivially on $QRM_m(q, r)$. For example, if $J = K \backslash \{i\}$ then $|J|$ is too large for J to be in $\mathcal{Q}_{k-1}$, and, in particular, its dimension is large enough to imply that $\widetilde{Z}(k-1)_{\langle J \rangle} \in \mathcal{S}^{(k-1)}$ by Theorem 4.2.3. In the next few results, we enumerate all possibilities for the logic implemented by $Z(k)_{\langle K \rangle} \in \mathcal{N}^{(k)}$ in terms of the logic implemented by the signed operators.

Theorem 5.3.3 (Conditions when $Z(k)_{\langle K \rangle} \equiv \widetilde{Z}(k)_{\langle K \rangle}$)**.** *Consider $QRM_m(q, r)$ and let $K \in \mathcal{Q}_k$. The following are true:*

1. *If $q \geq 1$ then $Z(k)_{\langle K \rangle} \equiv \widetilde{Z}(k)_{\langle K \rangle}$.* (Fig. 5.3a)

2. *If $|K| \geq q + kr + 2$ then $Z(k)_{\langle K \rangle} \equiv \widetilde{Z}(k)_{\langle K \rangle}$.* (Fig. 5.3b)

Proof. Consider an operator $\widetilde{Z}(k-j)_{\langle J \rangle}$, $|J| = |K| - j$, in the decomposition of $Z(k)_{\langle K \rangle}$ given in Eq. (5.16). The assertions will hold if for each $j \geq 1$, $\widetilde{Z}(k-j)_{\langle J \rangle} \in \mathcal{S}^{(k-j)}$. By Theorem 4.2.3, it is sufficient to show $|J| \geq (k - j + 1)r + 1$ in both cases.

As $r > q \geq 0$, for all $j \geq 1$ we have the inequality $(j-1)r \geq j-1$, which can be rewritten as

$$kr + 2 - j \geq (k - j + 1)r + 1.$$

In both cases in the statement, $|J|$ is larger than the term on the left-hand side:

1. If $q \geq 1$ then $|J| \geq q + kr + 1 - j \geq kr + 2 - j$.

2. Since $q \geq 0$, if $|K| \geq q + kr + 2$ then, once again, $|J| \geq q + kr + 2 - j \geq kr + 2 - j$.

Thus, $j \geq 1$ implies that $|J| \geq (k-j+1)r+1$, which by Theorem 4.2.3 forces $\widetilde{Z}(k-j)_{\langle J \rangle} \in \mathcal{S}^{(k-j)}$. So $Z(k)_{\langle K \rangle} \equiv \widetilde{Z}(k)_{\langle K \rangle}$, as desired. □

Theorems 4.2.3 and 5.3.3 imply that, in order for $Z(k)_A$ and $\widetilde{Z}(k)_A$ to perform different (non-trivial) actions on $QRM_m(q, r)$, it is necessary that $q = 0$ and $|K| = kr + 1$.

Lemma 5.3.4 (Fig. 5.3c)**.** *Consider $QRM_m(0, r)$ and suppose that $K \subseteq S$ satisfies $|K| = kr + 1$ for $k \in \mathbb{Z}_{\geq 0}$. If $r \geq 2$ then*

$$Z(k)_{\langle K \rangle} \equiv \overline{C^{\mathcal{F}(K)} Z} \cdot \prod_{i \in K} \overline{C^{\mathcal{F}(K \setminus \{i\})} Z}.$$

Proof. When $r \geq 2$, inequality $(j-1)r \geq j$ holds for all $j \geq 2$, and with rearranging, is equivalent to

$$kr + 1 - j \geq (k - j + 1)r + 1$$

for all $j \geq 2$. Thus, for each $\widetilde{Z}(k-j)_{\langle J \rangle}$ in the decomposition of $Z(k)_{\langle K \rangle}$ in Eq. (5.16) with $j \geq 2$, we have that $|J| = kr+1-j \geq (k-j+1)r+1$. By Theorem 4.2.3 this implies that $\widetilde{Z}(k-j)_{\langle J \rangle} \in \mathcal{S}^{(k-j)}$, and so

$$Z(k)_{\langle K\rangle} \equiv \widetilde{Z}(k)_{\langle K\rangle} \cdot \prod_{J\subseteq K:\, |J|=kr} \widetilde{Z}(k-1)_{\langle J\rangle}.$$

Since every J considered here satisfies $|J| \geq (k-1)r+1$, we conclude that $J \in \mathcal{Q}_{k-1}$. The desired result then holds by Theorem 5.2.1. □

It remains to consider the cases of $q = 0, 1$.

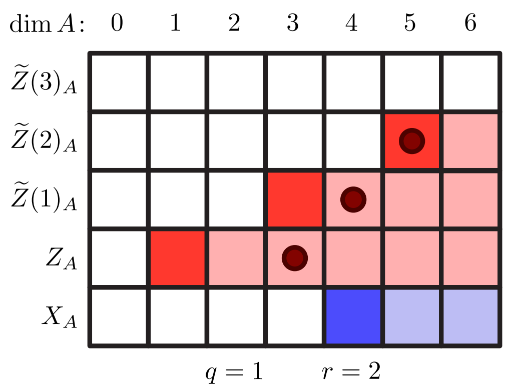
Lemma 5.3.5 (Fig. 5.3d)**.** *Consider the hypercube code family,* $QRM_m(0,1)$*. For each* $K \subseteq S$*,*

$$Z(|K|-1)_{\langle K\rangle} \equiv \overline{C^{\mathscr{P}(K)}Z}.$$

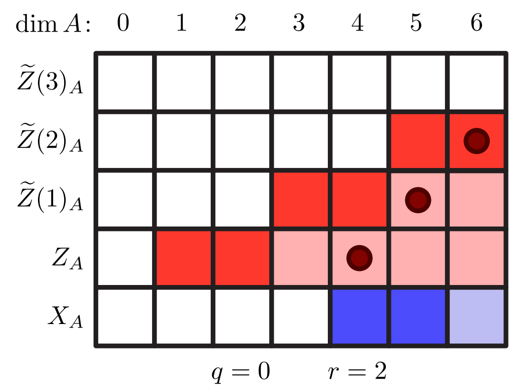
Proof. By Eq. (5.16),

$$Z(|K|-1)_{\langle K\rangle} = \prod_{J\subseteq K\setminus\emptyset} \widetilde{Z}(|J|-1)_{\langle J\rangle}.$$

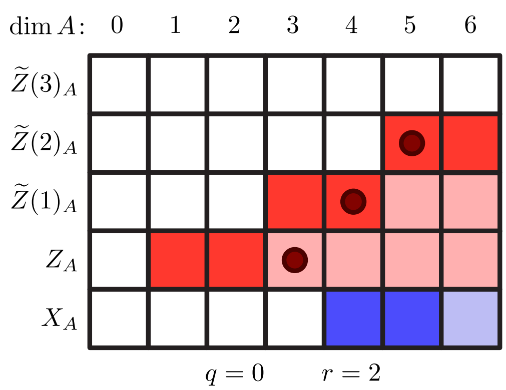
As $|J| = (|J|-1)+1$ we have that $J \in \mathcal{Q}_{|J|-1}$, so by Theorem 4.2.3 it must be that $\widetilde{Z}(|J|-1)_{\langle J\rangle} \in \mathcal{E}^{(|J|-1)}$. The result holds by Theorem 5.2.1 and by definition of the composition of multi-controlled-Z circuits. □



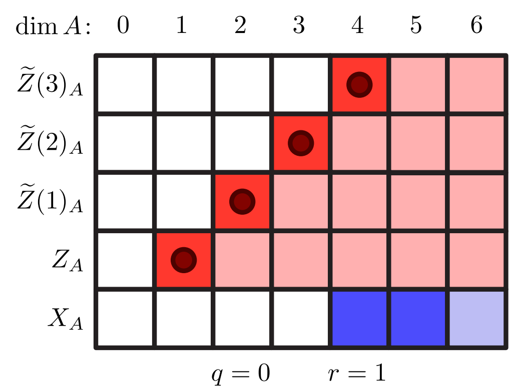
(a) (Theorem 5.3.3.1) Decomposition of $Z(2)_{\langle K \rangle}$ where $|K| = 5$, acting on $QRM_6(1, 2)$. Since $q \geq 1$, the dimensions that admit logical operators *do not* partition $\mathbb{N}$. As a result, every operator $\widetilde{Z}(k - j)_{\langle J \rangle}$ with $j \geq 1$ necessarily has size *larger* than the bounds for its given logical index set $\mathcal{Q}_{k-j}$. That is, other than the $\widetilde{Z}(k)_{\langle K \rangle}$ operator, every signed operator in the decomposition acts trivially on the code.



(b) (Theorem 5.3.3.2) Decomposition of $Z(2)_{\langle K \rangle}$ where $|K| = 6$, acting on $QRM_6(0, 2)$. As $|K| = 5$ is *not* the lowest size for a set in $\mathcal{Q}_2$, reducing the dimension/level of the CH by one immediately implies that an operator is trivial. This case can only happen when $r - q \geq 2$, but is independent of the choice of q.



(c) (Lemma 5.3.4) Decomposition of $Z(2)_{\langle K \rangle}$ where $|K| = 5$, acting on $QRM_6(0, 2)$. Since $q = 0$, every dimension does admit a logical operator. As $|K| = 5$ is the lowest size for a set in $\mathcal{Q}_2$, reducing the dimension/level of the CH by one remains a logical operation. However, as $r \geq 2$ every operator $\widetilde{Z}(k - j)_{\langle J \rangle}$ with $j \geq 2$ necessarily acts trivially on the code.



(d) (Lemma 5.3.5) Decomposition of $Z(5)_{\langle K \rangle}$ where $|K| = 4$, acting on the hypercube code $QRM_6(0, 1)$. Each time the dimension/level of the CH is reduced by one, the operator in the decomposition remains a logical operator for the code.

Figure 5.3: For $K \in \mathcal{Q}_k$, the unsigned subcube operator $Z(k)_{\langle K \rangle}$ can be decomposed as a product of signed subcube operators $\widetilde{Z}(k - j)_{\langle J \rangle}$ ($J \subseteq K$ with $|J| = |K| - j$) via Eq. (5.16). In the above figures, a dark box indicates a dimension where the subcube operator of the given level of the Clifford Hierarchy acts as a logical operator, a light box indicates a dimension where the operator acts trivially, and a white box indicates that the operator does not preserve the code space. In each of them, we consider the decomposition of an unsigned operator (specified in the subcaption) into a product of signed operators, represented by red dots.

5.4 Examples

We now explore some of the structures in the logical circuits we have defined for quantum RM codes. While the language of minimal covers is essentially the simplest general description of the logic implemented by subcube operators, the logic for the $[[2^m, m, 2]]$ hypercube codes and the more general $[[2^m, \binom{m}{r}, 2^{\min(m-r,r)}]]$ $QRM_m(r-1, r)$ codes can be phrased in a simpler way; we detail this in Sections 5.4.1 and 5.4.2, respectively.

Below we rely on the notation introduced before Definition 1.1.2. Additionally, as the logical qubits of a quantum RM code are indexed by subsets of S, we find the notation "$J = \{1, 3, 5\}$" more intuitive than the proper notation $J = \{e_1, e_3, e_5\}$. In this way, the standard cube $\langle 1, 3, 5\rangle$ is the set of length-m bit strings that are supported on the subset $\{1, 3, 5\}$ of the coordinates.

5.4.1 $QRM_m(0, 1)$

As a simple example, we first consider the hypercube code family, $QRM_m(0, 1)$. In this case, the logical qubit set $\mathcal{Q}$ is defined as $\mathcal{Q} := \left\{ \{i\} \;\middle|\; i \in S \right\}$, i.e., all single-element subsets of S. To simplify notation, we will denote these sets as $\bar{i} := \{i\}$, so that the i-th logical qubit of $QRM_m(0, 1)$ is given by the index $\bar{i}$. Similarly, the k-th level logical index sets are defined by $\mathcal{Q}_k := \left\{ K \subseteq S \;\middle|\; |K| = k + 1 \right\}$, i.e., all $(k + 1)$-element subsets of S. Thus, by definition *every* subset of S is in $\mathcal{Q}_k$ for some $k \in \mathbb{Z}_{\geq 0}$, and so by Theorem 4.2.3 *every* signed and unsigned standard subcube $\langle K\rangle$, $K \subseteq S$, gives rise to a logical operator in the $(|K| - 1)$-th level of the Clifford hierarchy. See Fig. 5.4 for a visual representation of this fact.

