University of Amsterdam

MSc Mathematics

Master Thesis

Gowers U^3 inverse theorem for quantum states

Author:
Philippe van Dordrecht

Supervisor:
dr. Jop Briët
dr. Jeroen Zuiddam

Examination date:
February 27th, 2025

Korteweg-de Vries Institute for Mathematics

Centrum voor Wiskunde en Informatica

Abstract

We prove a Gowers U^3 inverse theorem for functions $f : \mathbb{F}_p^n \to \mathbb{C}$ with $||f||_2 = 1$. This theorem tells us that if f has Gowers U^3-norm at least ϵ, then there exists a function s with $||s||_2 = 1$ and $||s||_{U^3} = 1$ that has $|\langle s, f\rangle| \geq C_2\epsilon^{C_1}$ for some constants C_1, C_2, depending only on p. A function s with these properties is known in quantum information theory as a stabilizer state [1, 2]. The polynomial dependence on ϵ is facilitated by the recent breakthrough result of Green, Gowers, Marton and Tao [3],[4]. This theorem implies a polynomial time tolerant stabilizer testing algorithm for quantum states [5]. For our proof, we prove a finite field analog of the Stone-von Neumann Theorem. As far as we are aware, no proof of this theorem exists in the literature in the case that $p = 2$.

Title: Gowers U^3 inverse theorem for quantum states
Author: Philippe van Dordrecht, philippevdord@gmail.com, 11321385
Supervisor: dr. Jop Briët, dr. Jeroen Zuiddam
Second Examiner: dr. Guus Regts
Examination date: February 27th, 2025

Korteweg-de Vries Institute for Mathematics
University of Amsterdam
Science Park 105-107, 1098 XG Amsterdam
`http://kdvi.uva.nl`

Centrum voor Wiskunde en Informatica
Science Park 123, 1098 XG Amsterdam
`http://www.cwi.nl`

Contents

1 Introduction

This thesis will be about three topics in mathematics, namely, additive combinatorics, higher order Fourier analysis and quantum computing. Additive combinatorics is a field that studies additive patterns in sets of numbers [6, 7]. One of the most important theorems in additive combinatorics is Szemerédi's theorem (1975), Theorem 1.2.1 [8]. This theorem gives us an upper bound on the sizes sets of integers that avoid additive patterns known as arithmetic progressions. This theorem was reproven by Gowers in 2001 [9]. Gowers' work is seen as the beginning of the field of higher order Fourier analysis [10]. This field studies functions known as polynomial phase functions. One application of higher order Fourier analysis is the celebrated Green-Tao theorem (2004), which states that the prime numbers contain arbitrarily long arithmetic progressions [11].

Quantum computing is concerned with quantum computers, a type of computer that uses the laws of quantum mechanics [12, 13]. By the nature of quantum mechanics, if a quantum state is measured, it is destroyed. For this reason, it is hard to determine a description of a quantum state. The field of quantum tomography is concerned with finding ways of measuring a state in a clever way, in order to learn about the state [14].

The main result of our thesis, Theorem 1.2.5 gives rise to an algorithm that determines whether a given state is close to a special set of states known as *stabilizer states*. In the rest of the introduction, we will first give a brief overview of stabilizer states. Then we give some context to Theorem 1.2.5 from additive combinatorics. Then we give the context in tomography, specifically stabilizer testing. Lastly, we give an outline of the contents of each chapter.

1.1 Stabilizer States

We will be studying quantum states on n qudits with local dimension equal to some prime number p, . A quantum state $|\psi\rangle$ on n qudits is given by a function $f : \mathbb{F}_p^n \to \mathbb{C}$ with $||f||_2 = 1$, where p is a prime. Then,

$$|\psi\rangle = \sum_{x \in \mathbb{F}_p^n} f(x)|x\rangle. \tag{1.1}$$

We will prove a result about a norm called the Gowers U^3-norm. The Gowers U^3-norm is written as $||f||_{U^3}$. The Gowers U^3-norm of a quantum state is a real number in the interval $[0, 1]$.

As it turns out this norm captures, in some sense, the amount of stucture present in f. The states for which the Gowers U^3-norm is equal to 1 are very structured objects,

called *stabilizer states* [15]. Theorem 1.2.5, the main theorem of this thesis, tell us that if a state has high Gowers U^3-norm, then it must be close to a stabilizer state in inner product.

The states for which the Gowers U^3-norm is equal to 1, the aforementioned stabilizer sates, are a familiar object in quantum information theory [2].

Stabilizer states are relevant for quantum error correction [16, 17]. A Clifford circuit is a circuit that maps stabilizer states to stabilizer states. By the Gottesmann-Knill theorem, a quantum circuit that only uses Clifford circuits is efficiently simulable on a classical computer [1].

Another reason stabilizer states are interesting is because they have short descriptions. There are approximately $2^{n^2/2}$ possible stabilizers [18]. This implies that in order to describe a stabilizer, we need approximately $n^2/2$ bits. A general quantum state on n qubits is given by 2^n complex numbers, so we need order of 2^n bits to describe a general state. This means that stabilizer states are states with a short (polynomial) description.

1.2 Uniformity norms

Here we will give some context for the Gowers U^3-norm. The norm comes from the field of additive combinatorics. The following theorem was proven by Szemerédi [8]. By a k-term arithmetic progression we mean a set of the form $\{a, a+d, \ldots, a+(k-1)d\} \subseteq G$ for $a, d \in G$, where G is an additive group, such as $\mathbb{Z}$ or $\mathbb{F}_p^n$.

Theorem 1.2.1. *For any $\epsilon > 0, k \in \mathbb{N}$, there exists an $N_0 \in \mathbb{N}$ such that if $N \geq N_0$, and $A \subseteq [N_0]$, then $\frac{|A|}{N_0} \geq \epsilon$ implies that A contains a k-term arithmetic progression.*

In 2001 Gowers reproved this theorem using Fourier-analytic methods [9]. In this work, he introduced the uniformity norms, which were later named the Gowers uniformity norms. In this thesis we will be concerned with the 3-rd uniformity norm, or U^3-norm, which we will define as follows. For $f : \mathbb{F}_p^n \to \mathbb{C}$, we will use the notation $\Delta_h f(x) = \overline{f(x)} f(x+h)$.

Definition 1.2.2 (U^3-norm, version for L^∞ normalized functions)**.** For $f : \mathbb{F}_p^n \to \mathbb{C}$ with $\max_{x \in \mathbb{F}_p^n} |f(x)| \leq 1$ we define the Gowers U^3-norm as

$$||f||_{U^3} = (\mathbb{E}_{h_1,h_2,h_3,x \in \mathbb{F}_p^n} \Delta_{h_1} \Delta_{h_2} \Delta_{h_3} f(x))^{1/8}. \tag{1.2}$$

where the expectation is taken over uniform $x, h_1, h_2, h_3 \in \mathbb{F}_p^n$.

By the triangle inequality, for any f, if $||f||_\infty = 1$, then $||f||_{U^3} \leq 1$.

