# The Rate and Structure of Square Codes

by

Shiri Sivan

Advisor: Prof. Irit Dinur

Thesis for the degree

Master of Science

מכון ויצמן למדע

WEIZMANN INSTITUTE OF SCIENCE

Submitted to the Scientific Council of the Weizmann Institute of Science

Rehovot, Israel

January 2024

# Abstract

Dinur et al. [2] solved the long-standing open problem concerning the existence of locally testable codes with constant rate, distance, and locality, by constructing the so-called *Square Codes*, which we further study in this thesis. Their paper provides a lower bound for the rate of square codes using a generic technique, namely, the bound is obtained by counting the number of constraints in the parity check matrix of the code. Although this method yields tight bounds for the rate of expander codes, that does not seem to be the case for square codes. In fact, we show that if most expander codes *meet* the generic rate lower-bound (as is often observed in practice), then most square codes have rate well *above* the generic bound.

In this thesis we study the rate and structure of square codes. We find better rate lower bounds that depend on algebraic properties of the code. We also show that under certain assumptions square codes can be constructed as a convolution of two expander codes, and construct a basis for the square code by applying the convolution operator on the bases of two expander codes.

# Acknowledgements

I want to thank my advisor, Irit Dinur, for introducing me to coding theory and high dimensional expanders. I am grateful for many inspiring interactions as well as the complete freedom she provided for me to pursue my own interests, all while academically supporting my path.

I would also like to thank Oded Goldreich who served as both a mentor and academic advisor. Some of his guidance was practical; for instance, when I encountered challenges in proving a result, Oded suggested a more achievable goal, leading to my first publication. Yet, beyond the practical advice, Oded profoundly influenced me by instilling the confidence to follow my own path.

I am deeply thankful to my family for relocating to Israel in support of my studies and for accommodating the unconventional schedule that research often demands. As my 3-year-old daughter put it– she will one day do a lot of ”matica” (math) too.

Finally, I want to express my gratitude to all those who contributed to this project. Guy Weissenberg programmed and ran experiments to assess the rate of square codes. The outcomes not only offered a significant clue in the right direction but also served as motivation to delve deeper into understanding and explaining these results. Irit Dinur greatly improved and simplified the proof of Lemma 5.5. Oded Goldreich edited and reviewed multiple drafts.

# Contents

# Chapter 1

# Introduction

We study the rate and structure of "Square Codes" presented in "*Locally Testable Codes with constant rate distance, and locality*" by Dinur et al. (see [2]). These codes constructively resolve a long standing question regarding the existence of LTCs with constant rate, distance, and locality. "Square Codes" arise from *expander codes*, which are a family of error correcting codes constructed from a *fixed* **base code** $c_0 \subseteq \mathbb{F}_2^d$ ($d$ is constant) and an **infinite** family of $d$-regular expander graphs $G_n = (V_n, E_n)$ $(n \to \infty)$, such that the code corresponding to $G_n$ consists of functions on $E_n$ that, for every vertex in $V_n$, have a "local view" in $c_0$. That is

$$C_n = \{f : E_n \to \mathbb{F}_2 \big| \, \forall v \in V_n, f|_{edges(v)} \in c_0\} \tag{1.1}$$

Square codes are similar, only that there are now two base codes $c_A$ and $c_B$, and instead of a graph, the underlying combinatorial object is a 2-dimensional complex, which along with vertices and edges, also contains squares; two-dimensional faces that contain four edges and vertices. The complex has two disjoint sets of edges $E_A \sqcup E_B$, and each square contains exactly two edges from each set, appearing in alternating order. Each edge in $E_A$ touches $|B|$ squares while $E_B$ edges touch $|A|$ squares. Let us present a slightly more formal definition of this complex.

**Left-Right Cayley Complex**. Let $G$ be a finite group with two symmetric[1] sets of generators $A, B \subset G$. The left-right Cayley complex $X = Cay^2(A, G, B)$ is defined as follows.

- The vertices are $X(0) = G$.

[1] A symmetric set of generators $A$, is a set that satisfies the condition $a \in A \iff a^{-1} \in A$, for all $a \in A$.

- The edges are $X(1) = X^A(1) \sqcup X^B(1)$ where $A$-edges are obtained by left multiplication, and $B$-edges by right multiplication. That is,

$$X^A(1) = \{\{g, ag\} | g \in G, a \in A\}, \;\; X^B(1) = \{\{g, gb\} | g \in G, b \in B\}$$

- The squares are

$$X(2) = \{(g, ag, agb, gb, g) | g \in G, a \in A, b \in B\}$$

**The square code**. Fix a left-right Cayley complex $X = Cay^2(A, G, B)$ and base codes $c_A \subseteq \mathbb{F}_2^A$ and $c_B \subseteq \mathbb{F}_2^B$. The codewords are functions on the **squares** of the complex that satisfy edge constraints. That is,

$$C = \{f : X(2) \to \mathbb{F}_2 \big| \; \forall e_1 \in E_A, e_2 \in E_B, f|_{squares(e_1)} \in c_B, f|_{squares(e_2)} \in c_A\} \tag{1.2}$$

Note that $(X^A(1), X(0))$ is the left multiplication Cayley graph $Cay(G, A)$ and $(X^B(1), X(0))$ is the right multiplication Cayley graph $Cay(G, B)$. Throughout this thesis we will use the two induced expander codes laying on the edges of these graphs:

$$C_A = \{f : X^A(1) \to \mathbb{F}_2 \big| \; \forall g \in G, f|_{X^A(g)} \in c_A\}$$

and

$$C_B = \{f : X^B(1) \to \mathbb{F}_2 \big| \; \forall g \in G, f|_{X^B(g)} \in c_B\}$$

where $X^A(g)$ (or $X^B(g)$) denotes the set of $A$-edges (or $B$-edges) touching a vertex $g \in G$.

In this thesis we study the rate and structure of square codes. Towards this end, it is instructive to consider the tensor code of the expander codes $C_A$ and $C_B$. The tensor code $C_A \otimes C_B$ is fully understood in terms of $C_A$ and $C_B$; we know that $Rate(C_A \otimes C_B) = Rate(C_A) \cdot Rate(C_B)$. Moreover, given bases $\mathcal{B}(C_A)$ and $\mathcal{B}(C_B)$, a basis for $C_A \otimes C_B$ is $\mathcal{B}(C_A) \otimes \mathcal{B}(C_B) = \{v \otimes u : v \in \mathcal{B}(C_A), u \in \mathcal{B}(C_B)\}$.

We follow a similar path to construct square codes. Namely, we describe $C$ as the space spanned by $C_A * C_B$, where $*$ is a convolution operator. We find a basis for $C$, and calculate the exact rate of square codes under certain assumptions. Our operator is a convolution on *groups*, meaning that the summation domain is a subset $W \subseteq G$, determined by the operands, and the elements of $W$ *act* on the operands by "rotating" them on the graph. That is, for every $f_A \in C_A$, $f_B \in C_B$ we define the convolution by

$$f_A * f_B = \sum_{h \in W} f_A^h \cdot^{h^{-1}} f_B$$

where $f_A^h$ denotes the right action of $h$ on $f_A$, ${}^{h^{-1}}f_B$ denotes the left action of $h^{-1}$ on $f_B$, and $\cdot$ is the point-wise product. Unlike tensor codes, in order to obtain a full description of $C$ we must rely on one of two assumptions: Either both bases $\mathcal{B}(C_A)$ and $\mathcal{B}(C_B)$ are invariant[2] to the group action, or one of the bases is invariant and also has full orbits[3] (namely, the only group element acting trivially on basis elements, is the group's unit). Another difference between tensor codes and square codes, is that our exact rate expression depends not only on $Rate(C_A)$ and $Rate(C_B)$, but also on orbit sizes. This approach does not only lead us to a tight rate bound, but also to a better structural understanding of square codes. We now present our main results.

**Theorem 1.1.** *If $\mathcal{B}(C_B)$ is closed under the action of $G$ and every orbit in $\mathcal{B}(C_B)$ has length $|G|$, then*

$$Rate(C) = Rate(C_A)Rate(C_B)\ .$$

**Theorem 1.2.** *If $\mathcal{B}(C_A)$ and $\mathcal{B}(C_B)$ are closed under the action of $G$, then*

$$Rate(C) = Rate(C_A)Rate(C_B) \cdot \frac{|G|}{\bar{O}}\ ,$$

*where $\bar{O}$ is the average orbit length in $\mathcal{B}(C_A) \otimes \mathcal{B}(C_B)$.*

**Theorem 1.3.** *If $\mathcal{B}(C_B)$ is closed under the action of $G$, and one of the following holds:*

1. *$\mathcal{B}(C_A)$ is closed.*

2. *$\mathcal{B}(C_B)$ has full orbits.*

*then*

$$C = C_A * C_B.$$

We also provide weaker lower bounds for $Rate(C)$, under weaker assumptions (see Theorems 4.1 and 4.2). However, we conjecture that *every* square code has rate at least $Rate(C_A) \cdot Rate(C_B)$ (see Conjecture 6.4).

[2] A set $S$ is invariant to the group action if it contains all the "rotations" of its elements, i.e., applying the group action on any element of $S$, yields an element of $S$.

[3] The orbit of a codeword is the set of words obtained by applying the group action on the codeword.

## 1.1 A comparison to previously known bounds

Under certain assumptions we have

$$Rate(C) = Rate(C_A \otimes C_B) = Rate(C_A) \cdot Rate(C_B) \tag{1.3}$$

It is a well known fact (see e.g. [4]) that any expander code $C$ on $Cay(G, S)$ with base code $c \subseteq \{0,1\}^{|S|}$ satisfies

$$Rate(C) \geq 2Rate(c) - 1$$

Plugging this into Equation (1.3) yields a lower bound in terms of the base code rates $\rho_A = Rate(c_A)$ and $\rho_B = Rate(c_B)$:

$$Rate(C) \geq (2\rho_A - 1) \cdot (2\rho_B - 1)$$

We compare this bound with the two bounds provided by [2].

- Lemma 4.2 in [2] gives the bound

$$Rate(C) \geq 2(\rho_A + \rho_B) - 3$$

- Lemma 4.3 in [2] provides a bound that depends on the size of a minimal vertex cover of $(X(1), X(0))$ (the graph obtained by the first 2 levels of the complex[4]). At best, this graph is bipartite and then Lemma 4.3 assures that

$$Rate(C) \geq 2\rho_A\rho_B - 1$$

As demonstrated in the Examples section, there are codes that meet our bound, so there cannot be a general lower-bound above $Rate(C_A)Rate(C_B)$.

## 1.2 Organization

In Chapter 2 we present definitions as well as some basic auxiliary lemmas. Chapter 3 establishes an isomorphism between $C$ and a subspace of the tensor code $C_A \otimes C_B$ (see Theorem 3.3). We study the rate and structure of $C$ through this isomorphic space. The main results of this thesis are presented in Chapters 4 to 7. Chapter 4 provides lower bounds for the rate of $C$

[4] Also referred to as the 1-skeleton of $X$.