Recall that by Theorem 5.2.1, for $K \in \mathcal{Q}_k$ the operator $\widetilde{Z}(k)_{\langle K\rangle}$ implements the logical multi-controlled-Z circuit corresponding to the collection of minimal covers of K. Given $K \in \mathcal{Q}_k$, we

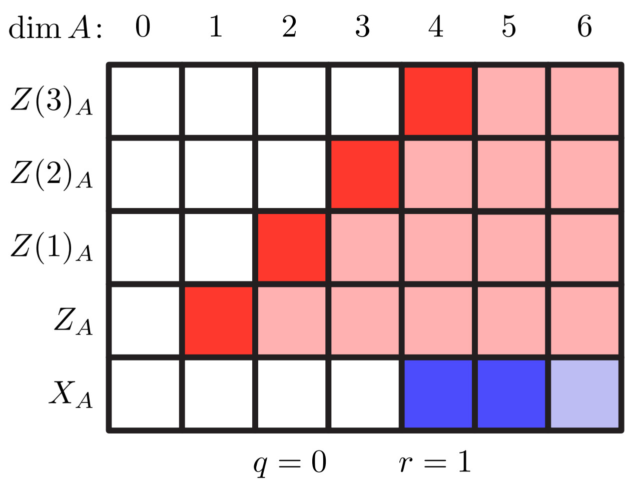


Figure 5.4: Consider the hypercube code family $QRM_m(0, 1)$. In the above figure, the shade of a given box indicates how the given operator for the given dimension will act on the code space:
(1) A dark box indicates logic,
(2) A light box indicates a logical identity, and
(3) A white box indicates the code space is not preserved.

proceed to compute this set $\mathcal{F}(K)$.

By definition, a subset of qubits $\mathcal{J} \subseteq \mathcal{Q}$ is a minimal cover for K if: (1) $\bigcup_{\bar{i} \in \mathcal{J}} \bar{i} = K$, and (2) $|\mathcal{J}| = k + 1$. As each logical qubit $\bar{i}$ is a single-element subset, the only collection of logical qubits whose union is all of K is precisely the set $\mathcal{K} := \{\bar{i} \mid i \in K\}$. Thus, we see there is only a single minimal cover for K and that $\mathcal{F}(K) = \{\mathcal{K}\}$.

Using Theorem 5.2.1 we can succinctly detail the logical circuit given by $\widetilde{Z}(|K| - 1)_{\langle K \rangle}$:

Logical Circuit 5.4.1. Let $K \subseteq S$ be any subset of $k + 1$ generators. Denote the $(k + 1)$-element collection of logical qubits $\mathcal{K} := \{\bar{i} \mid i \in K\}$. For a hypercube code, the signed $Z(k)$ operator applied to the physical qubits in $\langle K \rangle$ implements a single $(k + 1)$-qubit multi-controlled-Z operator on the logical qubits in $\mathcal{K}$: $\widetilde{Z}(k)_{\langle K \rangle} \equiv \overline{C^{\mathcal{K}} Z}$.

Remark 5.4.2. One may be tempted to use the sets K and $\mathcal{K}$ interchangeably as they have the same size and each element of $\mathcal{K}$ is defined using an element of K. We reiterate that logical qubits are necessarily *subsets* of generators, themselves. There is essentially no difference in the case of hypercube codes as the logical qubits are single-element subsets, but for other choices of q and r this distinction is important.

Lemma 5.3.5 gives us the logical circuit of any unsigned operator on a standard subcube.

Logical Circuit 5.4.3. Let $K \subseteq S$ be any subset of $k+1$ generators and let $\mathcal{K} := \left\{\bar{i} \mid i \in K\right\}$. For a hypercube code, the transversal $Z(k)$ operator applied to the physical qubits in $\langle K \rangle$ implements a multi-controlled-Z gate to every possible subset of qubits in $\mathcal{K}$: $Z(k)_{\langle K \rangle} \equiv \prod_{\mathcal{J} \subseteq \mathcal{K}} \overline{C^{\mathcal{J}} Z}$.

Using Theorem 4.2.3 (or alternatively, Corollary 4.2.10), subcube operators in lower levels of the Clifford hierarchy other than those above are necessarily trivial:

Fact 5.4.4. Let $K \subseteq S$ be any subset of $k+1$ generators. The signed and unsigned $Z(j)$ operators applied to the physical qubits in $\langle K \rangle$ are both stabilizers of the hypercube code for every $j < k$:

$$Z(j)_{\langle K \rangle} \equiv \widetilde{Z}(j)_{\langle K \rangle} \equiv \bar{\mathbb{I}} \quad \text{for all } j < k.$$

Lastly, Theorems 4.2.3 and 5.2.5 imply the following result for *arbitrary* subcube operators:

Logical Circuit 5.4.5. Signed and unsigned subcube operators of the same type necessarily implement the same logical circuits. That is, for any subset $K \subseteq S$ of $(k+1)$-generators, any $x \in \mathbb{Z}_2^m$, and $\mathcal{K}$ as defined above, the following hold for a hypercube code,

$$\widetilde{Z}(k)_{x+\langle K \rangle} \equiv \widetilde{Z}(k)_{\langle K \rangle} \equiv \overline{C^{\mathcal{K}} Z},$$

$$Z(k)_{x+\langle K \rangle} \equiv Z(k)_{\langle K \rangle} \equiv \prod_{\mathcal{J} \subseteq \mathcal{K}} \overline{C^{\mathcal{J}} Z}.$$

5.4.2 $QRM_m(r-1,r)$

Perhaps the most natural generalization of the hypercube code is the family of quantum RM codes given by $QRM_m(r-1,r)$. Some subcube operators for these codes have been considered in earlier works. In particular, [RCNP20, HLC22b, HLC22a] gave descriptions of *global* transversal operators on $QRM_m(r-1,r)$. In addition, [RCNP20] gave sufficiency for the $Z(k)_A$ operator when $A=\mathbb{Z}_2^m$ is the *entire* hypercube, and described the logical circuit that it implements[4]. Necessity in the global case was proved in [HLC22a]. Here we detail the implemented logical circuits for arbitrary $Z(k)_{\langle K\rangle}$ operators when $K\in\mathcal{Q}_k$.

The logical qubits of $QRM_m(r-1,r)$ are indexed by the set $\mathcal{Q}:=\{J\subset S \mid |J|=r\}$, i.e., all r-sized subsets of generators. The first convenient fact about $QRM_m(r-1,r)$ codes is that the X logical operators can be given by *standard* subcube operators, rather than subcube operators that have been shifted away from the 0^m vertex.

Fact 5.4.6. For $QRM_m(r-1,r)$, $X_{\langle S\setminus J\rangle}\equiv X_{x+\langle S\setminus J\rangle}$ *for every* $x\in\mathbb{Z}_2^m$.

Thus, for $QRM_m(r-1,r)$ the sets $\{Z_{\langle J\rangle}\mid |J|=r\}$ and $\{X_{\langle J\rangle}\mid |J|=m-r\}$ form a symplectic basis for the space of logical Pauli operators of $QRM_m(r-1,r)$.

Similarly to how the logical qubit index sets are defined by subsets of S with a particular size, the k-th level logical index sets are also highly restricted: $\mathcal{Q}_k:=\{K\subseteq S\mid |K|=(k+1)r\}$. Thus, for increasing values of r there are more and more dimensions that do not support logical subcube operators. Theorem 4.2.3 for $QRM_m(r-1,r)$ can now be stated as:

[4] We denote the Pauli operators as the 0-th level of the Clifford hierarchy, whereas [RCNP20] uses the 1-st level of the Clifford hierarchy to represent the Paulis. Thus, Theorem 19 in [RCNP20] states that the condition $r\mid m$ implies that $Z(\frac{m}{r}-1)$ is a logical operator for the code.

Fact 5.4.7. Consider the quantum RM code $QRM_m(r-1,r)$ and let $A \sqsubseteq \mathbb{Z}_2^m$ be any subcube. The operators $Z(k)_A$ and $\widetilde{Z}(k)_A$ are logical operators if and only if $\dim A = (k+1)r$.

As in the case of hypercube codes, we will determine the collection of minimal covers for a set $K \in \mathcal{Q}_k$. By definition, a subset of qubits $\mathcal{J} \subseteq \mathcal{Q}$ is a minimal cover for K if: (1) $\bigcup_{J \in \mathcal{J}} J = K$, and (2) $|\mathcal{J}| = k+1$. As each logical qubit index $J \in \mathcal{Q}$ contains precisely r elements, and we seek a collection of $k+1$ logical qubit indices whose union contains precisely $(k+1)r$ elements, we see that $\mathcal{J}$ is necessarily a (pairwise disjoint) partition of K into subsets of size r. Given a set K of $(k+1)r$ elements, a collection of subsets of K, $\mathcal{J} \subset \mathscr{P}(K)$, is said to be an *$r$-partition* of K, denoted by $\mathcal{J} \vdash_r K$, if (1) every $J \in \mathcal{J}$ has size $|J| = r$, and (2) $\mathcal{J}$ is a cover of K. Note that for $|K| = (k+1)r$, these two conditions are enough to guarantee that the sets in $\mathcal{J} \vdash_r K$ are disjoint. Ultimately, the minimal covers for $K \in \mathcal{Q}_k$ are given by $\mathcal{F}(K) = \{\mathcal{J} \mid \mathcal{J} \vdash_r K\}$, which is equal to the previous definition for hypercube codes when $r = 1$.

We already considered the case of $r = 1$ in the previous section. For the remainder of this section, we suppose that $r \geq 2$. This assumption affords us the following via Theorem 5.3.3:

Fact 5.4.8. Consider $QRM_m(r-1,r)$, where $r \geq 2$. For every $K \in \mathcal{Q}_k$, the signed and unsigned $Z(k)$ operators applied to $\langle K \rangle$ perform the same logical circuit, $Z(k)_{\langle K \rangle} \equiv \widetilde{Z}(k)_{\langle K \rangle}$.

Given that we have already determined $\mathcal{F}(K)$, we now have the following:

Logical Circuit 5.4.9. For the code $QRM_m(r-1,r)$, $r \geq 2$, and $K \subseteq S$ with $|K| = (k+1)r$, the transversal $Z(k)$ operator applied to the physical qubits in $\langle K \rangle$ implements $(k+1)$-qubit multi-controlled-Z gates to every subset of logical qubits whose index sets partition K:

$$Z(k)_{\langle K \rangle} \equiv \prod_{\mathcal{J} \vdash_r K} \overline{C^{\mathcal{J}} Z}.$$

For the case of $A = \mathbb{Z}_2^m$, this was previously proved in [RCNP20] (phrased in the language of phase polynomials).

Lastly, we note that in $QRM_m(r-1,r)$ codes, we can use any subcube of a particular type to implement the desired logical circuit. That is, Theorems 4.2.3 and 5.2.5 imply the following result for arbitrary subcube operators:

Logical Circuit 5.4.10. Subcube operators of the same type necessarily implement the same logical circuits. That is, for any subset $K \in \mathcal{Q}_k$ and any $x \in \mathbb{Z}_2^m$, the following holds for $QRM_m(r-1,r)$,

$$Z(k)_{x+\langle K\rangle} \equiv Z(k)_{\langle K\rangle}.$$

Example circuits: Fig. 5.5 demonstrates example logical circuits produced via signed subcube operators, which are non-trivial to describe without the "minimal cover" terminology. Fig. 5.5(a) and Fig. 5.5(b) demonstrate that applying a signed subcube of different dimensions affects completely different logic. We also observe that Fig. 5.5(a),(c) affect the same logical circuit, despite the fact that the QRM codes have a different m parameter.