There is a reason this norm is interesting in the context of additive combinatorics. Let $A \subseteq \mathbb{F}_p^n$ be a set without any 4-term arithmetic progressions, where $p \geq 5$, and let $\alpha = \frac{|A|}{p^n}$ be the density of A. Let $1_A : \mathbb{F}_p^n \to \mathbb{C}$ be defined by $1_A(x) = \mathbb{1}[x \in A]$. Then the function $1_A - \alpha$ has Gowers U^3-norm at least $||1_A - \alpha||_{U^3} \geq 2^{-5}\alpha^3$.

Green and Tao later proved Theorem 1.2.3 [19]. Phase polynomials of degree 2 are functions $g : \mathbb{F}_p^n \to \mathbb{C}$ of the form

$$g(x) = \omega_p^{q(x)}, \tag{1.3}$$

where q a degree 2 polynomial in $\mathbb{F}_p[x_1, \ldots, x_n]$. It is easy to verify that if $g(x)$ is a degree k phase polynomial, then $\Delta_h g(x)$ is a degree $k-1$ phase polynomial. For this reason, $\Delta_{h_1}\Delta_{h_2}\Delta_{h_3}\omega_p^{q(x)} = 1$ and the Gowers U^3-norm $\omega_p^{q(x)}$ is 1.

It turns out that if the Gowers U^3-norm of a function $f : \mathbb{F}_p^n \to \mathbb{C}$ is high, then this function will have high correlation with a polynomial phase function of degree 2. This is the content of Theorem 1.2.3. Green and Tao [19] proved this theorem for uneven p. Later, Samorodnitsky [20] proved the theorem where p is even.

Theorem 1.2.3. *Let $\epsilon > 0$. Let $f : \mathbb{F}_p^n \to \mathbb{C}$ be a function with $|f(x)| \leq 1$ for all $x \in \mathbb{F}_p^n$. Suppose that $||f||_{U^3} \geq \epsilon$. Then, there exists a phase polynomial of degree 2 such that $\mathbb{E}_{x \in \mathbb{F}_p^n} f(x)\overline{g(x)} \geq \delta$, where $\delta > 0$ depends only on ϵ and p.*

We are interested in a different setting, namely the setting where f describes a quantum state $|\psi\rangle$ on n qudits:

$$|\psi\rangle = \sum_{x \in \mathbb{F}_p^n} f(x)|x\rangle. \tag{1.4}$$

In this case, we have a different normalization assumption, namely that $||f||_2 = 1$. Accordingly, we will define the Gowers U^3-norm with a different normalization.

Definition 1.2.4 (U^3-norm, version for L^2 normalized functions)**.** For $f : \mathbb{F}_p^n \to \mathbb{C}$ we define the Gowers U^3-norm as

$$||f||_{U^3} = \left(\sum_{h_1,h_2,h_3,x \in \mathbb{F}_p^n} \Delta_{h_1}\Delta_{h_2}\Delta_{h_3} f(x) \right)^{1/8}. \tag{1.5}$$

Now, like before, for any function f with $||f||_2 = 1$, we have $||f||_{U^3} \leq 1$. We prove this in Proposition 2.2.6.

We will define the set of L^2 normalized functions s with $||s||_{U^3} = 1$ as $\mathcal{S}$. Let

$$\mathcal{S} = \{f : \mathbb{F}_p^n \to \mathbb{C} \text{ such that } ||f||_2 = 1 \text{ and } ||f||_{U^3} = 1\}. \tag{1.6}$$

In Proposition 2.2.8, 2.2.9 we will give a simple characterization of these functions, which is reminiscent of the quadratic phase functions of Theorem 1.2.3.

The following theorem, which is the main result in our thesis, tells us that if an L^2 normalized function $f : \mathbb{F}_p^n \to \mathbb{C}$ has Gowers U^3-norm is at least ϵ, then it must be close in inner product to an L^2 normalized function with Gowers U^3-norm 1:

Theorem 1.2.5. *Let p be a prime. Supose that $f : \mathbb{F}_p^n \to \mathbb{C}$ is a function satisfying $||f||_2 = 1$, and $||f||_{U^3} \geq \epsilon$. There exist constants $C_1, C_2 > 0$ only depending on p, such that there exists a function $s : \mathbb{F}_p^n \to \mathbb{C}$ with $s \in \mathcal{S}$ such that $|\langle f, s\rangle|^2 \geq C_2\epsilon^{C_1}$.*

1.3 Bell sampling and (tolerant) stabilizer testing

In 2017, Montanaro introduced a procedure called Bell sampling [21]. This procedure implies an algorithm that identifies a stabilizer state. With this algorithm, given a stabilizer state $|\phi\rangle$, it is possible to give a full description of the state $|\phi\rangle$ given $O(n)$ copies of $|\phi\rangle$. This was, to our knowledge, the first time Bell sampling had been used to design a stabilizer testing algorithm.

Gross, Nezami and Walter proved in 2021 that Bell sampling can be used for one-sided testing of stabilizer states [22]. In this procedure, we are given many copies of a state $|\psi\rangle$, with the promise that either (1) $|\psi\rangle$ is a stabilizer state, or (2) any stabilizer state $|\phi\rangle$ has inner product $|\langle\psi|\phi\rangle|^2 < \epsilon_2$. The task at hand is to determine which is the case.

Our result enables a tolerant testing algorithm that tests whether or not a given quantum state is close in inner product to a stabilizer [5]. In the tolerant testing framework, we are given a state $|\psi\rangle$, and $1 \geq \epsilon_1 > \epsilon_2 > 0$ with the promise that either (1) there is a stabilizer state $|\phi\rangle$ for which $|\langle\phi|\psi\rangle|^2$ is larger than some ϵ_1, or there is no stabilizer state for which $|\langle\phi|\psi\rangle|^2$ is larger than ϵ_2. Our task is to find out whether (1) or (2) is the case. Using Theorem 1.2.5, we can design a tester that works for $\epsilon_2 = \epsilon_1^C$ for some constant C.

Theorem 1.2.5 was first conjectured by Arunachalam and Dutt [15, version 2] in august of 2024. It was proven by Bao, Helsen and van Dordrecht in October of 2024 [5]. The latter was accepted to STOC 2025 (Symposium on the Theory Of Computing) Later, Arunachalam and Dutt, toghether with Bravyi, produced their own proof [15, version 3].

The proof in [5] relied on the Lovász theta number as well as the Balog-Szemerédi-Gowers theorem and the Polynomial Freĭman-Ruzsa theorem. The proof in this thesis, aside from the Balog-Szemerédi-Gowers theorem and the Polynomial Freĭman-Ruzsa theorem, only relies on some basic facts from linear algebra and representation theory of finite groups. It is our hope that a self-contained version of the proof, as given in this thesis, will lead the way to a U^4 version of Theorem 1.2.5. Further, our current proof also covers the case where p is any uneven prime, whereas [5] only shows Theorem 1.2.5 for $p = 2$.

1.4 Outline of the thesis

The rest of this thesis contains the proof of Theorem 1.2.5.

In chapter 2 we give some definitions and basic results about higher order Fourier analysis. Here we formally define the Gowers U^3-norm and prove some properties about it.

In chapter 3 we will define a set $X \subseteq \mathbb{F}_p^{2n}$ based on a function $f : \mathbb{F}_p^n \to \mathbb{C}$ with high Gowers U^3-norm. This set will have high energy, which is a concept from addtivie combinatorics, that captures, in some sense, the linearity of X.