(see Theorems 4.1 and 4.2). In Chapter 5 we prove Theorems 1.1 and 1.2, thereby determining the precise rate of square codes under the mentioned assumptions. The assumptions in Chapter 4 are weaker than those in Chapter 5, and unsurprisingly yield weaker results. In Chapter 6 we provide a sufficient condition assuring the existence of a closed basis with full orbits. We then conjecture that most expander codes have such a basis (see Conjecture 6.3), and that the lower bound $Rate(C) \geq Rate(C_A) \cdot Rate(C_B)$ always holds (see Conjecture 6.4). In Chapter 7 we show that the square code is the convolution of expander codes, that is, we prove Theorem 1.3. Beyond this conceptual contribution, we also show how to construct a basis for square codes, given bases for the expander codes. Chapter 8 contains two examples of square codes with $Rate(C) = Rate(C_A)Rate(C_B)$ (which is the rate provided by Theorem 1.1 and our conjectured "worst case" scenario). Finally, the appendix contains an alternative proof for Theorem 4.1 (Section 9.1) as well as a brief description of another project completed during my master's studies (Section 9.2).

# Chapter 2

# Preliminaries

## 2.1 The complexes

The following definitions are taken from [2].

**Definition 2.1.** (Left-Right Cayley Complex) Let $G$ be a group with two symmetric sets of generators $A, B$, namely, each is closed under taking inverses. We assume that the identity element of $G$ is neither in $A$ nor in $B$. Define the *Left-Right Cayley Complex* $X = Cay^2(A, G, B)$ as follows

- The vertices are $X(0) = G$.
- The edges are $X(1) = X^A(1) \sqcup X^B(1)$ where

  $$X^A(1) = \{[g, a] | g \in G, a \in A\}, \quad X^B(1) = \{[g, b] | g \in G, b \in B\}$$

  and $[g, a] = \{g, ag\}$ for every $a \in A, g \in G$ (and similarly $[g, b] = \{g, gb\}$ for $b \in B, g \in G$)
- The squares are the equivalence classes of $A \times G \times B$, where two triples are equivalent if they form the same 4-cycle; that is, for any $g \in G$ the square $(a, g, b)$ is obtained by the left-right and right-left paths to the vertex $agb$ (i.e. the paths $[g, a], [ag, b]$ and $[g, b], [gb, a]$).

  Formally, $X(2) = A \times G \times B / \sim$ where $\sim$ denotes the relation

  $$(a, g, b) \sim (a^{-1}, ag, b) \sim (a^{-1}, agb, b^{-1}) \sim (a, gb, b^{-1})$$

for every $a \in A, b \in B, g \in G$. We denote the equivalence class of $(a, g, b)$ obtained by this relation by $[a, g, b]$, so

$$[a, g, b] = \{(a, g, b), (a^{-1}, ag, b), (a^{-1}, agb, b^{-1}), (a, gb, b^{-1})\}.$$

We note that $(X(0), X^A(1)) = Cay(G, A)$ and $(X(0), X^B(1)) = Cay(G, B)$.

**Definition 2.2.** (TNC) A left-right Cayley complex satisfies the total no-conjugacy condition if

$$\forall a \in A, b \in B, g \in G, \quad g^{-1}ag \neq b \tag{TNC}$$

Assuming (TNC) the complex is regular. Specifically, each vertex has edge degree[1] $|A| + |B|$ and square degree $|A| \cdot |B|$. Every $A$ edge has square degree $|B|$, and every $B$ edge has square degree $|A|$. Finally, every square contains 4 vertices. We conclude that

$$|X(1)| = \frac{|A| + |B|}{2} \cdot |G| \text{ and } |X(2)| = \frac{|A||B|}{4} \cdot |G|.$$

The next definition will be used in section 7.

**Definition 2.3.** (Graph product) The product of two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ is a square complex $X = G_1 \times G_2$ defined as follows.

- The vertices are $X(0) = V_1 \times V_2$
- Two vertices $(u, v)$ and $(u', v)$ are connected if and only if $\{u, u'\} \in E_1$. Similarly, $(u, v)$ and $(u, v')$ are connected if and only if $\{v, v'\} \in E_2$. Formally, the edges are $X(1) = E_1 \times V_2 \sqcup V_1 \times E_2$, where an edge $(\{u, u'\}, v) \in E_1 \times V_2$ connects $(u, v)$ with $(u', v)$, and and edge $(u, \{v, v'\}) \in V_1 \times E_2$ connects $(u, v)$ with $(u.v')$.
- The squares $X(2)$ are identified with $E_1 \times E_2$, so that the square corresponding to the pair of edges $e_1 = \{u, u'\} \in E_1$ and $e_2 = \{v, v'\} \in E_2$ is the four-cycle

$$(u, v) \to (u, v') \to (u', v') \to (u', v) \to (u, v).$$

In our context we will only deal with products of Cayley graphs $Cay(G, A)$ and $Cay(G, B)$. We note that $Cay(G, A) \times Cay(G, B) = Cay^2(A \times \{1_G\}, G \times G, \{1_G\} \times B)$ so

[1] Throughout this document the degree of a set in the complex refers to the number of sets that contain it. For example, a square degree of a vertex is the number of squares that the vertex touches.

- The vertices are $X(0) = G \times G$.
- The edges are $X(1) = G \times G \times A \sqcup G \times G \times B$, where an edge $[g, g', a]$ connects $(g, g')$ with $(ag, g')$ and an edge $[g, g', b]$ connects $(g, g')$ with $(g, g'b)$.
- The squares are $X(2) = A \times G \times G \times B \cong X^A(1) \times X^B(1)$.

## 2.2 The codes

Let $G$ be a group, $A, B \subset G$ symmetric sets of generators, and let $c_A \subset \{0,1\}^{|A|}$ and $c_B \subset \{0,1\}^{|B|}$ be (base) codes. We denote $[g, A]$, the set of edges $\{[g, a] : a \in A\} \subseteq X^A(1)$ and describe the following codes:

- The expander code associated with $Cay(G, A)$.

$$C_A = \{f : X^A(1) \to \mathbb{F}_2 \big| \, \forall g \in G, f[g, A] \in c_A\}$$

  $C_B$ is defined similarly.

- The squares code (associated with $Cay^2(A, G, B)$).

$$C = \{f : X(2) \to \mathbb{F}_2 \big| \, \forall a \in A, b \in B, g \in G, f[a, g, \cdot] \in c_B, f[\cdot, g, b] \in c_A\} \qquad (2.1)$$

- The tensor product of $C_A$ and $C_B$ (associated with $Cay(G, A) \times Cay(G, B)$).

$$C_A \otimes C_B = \{f : A \times G \times G \times B \to \mathbb{F}_2 \big| \forall g, g' \in G, a \in A, b \in B, f(\cdot, \cdot, g, b) \in C_A, f(a, g', \cdot, \cdot) \in C_B\} \qquad (2.2)$$

Equation 2.2 defines tensor codes in terms of $C_A$ and $C_B$ constraints. Equation 2.1 defines square codes in terms of edge constraints. It is important to note that in the context of cayley graphs, these codes can be defined in a more unified way, that is:

1. Through vertex constraints (see Lemma 2.4).
2. Through edges constraints. See equation 2.1 for square codes. If we set $X = Cay(G, A) \times Cay(G, B)$, the edge constraint definition of tensor codes is:

$$C_A \otimes C_B = \{f : X(2) \to \mathbb{F}_2 \big| \, \forall a \in A, b \in B, g, g' \in G, f[a, g', g, \cdot] \in c_B, f[\cdot, g', g, b] \in c_A\}$$

As one can observe by these unified definitions- tensor codes are actually square codes. We will mostly use the vertex view, so we prove that this type of definition is equivalent to the code definitions in equations 2.2 and 2.1.

**Lemma 2.4.** *The following definitions are equivalent to equations 2.2 and 2.1:*

1. *Set $X = Cay(G,A) \times Cay(G,B)$.*

$$C_A \otimes C_B = \{f : X(2) \to \mathbb{F}_2 \big| \, \forall g \in G \times G, \; f[\cdot, g, \cdot] \in c_A \otimes c_B\}$$

2. *Set $X = Cay^2(A,G,B)$*

$$C = \{f : X(2) \to \mathbb{F}_2 \big| \, \forall g \in X(0), f[\cdot, g, \cdot] \in c_A \otimes c_B\}$$

*Proof.* $f(\cdot,\cdot,g,b) \in C_A$ if and only if $\forall h \in G, \; f(\cdot,h,g,b) \in c_A$. Similarly, $f(a,g',\cdot,\cdot) \in C_B$ if and only if $\forall h \in G, \; f(a,g',h,\cdot) \in c_B$. So the condition in equation 2.2 is equivalent to the condition

$$\forall g,g' \in G, a \in A, b \in B \; f(\cdot,g',g,b) \in c_A, f(a,g',g,\cdot) \in c_B$$

Which is the same as

$$\forall g \in G \times G, \; f[\cdot, g, \cdot] \in c_A \otimes c_B$$

The proof of the second statement is similar. □

*Conclusion:* $C_A \otimes C_B$ is the *square code* associated with the left-right Cayley complex $Cay(G,A) \times Cay(G,B) = Cay^2(A \times \{1_G\}, G \times G, \{1_G\} \times B)$.

## 2.3 Group Theory definitions

**Definition 2.5.** (Group action on a code)

- For every $f_A \in C_A$, $g \in G$, we define the *right* action of $g$ on $f_A$ by

$$f_A^g[h,a] := f_A[hg^{-1},a]$$

for all $[h,a] \in X^A(1)$.

- For every $f_B \in C_B$, $g \in G$, the *left* action of $g$ on $f_B$ is defined by

  $$^g f_B[h,b] = f_B[g^{-1}h,b]$$

  for all $[h,b] \in X^B(1)$.

- The action of $G$ on $C_A \otimes C_B$ is induced by the actions on $C_A$ and $C_B$, specifically, for every $f \in C_A \otimes C_B$, $g \in G$, $g$ acts on $f$ by

  $$f^g[a,h,h',b] = f[a,hg^{-1},gh',b]$$

  for all $a \in A, b \in B$ and $h,h' \in G$. In particular, if $f = f_A \otimes f_B$ we get

  $$f^g = f_A^g \otimes^{g^{-1}} f_B \tag{2.3}$$

**Lemma 2.6.** *The actions in Definition 2.5 are well defined.*

*Proof.* In order to show that the actions on $C \in \{C_A, C_B, C_A \otimes C_B\}$ are well defined we need to show that for every $f \in C$:

1. $f^g \in C$ for all $g \in G$.

2. $f^{1_G} = f$.

3. $(f^g)^h = f^{gh}$ for all $g,h \in G$.

We start with the action of $G$ on $C_A$.

1. First we show that $f^g \in C_A$ for all $g \in G, f \in C_A$. $f^g$ is well defined because neighbors agree:

   $$f^g[v,a] = f[vg^{-1},a] = f[avg^{-1},a^{-1}] = f^g[av,a^{-1}], \;\; \forall v \in G, a \in A$$

   $f^g \in C_A$ because the vertex views are in $c_A$:

   $$f^g[v,\cdot] = f[vg^{-1},\cdot] \in c_A, \;\; \forall v \in G$$

2. $f^{1_G} = f$ for every $f \in C_A$.

3. $(f^g)^h = f^{gh}$ for all $g,h \in G, f \in C_A$:

   $$(f^g)^h[v,\cdot] = f^g[vh^{-1},\cdot] = f[vh^{-1}g^{-1},\cdot] = f[v(gh)^{-1},\cdot] = f^{gh}[v,\cdot]$$

We proceed with the action of $G$ on $C_B$.

1. ${}^g f \in C_B$ for all $g \in G$. It is easy to verify that neighbors agree and that the local view ${}^g f[v, \cdot]$ is in $c_B$ for every $f \in C_B$, $g, v \in G$.