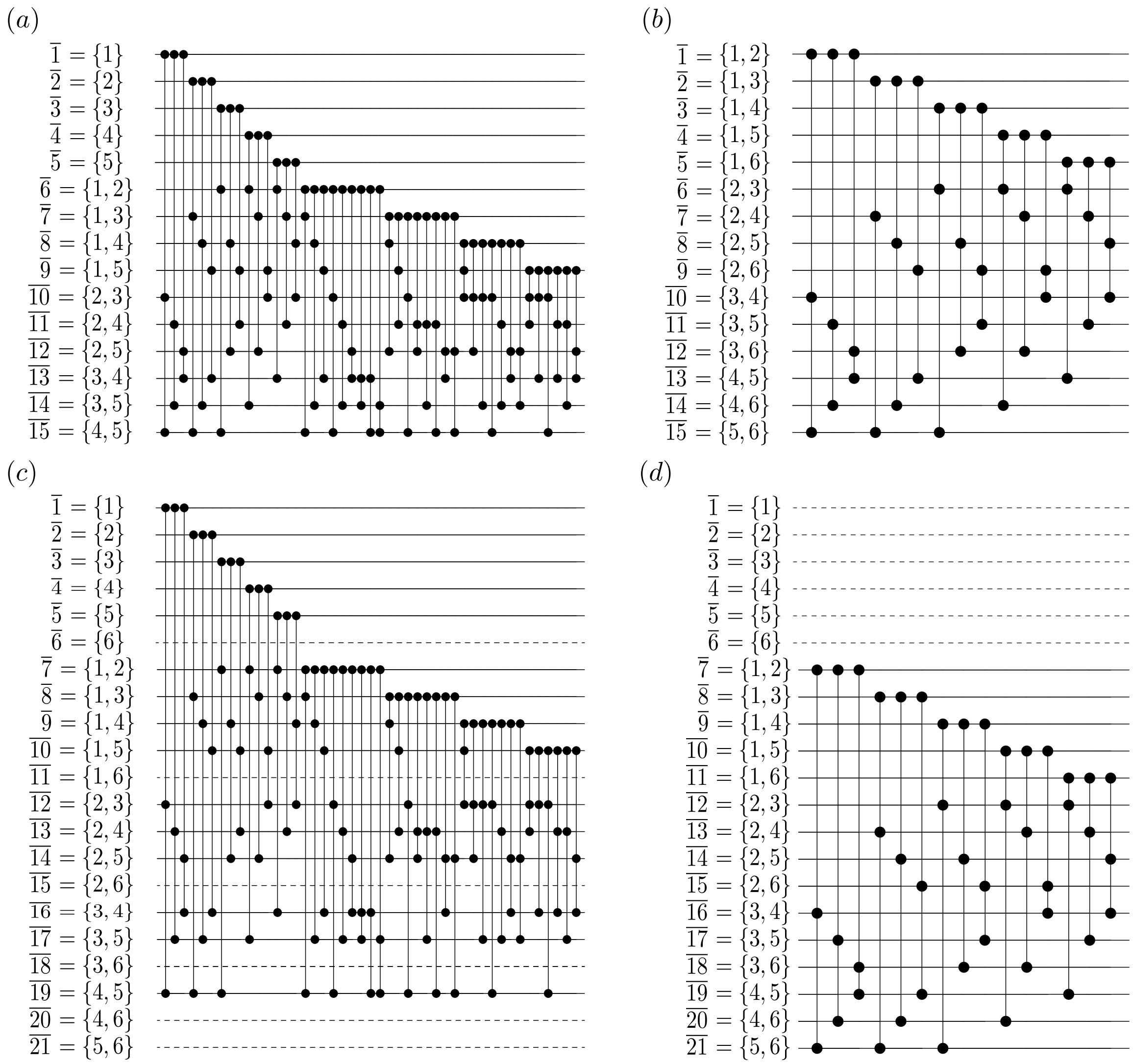


Figure 5.5: (a) Global signed T applied to $QRM_5(0,2)$. (b) Global signed T applied to $QRM_6(1,2)$. (c) Signed T operator applied to the $\langle 1,2,3,4,5 \rangle$ subcube of $QRM_6(0,2)$. Note that 6 qubits are unaffected (dotted lines) and that the circuit is identical to the one given in (a) on the remaining qubits. (d) Global signed T applied to $QRM_6(0,2)$. Note that 6 qubits are unaffected (dotted lines) and that the circuit is identical to the one given in (b) on the remaining qubits.

Chapter 6: Conclusion and Future Directions

In this dissertation, we introduced both classical and quantum Coxeter codes, new classes of error-correcting codes inspired by the combinatorial and geometric structure of Coxeter groups. We built these code by first framing Reed–Muller codes in terms of the Boolean hypercube, where the underlying Coxeter system is $\mathbb{Z}_2^m$ generated by weight-1 bit strings. In doing so, we have established a common language connecting algebraic coding theory, quantum error correction, and the combinatorial theory of Coxeter groups.

On the classical side, we defined Coxeter codes for any finite Coxeter system and showed that many of the hallmark structural properties of RM codes persist in this general setting. In particular, we established their hierarchical and multiplicative structure, constructed an explicit basis, established asymptotic normality of their rates, and proved an exponential lower bound on the distance of Coxeter codes. These results demonstrate that several essential algebraic features responsible for the good properties of RM codes can be understood in the much more general context of reflection groups.

On the quantum side, we extended the geometric and algebraic ideas underlying quantum RM codes to a broader class of quantum Coxeter codes. Our framework provides a new viewpoint from which we constructed natural logical operators in increasing levels of the Clifford hierarchy, that arise from the transversal application of certain diagonal gates. In the specific example of quantum RM codes we have fully characterized the logical multi-controlled-Z circuits that are affected by these operators.

We now detail several questions raised throughout this work, separating directions based on whether they pertain to either the classical or quantum versions of the codes.

6.1 Classical

6.1.1 Distance proof

An obvious open direction of our work is Conjecture 3.2.3 on the distance of a Coxeter code. In Theorem 3.2.4 we proved that the distance of the order-r code of any rank-m Coxeter system is $\geq 2^{m-r}$. To do so, we fixed a value of r and argued by induction on $m \geq r$, showing that for any non-trivial codeword in a rank $m+1$ code, there are at least two disjoint rank-m standard cosets on which the codeword is supported. One route toward proving the distance conjecture is by determining a more precise lower bound on the number, ℓ, of disjoint rank-m standard cosets supporting the codeword. If, for instance, ℓ satisfies

$$\min_{\substack{J \subseteq S \\ |J|=m-r}} |\langle J \rangle| = \ell \cdot \min_{\substack{J \subseteq S \\ |J|=m-r-1}} |\langle J \rangle|,$$

then Conjecture 3.2.3 would hold by induction.

6.1.2 Further combinatorial properties

We have introduced a broad family of binary codes that generalizes the classic Reed–Muller family and shares several of its key features. It is natural to wonder what other properties of RM codes are shared with the Coxeter code family beyond our conjectured value of the distance. For instance, what is the equivalent notion of a *projective* RM code for Coxeter codes? The codewords of minimum weight in RM codes are given by flats in the affine geometry; is there a geometric characterization of the minimum weight codewords for arbitrary Coxeter codes, and what kind of geometry could be involved?

Another line of thought is related to further combinatorial properties of Coxeter complexes, involving *residues* and f-*vectors* [Pet15]. We had initially phrased some of our definitions and proofs to involve these concepts before arriving at simpler arguments given here. At the same time, they may still find uses in uncovering further interesting properties of Coxeter codes and related code families.

6.1.3 Local testability.

RM codes are known to have the local testability property [AKK$^+$05]: simply check the parity of a random dual codeword of minimum weight. Supposing that their minimum weight codewords can be characterized, does the analogous local tester work for Coxeter codes? Coxeter codes are also related to codes on simplicial complexes, some of which have led to constructions of LTCs (for instance, the codes of [DLZ23]). In particular, the poset of all standard cosets of (W, S), ordered by reverse inclusion, forms a simplicial complex known as the *Coxeter complex*. By placing bits on the simplices of the highest dimension, the order-r Coxeter code has parity checks given by $(m-r-2)$-simplices. Is there a unifying framework connecting the local testability of such simplicial codes to that of RM codes?

6.1.4 Achieving capacity and automorphisms.

Switching to a probabilistic view, one could also study the capacity-achieving properties of Coxeter codes, extending the results for RM codes [KKM$^+$15], [RP23], [AS23]. For the binary erasure channel, it suffices to exhibit a doubly transitive action by the automorphism group of the code [KKM+15], and while the group W naturally acts on the code space (Theorem 1.2.6), this action is only singly transitive. The automorphism group of an RM code (supposing $r \notin \{-1, 0, m-1, m\}$) is given by the affine group $Aut(RM(r, m)) = \mathbb{Z}_2^m \rtimes GL(m, 2)$, far larger than simply $\mathbb{Z}_2^m$. Is there a suitable generalization of the affine group that captures the automorphisms of a Coxeter code?

By computer, we found that $|Aut(\mathsf{C}_{A_3}(1))| = 196608 = 3 \cdot 2^{16}$. This group is formed as a semi-direct product of the automorphisms of the Cayley graph of A_3 (given by $A3 \times A1$) together with the group generated by symmetries swapping each of the 12 pairs of opposite (same-color) edges in the 6 squares of the graph; see Fig. 1.1. This group acts transitively on the set of coordinates, but (again by computer) is not doubly transitive. Uncovering the structure of the group $Aut(\mathsf{C}_{A_m}(r))$ for arbitrary m, r is an interesting question, which appears nontrivial and which may elucidate the structure of $Aut(\mathsf{C}_W(r))$ in general.

6.1.5 Decoding algorithms

The accumulated lore of RM decoding comprises a vast body of results [ASSY23]. An algorithm that is attuned to our extension of the RM code family is *Recursive Projection Aggregation*, or RPA, suggested in [YA20]. Given a vector $y \in \mathbb{F}_2^{2^m}$ received from the channel, decoding proceeds recursively by reducing the decoding task to several decoding instances of codes of length 2^{m-1} and aggregating the obtained results by a majority decision. Each of the shorter codes is obtained as a "projection" of $RM(r, m)$ on a one-dimensional subspace $\langle x \rangle$ and its cosets in $\mathbb{F}_2^{2^m}$, so there are $2^m - 1$ distinct instances of decoding.

This procedure applies to the codes $\mathsf{C}_W(r)$, where we project the code on standard subgroups of rank 1 and their cosets. The authors of [YA20] consider this option in Sec.2 of their paper, where instead of all the subspaces, they limit the procedure to the m subspaces generated by the standard basis vectors. We leave a detailed analysis of this decoding for Coxeter codes for future work.

6.1.6 Generalizing to achieve better parameters

A major drawback of Coxeter codes is that they seemingly have worse parameters than RM codes for any given rank, m. In particular, the distance of high-order Coxeter codes is always equal to 2^{m-r} (Corollary 3.2.8), whereas the code length grows much faster than 2^m for most Coxeter codes aside from RM codes. The poor distance occurs because with high-order codes, one can always find $m-r$ commuting generators in (W, S), which form $(m-r)$-cubes. Generalizations of Coxeter codes could avoid this problem. We will mention two broad generalizations here, though we have not examined their viability in providing better parameters.

Sets of generators

The first generalization is to restrict the possible choices of standard cosets.

Definition 6.1.1. Let (W, S) be a rank-m Coxeter system, and consider some collection $\mathcal{S} \subseteq \mathcal{P}(S)$ of subsets of generators. The order-r Coxeter code of type $(W, \mathcal{S})$ is defined as

$$\mathcal{C}_{(W,\mathcal{S})}(r) \coloneqq \operatorname{Span}\left\{\mathbb{1}_{\sigma\left\langle\bigcup_{J\in\mathcal{J}} J\right\rangle} \mid \sigma \in W, \mathcal{J} \subseteq \mathcal{S}, |\mathcal{S}| = m-r\right\}.$$

If the collection $\mathcal{S}$ is chosen to be the collection of singletons $\mathcal{S} = \{\{s_i\} \mid i \in [m]\}$, then we recover the standard definition of a Coxeter code.

Group codes

The following is an extremely broad way to construct group codes, which has likely been studied in various capacities.

Definition 6.1.2. Let G be a finite group generated by a subset of m elements $S \subseteq G$, i.e., $G = \langle S \rangle$. The order-r group code of type (G, S) is a left ideal the group algebra $\mathbb{F}G \coloneqq \{f : G \to \mathbb{F}\}$, defined as

$$C_{(G,S)}(r) \coloneqq \operatorname{Span}\left\{\mathbb{1}_{g\langle J \rangle} \mid g \in G, J \subseteq S, |J| = m - r\right\}.$$

Given a group G, one can prove using standard results in group theory that each choice of generating set S gives a *filtration* of the group algebra $\mathbb{F}G$, i.e.,

$$\{0\} = C_{(G,S)}(-1) \;\subseteq\; C_{(G,S)}(0) \;\subseteq\; \cdots \;\subseteq\; C_{(G,S)}(m-1) \;\subseteq\; C_{(G,S)}(m) = \mathbb{F}G,$$

satisfying the multiplication property $C_{(G,S)}(r_1) \odot C_{(G,S)}(r_2) \subseteq C_{(G,S)}(r_1 + r_2)$. If this generating set contains only even-order elements, then $C_{(G,S)}(r) \subseteq C_{(G,S)}(m - r - 1)^{\perp}$, with equality likely depending on the particular combinatorial structure of the group.

A poor feature of all Coxeter codes is that for any family of Coxeter systems with increasing rank, $\{(W_m, S_m) \mid |S_m| = m\}_{m \geq 1}$, the group order scales *exponentially* in the rank, $|W_m| = \Omega(2^m)$. That is, from a finite-scale perspective, the length of Coxeter codes grows quickly out of control. A promising direction toward constructing families of shorter codes would be to consider group codes corresponding to a family of finite groups with explicit generating sets (G_i, S_i) for which the number of group elements (the code length) grows polynomially with the number of generators $|G_i| = \mathsf{poly}(|S_i|)$.

6.2 Quantum

6.2.1 Logic in quantum Coxeter codes

A natural future direction, following the main results of [BCHK25], is to give a combinatorial description of the logical circuit implemented by a $\widetilde{Z}(k)_A$ operator when A is a standard coset whose rank satisfies $q + kr + 1 \leq \operatorname{rank} A \leq (k+1)r$. A necessary first step would be to construct a symplectic basis for $\mathsf{QC}_W(q, r)$, as we did for quantum RM codes in Lemma 5.1.3. In a few cases— including the QRM family— the collections of forward and reverse extensions satisfy the symplectic condition. Unfortunately, this appears to only hold for Cartesian products of A_1 and A_2, and fails for all others.