In chapter 4 we will use two theorems from additive combinatorics to turn X into a

subspace $V \subseteq \mathbb{F}_p^{2n}$. Notably, we need the recent breakthrough result by Green, Gowers, Manners and Tao [3, 4], which enables the polynomial dependence on ϵ in Theorem 1.2.5.

In chapters 5, 6 and 7 we take V as given and obtain a *Lagrangian* subspace of $\mathbb{F}_p^{2n}$.

In chapter 8, we use this Lagrangian subspace L to prove that f has high correlation with a stabilizer state. Finally, in chapter 9 we put everything together, and give a proof of Theorem 1.2.5.

In chapter 10 we explain the tolerant testing result and give some more context from quantum computing.

1.5 Acknowledgements

I thank Jop Briët and Jeroen Zuiddam for their supervision and guidance. I thank Jonas Helsen and Zongbo Bao for the fruitful discussions and collaboration on stabilizer testing. I also wish to thank Josse ten Barge for being there for me in ways big and small.

2 Higher order Fourier analysis

In this chapter, we give a brief overview of the basic Fourier-analytic facts we will need in this thesis. We will deviate slightly from the usual definitions of the characters and Gowers uniformity norms in order to minimize the number of normalization constants floating around.

For $x, y \in \mathbb{F}_p^n$, we will denote the inner product over $\mathbb{F}_p$ by $\langle x, y\rangle = \sum_{i=1}^d x_i y_i$. For $x, y \in \mathbb{C}^d$, we will denote the inner product over complex vector spaces also by $\langle x, y\rangle = \sum_{i=1}^d x_i \overline{y_i}$. It will always be clear from context which of the two we mean. For p a prime, we will write $\omega_p = e^{2\pi i/p}$.

2.1 Basic Fourier analytic facts

For $a \in \mathbb{F}_p^n$, we will define the character function $\chi_a : \mathbb{F}_p^n \to \mathbb{C}$ as

$$\chi_a(x) = \frac{1}{\sqrt{p^n}} \omega_p^{\langle x,a\rangle}. \tag{2.1}$$

Let $\widehat{\mathbb{F}_p^n} = \{\chi_a : a \in \mathbb{F}_p^n\}$. This is a group with the pointwise multiplication operation.

$$(\chi_a \cdot \chi_b)(x) = \sqrt{p^n}\chi_a(x)\chi_b(x). \tag{2.2}$$

The map $\tau : \mathbb{F}_p^n \to \widehat{\mathbb{F}_p^n} : a \mapsto \chi_a$ is an isomorphism of groups:

Proposition 2.1.1. *For $a, b \in \mathbb{F}_p^n$, we have $\chi_a \cdot \chi_b = \chi_{a+b}$.*

Proof.

$$(\chi_a \cdot \chi_b)(x) = \sqrt{p^n}\chi_a(x)\chi_b(x) = \frac{1}{\sqrt{p^n}}\omega_p^{\langle a,x\rangle}\omega_p^{\langle b,x\rangle} = \frac{1}{\sqrt{p^n}}\omega_p^{\langle a+b,x\rangle} \tag{2.3}$$

$$= \chi_{a+b}(x) \tag{2.4}$$

□

Proposition 2.1.2. *For $a, x, y \in \mathbb{F}_p^n$, we have*

$$\chi_a(x+y) = \sqrt{p^n}\chi_a(x)\chi_a(y). \tag{2.5}$$

Proof.

$$\chi_a(x+y) = \frac{1}{\sqrt{p^n}}\omega_p^{\langle x+y,a\rangle} = \frac{1}{\sqrt{p^n}}\omega_p^{\langle x,a\rangle}\omega_p^{\langle y,a\rangle} = \sqrt{p^n}\chi_a(x)\chi_a(y) \tag{2.6}$$

□

Definition 2.1.3 (Fourier transform)**.** For $f : \mathbb{F}_p^n \to \mathbb{C}$ a function, define the Fourier transform $\widehat{f} : \widehat{\mathbb{F}_p^n} \to \mathbb{C}$ as

$$\widehat{f}(\chi) = \sum_{x \in \mathbb{F}_p^n} f(x)\overline{\chi(x)} \tag{2.7}$$

The characters satisfy the following very useful identity:

Proposition 2.1.4. *For $\chi_a \in \widehat{\mathbb{F}_p^n}$,*

$$\sum_{x \in \mathbb{F}_p^n} \chi_a(x) = \sqrt{p^n} \cdot \mathbb{1}[a = 0]. \tag{2.8}$$

Proof. First we assume $a = 0$. Then $\chi_a(x) = \frac{1}{\sqrt{p^n}}$, so $\sum_{x \in \mathbb{F}_p^n} \chi_a(x) = \sqrt{p^n}$. If $a \neq 0$, then there exists an $i \in [n]$ such that $a_i = 1$. Let $y \in \mathbb{F}_p^n$ be defined as $y_i = \mathbb{1}[i = j]$. Then $\chi_a(y) = -1$. On the other hand, by Proposition 2.1.2,

$$\chi_a(y) \sum_{x \in \mathbb{F}_p^n} \chi_a(x) = \frac{1}{\sqrt{p^n}} \sum_{x \in \mathbb{F}_p^n} \chi_a(x + y) = \frac{1}{\sqrt{p^n}} \sum_{x \in \mathbb{F}_p^n} \chi_a(x) \tag{2.9}$$

which implies that $\sum_{x \in \mathbb{F}_p^n} \chi_a(x) = 0$ □

There is a more general version of Proposition 2.1.4 which can be proved in the same way. For any subset $V \subseteq \mathbb{F}_p^n$, let $V^\perp = \{x \in \mathbb{F}_p^n : \langle x, y \rangle = 0 \text{ for all } y \in V\}$. Then,

Proposition 2.1.5. *Let $V \subseteq \mathbb{F}_p^n$ be a subspace of $\mathbb{F}_p^n$, and $a \in \mathbb{F}_p^n$. Then,*

$$\sum_{x \in V} \omega_p^{\langle x,a \rangle} = |V| \cdot \mathbb{1}[a \in V^\perp] \tag{2.10}$$

Proof. If $a \in V^\perp$, then $\omega_p^{\langle a,x \rangle} = 1$ for all $x \in V$, so (2.10) holds.

Next, assume that $a \notin V^\perp$. Then there exists $y \in V$ such that $\langle a, y \rangle \neq 0$, so $\omega_p^{\langle a,y \rangle} \neq 1$. Then,

$$\omega_p^{\langle y,a \rangle} \left(\sum_{x \in V} \omega_p^{\langle x,a \rangle} \right) = \sum_{x \in V} \omega_p^{\langle x+y,a \rangle} = \sum_{x \in V} \omega_p^{\langle x,a \rangle}. \tag{2.11}$$

Therefore, $\sum_{x \in V} \omega_p^{\langle x,a \rangle} = 0$. □

Since $\mathbb{F}_p^n \cong \widehat{\mathbb{F}_p^n}$ as groups, for $a \in \mathbb{F}_p^n$ we will write $\widehat{f}(a)$ to denote $\widehat{f}(\chi_a)$.