2. ${}^{1_G} f = f$ for every $f \in C_B$.

3. ${}^h({}^g f) =^{hg} f$ for all $g, h \in G$, $f \in C_B$:

$${}^h({}^g f)[v, \cdot] =^g f[h^{-1}v, \cdot] = f[g^{-1}h^{-1}v, \cdot] = f[(hg)^{-1}v, \cdot] =^{hg} f[v, \cdot]$$

We conclude that the actions on $C_A$ and $C_B$ are well defined. It follows that the action on $C_A \otimes C_B$ is well defined too. □

The following definitions are standard, see e.g. lecture notes by Hugh Osborn.

If a group $G$ acts on a set $X$, then the following relation is an equivalence relation:

$$x \sim x' \iff \exists g \in G : x^g = x'$$

**Definition 2.7.** (orbit) A congruence class of $x \in X$ under the relation described above is called the *orbit* of $x$ and is denoted by $O(x)$:

$$O(x) = \{x^g \bigm| g \in G\}$$

The set of orbits is denoted by $X/G$.

**Corollary 2.8.** *$X$ is the disjoint union of its orbits, so if $X/G = \{O(x_1), ..., O(x_r)\}$, then*

$$|X| = \sum_{i \in [r]} |O(x_i)|$$

**Definition 2.9.** (Stabilizer) Say a group $G$ acts on a set $X$. Then for every $x \in X$, the stabilizer $G_x$ is a subgroup of $G$ that contains all the elements that fix $x$, that is

$$G_x = \{g \in G \mid x^g = x\}$$

Every $x' \in O(x)$ is called a *representative of the orbit.* The set $[g]_x \subseteq G_x \backslash G$ is a set of size $|G_x|$ that contains all $h \in G$ that satisfy $x^h = x^g$. There is a bijection between $O(x)$ and $G_x \backslash G$ defined by $x^g \mapsto [g]_x$ for all $x^g \in O(x)$. That is, if $W \subseteq G$ is a set of representatives of $G_x \backslash G$, then $|W| = |O(x)|$ and $O(x) = \{x^w : w \in W\}$.

**Lemma 2.10.** *Let $H \leq G$ be a subgroup, and $W \subseteq G$ be a set of representatives of $H \backslash G$. Then for any $g \in G$, $Wg$ is a set of representatives of $H \backslash G$.*

*Proof.* For any $g \in G$,

$$Hwg = Hw'g \iff Hw = Hw'$$

so $[wg] = [w'g] \iff [w] = [w']$. We conclude that $Wg$ is a set of representatives of $H \backslash G$ if and only if $W$ is such a set. □

**Lemma 2.11.** *(The stabilizers of an orbit are conjugates)*

*For every $f \in C_A \otimes C_B$, $g \in G$,*

$$G_{f^g} = g^{-1} G_f g$$

*Proof.* We prove this statement by mutual inclusion.

- $g^{-1} G_f g \subseteq G_{f^g}$. For every $h \in G_f$,

  $$(f^g)^{g^{-1}hg} = f^{hg} = f^g$$

  thus $g^{-1}hg \in G_{f^g}$

- $G_{f^g} \subseteq g^{-1} G_f g$. For every $h \in G_{f^g}$,

  $$f^{ghg^{-1}} = (f^g)^{hg^{-1}} = (f^g)^{g^{-1}} = f$$

  $$\implies ghg^{-1} \in G_f \implies h \in g^{-1} G_f g$$

□

**Lemma 2.12.** *If $W \subseteq G$ is a set of representatives of $G_f \backslash G$ for some $f \in C_A \otimes C_B$, then for every $g \in G$, $g^{-1}Wg$ is a set of representatives of $G_{f^g} \backslash G$.*

*Proof.* Lemma 2.11 implies that for every $g \in G$, $G_f = g G_{f^g} g^{-1}$. Therefore, For every $w_1, w_2 \in W$,

$$G_f w_1 = G_f w_2 \iff g G_{f^g} g^{-1} w_1 = g G_{f^g} g^{-1} w_2$$

Multiplying the second expression on the right by $g$ and on the left by $g^{-1}$ yields

$$G_f w_1 = G_f w_2 \iff G_{f^g} g^{-1} w_1 g = G_{f^g} g^{-1} w_2 g$$

□

**Definition 2.13.** A closed basis for a code $C$, is a basis $\mathcal{B}(C)$ that satisfies

$$\mathcal{B}(C)^G = \mathcal{B}(C)$$

where

$$\mathcal{B}(C)^G := \{f^g \mid f \in \mathcal{B}(C), g \in G\}$$

# Chapter 3

# An isomorphic space

Denote by $C_A$ and $C_B$ the expander codes on $Cay(G, A)$ and $Cay(G, B)$ with corresponding base codes $c_A$ and $c_B$. Denote by $C$ the square code on $Cay^2(A, G, B)$ with base codes $c_A$ and $c_B$. Instead of studying $C$ directly, we study an isomorphic space. In this section we define this space and establish the isomorphism. More specifically, we present an embedding $\phi : C \to C_A \otimes C_B$ and conclude that $C \cong \phi C$ (see Lemma 3.4). Then we define a function $\mu : C_A \otimes C_B \to \phi C$ and prove that it is onto (see Lemma 3.5). Finally, we conclude that $C \cong \mu(C_A \otimes C_B)$ (see Theorem 3.3).

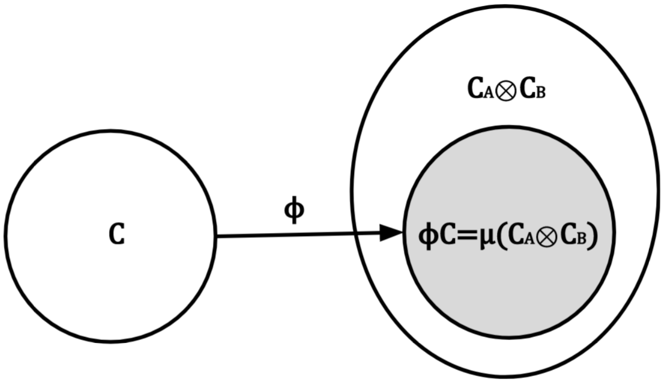

Figure 3.1: $\phi$ is an embedding of $C$ in the tensor code.
The equation $\phi C = Im(\mu)$ allows us to study $C$ as the image of $\mu$.

We start by defining $\phi$ and $\mu$ (see figure 3.1).

**Definition 3.1.** The function $\phi : C \to C_A \otimes C_B$ is defined by

$$\phi f[a, g_1, g_2, b] = f[a, g_1 g_2, b]$$

For all $f \in C, a \in A, b \in B, g_1, g_2 \in G$.

**Definition 3.2.** The function $\mu : C_A \otimes C_B \to \phi C$ is defined by:

$$\mu(f) = \sum_{f' \in O(f)} f'$$

We also use the notation

$$\mu(f) = \sum_{[g] \in G_f \backslash G} f^g$$

In this subsection we prove the following theorem.

**Theorem 3.3.**

$$C \cong \mu(C_A \otimes C_B)$$

*Proof of Theorem 3.3 assuming Lemmas 3.4 and 3.5.* By Lemma 3.4, $C \cong \phi C$. By Lemma 3.5, $\phi C = \mu(C_A \otimes C_B)$. Putting these facts together yields the desired isomorphism. □

**Lemma 3.4** (C is embedded in the tensor code)**.** *The function $\phi$ is:*

1. *Well defined.*

2. *Into $C_A \otimes C_B$.*

3. *Linear.*

4. *Injective.*

*Proof.* The function $\phi$ is:

1. Well defined. Here we need to show that the definition does not depend on the representatives. Indeed, for all $a \in A$ the $a$-column of $\phi f[\cdot, g_1, g_2, \cdot]$ agrees with the $a^{-1}$-column of $\phi f[\cdot, ag_1, g_2, \cdot]$:

$$\phi f[a, g_1, g_2, \cdot] = f[a, g_1 g_2, \cdot] = f[a^{-1}, ag_1 g_2, \cdot] = \phi f[a^{-1}, ag_1, g_2, \cdot]$$

   Similarly, $\phi f[\cdot, g_1, g_2, b] = \phi f[\cdot, g_1, g_2 b, b^{-1}]$ for all $b \in B$.

2. Into $C_A \otimes C_B$ because $f[\cdot, g, \cdot] \in c_A \otimes c_B$ for all $f \in C$, $g \in G$.

3. Injective, since $\phi f \equiv 0$ implies $f \equiv 0$.

4. Linear. For every $f, f' \in C$, $g_1, g_2 \in G$,

$$\phi(f+f')[\cdot, g_1, g_2, \cdot] = (f+f')[\cdot, g_1 g_2, \cdot] = f[\cdot, g_1 g_2, \cdot] + f'[\cdot, g_1 g_2, \cdot] = \phi(f)[\cdot, g_1, g_2, \cdot] + \phi(f')[\cdot, g_1, g_2, \cdot]$$

□

We conclude that $C \cong \phi C$.

**Lemma 3.5.** *The function $\mu$ (Definition 3.2) is onto $\phi C$.*

Before proving this Theorem we prove the following auxiliary lemma.

**Lemma 3.6.** *$\mu$ is invariant with respect to the action of $G$, that is, for every $f \in C_A \otimes C_B$, $g \in G$,*

$$\mu(f^g) = \mu(f) = \mu(f)^g$$

*Proof of Lemma 3.6.* Denote $W \subseteq G$ a complete set of representatives of $G_f \backslash G$. By Lemma 2.12, $g^{-1}Wg$ is a complete set of representatives of $G_{f^g} \backslash G$, therefore,

$$\mu(f^g) = \sum_{h \in W} (f^g)^{g^{-1}hg} = \sum_{h \in W} f^{hg} \tag{3.1}$$

- We show that $\mu(f^g) = \mu(f)$. By Lemma 2.10, $Wg$ is a complete set of representatives of $G_f \backslash G$, so

  $$\sum_{h \in W} f^{hg} = \sum_{h \in Wg} f^h = \mu(f)$$

  Plugging this into equation 3.1 we conclude that $\mu(f^g) = \mu(f)$.

- We show that $\mu(f^g) = \mu(f)^g$. Due to linearity of the group action,

  $$\sum_{h \in W} f^{hg} = (\sum_{h \in W} f^h)^g = \mu(f)^g$$

  Plugging this into equation 3.1 yields $\mu(f^g) = \mu(f)^g$.