6.2.2 Subcube operators in the X basis

Given the symmetry in the definition of QRM codes, the roles of X and Z stabilizers/logicals can be reversed by redefining $r \mapsto m - q - 1$ and $q \mapsto m - r - 1$. Thus, our results for the $Z(k)$ subcube operators translate directly to the case of $X(k) \coloneqq |+\rangle\langle+| + e^{i\frac{\pi}{2^k}} |-\rangle\langle-|$ operators. For instance, we have the following analogous version of Theorem 4.2.3 in the X basis:

Theorem 6.2.1. *Consider $QRM_m(q, r)$ and suppose $A \sqsubseteq \mathbb{Z}_2^m$ is a subcube of $\mathbb{Z}_2^m$.*

1. *$X(k)_A$ implements logical identity if and only if $\dim A \geq (k+1)(m-q-1)+1$.*
2. *$X(k)_A$ performs non-trivial logic if and only if $m-r+k(m-q-1) \leq \dim A \leq (k+1)(m-q-1)$.*

This bound for non-trivial logic is often incompatible with that of the Z-basis case in Theorem 4.2.3. Since the dimension of any subcube is at most m, Theorem 4.2.3 tells us that $Z(k)_A$ performs non-trivial logic only when $q + kr + 1 \leq m$. For the same reason, Theorem 6.2.1 implies that $X(k)_A$

performs non-trivial logic only when $m - r + k(m - q - 1) \leq m$. Adding these two bounds and rearranging terms, we see

$$q + kr + 1 + m - r + k(m - q - 1) \leq 2m, \tag{6.1}$$

$$q + kr + 1 - r + km - kq - k - m \leq 0, \tag{6.2}$$

$$(k-1)r - (k-1)q + (k-1)m - (k-1) \leq 0, \tag{6.3}$$

$$(k-1)(m - 1 + r - q) \leq 0. \tag{6.4}$$

This inequality is always satisfied when $k = 0$, indicative of the existence of logical Pauli operators. For $k \geq 2$ this inequality can never be satisfied, as $q < r \leq m$. Thus, a quantum Reed–Muller code can never simultaneously admit $Z(k)_A$ and $X(k)_B$ subcube operators when $k \geq 2$.

In the remaining case where $k = 1$, the inequality is always satisfied. The bound from Theorem 4.2.3 implies that $m \geq q + r + 1$ and the bound from Theorem 6.2.1 implies that $m \leq q + r + 1$, so $m = q + r + 1$ is necessary. Ultimately, we have the following:

Corollary 6.2.2.

1. *For subcubes $A, B \sqsubseteq \mathbb{Z}_2^m$, if a quantum Reed–Muller codes supports a transversal $Z(k)_A$ for some $k \geq 2$, then it cannot support a transversal $X(k)_B$ for* any *$k > 0$, and vice versa.*

2. *When $m = q + r + 1$ the code $QRM_{q+r+1}(q, r)$ simultaneously supports global $Z(1)$, $X(1)$, and Hadamard operators. It does not support logical $Z(k)$ or $X(k)$ subcube operators for any $k \geq 2$.*

6.2.3 Diagonal and transversal operators in the Clifford hierarchy

The physical operators we consider all share a common *DTC structure*: they are (1) diagonal, (2) transversal, and (3) lie in the Clifford hierarchy. Denoting the group of all unitary operators satisfying these conditions by $\mathrm{DTC} \leq \mathrm{U}(2)^{\otimes 2^m}$, one implication of Theorem 4.2.3 is that

$$\left\{ Z(k)_{\langle K \rangle} \mid k \geq 0, K \in \mathcal{Q}_k \right\}$$

generates a group of logical gates for $QRM_m(q, r)$, all with the property that they lie in DTC. It is natural to wonder whether or not the converse is true: are there DTC operators that preserve the code space of $QRM_m(q, r)$, but that *cannot* be produced via products of the basis subcube operators indexed by the $\mathcal{Q}_k$ collections?

Theorem 4.2.3 says that the converse *does* hold for $Z(k)$ subcube operators. In particular, given a subcube $A \sqsubseteq \mathbb{Z}_2^m$, $\widetilde{Z}(k)_A$ has a decomposition into standard subcube operators indexed by $\mathcal{Q}_k$. Additionally, the CSS construction provides a converse statement when $k = 0$: if Z_M is a logical Z operator acting on an arbitrary *subset* $M \subseteq \mathbb{Z}_2^m$ then it necessarily can be decomposed as a product of $Z_{\langle J \rangle}$ operators for $J \in \mathcal{Q}$. This is, in fact, the statement that the group of undetectable Pauli Z errors for $QRM_m(q, r)$ is isomorphic to the *classical* Reed–Muller code of order $m - q - 1$, $RM(m - q - 1, m)$.

A possible converse can be formulated in the language of linear codes over *rings* instead of fields. For the ring $R_k := \mathbb{Z}_{2^{k+1}}$, one can construct a family of Reed–Muller-codes over R_k as submodules of $R_k^{2^m}$ by drawing inspiration from the geometric construction of RM codes used throughout our paper.[1] Do these R_k-Reed–Muller codes fully characterize the DTC logic for quantum RM codes? A more

[1] Generalizations of Reed–Muller codes to ring alphabets have been previously studied within the framework of finite ring extensions and Galois rings [BW10]. We believe that the codes we define here are different from the code families considered in the literature.

detailed explanation of can be found in Appendix A.

Beyond DTC operators, one can also consider the space of diagonal operators in the Clifford hierarchy, fully classified in [CGK17]. This prompts us to pose the following question: Can the geometric structure of quantum RM codes be used to give necessary and sufficient conditions for when *constant-depth circuits* from the diagonal Clifford hierarchy perform logic? We have not attempted to answer it in this paper.

6.2.4 Reducing physical qubit overhead

While we have shown that quantum RM codes support non-trivial logical circuits through the physical implementation of subcube operators, a priori the parameters of quantum RM codes are largely impractical for, say, magic-state distillation. For instance, the code length grows exponentially in the dimension m of the hypercube. The maximal level of the Clifford hierarchy attainable with $QRM_m(q,r)$, $k_{\max}$, must satisfy $q + k_{\max} r + 1 \leq m$, so the number of physical qubits needed will likewise grow exponentially in $k_{\max}$. A crucial next step is to reduce the physical qubit overhead of codes that support transversal logic in higher levels of the Clifford hierarchy.

Puncturing, or removing qubits, is one way to reduce the qubit overhead. Though several magic-state distillation protocols employ punctured or shortened quantum RM codes, the transversal logic of punctured quantum RM codes in general is not particularly well understood from both a theoretical or practical standpoint. The theoretical intuition for how deformed operators perform is nascent, with early work studying specific deformations [VK22a] or exhaustively enumerating valid code instances [RCNP20]. Practically, exhaustive enumeration strategies are intractable for larger m; this prevents the design of distilleries with optimal rate given specified parameters. We hope that an extension of our formalisms could elucidate the effects of puncturing, enabling the dynamic design of magic-state factories.

Our geometric construction of quantum RM codes hints at another way to reduce the number of physical qubits. Drawing inspiration from several recent works on asymptotically good qLPDC codes [PK22, LZ22] and constructions of some quantum locally-testable codes [LLZ22], one could consider the *quotient* of the hypercube by the action of a group. As an example, consider the *folded cube graph* obtained by identifying every vertex $x \in \mathbb{Z}_2^m$ with its opposite vertex, $\bar{x} = x + 1^m$ and likewise identifying a subcube $A \sqsubseteq \mathbb{Z}_2^m$ with its opposite, $\bar{A} = 1^m + A$. This action preserves the commutativity of X and Z operators defined using $(m-q)$-cubes and $(r+1)$-cubes, respectively, and therefore produces a quantum code with $2^m/2$ qubits instead of 2^m qubits. A natural question is whether or not these codes support transversal logic in the same way as quantum RM codes. More general group actions can also preserve commutativity of appropriate choices of X and Z subcube operators, while reducing physical qubit overhead by increasing multiplicative factors. Can the transversal logic implemented on such codes also be understood using techniques from our work?

6.2.5 The dual view

We have described our results in terms of the m-dimensional hypercube and its complex of subcubes, but there is another equivalent description of quantum RM codes in terms of the *hyperoctahedral complex* in m dimensions, which is dual to the hypercube construction. We will now detail this alternative construction and also show its connection to the ball codes of [VK22a].

In three dimensions there is a well-known duality between the cube and octahedron, where the vertices of the cube correspond to the triangular faces of the octahedron and the vertices of the octahedron correspond to the squares of the cube. This duality is easily extended to the higher dimensional *hyperoctahedron*. Consider m-dimensional real Euclidean space, $\mathbb{R}^m$, and define the coordinate, p_i, which has a 1 in the i-th position and 0's elsewhere. In short, the hyperoctahedron in m-dimensional space can be defined as the convex hull of the $2m$ points $\{\pm p_i\}_{i\in[m]}$. This definition, although simple, does not capture the full *simplicial* structure of the hyperoctahedron, in the same way that the Boolean hypercube $\mathbb{Z}_2^m$ does not immediately capture the subcube structure of the hypercube.

Geometrically, an *ℓ-simplex* σ is a collection of $\ell + 1$ (affinely) independent set of points in Euclidean space, i.e., the convex hull of σ does not lie in an ℓ-dimensional flat. The dimension of a simplex is defined as $\dim \sigma = |\sigma| - 1$. If one simplex ρ is contained in another, $\rho \subseteq \sigma$, the ρ is said to be *incident to* σ and this incidence is denoted by $\rho \preceq \sigma$. A *geometric simplicial complex* is a collection of simplices $\mathcal{X} = \{\sigma\}$ which is (1) downward closed (if $\sigma \in \mathcal{X}$ and $\rho \preceq \sigma$ then $\rho \in \mathcal{X}$), and (2) closed under intersections. We note that the downward closure property implies that $\emptyset \in \mathcal{X}$ for any simplicial complex.

The $2m$ points $V \coloneqq \{\pm p_i\}_{i\in[m]}$ can be used to define the *m-dimensional hyperoctahedral (simplicial) complex*, H_m: A subset of points $\sigma \subseteq V$ is a simplex in H_m if σ contains at most one of p_i and $-p_i$ for each $i \in m$ (but possibly neither). In particular, for each $\sigma \in H_m$ there is a unique string $x \in \{0, 1, *\}^m$ where $x_i = 0$ if $p_i \in \sigma$, $x_i = 1$ if $-p_i \in \sigma$, and $x_i = *$ if neither $\pm p_i \in \sigma$. Note that the dimension of σ is the number of non-null ($*$) positions in the corresponding x, and so the dimension of any simplex in H_m is at most $m - 1$. In fact, the set $\{0, 1, *\}^m$ is in 1-to-1 correspondence with the simplices in H_m. The *vertices* of H_m are the strings $x \in \{0, 1, *\}^m$ with a single non-null entry (i.e., corresponds to a point in $\{\pm p_i\}$) and the *facets* of H_m are the bit strings $x \in \{0, 1\}^m$. It is straightforward to show that H_m satisfies the conditions of a simplicial complex. In fact, it is a *homogenenous* simplicial complex, meaning that every simplex is incident to some facet in H_m. Further, H_m yields a *simplicial structure* on the $(m-1)$-dimensional sphere $S^{m-1} \subseteq \mathbb{R}^m$: each point $\pm p_i$ has unit length, and for a simplex in H_m one can take the convex hull of σ on the sphere.

We now connect the m-dimensional hyperoctahedral complex to the hypercube complex. We recall the definition of the hypercube complex. Consider $\mathbb{Z}_2^m$ with its standard generating set $S \coloneqq \{e_i\}$. The m-dimensional hypercube is the complex of *standard cosets of S in $\mathbb{Z}_2^m$*,

$$\left\{ z + \langle J \rangle \;\middle|\; J \subseteq S,\ z \in \mathbb{Z}_2^m \right\}. \tag{6.5}$$

In particular, a coset $z + \langle J \rangle$ is a $|J|$-dimensional subcube of $\mathbb{Z}_2^m$. The duality between the hyperoctahedron $H_m = \{\{0,1,*\}^m\}$ and the hypercube $\mathbb{Z}_2^m$ is given by

$$x \in \{0,1,*\}^m \mapsto z + \langle J \rangle \text{ where } \begin{pmatrix} z_i = x_i \text{ if } x_i \neq * \\ z_i = 0 \text{ otherwise} \end{pmatrix} \text{ and } J \coloneqq \left\{ e_i \;\middle|\; x_i = * \right\}, \tag{6.6}$$

$$z + \langle J \rangle \mapsto x \in \{0,1,*\}^m \text{ where } \begin{pmatrix} x_i = z_i \text{ if } e_i \notin J \\ x_i = * \text{ if } e_i \in J \end{pmatrix}. \tag{6.7}$$

Under this correspondence, vertices of H_m are equivalent to $(m-1)$-cubes in $\mathbb{Z}_2^m$ and facets of H_m are equivalent to vertices in (elements of) $\mathbb{Z}_2^m$. In general, ℓ-simplices in H_m are equivalent to $(m-\ell-1)$-cubes in $\mathbb{Z}_2^m$. For instance, the empty simplex in H_m corresponds to the *entire* hypercube. See Fig. 6.1 for the correspondence between the 4 dimensional hypercube and hyperoctahedron.