Proposition 2.1.6 (Parseval)**.** *Let $f : \mathbb{F}_p^n \to \mathbb{C}$. Then $||f||_2^2 = \sum_{\chi \in \widehat{\mathbb{F}_p^n}} |\widehat{f}(\chi)|^2$.*

Proof. Starting from the right hand side, we get

$$\sum_{a\in\mathbb{F}_p^n} |\widehat{f}(a)|^2 = \sum_{a\in\mathbb{F}_p^n} \left| \sum_{x\in\mathbb{F}_p^n} \frac{1}{\sqrt{p^n}} f(x)\omega_p^{\langle a,x\rangle} \right|^2 \tag{2.12}$$

$$= \frac{1}{p^n} \sum_{a\in\mathbb{F}_p^n} \sum_{x,y\in\mathbb{F}_p^n} f(x)\overline{f(y)}\omega_p^{\langle a,x-y\rangle} \tag{2.13}$$

$$= \frac{1}{p^n} \sum_{x,y\in\mathbb{F}_p^n} f(x)\overline{f(y)}p^n \mathbb{1}[x-y=0] \tag{2.14}$$

$$= \sum_{x\in\mathbb{F}_p^n} |f(x)|^2 \tag{2.15}$$

using Proposition 2.1.4 in the third equality. □

Proposition 2.1.7. *The group of characters, when viewed as a set of complex vectors, is an orthonormal basis for* $\mathbb{C}^{p^n}$.

Proof.

$$\langle \chi_a, \chi_b \rangle = \sum_{x\in\mathbb{F}_p^n} \chi_a(x)\overline{\chi_b(x)} = \sum_{x\in\mathbb{F}_p^n} \frac{1}{\sqrt{p^n}} \chi_{a-b}(x) = \mathbb{1}[a-b=0] \tag{2.16}$$

and $a - b = 0$ if and only if $a = b$. □

We can also define the characters of a subspace $S \subseteq \mathbb{F}_p^n$. Suppose that $\{s_1, \ldots, s_r\}$ is a basis for S. Let $B : S \to \mathbb{F}_p^r$ be the matrix that acts as

$$B : \sum_{i=1}^{r} \alpha_i s_i \mapsto \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_r \end{pmatrix} \tag{2.17}$$

For any $a \in \mathbb{F}_p^k$, the character χ_a is given by

$$\chi_a(x) = \frac{1}{\sqrt{|S|}} \omega_p^{\langle a, Bx\rangle} = \omega_p^{\langle B^T a, x\rangle} \tag{2.18}$$

Then we define the character group as $\widehat{S} = \{\chi_a : a \in \mathrm{im}(B^T)\}$.

We define the Fourier transform of a function $f : S \to \mathbb{C}$ as

$$\widehat{f}(\chi) = \sum_{x\in S} f(x)\overline{\chi(x)} \tag{2.19}$$

Proposition 2.1.8 (Parseval, again)**.** *Let S be a subspace of $\mathbb{F}_p^n$. Let $f : S \to \mathbb{C}$ be a function. Then,*

$$||f||_2^2 = \sum_{\chi \in \widehat{S}} |\widehat{f}(\chi)|^2 \tag{2.20}$$

Proof. Starting from the right hand side, letting B be defined as above,

$$\sum_{a \in \mathrm{im}(B^T)} |\widehat{f}(a)|^2 = \sum_{a \in \mathbb{F}_p^r} \left| \sum_{x \in S} \frac{1}{\sqrt{|S|}} f(x) \omega_p^{\langle B^T a, x \rangle} \right|^2 \tag{2.21}$$

$$= \sum_{a \in \mathbb{F}_p^r} \left| \sum_{x \in S} \frac{1}{\sqrt{|S|}} f(x) \omega_p^{\langle a, Bx \rangle} \right|^2 \tag{2.22}$$

$$= \frac{1}{|S|} \sum_{a \in \mathbb{F}_p^r} \sum_{x,y \in S} f(x) \overline{f(y)} \omega_p^{\langle a, B(x-y) \rangle} \tag{2.23}$$

$$= \frac{1}{|S|} \sum_{x,y \in S} f(x) \overline{f(y)} |S| \mathbb{1}[B(x-y) = 0] \tag{2.24}$$

$$= \sum_{x \in \mathbb{F}_p^n} |f(x)|^2 \tag{2.25}$$

using Proposition 2.1.4 in the third equality. □

2.2 Uniformity norms

Definition 2.2.1. Let $f : \mathbb{F}_p^n \to \mathbb{C}$ be a function. We define the multiplicative derivative of f in the direction h as

$$\Delta_h f(x) = \overline{f(x)} f(x+h). \tag{2.26}$$

Definition 2.2.2. Let G be a subspace of $\mathbb{F}_p^n$. We define the second and third Gowers uniformity norms as follows:

$$||f||_{U^2(G)} = \left(\sum_{h_1, h_2, x \in G} \Delta_{h_1} \Delta_{h_2} f(x) \right)^{1/4} \tag{2.27}$$

$$||f||_{U^3(G)} = \left(\sum_{h_1, h_2, h_3, x \in G} \Delta_{h_1} \Delta_{h_2} \Delta_{h_3} f(x) \right)^{1/8}. \tag{2.28}$$

In the case where $G = \mathbb{F}_p^n$, we will leave out the dependency on G and we will denote $||f||_{U^k(G)}$ by $||f||_{U^k}$.

Proposition 2.2.3. *If $f : \mathbb{F}_p^n \to \mathbb{C}$ is a function with $||f||_2 = 1$, then*

$$\sum_{h,a \in \mathbb{F}_p^n} |\widehat{\Delta_h f}(a)|^2 = 1. \tag{2.29}$$

Also, for all $(h, a) \in \mathbb{F}_p^{2n}$, $|\widehat{\Delta_h f}(a)|^2 \leq \frac{1}{p^n}$.

Proof. By Parseval's identity, Proposition 2.1.6,

$$\begin{aligned}
\sum_{h,a \in \mathbb{F}_p^n} |\widehat{\Delta_h f}(a)|^2 &= \sum_{x,h \in \mathbb{F}_p^n} |\Delta_h f(x)|^2 && (2.30)\\
&= \sum_{x,h \in \mathbb{F}_p^n} |f(x)|^2 |f(x+h)|^2 && (2.31)\\
&= \sum_{x \in \mathbb{F}_p^n} |f(x)|^2 \left(\sum_{h \in \mathbb{F}_p^n} |f(x+h)|^2 \right) && (2.32)\\
&= ||f||_2^4. && (2.33)
\end{aligned}$$

For the second property, we note that

$$|\widehat{\Delta_h f}(a)|^2 = \frac{1}{p^n} \left| \sum_{x \in \mathbb{F}_p^n} \Delta_h f(x) \omega_p^{\langle x,a \rangle} \right|^2 \tag{2.34}$$

By the triangle inequality and Cauchy-Schwarz,

$$\begin{aligned}
\left| \sum_{x \in \mathbb{F}_p^n} \Delta_h f(x) \omega_p^{\langle x,a \rangle} \right| &\leq \sum_{x \in \mathbb{F}_p^n} |\Delta_h f(x)| \cdot |\omega_p^{\langle x,a \rangle}| && (2.35)\\
&= \sum_{x \in \mathbb{F}_p^n} |\Delta_h f(x)| && (2.36)\\
&= \sum_{x \in \mathbb{F}_p^n} |f(x)| \cdot |f(x+h)| && (2.37)\\
&\leq \left(\sum_{x \in \mathbb{F}_p^n} |f(x)|^2 \right)^{1/2} \cdot \left(\sum_{x \in \mathbb{F}_p^n} |f(x+h)|^2 \right)^{1/2} && (2.38)\\
&= 1 && (2.39)
\end{aligned}$$

and the result follows. □

The following lemma is standard in higher order Fourier analysis and gives us a simple form for the second Gowers uniformity norm.