□

*Proof of Lemma 3.5.* First we show that $\mu$ is *into* $\phi C$. That is, every $f_\otimes \in C_A \otimes C_B$ has a word $f \in C$ s.t. $\mu(f_\otimes) = \phi f$. Specifically, the word $f$ defined by

$$\forall g \in G, a \in A, b \in B, \quad f[a, g, b] := \mu(f_\otimes)[a, 1_G, g, b]$$

is in $C$, and $\mu(f_\otimes) = \phi(f)$

- The definition of $f$ does not depend on the representatives. That is, for every $a \in A$, $f[a, g, \cdot] = f[a^{-1}, ag, \cdot]$ and for every $b \in B$, $f[\cdot, g, b] = f[\cdot, gb, b^{-1}]$. Indeed,

  $$f[a^{-1}, ag, \cdot] = \mu(f_{\otimes})[a^{-1}, 1_G, ag, \cdot] = \mu(f_{\otimes})^{a^{-1}}[a^{-1}, 1_G, ag, \cdot] =$$

  $$\mu(f_{\otimes})[a^{-1}, a, g, \cdot] = \mu(f_{\otimes})[a, 1_G, g, \cdot] = f[a, g, \cdot]$$

  where the 2nd transition is due to lemma 3.6, the 3rd transition is by the definition of the group action, and the 4th transition is true since $[a, a^{-1}] = [1_G, a]$ (by the notation of edges in $X^A(1)$). The equality $f[\cdot, g, b] = f[\cdot, gb, b^{-1}]$ is immediate:

  $$f[\cdot, gb, b^{-1}] = \mu(f_{\otimes})[\cdot, 1_G, gb, b^{-1}] = \mu(f_{\otimes})[\cdot, 1_G, g, b] = f[\cdot, g, b]$$

- $f \in C$. Let $W \subseteq G$ be a set of representatives of $G_{f_{\otimes}} \backslash G$, then

  $$f[\cdot, g, \cdot] = \mu(f_{\otimes})[\cdot, 1_G, g, \cdot] = \sum_{h \in W} f_{\otimes}^{h}[\cdot, 1_G, g, \cdot]$$

  $f$ is clearly a word in $C$; for every $g \in G$, its local view is a sum of words in $c_A \otimes c_B$ which is itself a word in $c_A \otimes c_B$. By the definition of square codes we conclude that indeed $f \in C$.

- Now we show that $\mu(f_{\otimes}) = \phi f$. For all $g, g' \in G$,

  $$\phi f[\cdot, g, g', \cdot] = f[\cdot, gg', \cdot] = \mu(f_{\otimes})[\cdot, 1_G, gg', \cdot] = \mu(f_{\otimes})^{g^{-1}}[\cdot, 1_G, gg', \cdot] = \mu(f_{\otimes})[\cdot, g, g', \cdot]$$

  Where the 2nd transition follows from the definition of $f$, the 3rd transition is due to Lemma 3.6, and the last transition is by the definition of the action of $G$ on $C_A \otimes C_B$.

We conclude that $\mu$ is **into** $\phi C$.

Now we show that $\mu$ is **onto** $\phi C$. We do this by showing that $\mu\big|_{\phi C} = Id$. Note that for every $\tilde{f} = \phi f \in \phi C$, $O(\tilde{f}) = \{\tilde{f}\}$ because $\phi C$ is invariant with respect to the action of $G$. That is, for all $g, g', h \in G$,

$$\tilde{f}^h[\cdot, g, g', \cdot] = \phi f[\cdot, gh^{-1}, hg', \cdot] = f[\cdot, gg', \cdot] = \phi f[\cdot, g, g', \cdot] = \tilde{f}[\cdot, g, g', \cdot]$$

We conclude that $\mu(\tilde{f}) = \tilde{f}$ for all $\tilde{f} \in \phi C$, and thus $\mu(\phi C) = \phi C$ and $\mu$ is onto.

□

We completed the proof of Theorem 3.3, establishing the isomorphism $C \cong \mu(C_A \otimes C_B)$. From now on we study the structure and rate of $C$ indirectly, through the study of $\mu(C_A \otimes C_B)$.

# Chapter 4

# Lower-bounding the rate of square codes

In this chapter we prove the following theorems.

**Theorem 4.1.** *Assume that $W_A \subseteq C_A$ and $W_B \subseteq C_B$ are independent sets that are closed under the action of $G$, and denote $\bar{O}$, the average size of an orbit in $W_A \otimes W_B/G$*[1]*. Then*

$$Rate(C) \geq \frac{|W_A|}{|X^A(1)|} \cdot \frac{|W_B|}{|X^B(1)|} \cdot \frac{|G|}{\bar{O}}$$

*If $W_A$ and $W_B$ are bases of their respective codes, then*

$$Rate(C) \geq Rate(C_A)Rate(C_B) \cdot \frac{|G|}{\bar{O}} \tag{4.1}$$

**Theorem 4.2.** *If $W_B$ is independent, closed under the action of $G$, and every orbit in $W_B$ has size $|G|$, then*

$$Rate(C) \geq Rate(C_A) \cdot \frac{|W_B|}{|X^B(1)|}$$

*If $W_B$ is a basis for $C_B$, then*

$$Rate(C) \geq Rate(C_A)Rate(C_B) \tag{4.2}$$

Note that Theorem 4.2 provides a substantial lower bound of $Rate(C_A) \cdot \frac{2}{|B|}$, even if $W_B$ comprises only a single orbit. In both theorems, assuming that $W_A$ and $W_B$ form bases for their respective codes, the rate of the square codes is at least the rate of the associated tensor code. We will see in Example 8.2 a family of codes where $\bar{O} = |G|$, leading to the conclusion that bound (4.2) is tight.

[1] Note that all orbits in $W_A \otimes W_B/G$ have size $|G|$ at most, so $\bar{O} \leq |G|$.

## 4.1 Making assumptions on both expander codes

Let us first assume that $W_A^G = W_A$ and $W_B^G = W_B$. This implies the closure of $W_A \otimes W_B$ under the action of $G$ (as defined by Equation (2.3)). Let $F = \{f_1, ..., f_\ell\} \subseteq W_A \otimes W_B$ be a set of *representatives* of the orbits $W_A \otimes W_B/G$. That is, every $O(f) \in W_A \otimes W_B/G$ has exactly one representative in $F$, and

$$W_A \otimes W_B = \bigcup_{i\in[\ell]} O(f_i)$$

**Lemma 4.3.** *If $W_A$ and $W_B$ are independent and closed under the action of $G$, $\mu(F)$ is an independent set of size $|F|$.*

*Proof.* Assume that for some $\boldsymbol{\alpha} \in \{0,1\}^\ell$,

$$\sum_{i=1}^{\ell} \alpha_i \mu(f_i) = \sum_{i=1}^{\ell} \sum_{f_i' \in O(f_i)} \alpha_i f_i' = 0$$

Since $W_A \otimes W_B = \bigcup_{i\in[\ell]} O(f_i)$ is an independent set, we conclude that $\boldsymbol{\alpha} = \mathbf{0}$ and thus $\mu(F)$ is an independent set of size $|F|$. □

Now we are ready to prove Theorem 4.1.

*Proof of Theorem 4.1.* By Theorem 3.3,

$$C \cong \mu(C_A \otimes C_B)$$

By Lemma 4.3, $\mu(F)$ is an independent set of size $|F|$ so

$$dim(C) \geq |F| \tag{4.3}$$

Note that

$$|W_A| \cdot |W_B| = |W_A \otimes W_B| = \sum_{f\in F} |O(f)| = |F| \cdot \bar{O}$$

and therefore

$$|F| = |W_A| \cdot |W_B| / \bar{O}$$

We plug this expression into Equation (4.3), divide both sides of the equation by $|X(2)| = |X^A(1)| \cdot |X^B(1)|/|G|$ and get

$$Rate(C) \geq \frac{|W_A|}{|X^A(1)|} \cdot \frac{|W_B|}{|X^B(1)|} \cdot \frac{|G|}{\bar{O}}$$

If $W_A$ and $W_B$ are bases, then $|W_A| = dim(C_A)$ and $|W_B| = dim(C_B)$ and we obtain the lower bound

$$Rate(C) \geq Rate(C_A)Rate(C_B) \cdot \frac{|G|}{\bar{O}}$$

$\square$

## 4.2 Making assumptions on only one expander code

We proceed to prove Theorem 4.2. We assume only that $W_B$ is independent and closed and make no assumptions on $C_A$. The closure of $W_B$ implies that $G$ acts on it. Let $F_B = \{f_1, ..., f_\ell\}$ denote a set of representatives of the orbits $G \backslash W_B$.

We will now define functions $\mu^H : C_A \to C_A$ ($H \subseteq G$) and use them to lower-bound the dimension of $\mu(C_A \otimes C_B)$. This may be viewed as a reduction from the problem of calculating the image of $\mu(C_A \otimes C_B)$ to the problem of calculating the image of $\mu^H(C_A)$.

**Definition 4.4.** For any subgroup $H \subseteq G$, we define $\mu^H : C_A \to C_A$ by

$$\mu^H(f) = \sum_{[h] \in G_f \cap H \backslash H} f^h$$

Just like $\mu$, the functions $\mu^H$ are not generally linear, but are functions from a linear space onto a linear subspace. Specifically, $\mu^H(C_A)$ is the space $C_A^H := \{f \in C_A | H \subseteq G_f\}$:

- $\mu^H$ is *into* $C_A^H$ due to Lemma 4.8.

- $\mu^H$ is *onto* $C_A^H$ because $\mu^H(f) = f$ for every $f \in C_A^H$.

**Lemma 4.5.** *If $W_B \subseteq C_B$ is a closed and independent set, then*

$$dim(\mu(C_A \otimes C_B)) \geq \sum_{f_B \in F_B} dim(\mu^{G_{f_B}}(C_A))$$

*Proof.* For every $f_B \in F_B$ denote $V_{f_B} = Span\{O(f_B)\}$. By the independence of $W_B$ we have

$$C_A \otimes C_B \supseteq \bigoplus_{f_B \in F_B} C_A \otimes V_{f_B}$$

where $C_A \otimes V_{f_B} := Span\{f_1 \otimes f_2 | f_1 \in C_A, f_2 \in V_{f_B}\}$. For every $f_B \in F_B$, $\mu(C_A \otimes \{f_B\}) \subseteq C_A \otimes V_{f_B}$. It follows that

$$dim(\mu(C_A \otimes C_B)) \geq \sum_{f_B \in F_B} Rank(\mu(C_A \otimes \{f_B\})) \tag{4.4}$$

Now we lower-bound $Rank(\mu(C_A \otimes \{f_B\}))$ for every $f_B \in F_B$. Let $\mathcal{B}$ denote a basis for $\mu^{G_{f_B}}(C_A)$. By Lemma 4.8, for every $f_A \in \mu^{G_{f_B}}(C_A)$, $G_{f_B} \subseteq G_{f_A}$, and therefore, $G_{f_A} \cap G_{f_B} = G_{f_B}$. By Lemma 4.7, $G_{f_A \otimes f_B} = G_{f_A} \cap G_{f_B}$ so $\mu(f_A \otimes f_B)$ sums over representatives of $G_{f_B} \backslash G$. Now we show that $\{\mu(f \otimes f_B) \big| f \in \mathcal{B}\}$ is an independent set. Let $\boldsymbol{\alpha} \in \{0,1\}^{|\mathcal{B}|}$, and assume that

$$0 = \sum_{f \in \mathcal{B}} \alpha_f \mu(f \otimes f_B) = \sum_{f \in \mathcal{B}} \alpha_f \sum_{[g] \in G_{f_B} \backslash G} f^g \otimes^{g^{-1}} f_B = \sum_{[g] \in G_{f_B} \backslash G} (\sum_{f \in \mathcal{B}} \alpha_f f)^g \otimes^{g^{-1}} f_B$$

Since $O(f_B)$ is an independent set, the equation above implies that

$$\sum_{f \in \mathcal{B}} \alpha_f f = 0$$

which implies that $\boldsymbol{\alpha} = \mathbf{0}$. We conclude that for every $f_B \in F_B$,

$$Rank(\mu(C_A \otimes \{f_B\})) \geq dim(\mu^{G_{f_B}}(C_A))$$

Plugging this inequality into Equation (4.4) completes the proof. □

**Corollary 4.6.** *If $W_B$ is a closed and independent set, and for every $f_B \in F_B$,*

$$dim(\mu^{G_{f_B}}(C_A)) \geq \frac{dimC_A}{|G_{f_B}|}$$

*then*

$$Rate(C) \geq Rate(C_A) \cdot \frac{|W_B|}{|X^B(1)|}$$

*Proof.* Applying Lemma 4.5 yields

$$dim(\mu(C_A \otimes C_B)) \geq \sum_{f_B \in F_B} \frac{dim(C_A)}{|G_{f_B}|} = \frac{dim(C_A)}{|G|} \sum_{f_B \in F_B} \frac{|G|}{|G_{f_B}|} =$$

$$\frac{dim(C_A)}{|G|} \sum_{f_B \in F_B} |O(f_B)| = dim(C_A) \cdot |W_B|/|G|$$

Recall that $C \cong \mu(C_A \otimes C_B)$ (see Theorem 3.3). Dividing both sides of the inequality $dim(C) \geq dim(C_A) \cdot |W_B|/|G|$ by $|X(2)| = |X^A(1)| \cdot |X^B(1)|/|G|$ leads to the desired rate lower bound. □

Now we are ready to prove Theorem 4.2.