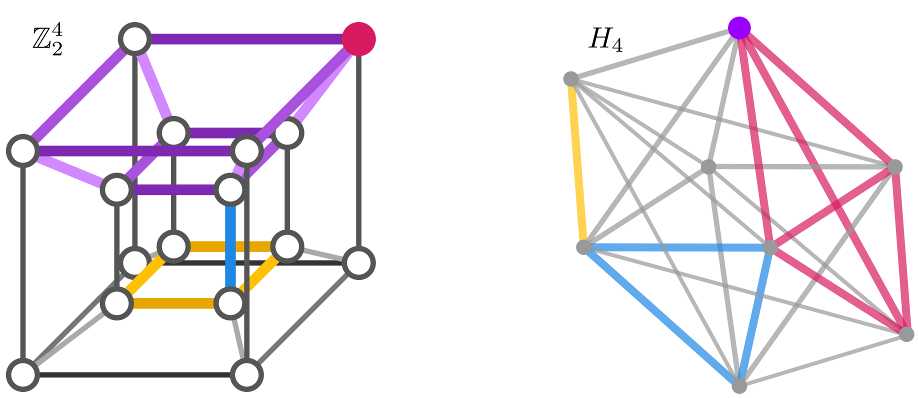
We can define quantum RM codes using the structure of the hyperoctahedral complex. As there are 2^m facets in H_m, we will associate physical qubits with these $(m-1)$-dimensional simplices in H_m. Given a simplex $\sigma \in H_m$, its *neighborhood* is defined at the set of facets that it is incident to, $\mathrm{N}(\sigma) \coloneqq \{\rho \in H_m \mid \sigma \preceq \rho,\ \dim \rho = m-1\}$. In the same way that we defined subcube operators, we can likewise define a *simplex operator* U_σ as the operator which acts as the single-qubit gate U on the qubits in $\mathrm{N}(\sigma)$ and as identity otherwise.

Definition 6.2.3 (Alternative definition of $QRM_m(q,r)$, *cf.* Definition 1.4.1)**.** Let $0 \leq q \leq r \leq m$ be non-negative integers. The *quantum Reed–Muller code* of order (q,r) and length 2^m, denoted by $QRM_m(q,r)$, is defined as the common $+1$ eigenspace of a Pauli stabilizer group $\mathcal{S} \coloneqq \langle S_X, S_Z \rangle$, with stabilizer generators given by

$$S_X \coloneqq \left\{ X_\sigma \;\middle|\; \sigma \text{ is a } (q-1)\text{-simplex} \right\}, \tag{6.8}$$

$$S_Z \coloneqq \left\{ Z_\sigma \;\middle|\; \sigma \text{ is an } (m-r-2)\text{-simplex} \right\}, \tag{6.9}$$

This definition is equivalent to the ball code definition of the hypercube code family given in [VK22a], where the central vertex of the ball code is given by the empty simplex.



red vertex $\longleftrightarrow$ red 3-simplex
blue edge $\longleftrightarrow$ blue triangle
yellow square $\longleftrightarrow$ yellow edge
purple cube $\longleftrightarrow$ purple vertex

Figure 6.1: Equivalence between subcubes of $\mathbb{Z}_2^4$ and simplices in H_4.

Appendix A: Diagonal, Transversal, and Clifford Logic for QRM Codes

Consider the space of integer-valued functions on the Boolean hypercube, $\mathbb{Z}[\mathbb{Z}_2^m] \coloneqq \{f\colon \mathbb{Z}_2^m \to \mathbb{Z}\}$, and define the unsigned (resp. signed) indicator function of $A \sqsubseteq \mathbb{Z}_2^m$ as $\mathbb{1}_A(x) \coloneqq 1$ if $x \in A$ and 0 otherwise (resp. $\widetilde{\mathbb{1}}_A(x) \coloneqq (-1)^{|x|}$ if $x \in A$ and 0 otherwise). These indicator functions are defined so that

$$\left\langle Z(k)_A \right\rangle \cong \left\langle \mathbb{1}_A \pmod{2^{k+1}} \right\rangle, \tag{A.1}$$

$$\left\langle \widetilde{Z}(k)_A \right\rangle \cong \left\langle \widetilde{\mathbb{1}}_A \pmod{2^{k+1}} \right\rangle. \tag{A.2}$$

Theorem 4.2.3 implies the following:

$$\left\langle e^{i\theta} \widetilde{Z}(k)_{\langle K \rangle} \;\middle|\; k \in \mathbb{Z}_{\geq 0},\ K \subseteq S,\ |K| \geq (k+1)r + 1,\ \theta \in [0, 2\pi) \right\rangle \subseteq \bigcup_{k \in \mathbb{Z}_{\geq 0}} \mathcal{S}^{(k)}, \tag{A.3}$$

and

$$\left\langle e^{i\theta} \widetilde{Z}(k)_{\langle K \rangle} \;\middle|\; k \in \mathbb{Z}_{\geq 0},\ K \subseteq S,\ |K| \geq q + kr + 1,\ \theta \in [0, 2\pi) \right\rangle \subseteq \bigcup_{k \in \mathbb{Z}_{\geq 0}} \mathcal{N}^{(k)}. \tag{A.4}$$

A natural open question of our work is whether or not the *reverse* inclusion holds, as well. For simplicity we will consider only the undetectable error set, and without global phases. That is, consider the subgroup generated by the $\widetilde{Z}(k)_{\langle K\rangle}$ operators for $K \in \mathcal{Q}_k$, the index set of k-th level logical operators:

$$\left\langle \widetilde{Z}(k)_{\langle K\rangle} \;\middle|\; k \in \mathbb{Z}_{\geq 0},\ K \in \mathcal{Q}_k \right\rangle. \tag{A.5}$$

Question A.1. Does the group generated by standard subcube operators given in Eq. (A.5) fully characterize the group of undetectable Clifford errors for the code $QRM_m(q, r)$ that are diagonal and transversal? That is, up to global phases, does

$$\left\langle \widetilde{Z}(k)_{\langle K\rangle} \;\middle|\; k \in \mathbb{Z}_{\geq 0},\ K \in \mathcal{Q}_k \right\rangle = \bigcup_{k\in\mathbb{Z}_{\geq 0}} \left(\mathrm{DTC}^{(k)} \cap \mathcal{N}^{(k)}\right) ? \tag{A.6}$$

Our goal in this section is to give a coding-theoretic interpretation of the group in Eq. (A.5). In particular, we begin by defining so-called linear codes over $\mathbb{Z}_{2^{k+1}}$.

For $k \in \mathbb{N}$, let $R_k := \mathbb{Z}_{2^{k+1}}$ denote the ring of integers modulo 2^{k+1}. Consider now the space of R_k-valued functions on the Boolean hypercube, $R_k[\mathbb{Z}_2^m] := \{f : \mathbb{Z}_2^m \to R_k\}$. $R_k[\mathbb{Z}_2^m]$ is a free module over R_k. A submodule, $C \subseteq R_k[\mathbb{Z}_2^m]$, is called an *$R_k$-linear code of length* 2^m, or simply a linear code. For two linear codes, $A, B \subseteq R_k[\mathbb{Z}_2^m]$, their sum $A + B \subseteq R_k[\mathbb{Z}_2^m]$ is a linear code defined by taking sums of elements in A and B.

As R_k is not a principal ideal domain (for $k > 0$), the space $R_k[\mathbb{Z}_2^m]$ fails to have many properties that a vector space over a field does. For example, not every linear code will have a basis, and even if a code has a basis the number of elements in two given bases may be different. In other words, the dimension of an R_k-linear code may not be well-defined.

Given a function $f \in R_k[\mathbb{Z}_2^m]$ it is straightforward to construct a diagonal and transversal operator in the k-th level of the Clifford Hierarchy. In particular, define $Z(f) \in \mathrm{Cl}^{(k)}$ to be

$$Z(f) = \bigotimes_{x \in \mathbb{Z}_2^m} Z(k)^{f(x)}. \tag{A.7}$$

That is, $Z(f)$ acts as $Z(k)^{f(x)}$ on the physical qubit indexed by $x \in \mathbb{Z}_2^m$. Similarly, supposing that $U = \bigotimes_{x \in \mathbb{Z}_2^m} Z(k)^{P_x} \in \mathrm{Cl}^{(k)}$ is a diagonal and transversal operation in the k-th level of the Clifford Hierarchy where each $P_x \in \mathbb{Z}$, we can define a function $f_U \in R_k[\mathbb{Z}_2^m]$ via

$$f_U(x) \coloneqq P_x \pmod{2^{k+1}}. \tag{A.8}$$

The space of *diagonal, transversal, and k-th level Clifford operators*, $\mathrm{DTC}^{(k)}$, is defined as

$$\mathrm{DTC}^{(k)} \coloneqq \left\{ \bigotimes_{x \in \mathbb{Z}_2^m} Z(k)^{f(x)} \;\middle|\; f \in \mathbb{Z}[\mathbb{Z}_2^m] \right\} \tag{A.9}$$

As the diagonal and transversal operators in the k-th level of the Clifford Hierarchy admit a natural action via R_k by taking powers, we see that

$$R_k[\mathbb{Z}_2^m] \cong \mathrm{DTC}^{(k)} \tag{A.10}$$

as modules over R_k.

We now proceed to generalize construction of classical RM codes:

Definition A.2 ($RM_k(r, m)$)**.** For $r \in \{-1, 0, \ldots, m\}$, the Generalized Reed–Muller (GRM) code of *order* r over R_k, denoted $RM_k(r,m)$, is defined as the linear code generated by the signed indicator functions of standard subcubes of dimension at least $m-r$, taken modulo 2^{k+1}:

$$RM_k(r,m) := \left\langle \widetilde{\mathbb{1}}_{\langle J \rangle} \pmod{2^{k+1}} \;\middle|\; J \subseteq S,\ |J| \geq m-r \right\rangle.$$

We note that for all $k \in \mathbb{Z}_{\geq 0}$,

$$\left\langle \widetilde{Z}(k)_{\langle K \rangle} \;\middle|\; K \subseteq S,\ |K| \geq (k+1)r+1 \right\rangle \cong RM_k\big(m-((k+1)r+1),m\big). \tag{A.11}$$

Thus, sufficiency in Theorem 4.2.3 can be rephrased as:

Theorem A.3. *Consider $QRM_m(q,r)$.*

1. *If $f \in RM_k\big(m-((k+1)r+1),m\big)$, then $Z(f) \in \mathcal{S}^{(k)}$.*

2. *If $f \in RM_k\big(m-(q+kr+1),m\big)$, then $Z(f) \in \mathcal{N}^{(k)}$.*

Ideally, the converse would hold as well, that any operator $U \in \mathrm{DTC}^{(k)}$ that is a Clifford error for $QRM_m(q,r)$ *must* arise in this way. That is, it would be convenient if the code $RM_k\big(m-(q+kr+1),m\big)$ completely characterized $\mathcal{N}^{(k)} \cap \mathrm{DTC}^{(k)}$. This, however, cannot be the case. In particular, every function in one level below, $k-1$, gives rise to an operator in $\mathcal{N}^{(k)}$ via *squaring*: if $f \in RM_{k-1}\big(m-(q+(k-1)r+1),m\big)$ then $Z(f)^2 \in \mathcal{N}^{(k)}$. However, $RM_{k-1}\big(m-(q+(k-1)r+1),m\big)$ is *not* a subcode of $RM_k\big(m-(q+kr+1),m\big)$. In fact, a priori it is not even an R_k-module! At every increased level of the Clifford Hierarchy we must include all *squares* from the level below. We will do so through the use of the sum of codes, $A+B$.

To begin with, we must turn $RM_{k-1}\big(m-(q+(k-1)r+1),m\big)$ into an R_k-module. For

$i \in \{-1, \ldots, k\}$, define the linear code, $2^{k-i} \cdot RM_k(r, m) \subseteq R_k[\mathbb{Z}_2^m]$, via

$$2^{k-i} \cdot RM_k(r, m) \coloneqq \left\langle 2^{k-i} \cdot \widetilde{\mathbb{1}}_{\langle J \rangle} \pmod{2^{k+1}} \;\middle|\; J \subseteq [m],\ |J| \geq m - r \right\rangle. \tag{A.12}$$

Note that if $i = -1$ then $2^{k-i} \cdot RM_k(r, m) = \{0\}$, and for $i \geq 0$ we have $2^{k-i} \cdot RM_k(r, m) \cong RM_i(r, m)$ as Abelian groups.

For any fixed $k \in \mathbb{Z}_{\geq 0}$ we now have the following isomorphisms of Abelian groups:

$$\bigoplus_{i=0}^{k} 2^{k-i} \cdot RM_k\big(m - ((i+1)r + 1), m\big) \cong \left\langle \widetilde{Z}(i)_{\langle K \rangle} \;\middle|\; i \in \{0, \ldots, k\},\ K \subseteq S,\ |K| \geq (i+1)r + 1 \right\rangle, \tag{A.13}$$

and

$$\bigoplus_{i=0}^{k} 2^{k-i} \cdot RM_k\big(m - (q + ir + 1), m\big) \cong \left\langle \widetilde{Z}(i)_{\langle K \rangle} \;\middle|\; i \in \{0, \ldots, k\},\ K \subseteq S,\ |K| \geq q + ir + 1 \right\rangle. \tag{A.14}$$

We can therefore rephrase Question A.1 in a coding-theoretic language:

Question A.4. Suppose that $U \in \mathrm{DTC}^{(k)}$ for $k \in \mathbb{Z}_{\geq 0}$ and consider $QRM_m(q, r)$. If $U \in \mathcal{N}^{(k)}$ then does it hold that

$$f_U \in \bigoplus_{i=0}^{k} 2^{k-i} \cdot RM_k\big(m - (q + ir + 1), m\big)? \tag{A.15}$$

In particular, does the following isomorphism hold:

$$\mathrm{DTC}^{(k)} \cap \mathcal{N}^{(k)} \cong \bigoplus_{i=0}^{k} 2^{k-i} \cdot RM_k\big(m - (q + ir + 1), m\big)\ ? \tag{A.16}$$

Note that the base case of this statement is already true, i.e., when $k = 0$, Question A.4 asks if

$$\mathcal{N}_Z \cong RM(m - q - 1, m), \tag{A.17}$$

where $\mathcal{N}_Z$ is the group of Pauli Z errors for the code and $RM(m - q - 1, m)$ is a classical binary RM code. This statement is true, and it can be shown that treated as vectors of $\mathbb{F}^{2^m}$ a Z logical must be dual to every X stabilizer. In other words, one shows that $\mathcal{N}_Z \cong RM(m - q - 1, m)$ by, in fact, proving that $\mathcal{N}_Z \cong RM(q, m)^{\perp}$, and using the duality relation of RM codes the desired characterization holds.