Lemma 2.2.4. *Let $f : G \to \mathbb{C}$ be a function defined on a subspace $G \subseteq \mathbb{F}_p^n$. Then,*

$$||f||_{U^2(G)}^4 = |G| \sum_{x \in G} |\widehat{f}(x)|^4 \tag{2.40}$$

Proof. Beginning from the left hand side of (2.40), we get

$$\begin{aligned}
||f||_{U^2}^4 &= \sum_{h_1,h_2,x \in G} \Delta_{h_1}\Delta_{h_2} f(x) && (2.41)\\
&= \sum_{h_1,h_2,x \in G} \overline{\Delta_{h_2} f(x)} \Delta_{h_2} f(x+h_1) && (2.42)\\
&= \sum_{h_1,h_2,x \in G} f(x)\overline{f(x+h_1)f(x+h_2)} f(x+h_1+h_2) && (2.43)\\
&= \sum_{a,b,c,d \in G : d=-a+b+c} f(a)\overline{f(b)f(c)} f(d) && (2.44)
\end{aligned}$$

From the right hand side of (2.40) we get

$$\begin{aligned}
|G| \sum_{x \in G} |\widehat{f}(x)|^4 &= |G| \sum_{x \in G} \left| \sum_{a \in G} f(a) \frac{1}{p^{n/2}} \omega_p^{\langle a,x \rangle} \right|^4 && (2.45)\\
&= |G| \sum_{x \in G} \sum_{a,b,c,d \in G} f(a)\overline{f(b)f(c)} f(d) \frac{1}{|G|^2} \omega_p^{\langle a-b-c+d,x \rangle} && (2.46)\\
&= |G| \sum_{a,b,c,d \in G} f(a)\overline{f(b)f(c)} f(d) \frac{1}{|G|^2} |G| \mathbb{1}[a-b-c+d=0] && (2.47)\\
& && (2.48)
\end{aligned}$$

which is equal to (2.44). □

Proposition 2.2.5. *The Gowers norms satisfy the relation*

$$||f||_{U^3(G)}^8 = \sum_{h \in G} ||\Delta_h f||_{U^2(G)}^4. \tag{2.49}$$

Proof. We have

$$\begin{aligned}
||f||_{U^3(G)}^8 &= \sum_{h_1,h_2,h_3,x \in G} \Delta_{h_1}\Delta_{h_2}\Delta_{h_3} f(x) && (2.50)\\
&= \sum_{h_3 \in G} \sum_{x,h_1,h_2 \in G} \Delta_{h_1}\Delta_{h_2}(\Delta_{h_3} f)(x) && (2.51)\\
&= \sum_{h_3 \in G} ||\Delta_{h_3} f||_{U^2(G)}^4. && (2.52)
\end{aligned}$$

□

We are now ready to prove that the third Gowers uniformity norm is bounded by $||f||_2$:

Proposition 2.2.6. *Let $f : \mathbb{F}_p^n \to \mathbb{C}$ satisfy $||f||_2 = 1$. Then*

$$||f||_{U^3} \leq 1. \tag{2.53}$$

Proof. By Lemma 2.2.4 and Proposition 2.2.5, $||f||_{U^3}^8 = p^n \sum_{h,a} |\widehat{\Delta_h f}(a)|^4$ and by Proposition 2.2.3,

$$\sum_{h,a} |\widehat{\Delta_h f}(a)|^4 \leq \frac{1}{p^n} \sum_{h,a} |\widehat{\Delta_h f}(a)|^2 = \frac{1}{p^n}. \tag{2.54}$$

□

Definition 2.2.7. We define the set $\mathcal{S}$ as

$$\mathcal{S} = \{f : \mathbb{F}_p^n \to \mathbb{C} \text{ such that } ||f||_2 = 1, ||f||_{U^3} = 1\}. \tag{2.55}$$

Arunachulam and Dutt identify $\mathcal{S}$ with the set of stabilizer states [15, Theorem 3.4]. Dehaene, De Moor and Hostens showed that the stabilizer states ahve a specific form [23, 24]. Their result is the content of the following propositions.

Proposition 2.2.8. *Let $f : \mathbb{F}_2^n \to \mathbb{C}$ be a function with $||f||_2 = 1$. Then $f \in \mathcal{S}$ if and only if there exist a degree 1 polynomial $\ell \in \mathbb{F}_2[x_1, \ldots, x_n]$ and a degree 2 polynomial $q \in \mathbb{F}_2[x_1, \ldots, x_n]$, and an affine subspace $S \subseteq \mathbb{F}_2^n$ such that for all $x \in \mathbb{F}_2^n$,*

$$f(x) = \frac{1}{\sqrt{|S|}} i^{\ell(x)} (-1)^{q(x)} \mathbb{1}[x \in S]. \tag{2.56}$$

A similar thing holds for p uneven:

Proposition 2.2.9. *Let $f : \mathbb{F}_p^n \to \mathbb{C}$ be a function with $||f||_2 = 1$. Then $f \in \mathcal{S}$ if and only if there exist a degree 1 polynomial $l \in \mathbb{F}_p[x_1, \ldots, x_n]$ and a degree 2 polynomial $q \in \mathbb{F}_p[x_1, \ldots, x_n]$, and an affine subspace $S \subseteq \mathbb{F}_p^n$ such that for all $x \in \mathbb{F}_p^n$,*

$$f(x) = \frac{1}{\sqrt{|S|}} \omega_p^{q(x)} \mathbb{1}[x \in S]. \tag{2.57}$$

3 From a high U^3-norm to a high energy set

We start this section with $f : \mathbb{F}_p^n \to \mathbb{C}$, with $||f||_{U^3} \geq \epsilon$ for some $\epsilon > 0$ and $||f||_2 = 1$. Based on this function, we will define a set $X \subseteq \mathbb{F}_p^{2n}$ containing all $(h, a) \in \mathbb{F}_p^{2n}$ for which $|\widehat{\Delta_h f}(a)|^2$ is high. We will give a simple argument to show that the size of X is $\Theta(p^n)$, with constants dependent on ϵ. Then we will define a property of a set called the *energy*, which captures, in some sense, the linearity of the set. Finally, we calculate a lower bound for the energy of X. The argument giving the lower bound for the energy is due to Green (see [25]), we only make some minor modifications.