*Proof of Theorem 4.2.* We assume that $G_{f_B} = \{1_G\}$ for all $f_B \in W_B$ so $\mu^{G_{f_B}} = Id$ and

$$dim(\mu^{G_{f_B}}(C_A)) = dim(C_A)$$

By Corollary 4.6,

$$Rate(C) \geq Rate(C_A) \cdot \frac{|W_B|}{|X^B(1)|}$$

If $|W_B| = dim(C_B)$, the last inequality turns into

$$Rate(C) \geq Rate(C_A) \cdot Rate(C_B)$$

□

We note that Lemma 4.5 can be used to obtain the same lower bound as in Theorem 4.1 (see Lemma 9.1 in the appendix). However, this path is somewhat longer than the proof we provided in the current section. We conclude this section with two lemmas we used for the proofs of Theorems 4.1 and 4.2.

**Lemma 4.7.** *If $f = f_A \otimes f_B$ for some $f_A \in C_A, f_B \in C_B$ then*

$$G_f = G_{f_A} \cap G_{f_B}$$

*Proof.* Clearly, every $g \in G_{f_A} \cap G_{f_B}$ is in $G_f$, so $G_{f_A} \cap G_{f_B} \subseteq G_f$. Now we show that $G_f \subseteq G_{f_A} \cap G_{f_B}$. Let $g \in G_f$, then

$$f_A^g \otimes^{g^{-1}} f_B = (f_A \otimes f_B)^g = f_A \otimes f_B$$

Since $\otimes$ is an injective operator, the equation above implies that $(f_A^g, ^{g^{-1}} f_B) = (f_A, f_B)$ so $g \in G_{f_A} \cap G_{f_B}$. □

**Lemma 4.8.** *For every $f' = \mu^H(f)$,*

$$H \subseteq G_{f'}$$

*Proof.* Let $W$ denote a set of representatives of $G_f \cap H \backslash H$. For every $h \in H$,

$$(f')^h = (\mu^H(f))^h = \sum_{w \in W} f^{wh} = \sum_{w \in Wh} f^w = \mu^H(f) = f'$$

Where the last equation is due to Lemma 2.10. □

# Chapter 5

# The exact rate of square codes

In this chapter we calculate the exact rate of square codes, in two settings– under the assumption the both $C_A$ and $C_B$ have a closed basis, or under the assumption that $C_B$ has a closed basis of full orbits. Recall that in Chapter 4 we obtained lower bounds also for codes that *contain* independent sets that are closed or have full orbits. In this part we require that the *complete* bases comply with one of the aforementioned assumptions. We denote $\mathcal{B}(C_A)$ and $\mathcal{B}(C_B)$, bases for $C_A$ and $C_B$. We prove two theorems in this Chapter. Section 5.1 contains the proof of the following Theorem.

**Theorem 5.1.** *If $\mathcal{B}(C_A)$ and $\mathcal{B}(C_B)$ are closed under the action of $G$, then*

$$Rate(C) = Rate(C_A)Rate(C_B) \cdot \frac{|G|}{\bar{O}}$$

*where $\bar{O}$ is the average orbit length in $\mathcal{B}(C_A) \otimes \mathcal{B}(C_B)/G$.*

The proof of the following theorem can be found in Section 5.2.

**Theorem 5.2.** *If $\mathcal{B}(C_B)$ is closed and has full orbits, then*

$$Rate(C) = Rate(C_A) \cdot Rate(C_B)$$

## 5.1 Assuming both expander codes have closed bases

In this section we assume that the bases $\mathcal{B}(C_A)$ and $\mathcal{B}(C_B)$ are closed under the action of $G$. The lower bound in Chapter 4 followed from $\mu(F)$ being an independent set. To prove the upper bound, we need to show that $\mu(F)$ actually **spans** $\phi C$. We find it noteworthy, that **had**

$\mu$ been a linear function, the task of this section would be easy (i.e., showing that $\phi C$ is spanned by $\mu(F)$). We elaborate.

- Lemma 3.5 assures that $\mu$ is **onto** $\phi C$.
- If $\mu$ is a linear function then $\phi C$ is spanned by $\mu(\mathcal{B}(C_A) \otimes \mathcal{B}(C_B))$.
- It is also easy to see[1] that

$$\mu(\mathcal{B}(C_A) \otimes \mathcal{B}(C_B)) = \mu(F)$$

All of the above leads to the conclusion that if $\mu$ is a linear function, then $\phi C = Span\{\mu(F)\}$, as desired. Unfortunately, $\mu$ is **not** generally a linear function. Nevertheless, $\phi C$ is indeed spanned by $\mu(F)$, alas, we need to work harder to prove it. Let $F = \{f_1, f_2, ..., f_\ell\} \subseteq \mathcal{B}(C_A) \otimes \mathcal{B}(C_B)$ denote a set of representatives of the orbits $\mathcal{B}(C_A) \otimes \mathcal{B}(C_B)/G$.

**Lemma 5.3.** *If $\mathcal{B}(C_A)$ and $\mathcal{B}(C_B)$ are closed under the action of $G$, then*

$$\mu(C_A \otimes C_B) = Span\{\mu(F)\}$$

Lemma 5.3 leads directly Theorem 5.1.

*Proof of Theorem 5.1 assuming Lemma 5.3.* By Theorem 3.3 we know that

$$dim(C) = dim(\mu(C_A \otimes C_B))$$

By Lemma 5.3, $\mu(C_A \otimes C_B) = Span\{\mu(F)\}$ which implies that

$$dim(C) = Rank(\mu(F))$$

Lemma 4.3 assures that $\mu(F)$ is an independent set of size $|F|$. Putting these facts together yields

$$dim(C) = |F|$$

By the definition of $F$ and the closure assumption, $|F| = dim(C_A)dim(C_B)/\bar{O}$, so

$$dim(C) = dim(C_A)dim(C_B)/\bar{O}$$

We divide both sides of the equation by $|X(2)| = |X^A(1)| \cdot |X^B(1)|/|G|$ and obtain the desired rate expression

$$Rate(C) = Rate(C_A)Rate(C_B) \cdot |G|/\bar{O}$$

□

[1] Note that by Lemma 3.6 $\mu$ is constant on orbits $O(f_i)$ for every $f_i \in F$.

We restate Lemma 5.3 and prove it:

**Lemma 5.3** (Restated)**.** If $\mathcal{B}(C_A)$ and $\mathcal{B}(C_B)$ are closed under the action of $G$, then

$$\mu(C_A \otimes C_B) = Span\{\mu(F)\}$$

*Proof of Lemma 5.3.* We prove this by mutual inclusion. $Span\{\mu(F)\} \subseteq \mu(C_A \otimes C_B)$ since $\mu(F) \subseteq \mu(C_A \otimes C_B)$ and $\mu(C_A \otimes C_B) = \phi C$ is a linear space. It remains to show that

$$\mu(C_A \otimes C_B) \subseteq Span\{\mu(F)\}$$

As mentioned before, $\mathcal{B}(C_A) \otimes \mathcal{B}(C_B)$ is a basis for $C_A \otimes C_B$. Closure of the expander code bases implies the closure of $\mathcal{B}(C_A) \otimes \mathcal{B}(C_B)$ under the action of $G$. As before, we denote $F = \{f_1, ..., f_\ell\}$ a set of representatives of the orbits. Denote also $V_i = Span\{O(f_i)\}$ for every $i \in [\ell]$. The closure of $\mathcal{B}(C_A) \otimes \mathcal{B}(C_B)$ implies that $C_A \otimes C_B = \bigoplus_{i \in [\ell]} V_{f_i}$, so every $f \in C_A \otimes C_B$ may be expressed as a sum

$$f = \sum_{i=1}^{\ell} \tilde{f}_i$$

where $\tilde{f}_i \in V_i, \quad \forall i \in [\ell]$. In order to show that $Im(\mu) \subseteq Span\{\mu(F)\}$, we need to prove that $\mu(f) \in Span\{\mu(F)\}$. We do this in two steps. First we show that $\mu(f) \in Span\{\mu(\tilde{f}_i) \mid \forall i \in [\ell]\}$, and then we apply Lemma 5.5 which states that $\mu(\tilde{f}_i) \in \{\mu(f_i), 0\}$ for every $i \in [\ell]$. We conclude that $\mu(f) \in Span\{\mu(F)\}$.

By definition of $\mu$ and linearity of the action of $G$,

$$\mu(f) = \mu(\sum_{i=1}^{\ell} \tilde{f}_i) = \sum_{[g] \in G_f \backslash G} \sum_{i=1}^{\ell} \tilde{f}_i^g = \sum_{i=1}^{\ell} \sum_{[g] \in G_f \backslash G} \tilde{f}_i^g \tag{5.1}$$

We now show that $\sum_{[g] \in G_f \backslash G} \tilde{f}_i^g \in \{\mu(\tilde{f}_i), 0\}$ for every $i \in [\ell]$. Recall that $G_{\tilde{f}_i}$ stabilizes $\tilde{f}_i$. By Lemma 5.4, $G_f = \bigcap_{i=1}^{\ell} G_{\tilde{f}_i}$ so $G_f \subseteq G_{\tilde{f}_i}$ $(\forall i \in [\ell])$ which means that the equivalence relation associated with $f$ **refines** the relation associated with $\tilde{f}_i$. In particular, every class of $G_{\tilde{f}_i} \backslash G$ contains exactly $\frac{|G_{\tilde{f}_i}|}{|G_f|}$ classes of $G_f \backslash G$. These $f$-classes are $\tilde{f}_i$-equivalent, therefore,

$$\forall i \in [\ell], \quad \sum_{[g] \in G_f \backslash G} \tilde{f}_i^g = \sum_{[g] \in G_{\tilde{f}_i} \backslash G} \frac{|G_{\tilde{f}_i}|}{|G_f|} \tilde{f}_i^g = \frac{|G_{\tilde{f}_i}|}{|G_f|} \mu(\tilde{f}_i).$$

Plugging this expression into equation (5.1) yields

$$\mu(f) = \frac{1}{|G_f|} \sum_{i=1}^{\ell} |G_{\tilde{f}_i}| \cdot \mu(\tilde{f}_i) \tag{5.2}$$

By Lemma 5.5, $\mu(\tilde{f_i}) \in \{0, \mu(f_i)\}, \;\; \forall i \in [\ell]$, so we conclude that $\mu(f) \in Span\{\mu(F)\}$. □

To prove Lemma 5.3 we used the following lemmas.