A potential proof of Question A.4 would likely follow the same line of thought: given a $Z(f) \in \mathcal{N}^{(k)}$ can one prove that $f \in R_k[\mathbb{Z}_2^m]$ is *dual* to every function g where

$$g \in \left(\bigoplus_{i=0}^{k} 2^{k-i} \cdot RM_k\big(m - (q + ir + 1), m\big) \right)^{\perp} ? \tag{A.18}$$

We have not defined a symmetric bilinear form on $R_k[\mathbb{Z}_2^m]$ here, though a natural one can be defined and dual spaces behave as one may expect, e.g., $(C^{\perp})^{\perp} = C$, even in the case of R_k-modules. A natural first step towards answering Question A.4 in the affirmative would be characterizing the space in Eq. (A.18) in terms of generalized RM codes, as opposed to the *dual* of generalized RM codes.

Appendix B: Building Codes

We now detail constructions of two more classical code families, each of which is a direct generalization of the Coxeter code family. This generalization will be based on the notion of a Tits building, or simply, a *building*.

As usual, let (W, S) be a Coxeter system with finite W. The main group-theoretic object needed to define Coxeter codes was the collection of all standard cosets $\{w\langle J\rangle\}$ of W. Informally speaking, this collection is known as the *Coxeter complex* corresponding to (W, S); Coxeter complexes are the simplest examples of buildings. Before we give the formal definition of buildings, we will provide some intuition and give two characterizations of standard cosets that lead to our generalizations.

First, recall the definition of the Cayley graph of a Coxeter system:

Definition 3.4.1. The *Cayley graph* of a Coxeter system (W, S) is a graph $G = (V, E)$ with vertices given by elements of the group $V := W$, and with edges given by

$$E := \left\{(w, v) \mid w^{-1}v \in S\right\}.$$

Fig. B.1 shows several Cayley graphs of both reducible (Cartesian product) and irreducible Coxeter systems.

The first characterization of standard cosets is the following: a standard coset of type J is a subset of vertices in G whose induced subgraph is isomorphic to the Cayley graph for the Coxeter system $(\langle J\rangle, J)$. Essentially, standard cosets are collections of group elements which, themselves, look like Coxeter subcomplexes within W. We refer to standard cosets in this view as "subapartments" of the Coxeter complex; the terminology will be explained later.

The second characterization is also quite simple, but we will need to make use of a natural edge coloring on G (which we have alluded to in Fig. B.1). To each generator in the set S we associate a unique color. An edge coloring $c\colon E \to S$ is given via the following: for a pair of vertices $w, v \in W$ connected by an edge $(w, v) \in E$, declare the color of the edge to be $c(w, v) := w^{-1}v \in S$. By abuse of terminology we will refer to elements of S as generators or colors, interchangeably.

Now, consider a set $J \subseteq S$ of colors and remove all edges with colors not in J. A standard coset of type J is then a connected component of this induced subgraph. In this view, standard cosets are called "residues" of the Coxeter complex. Residues are characterized by the fact that for each pair of elements $w_1, w_2 \in w\langle J\rangle$, the geodesics (paths of minimal length) from w_1 to w_2 contain only colors from J, and a geodesic from $w_1 \in w\langle J\rangle$ to any element $v \notin w\langle J\rangle$ must contain a color outside of J.

To motivate buildings, we note that the edge coloring on G is intimately related to the structure

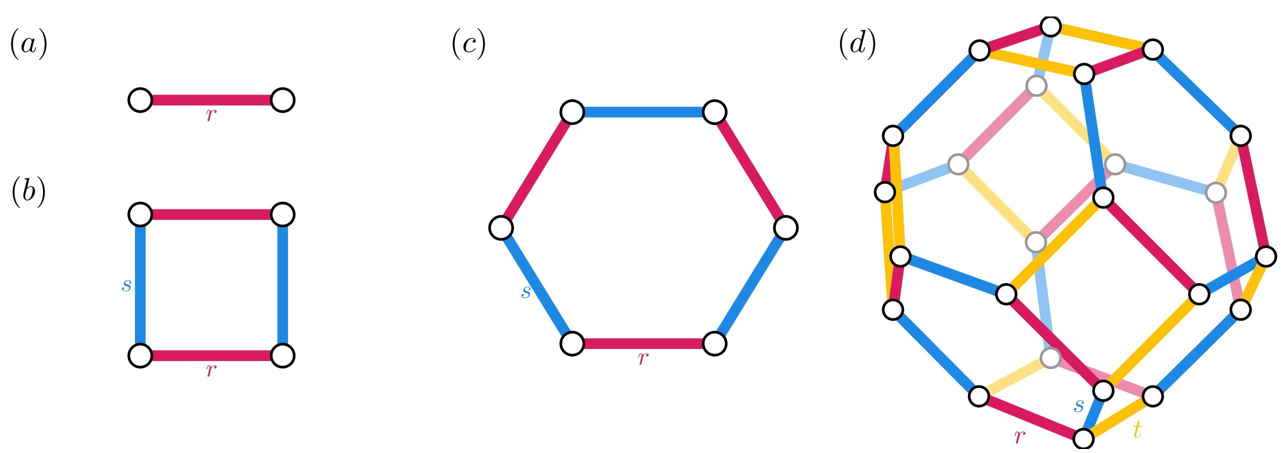


Figure B.1: Cayley graphs of some simple Coxeter systems: (a) A_1, generated by a single reflection. (b) $A_1 \times A_1$, generated by two commuting reflections. (c) A_2, the symmetric group on 3 letters. (d) A_3, the symmetric group on 4 letters. We have seen this earlier in Fig. 1.1.

of W (in many more ways than we can describe here). For example, recall that the length of an element $w \in W$ is the minimum number of elements from S needed to generate it. That is, $\ell(w) = \ell'$ if there is a decomposition $w = \sigma_1\sigma_2 \cdots \sigma_{\ell'}$ with $\sigma_i \in S$ for all $i \in [\ell']$, and *any* decomposition of w using elements of S contains at least ℓ' terms. Proposition 2.16 of [AB08] demonstrates that the set of elements from S appearing in such a minimum-length decomposition of w is unique. In terms of the Cayley graph, this implies that any geodesic connecting the vertex representing the identity element in G to the vertex representing w contains only colors from this set.

The edge-coloring of G can be extended in a way that is far more powerful: the *W-metric*, or Weyl metric, on W is a function $\delta\colon W \times W \to W$ defined via $\delta(w, v) := w^{-1}v$ for all $w, v \in W$. The "metric" terminology refers to the fact that $\delta(w, v)$ captures information about both geodesics and distances within the Cayley graph: In analogy to geodesics from identity to an element $w \in W$, for *any* pair of elements $w, v \in W$ the set of edge colors in a geodesic from w to v is an invariant—in particular, it is all generators appearing in a minimum-length decomposition of the Weyl distance $\delta(w, v)$. Further, the length of $\delta(w, v)$ corresponds to the distance between the two vertices: $\ell(\delta(w, v)) = \mathrm{dist}(w, v)$.

The following definition, which is formally very similar to the notion of an edge-colored graph, is one common starting point for buildings.

Definition B.1 (Chamber systems; Adapted from [AB08], Def 5.21)**.** A *chamber system* over an arbitrary finite set I is a non-empty set Δ, whose elements are called *chambers*, together with $|I|$ equivalence relations $\{\sim_i\}_{i \in I}$ on Δ. Two distinct chambers $w, v \in \Delta$ are called i-*adjacent* if $v \sim_i w$, and simply *adjacent* if they are i-adjacent for some $i \in I$. The equivalence classes with respect to $\sim_i$ are called i-*panels*, and a *panel* is an i-panel for some $i \in I$.

A *gallery of length* ℓ' *connecting* $g_0, g_{\ell'} \in \Delta$ is a sequence of consecutively adjacent chambers $g_0, g_1, \ldots, g_{\ell'}$. The *type* of the gallery is the sequence $\vec{\sigma} := (i_1, \ldots, i_{\ell'})$ where g_{j-1} and g_j are i_j-adjacent for $i_j \in I$.

One can visualize a chamber system Δ over I as an edge-colored graph with vertices given by the chambers and with i-colored edges given by i-adjacent chambers $w, v \in \Delta$. [1] Since $\sim_i$ is an equivalence relation, such a graph will contain many single-color cliques; these cliques are precisely the panels.

As the generators of a Coxeter system are involutive, the Cayley graph of (W, S) is a chamber system over the set of generators S; buildings are certain chamber systems over the generators of a Coxeter system that share many structural properties with Coxeter complexes. As usual, we suppose that (W, S) is a fixed Coxeter system.

Definition B.2 ([AB08], Prop. 5.23)**.** A pair (Δ, δ) is a *building of type* (W, S) if Δ is a chamber system over S, and $\delta \colon \Delta \times \Delta \to W$ is a map, called the *Weyl distance* function, which satisfies the following for all pairs $g, h \in \Delta$ and all sequences of generators $\vec{\sigma} := (\sigma_1, \sigma_2, \ldots, \sigma_{\ell'})$ for which $\ell(\sigma_1 \sigma_2 \cdots \sigma_{\ell'}) = \ell'$:

There exists a gallery of type $\vec{\sigma}$ connecting g and h if and only if $\delta(g, h) = \sigma_1 \sigma_2 \cdots \sigma_{\ell'}$.

The *rank* of (Δ, δ) is $|S|$. For simplicity, we will refer to Δ as a building.

We will not attempt to motivate the Weyl distance function, we will only note that W together with δ defined by $\delta(w, v) := w^{-1}v$ satisfies the requirements of a building. We also clarify that while we have not explicitly defined the equivalence relations $\sim_{s_i}$ needed in the definition of a chamber system, they are implicitly given by $g \sim_{s_i} h$ if and only if $\delta(g, h) = s_i$.

[1] Indeed, the approach taken in [Wei03] is to define chamber systems as certain edge-colored graphs.

It is perhaps surprising that a relatively short definition leads to such a bountiful area of mathematics, but indeed there are a plethora of textbooks dedicated to the study of buildings, [AB08, Wei03] being two popular choices. We will introduce only those concepts that directly pertain to the generalizations of Coxeter codes we construct. In particular, we will define the two extensions of standard cosets to the setting of buildings.

For the remainder, we suppose that Δ is a rank-m building of type (W, S), where $|W|$ and $|\Delta|$ are both finite. Such a building would typically be referred to as a *finite spherical building*, with "spherical" referring to the finiteness of the Coxeter group. Let $\mathbb{F}\Delta := \{f \colon \Delta \to \mathbb{F}\}$ denote the space of Boolean-valued functions on the chambers of Δ, and let $\operatorname{eval} f \in \mathbb{F}^{|\Delta|}$ denote the bit string of length $|\Delta|$ obtained by evaluating f on each of the chambers (the ordering can be chosen arbitrarily). Our generalizations of Coxeter codes will be subspaces of $\mathbb{F}^{|W|}$.

Definition B.3. A building is called *thick* (resp. *thin*) if every panel contains at least 3 (resp. exactly 2) chambers.

Note that because every generator of a Coxeter group is an involution, all Coxeter complexes are thin buildings. In Fig. B.2 we show a few simple examples of thick buildings. These figures will be a useful visual tool which we will refer to throughout.

Recall that our first characterization of standard cosets was as subsets of the Cayley graph of W that were isomorphic to Cayley graphs of standard subgroups. We will extend this definition to buildings via "subapartments".

Definition B.4. A *subbuilding* of Δ is a non-empty subset of chambers $\Delta_0 \subseteq \Delta$ for which (Δ_0, δ_0) is a building, itself, where δ_0 is the restriction of δ to $\Delta_0 \times \Delta_0$.

Definition B.5. An *apartment* of Δ is a thin subbuilding of Δ with rank equal to m, the rank of Δ. A *subapartment* is any subbuilding of an apartment, or, equvivalently, a thin subbuilding of Δ with rank possibly less than m.

Fact B.6 ([Wei03], Prop. 8.11)**.** A building (Δ, δ) of type (W, S) is thin if and only if $\Delta = W$ and $\delta(w, v) = w^{-1}v$ for all $w, v \in W$.[2]

Thus, apartments appear as copies of the Cayley graph of (W, S) within the graph of Δ, and subapartments appear as copies of standard subgroups of (W, S). While it is not immediately obvious that apartments must exist for every building, Theorem 5.73 of [AB08] proves that every building has apartments.