3.1 The set X and its size

Let $f : \mathbb{F}_p^n \to \mathbb{C}$ satisfy $||f||_{U^3} \geq \epsilon$ and $||f||_2 = 1$. Define

$$X = \{(h, a) \in \mathbb{F}_p^n \times \mathbb{F}_p^n : |\widehat{\Delta_h f}(a)|^2 \geq \frac{1}{5}\epsilon^{24}/p^n\}. \tag{3.1}$$

First, we prove that the size of X satisfies $\text{poly}(\frac{1}{\epsilon})p^n \leq |X| \leq \text{poly}(\epsilon)p^n$. For this we need the following lemma:

Lemma 3.1.1 (Markov's inequality)**.** *Let Y be a random variable with $|Y| \leq 1$, and let $c > 0$ be some constant. Suppose that $\mathbb{E}|Y| \geq \delta$. Then*

$$\mathbb{P}(|Y| \geq c\delta) \geq (1 - c)\delta \tag{3.2}$$

Proof. The random variable $|Y|$ can be upper bounded by

$$|Y| \leq c\delta + \mathbb{1}[|Y| \geq c\delta] \tag{3.3}$$

Taking expectations on both sides yields

$$\delta \leq \mathbb{E}|Y| \leq c\delta + \mathbb{P}(|Y| \geq c\delta) \tag{3.4}$$

and the result follows. □

Proposition 3.1.2. *The size of X is bounded from below by $|X| \geq \frac{4}{5}\epsilon^8 p^n$ and from above by $|X| \leq \frac{p^n}{\epsilon^{24}\frac{1}{5}}$*

Proof. The upper bound follows from Proposition 2.2.3 in the following way:

$$1 \geq \sum_{(h,a)\in X} |\widehat{\Delta_h f}(a)|^2 \geq |X|\frac{1}{5}\epsilon^{24}/p^n, \tag{3.5}$$

so therefore $|X| \leq \frac{p^n}{\frac{1}{5}\epsilon^{24}}$.

The lower bound is due to Markov's inequality (Lemma 3.1.1): Let Y have the following distribution: $Y = p^n|\widehat{\Delta_h f}(a)|^2$ with probability $|\widehat{\Delta_h f}(a)|^2$. Then

$$\mathbb{E}Y = p^n \sum_{h,a} |\widehat{\Delta_h f}(a)|^4 = ||f||_{U^3}^8 = \epsilon^8 \tag{3.6}$$

by Lemma 2.2.4 and Proposition 2.2.5. Therefore, by Lemma 3.1.1 with $c = \frac{1}{5}$ and $\delta = \epsilon^8$,

$$\frac{4}{5}\epsilon^8 \leq \mathbb{P}(Y \geq \frac{1}{5}\epsilon^8). \tag{3.7}$$

Since $\epsilon \leq 1$ by Proposition 2.2.6, we can upper bound

$$\mathbb{P}(Y \geq \frac{1}{5}\epsilon^8) \leq \mathbb{P}(Y \geq \frac{1}{5}\epsilon^{24}). \tag{3.8}$$

By definition, $(h,a) \in X$ if and only if $|\widehat{\Delta_h f}(a)|^2 \geq \frac{1}{5}\epsilon^{24}/p^n$ if and only if $Y \geq \frac{1}{5}\epsilon^{24}$.

$$\mathbb{P}(Y \geq \frac{1}{5}\epsilon^{24}) = \mathbb{P}(X) = \sum_{(h,a)\in X} |\widehat{\Delta_h f}(a)|^2. \tag{3.9}$$

By Proposition 2.2.3,

$$\sum_{(h,a)\in X} |\widehat{\Delta_h f}(a)|^2 \leq |X|\frac{1}{p^n}. \tag{3.10}$$

In summary, we get

$$\frac{4}{5}\epsilon^8 p^n \leq |X|. \tag{3.11}$$

□

3.2 The energy of X

Definition 3.2.1 (The energy of a set)**.** Let $X \subseteq \mathbb{F}_p^n$. An additive quadruple of X is a tuple $(a,b,c,d) \in X^4$ such that $a+b=c+d$. The energy $E(X)$ is defined as the number of additive quadruples of X.

Lemma 3.2.2. *Let $f : \mathbb{F}_p^n \to \mathbb{C}$ satisfy $||f||_{U^3} \geq \epsilon$ and $||f||_2 = 1$. Then the set*

$$X = \{(h, a) \in \mathbb{F}_p^n \times \mathbb{F}_p^n : |\widehat{\Delta_h f}(a)|^2 \geq \frac{1}{5}\epsilon^{24}/p^n\} \tag{3.12}$$

satisfies $E(X) \geq \frac{1}{5^4}\epsilon^{96}|X|^3$.

In order to prove Lemma 3.2.2, we need the following lemma by Samorodnitsky, see [25, Proposition 2.4].

Lemma 3.2.3 (Samorodnitsky)**.** *For any function $f : \mathbb{F}_p^n \to \mathbb{C}$,*

$$\sum_{\substack{h_1+h_2=h_3+h_4 \\ a_1+a_2=a_3+a_4}} |\widehat{\Delta_{h_1} f}(a_1)|^2|\widehat{\Delta_{h_2} f}(a_2)|^2|\widehat{\Delta_{h_3} f}(a_3)|^2|\widehat{\Delta_{h_4} f}(a_4)|^2 = p^{2n}\sum_{h\in\mathbb{F}_p^n} ||\widehat{\Delta_h f}||_8^8. \tag{3.13}$$

We will also need the following version of Hölder's inequality (see for example [26]):

Lemma 3.2.4 (Hölder's inequality, special version)**.** *Whenever $f, g : \mathbb{F}_p^n \to \mathbb{C}$, we have that*

$$\sum_{x\in\mathbb{F}_p^n} |f(x)g(x)| \leq \left(\sum_{x\in\mathbb{F}_p^n} |f(x)|^{3/2}\right)^{2/3}\left(\sum_{x\in\mathbb{F}_p^n} |g(x)|^3\right)^{1/3}. \tag{3.14}$$

Lemma 3.2.5. *Let $f : \mathbb{F}_p^n \to \mathbb{C}$ with $||f||_2 = 1$. Then,*

$$\sum_{\substack{h_1+h_2=h_3+h_4 \\ a_1+a_2=a_3+a_4}} |\widehat{\Delta_{h_1} f}(a_1)|^2|\widehat{\Delta_{h_2} f}(a_2)|^2|\widehat{\Delta_{h_3} f}(a_3)|^2|\widehat{\Delta_{h_4} f}(a_4)|^2 \geq \frac{1}{p^n}||f||_{U^3}^{24}. \tag{3.15}$$

Proof. By Lemma 3.2.3, we only need to show that

$$p^{2n}\sum_{h\in\mathbb{F}_p^n} ||\widehat{\Delta_h f}||_8^8 \geq \frac{1}{p^n}||f||_{U^3}^{24}. \tag{3.16}$$

By lemmas 2.2.4 and 2.2.5, we have

$$\frac{1}{p^n}||f||_{U^3}^8 = \sum_h ||\widehat{\Delta_h f}||_4^4. \tag{3.17}$$

We apply Hölder's inequality (Lemma 3.2.4) to $||\widehat{\Delta_h f}||_4^4$:

$$||\widehat{\Delta_h f}||_4^4 = \sum_x |\widehat{\Delta_h f}(x)|^{\frac{4}{3}+\frac{8}{3}} \tag{3.18}$$

$$\leq \left(\sum_x |\widehat{\Delta_h f}(x)|^{\frac{4}{3}\frac{3}{2}}\right)^{2/3}\left(\sum_x |\widehat{\Delta_h f}(x)|^{\frac{8}{3}3}\right)^{1/3} \tag{3.19}$$

$$= \left(||\widehat{\Delta_h f}||_2^2\right)^{2/3}\left(||\widehat{\Delta_h f}||_8^8\right)^{1/3} \tag{3.20}$$

$$= ||\widehat{\Delta_h f}||_2^{4/3}||\widehat{\Delta_h f}||_8^{8/3}. \tag{3.21}$$