**Lemma 5.4.** *Assume that $C_A \otimes C_B = \bigoplus_{i\in[\ell]} V_i$, and $V_i^G = V_i$ for all $i \in [\ell]$. Then for every $f = \sum_{i\in[\ell]} \tilde{f_i} \in C_A \otimes C_B$ ($\forall i \in [\ell], \tilde{f_i} \in V_i$),*

$$G_f = \bigcap_{i\in[\ell]} G_{\tilde{f_i}}$$

*Proof.* Clearly $G_f \supseteq \bigcap_{i\in[\ell]} G_{\tilde{f_i}}$ so we only need to show that $G_f \subseteq \bigcap_{i\in[\ell]} G_{\tilde{f_i}}$. For any $g \in G_f$,

$$\sum_{i\in[\ell]} \tilde{f_i} = f = f^g = \sum_{i\in[\ell]} \tilde{f}_i^g$$

Since $V_i^G = V_i$ for all $i \in [\ell]$, and $C_A \otimes C_B = \bigoplus_{i\in[\ell]} V_i$, the last equation implies that

$$\forall i \in [\ell], \;\; \tilde{f_i} = \tilde{f}_i^g$$

so $g \in \bigcap_{i\in[\ell]} G_{\tilde{f_i}}$.

□

**Lemma 5.5.** *Assume that*

- *$O(f)$ is an independent set for some $f \in C_A \otimes C_B$, and*
- *$\tilde{f} \in Span\{O(f)\}$.*

*then*

$$\mu(\tilde{f}) \in \{\mathbf{0}, \mu(f)\}$$

*Proof.* Since $\tilde{f} \in Span\{O(f)\}$ there exists a set of representatives $S \subseteq G$ s.t.

$$\tilde{f} = \sum_{h\in S} f^h$$

We denote $W \subseteq G$, a complete set of representatives of $G_{\tilde{f}} \backslash G$ and express $\mu(\tilde{f})$ in terms of $S$ and $W$:

$$\mu(\tilde{f}) = \sum_{w\in W} \tilde{f}^w = \sum_{w\in W} \sum_{h\in S} f^{hw}$$

For every $g \in G$ we define $n_g$ to be the number of pairs $(h, w) \in S \times W$ s.t. $[hw]_f = [g]_f$. That is,

$$n_g := |\{(h, w) \in S \times W \ : \ [hw]_f = [g]_f\}|$$

We express $\mu(\tilde{f})$ using this notation.

$$\mu(\tilde{f}) = \sum_{[g] \in G_f \backslash G} n_g f^g \tag{5.3}$$

We will show that the parity of $n_g$ is the same for all $g \in G$, and conclude that

$$\mu(\tilde{f}) \in \{\mathbf{0}, \mu(f)\}$$

where the value of $\mu(\tilde{f})$ follows from the parity of the $n_g$'s. Assume towards contradiction that for some $g_1, g_2 \in G$,

$$n_{g_1} \neq n_{g_2} (\text{mod } 2) \tag{5.4}$$

and set $h = g_2^{-1} g_1$ (so that $g_1 h^{-1} = g_2$). Let $T \subseteq G$ be a complete set of representatives of $G_f \backslash G$, then equation 5.3 implies that

$$\mu(\tilde{f})^h = \sum_{g \in T} n_g f^{gh} = \sum_{g \in T} n_{ghh^{-1}} f^{gh} = \sum_{g \in Th} n_{gh^{-1}} f^g = \sum_{[g] \in G_f \backslash G} n_{gh^{-1}} f^g$$

where the last transition is due to Lemma 2.10. By Lemma 3.6, $\mu(\tilde{f}) = \mu(\tilde{f})^h$ for every $h \in G$, so

$$0 = \mu(\tilde{f}) - \mu(\tilde{f})^h = \sum_{[g] \in G_f \backslash G} n_g f^g - \sum_{[g] \in G_f \backslash G} n_{gh^{-1}} f^g = \sum_{[g] \in G_f \backslash G} (n_g - n_{gh^{-1}}) f^g$$

The orbit $O(f)$ is an independent set, so for every $[g] \in G_f \backslash G$,

$$n_g = n_{gh^{-1}} (\text{mod } 2) \tag{5.5}$$

In particular, plugging $g = g_1$ and $g_1 h^{-1} = g_2$ into equation 5.5 leads to a contradiction to assumption 5.4. □

## 5.2 Assuming one expander code has a closed basis of full orbits

.

In this section we assume that the basis $\mathcal{B}(C_B)$ is closed under the action of $G$ and has full orbits (namely, $G_{f_B} = \{1_G\}$ for every $f_B \in \mathcal{B}(C_B)$). Recall that $F_B$ is a set of representatives of the orbits $G \backslash \mathcal{B}(C_B)$, so we have

$$|F_B| = \frac{dim(C_B)}{|G|}$$

*Proof of Theorem 5.2 assuming Lemma 5.8.* By Lemma 5.8, $\mu(C_A \otimes C_B)$ is spanned by

$$\{\mu(f_A \otimes f_B) | f_A \in \mathcal{B}(C_A), f_B \in F_B\}$$

This is a set of size at most

$$|\mathcal{B}(C_A)| \cdot |F_B| = dim(C_A) \cdot dim(C_B)/|G|$$

so

$$dim(C) = dim(\mu(C_A \otimes C_B)) \leq dim(C_A) \cdot dim(C_B)/|G|$$

We divide both sides by $|X(2)| = |X^A(1)| \cdot |X^B(1)|/|G|$ and get

$$Rate(C) \leq Rate(C_A) \cdot Rate(C_B)$$

The right side of the inequality is exactly the lower bound provided by Theorem 4.2, thus we conclude that

$$Rate(C) = Rate(C_A) \cdot Rate(C_B)$$

□

**Lemma 5.6.** *Assume that $\mathcal{B}(C_B)$ is closed and has full orbits. Let $f \in C_A \otimes V_{f_B}$ for some $f_B \in \mathcal{B}(C_B)$. Then there exists a set $T \subseteq G$ representing $|T|$ different $G_f \backslash G$ classes, and functions $f_t \in C_A, \forall t \in T$, s.t.*

$$f = \sum_{t \in T} \sum_{g \in G_f} (f_t \otimes^t f_B)^g$$

*Proof.* $f$ can always be expressed as

$$f = \sum_{s \in S} f_s \otimes^s f_B$$

for some set $S \subseteq G$, and $\{f_s\}_{s \in S} \subset C_A$.

For every $s \in S$ we show that $[s]_{G_f} \subseteq S$ and that $\{f_{s'}\}_{s' \in [s]_{G_f}} = \{f_s^g\}_{g \in G_f}$. For every $g \in G_f$,

$$\sum_{s \in S} f_s^g \otimes^{g^{-1}s} f_B = f^g = f = \sum_{s \in S} f_s \otimes^s f_B$$

The orbit $O(f_B)$ is an independent set and a full orbit, so the equation above implies that $g^{-1}S = S$. In other words, every $s \in S$ has exactly one $s' \in S$ s.t. $s' = g^{-1}s$ and

$$f_s^g \otimes^{s'} f_B = f_{s'} \otimes^{s'} f_B$$

which implies that

$$f_{s'} = f_s^g$$

so

$$f_{s'} \otimes^{s'} f_B = f_s^g \otimes^{g^{-1}s} f_B = (f_s \otimes^s f_B)^g$$

We denote $T \subseteq S$, a set of representatives of the $G_f \backslash G$ classes contained in $S$[2], and obtain the equation

$$f = \sum_{t\in T} \sum_{g\in G_f} (f_t \otimes^t f_B)^g$$

□

**Lemma 5.7.** *Assume that $\mathcal{B}(C_B)$ is closed and has full orbits, then*

$$\mu(C_A \otimes V_{f_B}) \subseteq Span\{\mu(f_A \otimes f_B) | f_A \in \mathcal{B}(C_A)\}$$

*for every $f_B \in \mathcal{B}(C_B)$.*

*Proof.* By Lemma 5.6 we can express any $f \in C_A \otimes V_{f_B}$ as

$$f = \sum_{t\in T} \sum_{g\in G_f} (f_t \otimes^t f_B)^g$$

where $T \subseteq G$ represent $|T|$ different $G_f \backslash G$ classes, and $f_t \in C_A, \forall t \in T$. $G_f W = G$ for every $W$, a set of representatives of $G_f \backslash G$, so

$$\mu(f) = \sum_{w\in W} \sum_{t\in T} \sum_{g\in G_f} (f_t \otimes^t f_B)^{gw} = \sum_{t\in T} \sum_{g\in G} (f_t \otimes^t f_B)^g =$$

$$\sum_{t\in T} \mu(f_t \otimes^t f_B) = \sum_{t\in T} \mu(f_t^t \otimes f_B)$$

The third equality is due to Lemma 4.7. The last equation is due to Lemma 3.6. So far we proved that $\mu(f) \in Span\{\mu(f_A \otimes f_B) | f_A \in C_A\}$. To complete our proof we must show

[2] That is, $S$ is the disjoint union $\bigcup_{t\in T} [t]_{G_f}$.

that $Span\{\mu(f_A \otimes f_B) | f_A \in C_A\} \subseteq Span\{\mu(f_A \otimes f_B) | f_A \in \mathcal{B}(C_A)\}$. Indeed, for every $f_A = \sum\limits_{f_i \in \mathcal{B}(C_A)} \alpha_i f_i \in C_A$,

$$\mu(f_A \otimes f_B) = \sum_{g \in G} [(\sum_{f_i \in \mathcal{B}(C_A)} \alpha_i f_i) \otimes f_B]^g = \sum_{g \in G} \sum_{f_i \in \mathcal{B}(C_A)} \alpha_i (f_i \otimes f_B)^g = \sum_{f_i \in \mathcal{B}(C_A)} \alpha_i \mu(f_i \otimes f_B)$$

□

**Lemma 5.8.** *Assume that $\mathcal{B}(C_B)$ is closed and has full orbits, then*

$$\mu(C_A \otimes C_B) = Span\{\mu(f_A \otimes f_B) | f_A \in \mathcal{B}(C_A), f_B \in F_B\}$$

*Proof.* The inclusion

$$Span\{\mu(f_A \otimes f_B) | f_A \in \mathcal{B}(C_A), f_B \in F_B\} \subseteq \mu(C_A \otimes C_B)$$

requires no proof. We prove the other direction. The closure of $\mathcal{B}(C_B)$ implies that

$$C_A \otimes C_B = \bigoplus_{f_i \in F_B} C_A \otimes V_{f_i}$$

where $V_{f_i} := Span\{O(f_i)\}$, and $C_A \otimes V_{f_i} := Span\{f_A \otimes f_B | f_A \in \mathcal{B}(C_A), f_B \in O(f_i)\}$ for every $f_i \in F_B$. So every $f \in C_A \otimes C_B$ can be expressed as a sum

$$f = \sum_{f_i \in F_B} \tilde{f_i}$$

where $\tilde{f_i} \in C_A \otimes V_{f_i}$ for all $f_i \in F_B$. Following the exact same steps as in Lemma 5.3 (see Equations (5.1) to (5.2)) yields

$$\mu(f) = \frac{1}{|G_f|} \sum_{i: f_i \in F_B} |G_{\tilde{f_i}}| \cdot \mu(\tilde{f_i})$$

By Lemma 5.7, for every $f_i \in \mathcal{B}(C_B)$,

$$\mu(\tilde{f_i}) \in Span\{\mu(f_A \otimes f_i) | f_A \in \mathcal{B}(C_A)\}$$

and we conclude that

$$\mu(f) \in Span\{\mu(f_A \otimes f_i) | f_A \in \mathcal{B}(C_A), f_i \in F_B\}$$

□

# Chapter 6

# Closed, full orbit bases are likely

The lower-bounds obtained in Chapter 4 rely on assumptions, while we have not actually presented a good code that satisfies any of those assumptions. However, it is likely that most expander codes have a large closed independent set of full orbits. In this short section we explain this statement. First, we must present another definition.