We now have our first generalization of Definition 1.2.1:

Definition B.7 (Subapartment codes)**.** Let Δ be a finite building of rank m. The *order-r subapartment code of type* Δ is defined as

$$\mathsf{A}_\Delta(r) \coloneqq \operatorname{Span}_{\mathbb{F}} \left\{ \operatorname{eval}(\mathbb{1}_{\mathcal{A}}) \;\middle|\; \mathcal{A} \text{ is a subapartment of } \Delta \text{ with } \operatorname{rank} \mathcal{A} = m - r \right\}. \tag{B.1}$$

Since the collection of subapartments with rank equal to 1 is exactly the set of edges in Δ, the code $\mathsf{A}_\Delta(m-1)$ is the single parity check code of length $|\Delta|$.

We now turn our attention to the second generalization.

Definition B.8 ([AB08], Def. 5.26)**.** Let $J \subseteq S$. Two chambers $g, h \in \Delta$ are called *J-equivalent* if $\delta(g, h) \in \langle J \rangle$. This is a valid equivalence relation on Δ, and the equivalence classes for a given J are called *J-residues*. The *rank* of a J-residue, $\mathcal{R} \subseteq \Delta$, is $\operatorname{rank} \mathcal{R} = |J|$. A *residue* is any J-residue with $J \subseteq S$; a panel is a residue with rank equal to 1.

[2] We really mean that Δ is *isometric* to the Coxeter complex of (W, S), in a certain technical sense.

As in the Coxeter group case, J-residues of Δ arise as connected components of the subgraph of Δ obtained by deleting edges with colors not in J. In particular, panels are the single-color cliques in Δ.

Definition B.9 (Residue codes)**.** Let Δ be a finite building of rank m. The *order-r residue code of type Δ* is defined as

$$\mathsf{B}_\Delta(r) \coloneqq \operatorname{Span}_{\mathbb{F}} \left\{ \operatorname{eval}(\mathbb{1}_{\mathcal{R}}) \;\middle|\; \mathcal{R} \text{ is a residue of } \Delta \text{ with } \operatorname{rank} \mathcal{R} = m - r \right\}. \tag{B.2}$$

As there is only a single residue of rank m, namely, the entirety of Δ, we have that $\mathsf{B}_\Delta(0)$ is the repetition code.

It is straightforward to verify that the subapartment and residue codes are valid generalizations of Coxeter codes:

Proposition B.10. *The definitions of residues and subapartments coincide in a Coxeter complex. In particular, for every (W, S) of rank m and $r \in \{-1, \dots, m\}$, we have $\mathsf{A}_W(r) = \mathsf{B}_W(r) = \mathsf{C}_W(r)$.*

Now, we note that the subapartment and residue code families already share some simple duality properties: Because $\mathsf{A}_\Delta(m-1)$ is the single parity-check code and $\mathsf{B}_\Delta(0)$ is the repetition code, we have $\mathsf{B}_\Delta(0)^\perp = \mathsf{A}_\Delta(m-1)$. What's more, the collections of rank-0 subapartments and residues coincide (corresponding to all of the chambers) and no rank-$(m+1)$ subapartments or residues exist. Thus, $\mathsf{A}_\Delta(m) = \mathsf{B}_\Delta(m) = \mathbb{F}^{|\Delta|}$, and $\mathsf{A}_\Delta(-1) = \mathsf{B}_\Delta(-1) = \left\{0^{|\Delta|}\right\}$, so we further have $\mathsf{A}_\Delta(-1)^\perp = \mathsf{B}_\Delta(m)$. In light of these dualities and Proposition B.10, one may naturally wonder the following:

Question B.11. Are the subapartment and residue codes dual to each other for every finite building? That is, do the codes satisfy $\mathsf{A}_\Delta(r) = \mathsf{B}_\Delta(m-r-1)^\perp$ for all finite rank-m buildings Δ and all possible orders r?

We do have evidence to believe Question B.11 is answered in the affirmative, aside from the fact it is true when Δ is thin. Numerically, it is easy to verify that the answer is yes in the case when Δ is a certain graph related to the Fano plane and when it is $\mathrm{Inc}(K_{3,3})$, the edge-vertex incidence graph of the complete bipartite graph with 3 left and right vertices each. See Fig. B.2 for pictures of these buildings.

Perhaps more indicative is the following duality relation:

Proposition B.12. *Let Δ be a finite building of rank m. For all $r \in \{0, \dots, m\}$, the subapartment and residue codes satisfy*

$$\mathsf{A}_\Delta(r) \subseteq \mathsf{B}_\Delta(m - r - 1)^\perp.$$

We will not prove this here, but the result is a fairly simple exercise once one grasps the basic properties of buildings. To prove Proposition B.12, one must simply show that every rank-$(m - r)$ subapartment and every rank-$(r+1)$ residue overlap on an even number of vertices. The intersection of two such subbuildings (supposing their intersection is non-empty) is necessarily a subapartment with strictly positive rank, which we showed explicitly for Coxeter systems in the proof of Lemma 2.6.5. Since subapartments are isomorphic to Coxeter complexes, Lemma 2.6.3 implies that the number of chambers in this intersection must be even.

Providing a positive answer to Question B.11 thus reduces to showing that the dimensions of the two codes are equal. In the case of Coxeter codes we did this by constructing a basis and by using the fact $\dim C + \dim C^\perp = n$ for all length n codes. While we have not explored this, there is a natural option to consider as a basis for the residue codes. There is a dual view to the chamber system definition of a building in terms of simplicial complexes. These simplicial complexes always admit a shelling order ([Sta96], Def. 2.1) which is automatically a basis of the space $\mathbb{F}\Delta$ in terms of indicator functions of residues with various ranks. This basis directly generalizes the extensions we used as a basis for a Coxeter code; perhaps an analogous version of Theorem 3.1.6 holds for the basis arising from a shelling. We leave this direction, as well as determining the validity of Question B.11, for future work.

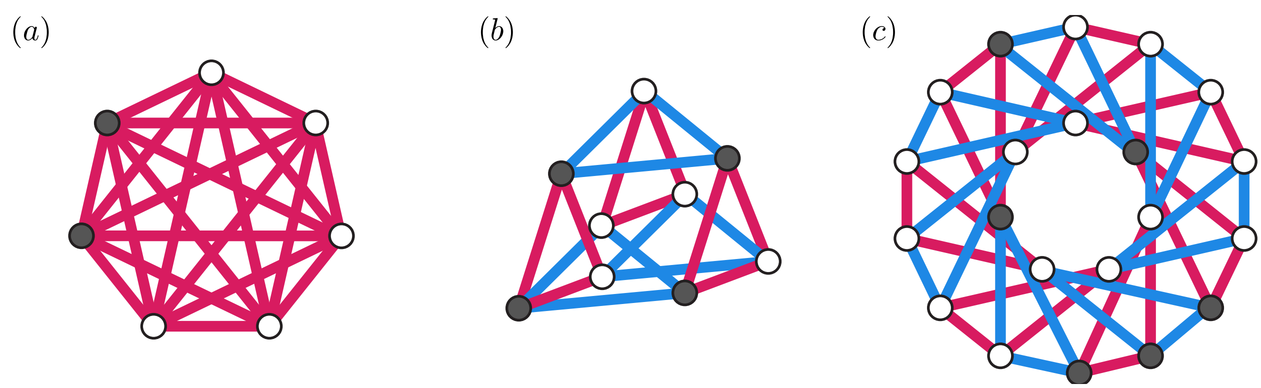


Figure B.2: Examples of thick finite spherical buildings. The subgraphs induced by shaded chambers denote an apartment in the building, and correspond to the respective Coxeter systems in Fig. B.1.
(a) A rank-1 building of type A_1. All buildings of this type are cliques.
(b) A rank-2 building of type $A_1 \times A_1$. The apartments in the building are all squares. This building corresponds to the edge-line incidence graph of the compete bipartite graph $K_{3,3}$. That is, chambers represent edges of $K_{3,3}$, and there is an edge in the building whenever two edges of $K_{3,3}$ are incident to the same vertex. Whether this connecting vertex is in the left or right vertex set determines the color of the edge in the building.
(c) A rank-2 building of type A_2. The apartments in the building are all hexagons. This building is related to the Fano plane, i.e., the finite projective plane $PG(2,2)$ in the following way: each chamber corresponds to a pair (p, L) where p is a point on the plane, L is a line on the plane, and p lies on L. Two chambers (p_1, L_1) and (p_2, L_2), are connected by a red (resp. blue) edge in the building whenever p_1 lies on L_2 (resp. p_2 lies on L_1).

Bibliography

[AABA+24] Rajeev Acharya, Laleh Aghababaie-Beni, Igor Aleiner, Trond I Andersen, Markus Ansmann, Frank Arute, Kunal Arya, Abraham Asfaw, Nikita Astrakhantsev, Juan Atalaya, et al. Quantum error correction below the surface code threshold. *arXiv preprint arXiv:2408.13687*, 2024.

[AB08] Peter Abramenko and Kenneth S. Brown. *Buildings: Theory and Applications*. Graduate Texts in Mathematics. Springer Science+Business Media, LLC, New York, NY, 2008.

[ABO97] Dorit Aharonov and Michael Ben-Or. Fault-tolerant quantum computation with constant error. In *Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing*, pages 176–188, 1997.

[ACLN21] Daniel Augot, Alain Couvreur, Julien Lavauzelle, and Alessandro Neri. Rank-metric codes over arbitrary galois extensions and rank analogues of reed–muller codes. *SIAM Journal on Applied Algebra and Geometry*, 5(2):165–199, 2021.

[ADP14] Jonas T. Anderson, Guillaume Duclos-Cianci, and David Poulin. Fault-tolerant conversion between the Steane and Reed-Muller quantum codes. *Phys. Rev. Lett.*, 113(8):080501, August 2014.

[AK98] E. F. Assmus, Jr. and J. D. Key. Polynomial codes and finite geometries. In *Handbook of Coding Theory*, volume II, pages 1269–1343. North-Holland, Amsterdam, 1998.

[AKK+05] Noga Alon, Tali Kaufman, Michael Krivelevich, Simon Litsyn, and Dana Ron. Testing Reed-Muller codes. *IEEE Transactions on Information Theory*, 51(11):4032–4039, 2005.

[ALM+98] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof verification and the hardness of approximation problems. *Journal of the ACM*, 45(3):501–555, May 1998.

[AS92] S. Arora and S. Safra. Probabilistic checking of proofs; a new characterization of NP. In *Proceedings., 33rd Annual Symposium on Foundations of Computer Science*, page 2–13, Pittsburgh, PA, USA, 1992. IEEE.

[AS23] Emmanuel Abbe and Colin Sandon. A proof that Reed-Muller codes achieve Shannon capacity on symmetric channels. In *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 177–193, 2023.

[ASSY23] Emmanuel Abbe, Ori Sberlo, Amir Shpilka, and Min Ye. Reed-Muller codes. *Foundations and Trends in Communications and Information Theory*, 20(1–2):1–156, 2023.

[BB05] Anders Björner and Francesco Brenti. *Combinatorics of Coxeter Groups*. Graduate texts in mathematics. Springer, New York, 2005.

[BCHK25] Alexander Barg, Nolan J. Coble, Dominik Hangleiter, and Christopher Kang. Geometric structure and transversal logic of quantum Reed–Muller codes. *IEEE Transactions on Information Theory*, pages 1–1, 2025.

[BEG+24] Dolev Bluvstein, Simon J Evered, Alexandra A Geim, Sophie H Li, Hengyun Zhou, Tom Manovitz, Sepehr Ebadi, Madelyn Cain, Marcin Kalinowski, Dominik Hangleiter, et al. Logical quantum processor based on reconfigurable atom arrays. *Nature*, 626(7997):58–65, 2024.

[Ben73] Edward A Bender. Central and local limit theorems applied to asymptotic enumeration. *Journal of Combinatorial Theory, Series A*, 15(1):91–111, 1973.

[Ber67] Samuil D Berman. On the theory of group codes. *Cybernetics*, 3(1):25–31, 1967.

[BH12] Sergey Bravyi and Jeongwan Haah. Magic-state distillation with low overhead. *Phys. Rev. A*, 86:052329, Nov 2012.

[BH13] Sergey Bravyi and Matthew B. Hastings. Homological product codes, 2013.

[BK05] Sergey Bravyi and Alexei Kitaev. Universal quantum computation with ideal Clifford gates and noisy ancillas. *Phys. Rev. A*, 71(2):022316, February 2005.

[BK13] Sergey Bravyi and Robert König. Classification of topologically protected gates for local stabilizer codes. *Phys. Rev. Lett.*, 110(17):170503, 2013.

[BKS+10] Arnab Bhattacharyya, Swastik Kopparty, Grant Schoenebeck, Madhu Sudan, and David Zuckerman. *Optimal Testing of Reed-Muller Codes*, pages 269–275. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[BKS21] Michael E Beverland, Aleksander Kubica, and Krysta M Svore. Cost of universality: A comparative study of the overhead of state distillation and code switching with color codes. *PRX Quantum*, 2(2):020341, 2021.

[BMD07] H. Bombin and M. A. Martin-Delgado. Topological computation without braiding. *Phys. Rev. Lett.*, 98:160502, Apr 2007.