Using the inequality we just found, we can apply Hölder again:

$$\sum_h ||\widehat{\Delta_h f}||_4^4 \leq \sum_h ||\widehat{\Delta_h f}||_2^{4/3} ||\widehat{\Delta_h f}||_8^{8/3} \tag{3.22}$$

$$\leq \left(\sum_h ||\widehat{\Delta_h f}||_2^{\frac{4}{3}\frac{3}{2}}\right)^{2/3} \left(\sum_h ||\widehat{\Delta_h f}||_8^{\frac{8}{3}3}\right)^{1/3} \tag{3.23}$$

$$= \left(\sum_h ||\widehat{\Delta_h f}||_2^2\right)^{2/3} \left(\sum_h ||\widehat{\Delta_h f}||_8^8\right)^{1/3} \tag{3.24}$$

$$= \left(\sum_h ||\widehat{\Delta_h f}||_8^8\right)^{1/3}, \tag{3.25}$$

where in the last step we use that $\sum_h ||\widehat{\Delta_h f}||_2^2 = 1$ by Proposition 2.2.3.

In summary, we have found that

$$\frac{1}{p^n}||f||_{U^3}^8 \leq \left(\sum_h ||\widehat{\Delta_h f}||_8^8\right)^{1/3} \tag{3.26}$$

and equation (3.16) follows by taking third powers on both sides. □

of Lemma 3.2.2. We start by noting that

$$\sum_{\substack{h_1+h_2=h_3+h_4\\ a_1+a_2=a_3+a_4\\ (a_1,h_1)\notin X}} |\widehat{\Delta_{h_1}} f(a_1)|^2 \cdots |\widehat{\Delta_{h_4}} f(a_4)|^2 \leq \sum_{\substack{h_1+h_2=h_3+h_4\\ a_1+a_2=a_3+a_4\\ (a_1,h_1)\notin X}} \frac{1}{5}\epsilon^{24}\frac{1}{p^n}|\widehat{\Delta_{h_2}} f(a_2)|^2 \cdots |\widehat{\Delta_{h_4}} f(a_4)|^2 \tag{3.27}$$

$$\leq \sum_{\substack{h_1+h_2=h_3+h_4\\ a_1+a_2=a_3+a_4}} \frac{1}{5}\epsilon^{24}\frac{1}{p^n}|\widehat{\Delta_{h_2}} f(a_2)|^2 \cdots |\widehat{\Delta_{h_4}} f(a_4)|^2 \tag{3.28}$$

$$= \sum_{\substack{h_1,h_2,h_3\\ a_1,a_2,a_3}} \frac{1}{5}\epsilon^{24}\frac{1}{p^n}|\widehat{\Delta_{h_2}} f(a_2)|^2 \cdots |\widehat{\Delta_{h_4}} f(a_4)|^2 \tag{3.29}$$

$$= \frac{1}{5}\epsilon^{24}\frac{1}{p^n}\left(\sum_{a,h} |\widehat{\Delta_h} f(a)|^2\right)^3 \tag{3.30}$$

$$= \frac{1}{5}\epsilon^{24}\frac{1}{p^n}, \tag{3.31}$$

where the last equality follows from Proposition 2.2.3.

Similarly, for $i \in \{2,3,4\}$,

$$\sum_{\substack{h_1+h_2=h_3+h_4\\ a_1+a_2=a_3+a_4\\ (a_i,h_i)\notin X}} |\widehat{\Delta_{h_1}} f(a_1)|^2 \cdots |\widehat{\Delta_{h_4}} f(a_4)|^2 \leq \frac{1}{5}\epsilon^{24}\frac{1}{p^n}. \tag{3.32}$$

Next, we note that

$$\sum_{\substack{h_1+h_2=h_3+h_4\\ a_1+a_2=a_3+a_4\\ (a_1,h_1),\ldots,(a_4,h_4)\in X}} |\widehat{\Delta_{h_1}} f(a_1)|^2 \cdots |\widehat{\Delta_{h_4}} f(a_4)|^2 \tag{3.33}$$

$$\geq \sum_{\substack{h_1+h_2=h_3+h_4\\ a_1+a_2=a_3+a_4}} |\widehat{\Delta_{h_1}} f(a_1)|^2 \cdots |\widehat{\Delta_{h_4}} f(a_4)|^2 \tag{3.34}$$

$$- \sum_{i\in\{1,2,3,4\}} \sum_{\substack{h_1+h_2=h_3+h_4\\ a_1+a_2=a_3+a_4\\ (a_i,h_i)\notin X}} |\widehat{\Delta_{h_1}} f(a_1)|^2 \cdots |\widehat{\Delta_{h_4}} f(a_4)|^2 \tag{3.35}$$

$$\geq \epsilon^{24}/p^n - 4\frac{1}{5}\epsilon^{24}/p^n. \tag{3.36}$$

by equation (3.32) and Lemma 3.2.5.

Finally, the engergy of X is equal to

$$E(X) = \sum_{\substack{h_1+h_2=h_3+h_4\\ a_1+a_2=a_3+a_4\\ (a_1,h_1),\ldots,(a_4,h_4)\in X}} 1 \geq p^{4n} \sum_{\substack{h_1+h_2=h_3+h_4\\ a_1+a_2=a_3+a_4\\ (a_1,h_1),\ldots,(a_4,h_4)\in X}} |\widehat{\Delta_{h_1}} f(a_1)|^2 \cdots |\widehat{\Delta_{h_4}} f(a_4)|^2 \tag{3.37}$$

$$\geq p^{3n}\frac{1}{5}\epsilon^{24}. \tag{3.38}$$

And since $p^n \geq |X|\epsilon^{24}\frac{1}{5}$ by Proposition 3.1.2, we get $E(X) \geq \frac{1}{5}\epsilon^{96}\frac{1}{5}^3|X|^3$. □

4 Balog-Szemerédi-Gowers and Polynomial Freĭman-Ruzsa

Now that we have defined X and shown that it has high energy, we will need to use two results from additive combinatorics known as the Balog-Szemerédi-Gowers theorem and the Polynomial Freĭman-Ruzsa Theorem. We will explain briefly what these theorems mean and then apply them. When we apply the Balog-Szemerédi-Gowers theorem to X, we get a set S. If we apply the Polynomial Freĭman-Ruzsa theorem to S, this will give us a subspace $V \subseteq \mathbb{F}_p^n$. The size of V satisfies $|V| = \Theta(p^n)$ with constants depending on ϵ. Further, V contains a large number of elements of X. Since for all $(h, a) \in X$, $|\widehat{\Delta_h f}(a)|^2$ is high, and V and X have large intersection, $\sum_{(h,a)\in V} |\widehat{\Delta_h f}(a)|^2$ is high.

4.1 Energy and doubling constant

In the previous chapter, we defined the energy of a set $X \subseteq \mathbb{F}_p^n$ as

$$E(X) = |\{(a, b, c, d) \in X^4 : a + b = c + d\}|. \tag{4.1}$$

Note that for every (ordered) pair a, b of distinct elements of X we get two additive quadruples, namely (a, b, a, b) and (a, b, b, a). Together with the $|X|$ additive quadruples of the form (a, a, a, a) this gives us a lower bound of $2|X|^2 - |X| \leq E(X)$.