**Definition 6.1** (Induced Sub-code)**.** Let $H$ be the parity check matrix of an expander code $C_B$, and $B_1 \subseteq B$ a symmetric set of generators. Denote $H_{B_1}$, the columns of $H$ corresponding to $B_1$-edges. We define

$$C_{B_1} := Ker(H_{B_1})$$

and say that $H_{B_1}$ has *maximal* rank if $Span\{Cols(H_{B_1})\} = Span\{Cols(H)\}$.

Note that $C_{B_1}$ is an expander code on $Cay(G, B_1)$ and is embedded in $C_B$. Denote $B_0 = B \setminus B_1$.

**Lemma 6.2.** *If $b^2 \neq 1_G$ for every $b \in B$, and $H_{B_1}$ has maximal rank, then the bits corresponding to $B_0$-edges may be used as message bits and*

$$Rate(C) \geq Rate(C_A) \cdot \frac{|B_0|}{|B|} \tag{6.1}$$

*If additionally $|X^{B_1}(1)| = Rank(H)$ then $C_B$ has a closed basis of full orbits and*

$$Rate(C) = Rate(C_A) \cdot Rate(C_B)$$

*Proof.* In order to show that the bits corresponding to $B_0$-edges may be used as message bits, we must prove that every $\mathbf{m} \in \mathbb{F}^{|X^{B_0}(1)|}$ can be encoded. The columns of $H_{B_1}$ span the column space of $H$, in particular, $-H_{B_0}\mathbf{m}$ is in the image of $H_{B_1}$. Let $\mathbf{x}$ be a vector s.t. $H_{B_1}\mathbf{x} = -H_0\mathbf{m}$, then $\begin{bmatrix} \mathbf{x} \\ \mathbf{m} \end{bmatrix}$ is a codeword in $C_B$, so $\mathbf{m}$ can be encoded.

We proceed to proving Equation (6.1). We find a closed independent set of full orbits, and size $|X^{B_0}(1)|$, and apply Theorem 4.2. For every $g \in G, b \in B_0$, let $\mathbf{1}_{[g,b]} \in \mathbb{F}^{|X^{B_0}(1)|}$ denote the indicator function of the edge $[g, b]$. The set

$$W_B = \{ENC(\mathbf{1}_{[g,b]})|g \in G, b \in B_0\} \tag{6.2}$$

is clearly independent and closed under the action of $G$. Additionally, every function in $W_B$ has a full orbit: Assume that ${}^h\mathbf{1}_{[g,b]} = \mathbf{1}_{[g,b]}$. Then, $\mathbf{1}_{[g,b]}[h^{-1}g, b] = \mathbf{1}_{[g,b]}[g, b] = 1$ which implies that $h = 1_G$. i.e., the stabilizer of $\mathbf{1}_{[g,b]}$ is trivial[1].

Theorem 4.2 assures that

$$Rate(C) \geq Rate(C_A) \cdot \frac{|W_B|}{|X^B(1)|}$$

We plug $|W_B| = |X^{B_0}(1)| = \frac{|B_0|}{2} \cdot |G|$ and $|X^B(1)| = \frac{|B|}{2} \cdot |G|$ into this expression and get

$$Rate(C) \geq Rate(C_A) \cdot \frac{|B_0|}{|B|}$$

If $|X^{B_1}(1)| = Rank(H)$ then $X^{B_0}(1)$ are exactly the message bits of $C_B$, and $W_B = \mathcal{B}(C_B)$ is a closed basis of full orbits. By Theorem 5.2

$$Rate(C) = Rate(C_A) \cdot Rate(C_B)$$

□

We conjecture that $Rank(H_{B_1}) = |X^{B_1}(1)| = Rank(H)$ is actually the typical case.

**Conjecture 6.3.** *If $b^2 \neq 1_G$ for every $b \in B$, $Cay(G, B)$ is an expander, and $c_B$ is a random code, then $H$ has full rank w.h.p.*

This conjecture implies that $H_{B_1}$ is likely to have full rank. If $H_{B_1}$ is square we get $Rank(H_{B_1}) = |X^{B_1}(1)| = Rank(H)$. Together with Lemma 6.2, this conjecture implies that typically, expander codes have a closed basis of full orbits and square codes have the same rate as their associated tensor code.

[1] This is where we used the assumption on the order of the elements in $B$. If there's an order 2 element $b$, then the stabilizer of $\mathbf{1}_{[g,b]}$ is $\{1_G, gbg^{-1}\}$ and the whole argument fails.

We would like to point out to the seeming irony in the last statement. Assuming that most expander codes have the worst possible rate (i.e., a full rank parity-check matrix), we obtain an "improved" rate for square codes. This seems very unreasonable, leading us to another conjecture.

**Conjecture 6.4.** *For all expander codes $C_A$ and $C_B$,*

$$Rate(C) \geq Rate(C_A) \cdot Rate(C_B)$$

# Chapter 7

# Square codes as a convolution of expander codes

Given $f_A \in C_A$ and $f_B \in C_B$ we define the convolution operator by

$$(f_A * f_B)[a,g,b] = \sum_{[h] \in G_{f_A} \cap G_{f_B} \backslash G} f_A[h^{-1}, a] \cdot f_B[hg, b] = \sum_{[h] \in G_{f_A} \cap G_{f_B} \backslash G} f_A^h[1_G, a] \cdot^{h^{-1}} f_B[g,b] \quad (7.1)$$

for every $a \in A, b \in B, g \in G$. In this section, we explore $C$ as an operation on two codes similarly to the tensor code as a product of two codes. However, while $\mathcal{B}(C_A) \otimes \mathcal{B}(C_B)$ forms a basis for $C_A \otimes C_B$, $\mathcal{B}(C_A) * \mathcal{B}(C_B)$ is usually not an independent set, but we will prove in the following Theorem, that it *contains* a basis for $C$.

**Theorem 7.1.** *If $\mathcal{B}(C_B)$ is closed and one of the following holds:*

1. *$\mathcal{B}(C_A)$ is closed.*

2. *$\mathcal{B}(C_B)$ has full orbits.*

*then*

$$C = C_A * C_B$$

where

$$C_A * C_B := Span\{f_A * f_B \mid f_A \in \mathcal{B}(C_A), f_B \in \mathcal{B}(C_B)\}$$

Towards this end we prove the following lemma.

**Lemma 7.2.** *For every $f_A \in C_A, f_B \in C_B, g \in G, a \in A, b \in B$,*

$$\phi^{-1} \circ \mu(f_A \otimes f_B) = f_A * f_B$$

*where $\phi^{-1} : \phi C \to C$ is defined by*[1]

$$\phi^{-1} f([a, g, b]) := f[a, 1_G, g, b]$$

*Proof.* First we show that $\phi^{-1}$ is indeed the inverse of $\phi$:

$$\forall f \in C, \quad \phi^{-1} \circ \phi f[a, g, b] = \phi f[a, 1_G, g, b] = f[a, g, b]$$

We move on to prove the main statement. For every $a \in A, b \in B, g \in G$,

$$\phi^{-1} \circ \mu(f_A \otimes f_B)[a, g, b] = \mu(f_A \otimes f_B)[a, 1_G, g, b] = \sum_{[h] \in G_{f_A} \cap G_{f_B} \backslash G} (f_A^h \otimes^{h^{-1}} f_B)[a, 1_G, g, b] =$$

$$\sum_{[h] \in G_{f_A} \cap G_{f_B} \backslash G} f_A^h[1_G, a] \cdot^{h^{-1}} f_B[g, b] = (f_A * f_B)[a, g, b]$$

The second transition is due to Lemma 4.7 (which states that $G_{f_A \otimes f_B} = G_{f_A} \cap G_{f_B}$). □

**Corollary 7.3.** *If $\mathcal{B}(C_A)$ and $\mathcal{B}(C_B)$ are closed under the action of $G$ then*

$$\mathcal{B}(C) = \{f_A * f_B \mid f_A \otimes f_B \in F\}$$

*forms a basis for $C$*[2]*.*

*Proof.* In previous sections we established that $\mu(F)$ is a basis for $\phi C$. The inverse of $\phi$ is a linear bijection from $\phi C$ onto $C$ and thus $\phi^{-1} \circ \mu(F)$ forms a basis for $C$. By Lemma 7.2, this set is no other than

$$\{f_A * f_B \mid f_A \otimes f_B \in F\}$$

We conclude that

$$\mathcal{B}(C) = \{f_A * f_B \mid f_A \otimes f_B \in F\}$$

is a basis for $C$. □

[1] Note that functions in $\phi C$ are constant on the squares $\{[a, h^{-1}, hg, b] \mid h \in G\}$ for every $g \in G$, $a \in A, b \in B$, so we could equally define $\phi^{-1}$ by $\phi^{-1} f([a, g, b]) := f[a, h^{-1}, hg, b]$ for any $h \in G$.

[2] Section 9.1 provides a more specific characterisation of $F$.

**Corollary 7.4.** *If $\mathcal{B}(C_B)$ is closed and has full orbits, then*

$$\mathcal{B}(C) = \{f_A * f_B | f_A \in \mathcal{B}(C_A), f_B \in F_B\}$$

*where $F_B$ is a set of representatives for the orbits $G \backslash \mathcal{B}(C_B)$.*

*Proof.* Lemma 5.8 shows that $\{\mu(f_A \otimes f_B) | f_A \in \mathcal{B}(C_A), f_B \in F_B\}$ is a basis for $\mu(C_A \otimes C_B) = \phi C$. Using this fact and following the same line of argumentation as in Corollary 7.3, proves this corollary. □

Now we are ready to prove our main theorem for this section.