[Bre94] Francesco Brenti. q-Eulerian polynomials arising from Coxeter groups. *European Journal of Combinatorics*, 15(5):417–441, 1994.

[BW10] Maheshanand Bhaintwal and Siri Krishan Wasan. Generalized Reed–Muller codes over $\mathbb{Z}_q$. *Designs, Codes and Cryptography*, 54(2):149–166, 2010.

[CAB12] Earl T Campbell, Hussain Anwar, and Dan E Browne. Magic-state distillation in all prime dimensions using quantum reed-muller codes. *Physical Review X*, 2(4):041021, 2012.

[Cam] Earl T. Campbell. The smallest interesting color code. Blog post https://earltcampbell.com/2016/09/26/the-smallest-interesting-colour-code/, accessed on 10/4/2024.

[CB25] Nolan J. Coble and Alexander Barg. Coxeter Codes: Extending the Reed–Muller Family. In *2025 IEEE International Symposium on Information Theory (ISIT)*, pages 1–6, 2025. arxiv:2502.14746.

[CC22] Nolan J. Coble and Matthew Coudron. Quasi-polynomial time approximation of output probabilities of geometrically-local, shallow quantum circuits. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 598–609, 2022.

[CCNN23] Nolan J. Coble, Matthew Coudron, Jon Nelson, and Seyed Sajjad Nezhadi. Local Hamiltonians with No Low-Energy Stabilizer States. *Leibniz Int. Proc. Inf.*, 266:14:1–14:21, 2023.

[CCNN24] Nolan J. Coble, Matthew Coudron, Jon Nelson, and Seyed Sajjad Nezhadi. Hamiltonians whose low-energy states require $\Omega(n)$ T gates, 2024.

[CGK17] Shawn X. Cui, Daniel Gottesman, and Anirudh Krishna. Diagonal gates in the Clifford hierarchy. *Physical Review A*, 95(1):012329, January 2017. arXiv:1608.06596 [quant-ph].

[CH17a] Earl T Campbell and Mark Howard. Unified framework for magic state distillation and multiqubit gate synthesis with reduced resource cost. *Physical Review A*, 95(2):022316, 2017.

[CH17b] Earl T Campbell and Mark Howard. Unifying gate synthesis and magic state distillation. *Phys. Rev. Lett.*, 118(6):060501, 2017.

[CMLM$^+$24] Eduardo Camps-Moreno, Hiram H. López, Gretchen L. Matthews, Diego Ruano, Rodrigo San–José, and Ivan Soprunov. Binary triorthogonal and css-t codes for quantum error correction. In *2024 60th Annual Allerton Conference on Communication, Control, and Computing*, pages 01–06, 2024.

[CRSS97] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum Error Correction and Orthogonal Geometry. *Physical Review Letters*, 78(3):405–408, Jan 1997.

[CRSS98] A.R. Calderbank, E.M. Rains, P.M. Shor, and N.J.A. Sloane. Quantum error correction via codes over GF(4). *IEEE Transactions on Information Theory*, 44(4):1369–1387, Jul 1998.

[CS96] A. R. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098–1105, August 1996.

[CTZ09] William Y. C. Chen, Robert L. Tang, and Alina F. Y. Zhao. Derangement polynomials and excedances of type B. *Electron. J. Combin.*, 16(2):Research Paper 15, 16, 2009.

[DLZ23] Irit Dinur, Siqi Liu, and Rachel Yun Zhang. New codes on high dimensional expanders. *arXiv preprint arXiv:2308.15563*, 2023.

[DSRABR$^+$24] MP Da Silva, C Ryan-Anderson, JM Bello-Rivas, A Chernoguzov, JM Dreiling, C Foltz, JP Gaebler, TM Gatterman, D Hayes, N Hewitt, et al. Demonstration of logical qubits and repeated error correction with better-than-physical error rates. *arXiv preprint arXiv:2404.02280*, 2024.

[Got96] Daniel Gottesman. Class of quantum error-correcting codes saturating the quantum Hamming bound. *Physical Review A*, 54(3):1862–1868, Sep 1996.

[Got24a] Hayato Goto. High-performance fault-tolerant quantum computing with many-hypercube codes. *Science Advances*, 10(36):eadp6388, 2024. arXiv:2403.16054.

[Got24b] Daniel Gottesman. Surviving as a Quantum Computer in a Classical World, 2024. book draft.

[HCD20] Hsien-Kuei Hwang, Hua-Huai Chern, and Guan-Huei Duh. An asymptotic distribution theory for Eulerian recurrences with applications. *Advances in Applied Mathematics*, 112:1–125, 2020.

[HH18] Jeongwan Haah and Matthew B Hastings. Codes and protocols for distilling T, controlled-S, and Toffoli gates. *Quantum*, 2:71, 2018.

[HLC21] Jingzhen Hu, Qingzhong Liang, and Robert Calderbank. Climbing the diagonal Clifford hierarchy. *arXiv preprint arXiv:2110.11923*, October 2021. arXiv:2110.11923 [quant-ph].

[HLC22a] Jingzhen Hu, Qingzhong Liang, and Robert Calderbank. Designing the quantum channels induced by diagonal gates. *Quantum*, 6:802, September 2022.

[HLC22b] Jingzhen Hu, Qingzhong Liang, and Robert Calderbank. Divisible codes for quantum computation, 2022.

[Hya16] Matthew Hyatt. Recurrences for Eulerian polynomials of type B and type D. *Annals of Combinatorics*, 20:869–881, 2016.

[JOKY18] Tomas Jochym-O'Connor, Aleksander Kubica, and Theodore J Yoder. Disjointness of stabilizer codes and limitations on fault-tolerant logical gates. *Physical Review X*, 8(2):021047, 2018.

[KB15] Aleksander Kubica and Michael E Beverland. Universal transversal gates with color codes: A simplified approach. *Physical Review A*, 91(3):032330, 2015.

[Kit97] A. Yu. Kitaev. Quantum computations: algorithms and error correction. *Russian Mathematical Surveys*, 52(6):1191–1249, 1997.

[KKM$^+$15] Shrinivas Kudekar, Santhosh Kumar, Marco Mondelli, Henry D. Pfister, Eren Sasoglu, and Rüdiger L. Urbanke. Reed–Muller codes achieve capacity on erasure channels. *IEEE Transactions on Information Theory*, 63:4298–4316, 2015.

[KLZ98] Emanuel Knill, Raymond Laflamme, and Wojciech H Zurek. Resilient quantum computation: error models and thresholds. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 454(1969):365–384, 1998.

[LLZ22] Anthony Leverrier, Vivien Londe, and Gilles Zémor. Towards local testability for quantum coding. *Quantum*, 6:661, 2022.

[LTZ15] Anthony Leverrier, Jean-Pierre Tillich, and Gilles Zemor. Quantum expander codes. In *2015 IEEE 56th Annual Symposium on Foundations of Computer Science*, page 810–824. IEEE, October 2015.

[LZ22] Anthony Leverrier and Gilles Zémor. Quantum Tanner codes. In *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 872–883. IEEE, 2022.

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland Pub. Co., Amsterdam; New York, N.Y., 1977.

[NJBG24] Priya J Nadkarni, Praveen Jayakumar, Arpit Behera, and Shayan Srinivasa Garani. Entanglement-assisted quantum Reed-Muller tensor product codes. *Quantum*, 8:1329, 2024.

[NK23] Lakshmi Prasad Natarajan and Prasad Krishnan. Berman codes: A generalization of Reed–Muller codes that achieve BEC capacity. *IEEE Transactions on Information Theory*, 69(11):6956–6980, 2023.

[OEI25] OEIS Foundation Inc. The On-Line Encyclopedia of Integer Sequences, 2025. Published electronically at `http://oeis.org`.

[Pet15] T Kyle Petersen. *Eulerian Numbers*. Springer, 2015.

[PK22] Pavel Panteleev and Gleb Kalachev. Asymptotically good quantum and locally testable classical LDPC codes. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, pages 375–388, 2022.

[PR13] Adam Paetznick and Ben W. Reichardt. Universal fault-tolerant quantum computation with only transversal gates and error correction. *Phys. Rev. Lett.*, 111(9):090505, August 2013.

[PY15] Fernando Pastawski and Beni Yoshida. Fault-tolerant logical gates in quantum error-correcting codes. *Physical Review A*, 91(1):012305, 2015.

[RABB$^+$24] C Ryan-Anderson, NC Brown, CH Baldwin, JM Dreiling, C Foltz, JP Gaebler, TM Gatterman, N Hewitt, C Holliman, CV Horst, et al. High-fidelity teleportation of a logical qubit using transversal gates and lattice surgery. *Science*, 385(6715):1327–1331, 2024.

[RAC$^+$24] Ben W. Reichardt, David Aasen, Rui Chao, Alex Chernoguzov, Wim van Dam, John P. Gaebler, Dan Gresh, Dominic Lucchetti, Michael Mills, Steven A. Moses, Brian Neyenhuis, Adam Paetznick, Andres Paz, Peter E. Siegfried, Marcus P. da Silva, Krysta M. Svore, Zhenghan Wang, and Matt Zanner. Demonstration of quantum computation and error correction with a tesseract code, 2024. arXiv2409.04628.

[RCNP20] Narayanan Rengaswamy, Robert Calderbank, Michael Newman, and Henry D Pfister. On optimality of CSS codes for transversal T. *IEEE Journal on Selected Areas in Information Theory*, 1(2):499–514, 2020.

[RGS23] Atri Rudra, Venkatesan Guruswami, and Madhu Sudan. Essential coding theory, 2023.

[RP23] Galen Reeves and Henry D Pfister. Reed–Muller codes on BMS channels achieve vanishing bit-error probability for all rates below capacity. *IEEE Transactions on Information Theory*, 70(2):920–949, 2023.

[SK05] Pradeep Kiran Sarvepalli and Andreas Klappenecker. Nonbinary quantum Reed–Muller codes. In *Pro. IEEE Int. Sympos. Inform. Theory, 2005. ISIT 2005.*, pages 1023–1027, 2005.

[Sor91] A.B. Sorensen. Projective reed-muller codes. *IEEE Transactions on Information Theory*, 37(6):1567–1576, 1991.

[SPW24] Thomas R Scruby, Arthur Pesah, and Mark Webster. Quantum rainbow codes. *arXiv preprint arXiv:2408.13130*, 2024.

[Sta96] R.P. Stanley. *Combinatorics and Commutative Algebra*. Combinatorics and Commutative Algebra. Birkhäuser Boston, 1996.

[Ste99] A.M. Steane. Quantum Reed-Muller codes. *IEEE Transactions on Information Theory*, 45(5):1701–1703, 1999.

[Ter15] Barbara M. Terhal. Quantum error correction for quantum memories. *Rev. Mod. Phys.*, 87:307–346, Apr 2015.

[VB22] Christophe Vuillot and Nikolas P Breuckmann. Quantum pin codes. *IEEE Transactions on Information Theory*, 68(9):5955–5974, 2022.

[VK22a] Michael Vasmer and Aleksander Kubica. Morphing quantum codes. *PRX Quantum*, 3(3):030319, 2022.

[VK22b] Michael Vasmer and Aleksander Kubica. Morphing quantum codes. *PRX Quantum*, 3(3), August 2022.

[Wag12] Stephan Wagner. Asymptotics of generalised trinomial coefficients. *arXiv preprint arXiv:1205.5402*, 2012.

[WBB22] Mark A. Webster, Benjamin J. Brown, and Stephen D. Bartlett. The XP stabiliser formalism: a generalisation of the Pauli stabiliser formalism with arbitrary phases. *Quantum*, 6:815, Sept. 2022.

[Wei03] Richard M. Weiss. *The Structure of Spherical Buildings*. Princeton University Press, 2003.

[YA20] Min Ye and Emmanuel Abbe. Recursive projection-aggregation decoding of Reed-Muller codes. *IEEE Transactions on Information Theory*, 66(8):4948–4965, 2020.

[YHH+23] Yangsen Ye, Tan He, He-Liang Huang, Zuolin Wei, Yiming Zhang, Youwei Zhao, Dachao Wu, Qingling Zhu, Huijie Guan, Sirui Cao, Fusheng Chen, Tung-Hsun Chung, Hui Deng, Daojin Fan, Ming Gong, Cheng Guo, Shaojun Guo, Lianchen Han, Na Li, Shaowei Li, Yuan Li, Futian Liang, Jin Lin, Haoran Qian, Hao Rong, Hong Su, Shiyu Wang, Yulin Wu, Yu Xu, Chong Ying, Jiale Yu, Chen Zha, Kaili Zhang, Yong-Heng Huo, Chao-Yang Lu, Cheng-Zhi Peng, Xiaobo Zhu, and Jian-Wei Pan. Logical magic state preparation with fidelity beyond the distillation threshold on a superconducting quantum processor. *Phys. Rev. Lett.*, 131(21):210603, November 2023.

[YTC16] Theodore J Yoder, Ryuji Takagi, and Isaac L Chuang. Universal fault-tolerant gates on concatenated stabilizer codes. *Physical Review X*, 6(3):031039, 2016.

[ZCC11] Bei Zeng, Andrew Cross, and Isaac L. Chuang. Transversality versus universality for additive quantum codes. *IEEE Transactions on Information Theory*, 57(9):6272–6284, 2011.