*Proof of Theorem 7.1.* We need to show that

$$C = Span\{\mathcal{B}(C_A) * \mathcal{B}(C_B)\}$$

In Corollary 7.3 and 7.4 we saw that $C$ is spanned by $\{f_A * f_B \mid f_A \otimes f_B \in F\} \subseteq \mathcal{B}(C_A) * \mathcal{B}(C_B)$ or $\{f_A * f_B \mid f_A \in \mathcal{B}(C_A), f_B \in F_B\} \subseteq \mathcal{B}(C_A) * \mathcal{B}(C_B)$, so we only need to show that $Rank\{\mathcal{B}(C_A) * \mathcal{B}(C_B)\}$ can be no larger than the size of these sets, which is true since $\phi^{-1}$ preserves the rank. □

# Chapter 8

# Examples- square codes that meet our bound

**Example 8.1.** $C_A \otimes C_B$ is the *square code* obtained by the left-right Cayley complex $Cay(G,A) \times Cay(G,B) = Cay^2(A \times \{1_G\}, G \times G, \{1_G\} \times B)$ and base codes $c_A$ and $c_B$. The expander codes $\tilde{C}_A$ and $\tilde{C}_B$, defined by $Cay(G,A) \times Cay(G,B)$ and base codes $c_A$ and $c_B$, are spanned by the $|G|$ "copies" of the base elements of $\mathcal{B}(C_A)$ and $\mathcal{B}(C_B)$, corresponding to the $|G|$ copies of $Cay(G,A)$ and $Cay(G,B)$ embedded in $Cay(G,A) \times Cay(G,B)$, so $|\mathcal{B}(\tilde{C}_A)| = |G| \cdot |\mathcal{B}(C_A)|$ and $|\mathcal{B}(\tilde{C}_B)| = |G| \cdot |\mathcal{B}(C_B)|$. The block-length of $\tilde{C}_A$ and $\tilde{C}_B$ is also $|G|$ times the block-length of $C_A$ and $C_B$. We conclude that $Rate(C_A) = Rate(\tilde{C}_A)$ and $Rate(C_B) = Rate(\tilde{C}_B)$. Without assuming anything on $\tilde{C}_A$ and $\tilde{C}_B$ we have

$$Rate(C_A \otimes C_B) = Rate(C_A) \cdot Rate(C_B) = Rate(\tilde{C}_A) \cdot Rate(\tilde{C}_B)$$

**Example 8.2.** Set $G = \mathbb{Z}_n \times \mathbb{Z}_n$, $\mathbf{a_1} = (1,0), \mathbf{a_2} = (0,1)$ and $\mathbf{b} = (1,-1)$. The sets of generators are $A = \{\mathbf{a_1}, -\mathbf{a_1}, \mathbf{a_2}, -\mathbf{a_2}\}$ and $B = \{\mathbf{b}, -\mathbf{b}\}$. The base codes are $c_A = Span\{\{a_1,-a_1\},\{a_2,-a_2\}\} \subset \{0,1\}^4$ and $c_B = Span\{\{b,-b\}\} \subset \{0,1\}^2$.

1. We find $\mathcal{B}(C_A)$ and $\mathcal{B}(C_B)$ of sizes $2n$ and $n$ that are closed under the action of $G$.

2. We show that for every $f_A \in \mathcal{B}(C_A)$, $f_B \in \mathcal{B}(C_B)$,

   $$|O(f_A \otimes f_B)| = |G|$$

   so $\bar{O} = |G|$.

3. We conclude from Theorem 5.1 that

$$dimC = dim(C_A)dim(C_B)/\bar{O} = (2n \cdot n)/n^2 = 2$$

We may visualize $Cay(G, A)$ as a grid–its horizontal edges corresponding to the generators $a_1$ and $-a_1$, and its vertical edges corresponding to the generators $a_2$ and $-a_2$. It is not hard to see that $C_A$ is spanned by the indicator functions of the horizontal and vertical lines. Similarly, $C_B$ is spanned by the indicator functions of the diagonal lines. We formally define the horizontal line indicators.

$$f_z^-[g, \cdot] := \begin{cases} \{a_1, -a_1\} & g \in (0, z) + \langle a_1 \rangle \\ \emptyset & \text{else} \end{cases}$$

Similarly, the vertical lines are indicated by

$$f_z^{|}[g, \cdot] := \begin{cases} \{a_2, -a_2\} & g \in (z, 0) + \langle a_2 \rangle \\ \emptyset & \text{else} \end{cases}$$

**Claim 8.3.** *$\{f_z^-, f_z^{|}\}_{z \in \mathbb{Z}_n}$ is a closed basis for $C_A$.*

*Proof.*

1. We show that $\{f_z^-, f_z^{|}\}_{z \in \mathbb{Z}_n}$ is a basis for $C_A$. The set $\{f_z^-, f_z^{|}\}_{z \in \mathbb{Z}_n}$ is obviously independent (no line is a sum of other lines). On the other hand, every $f \in C_A$ is constant on the lines (horizontal and vertical), so $\{f_z^-, f_z^{|}\}_{z \in \mathbb{Z}_n}$ spans $C_A$.

2. $G$ moves horizontal lines to horizontal lines (and vertical lines to vertical lines). Thus, $\{f_z^-, f_z^{|}\}_{z \in \mathbb{Z}_n}$ is closed under the action of $G$.

□

Similarly, the diagonal indicators defined bellow form a closed basis for $C_B$.

$$f_z^{\setminus}[g, \cdot] := \begin{cases} \{b, -b\} & g \in (z, 0) + \langle b \rangle \\ \emptyset & \text{else} \end{cases}$$

**Claim 8.4.** *For every $f_A \in \{f_z^-, f_z^{|}\}_{z \in \mathbb{Z}_n}$, $f_B \in \{f_z^{\setminus}\}_{z \in \mathbb{Z}_n}$, $|O(f_A \otimes f_B)| = |G|$.*

*Proof.* We show that the intersection $G_{f_A} \cap G_{f_B}$ is trivial for every $f_A \in \{f_z^-, f_z^{|}\}_{z \in \mathbb{Z}_n}$, $f_B \in \{f_z^{\setminus}\}_{z \in \mathbb{Z}_n}$. By Lemma 4.7,

$$G_{f_A \otimes f_B} = G_{f_A} \cap G_{f_B}$$

so $|O(f_A \otimes f_B)| = \frac{|G|}{|G_{f_A \otimes f_B}|} = |G|$ as desired. Assume WLOG that $f_A$ indicates a horizontal line, then $G_{f_A} = \mathbb{Z}_n \times \{0\}$. For every diagonal indicator $f_B$, $G_{f_B} = \mathbb{Z}_n \cdot (1, -1)$. The intersection of these sets is indeed trivial (the Singleton $\{(0, 0)\}$). □

Note that the last example actually demonstrates a somewhat more general phenomena. Namely, if $C_A$ is spanned by $k_A$ lines, $C_B$ is spanned by $k_B$ different lines, then $dim(C) = (k_A \cdot k_B)/n^2$, which is a constant, so $Rate(C) = O(\frac{1}{|\mathbb{Z}_n \times \mathbb{Z}_n|})$.

# Chapter 9

# Appendix

## 9.1 An alternative proof for Theorem 4.1

In Chapter 4 we used different tools to prove Theorems 4.1 and 4.2. Although longer, we present here a proof for Theorem 4.1 using the same technique as in Theorem 4.2. This proof reveals more about $F$, a set of representatives of the orbits $W_A \otimes W_B/G$. We saw in Chapter 4 that $\mu(F)$ is an independent set, a fact that allowed us to lower-bound $Rate(C)$. Here we learn that $F$ can be chosen as

$$\bigcup_{f_A \in F_A, f_B \in F_B} \{\mu^{G_{f_B}}(f_A^u) \otimes f_B | u \in U(f_A, f_B)\}$$

where $U(f_A, f_B)$ is a set of representatives of the double coset $G_{f_A} \backslash G / G_{f_B}$, $F_A$ is a set of representatives of $W_A/G$, and $F_B$ is a set of representatives of $G \backslash W_B$.

**Lemma 9.1.** *Assume that $W_A \subseteq C_A$ is independent and closed under the action of $G$. Then for every $f_B \in C_B$,*

$$Rank(\mu^{G_{f_B}}(C_A)) \geq \sum_{f_A \in F_A} \frac{|O(f_A)| \cdot |O(f_B)|}{|O(f_A \otimes f_B)|}$$

*where $F_A$ is a set of representatives of the orbits $W_A/G$.*

*Proof.* Since $C_A \subseteq \bigoplus_{f_A \in F_A} V_{f_A}$ and $\mu^H(V_{f_A}) \subseteq V_{f_A}$ for every $H \subseteq G$, $f_A \in F_A$ we have

$$Rank(\mu^{G_{f_B}}(C_A)) \geq \sum_{f_A \in F_A} Rank(\mu^{G_{f_B}}(V_{f_A}))$$

For every $f_A \in F_A$, denote $U$ a set of representatives of the double coset $G_{f_A} \backslash G / G_{f_B}$. We claim that the set

$$\{f_A^{ug} | u \in U, [g] \in G_{f_A^u} \cap G_{f_B} \backslash G_{f_B}\}$$

is independent. Since $O(f_A)$ is independent we only need to show that $f_A^{ug} = f_A^{u'g'}$ implies that $u = u'$ and $[g] = [g']$. Indeed, $f_A^{ug} = f_A^{u'g'}$ implies that

$$u'g'g^{-1}u^{-1} \in G_{f_A} \implies u' \in G_{f_A} u G_{f_B}$$

and $f_A^{ug} = f_A^{ug'}$ implies that $[g] = [g']$. An immediate conclusion is that

$$\{\mu^{G_{f_B}}(f_A^u) | u \in U\}$$

is independent, so

$$Rank(\mu^{G_{f_B}}(V_{f_A})) \geq |U| = \frac{|G|}{|G_{f_A} G_{f_B}|} = \frac{|G| \cdot |G_{f_A} \cap G_{f_B}|}{|G_{f_A}| \cdot |G_{f_B}|} =$$

$$\frac{|G|^2}{|G_{f_A}| \cdot |G_{f_B}|} \cdot \frac{|G_{f_A \otimes f_B}|}{|G|} = \frac{|O(f_A)| \cdot |O(f_B)|}{|O(f_A \otimes f_B)|}$$

Summing over $F_A$ concludes the proof. □

Lemma 9.1 leads to an alternative proof for Theorem 4.1.

*Alternative proof of Theorem 4.1.* Applying Lemmas 9.1 and 4.5 leads to the inequality

$$dim(\mu(C_A \otimes C_B)) \geq \sum_{f_B \in F_B} \sum_{f_A \in F_A} \frac{|O(f_A)| \cdot |O(f_B)|}{|O(f_A \otimes f_B)|} = |F|$$

where $F_B$ is a set of representatives of $G \backslash W_B$ and $F$ is a set of representatives of $W_A \otimes W_B / G$. The rest of the proof is identical to the proof provided in Section 4. □

## 9.2 Another project completed during my studies

I conclude this thesis by reviewing another project completed during my masters. I collaborated with Yotam Dikstein and Irit Dinur on developing efficient encoding algorithms for LDPC codes (LDPC stands for Low-Density Parity-Check). While working on this subject, we encountered a paper claiming to present a linear-time encoding algorithm for every LDPC code (see [3]), a claim that we dispute in [1]. In our refutation paper we present a family of counterexamples, and point out where the analysis in [3] fails. Specifically, the algorithm in [3] fails to encode our counterexample, let alone in linear time.

# Bibliography

[1] Yotam Dikstein, Irit Dinur, and Shiri Sivan. The linear time encoding scheme fails to encode. *ArXiv*, abs/2312.16125, 2023.

[2] Irit Dinur, Shai Evra, Ron Livne, Alexander Lubotzky, and Shahar Mozes. Locally testable codes with constant rate, distance, and locality. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2022, page 357–374, New York, NY, USA, 2022. Association for Computing Machinery.

[3] Jin Lu and José M. F. Moura. Linear time encoding of LDPC codes. *IEEE Transactions on Information Theory*, 56(1):233–249, 2010.

[4] M. Sipser and D.A. Spielman. Expander codes. *IEEE Transactions on Information Theory*, 42(6):1710–1722, 1996.