For an upper bound, we notice that if we fix a, b, c then d is determined to be $c - a - b$. Therefore, there can be at most $E(X) \leq |X|^3$.

Another way of measuring the additive structure in a set is the doubling constant:

Definition 4.1.1 (Doubling constant)**.** Let $X \subseteq \mathbb{F}_p^n$. We define the doubling constant $\Gamma(X)$ of X as

$$\Gamma(X) = \frac{|X + X|}{|X|}. \tag{4.2}$$

It is not hard to prove the following Proposition ([7, 7.13.4]):

Proposition 4.1.2. *Let $X \subseteq \mathbb{F}_p^n$. Then $\frac{E(X)}{|X|^3} \geq \frac{1}{\Gamma(X)}$.*

In words, if the doubling constant of a set is small, the energy must be large. What about the converse? Is it true that if the energy is high, the doubling constant must be small? The short answer is no, as the following example shows:

Example 4.1.3. Let $X = Y \cup Z \subseteq \mathbb{F}_p^{p^n+n}$ where Y is the set of standard basis vectors $Y = \{e_1, \ldots, e_{p^n}\}$ and Z the set of vectors $Z = \{0^{p^n} \times v : v \in \mathbb{F}_p^n\}$. Then the energy of X is at least equal to the energy of $E(Z) = |Z|^3 = p^{3n}$. So $E(X)/|X|^3 \geq \frac{p^{3n}}{(2p^n)^3}$. However, the set $X + X$ contains the set $\{(e_i + e_j) \times 0^n | i, j \in [p^n]\}$, which has size $\binom{p^n}{2}$. Therefore, the doubling constant is at least $\frac{1}{2}(p^n - 1)$.

As the last example shows, there are sets with high energy and arbitrarily large doubling. In this example however, X did have a large subset that has small doubling, namely Z.

As it turns out, this is not a coincidence: a set X with high energy will necessarily contain a fairly large subset with small doubling: this is the content of the Balog-Szemerédi-Gowers Theorem. This theorem was first proven by Balog and Szemerédi in [27], and later improved quantitatively by Gowers [9]. This version is due to Zhao [7].

Theorem 4.1.4 (Balog-Szemerédi-Gowers)**.** *Let X be a subset of $\mathbb{F}_p^{2n}$ with $E(X) \geq \delta |X|^3$. Then there exists a set $S \subseteq X$ such that $|S| \geq \delta^{C_{BSG}} |X|$, such that S has a small doubling constant $\frac{|S+S|}{|S|} \leq \delta^{-C_{BSG}}$ where C_{BSG} depends only on p.*

4.2 Polynomial Freĭman-Ruzsa

The following theorem is a classic result in additive combinatorics. It was first proved by Freĭman [28]. This version is due to Ruzsa and is a finite field version of the result of Freĭman [29].

Theorem 4.2.1 (Freĭman-Ruzsa)**.** *Let $S \subseteq \mathbb{F}_p^n$ have doubling constant $K = \Gamma(S)$. Then there exists an affine subspace W of $\mathbb{F}_p^n$ of size at most $K'|S|$ that contains S, where K' depends only on p and K.*

Corollary 4.2.2. *Let $S \subseteq \mathbb{F}_p^n$ have doubling constant $K = \Gamma(S)$. Then there exists an affine subspace V of $\mathbb{F}_p^n$ of size at most $|V| \leq |S|$ such that S is covered by $K'p$ translates of V.*

Proof. If we apply Theorem 4.2.1 to S, we get an affine subspace W with size $W \leq K'|S|$ that covers S. Let V be a subspace of $\mathbb{F}_p^n$ such that $V + H = W$ for some $H \subseteq \mathbb{F}_p^n$ and $d = \dim V$ is such that $|V| = p^d \leq |S|$ and $p^{d+1} > |S|$. Then $\frac{|S|}{|V|} \leq p$. Then the size of H is equal to $\frac{|W|}{|V|} \leq \frac{K'|S|}{|V|} \leq pK'$. Thus we have that $|H|$ copies of V cover S and $|H| \leq K'p$ □

For a long time, the best known dependence of K' on K was exponential. In [29], Imre Ruzsa states the conjecture that K' is polynomial in K, with exponent depending on p. Ruzsa attributes this conjecture to Marton.

The conjecture was proven by Green, Gowers, Manners and Tao ([3] in the case that $p = 2$, and [4] for p any prime). This is their theorem:

Theorem 4.2.3 (Polynomial Freĭman-Ruzsa)**.** *Let $S \subseteq \mathbb{F}_p^n$ have doubling constant $K = \Gamma(S)$. Then there exists a subspace V of $\mathbb{F}_p^n$, of size at most $|V| \leq |S|$ such that at most $(2K)^{O(p^3)}$ affine cosets of V cover S.*

We can summarize the results of this chapter in the following lemma:

Lemma 4.2.4. *Let $f : \mathbb{F}_p^n \to \mathbb{C}$ be a function with $||f||_2 = 1$ and $||f||_{U^3} \geq \epsilon$. There exists a subspace $V \subseteq \mathbb{F}_p^{2n}$ such that*

1. $\sum_{(h,a)\in V} |\widehat{\Delta_h f}(a)|^2 \geq \text{poly}(\epsilon)$
2. $|V| \leq \text{poly}(\epsilon)p^n$
3. $|V| \geq \text{poly}(\frac{1}{\epsilon})p^n$

Proof. If we first apply Theorem 4.1.4 to X, we get a set $S \subseteq \mathbb{F}_p^n$ with $|X| \geq |S| \geq \text{poly}(\epsilon)|X|$ and $\Gamma(S) \leq \text{poly}(\frac{1}{\epsilon})$.

If we apply Theorem 4.2.3 to S we get a subspace V, such that $(2\Gamma(S))^{O(p^3)} = \text{poly}(\frac{1}{\epsilon})$ affine translates of V cover S. The size of V satisfies $|V| \leq |S| \leq |X| \leq \text{poly}(\frac{1}{\epsilon})p^n$ and $|V| \geq \frac{1}{(2\Gamma(S))^{O(p^3)}}|S| \geq \text{poly}(\epsilon)|X| \geq \text{poly}(\epsilon)p^n$, by Proposition 3.1.2.

Let $Y \subseteq \mathbb{F}_p^{2n}$ be such that $S \subseteq V + Y$, where $|Y| = \text{poly}(\frac{1}{\epsilon})$. There must exist a $y \in Y$ such that $V + y$ contains at least $\frac{|S|}{|Y|}$ elements of X. Thus, using that $|S| \geq \text{poly}(\epsilon)|X|$, and $|Y| \leq \text{poly}(\epsilon^{-1})$, and $|X| \geq \text{poly}(\epsilon)p^n$

$$\sum_{(h,a)\in V+y} |\widehat{\Delta_h f}(a)|^2 \geq \frac{|S|}{|Y|}\frac{1}{5}\epsilon^{24}/p^n \tag{4.3}$$

$$\geq \frac{|X|}{|Y|}\text{poly}(\epsilon)/p^n \tag{4.4}$$

$$\geq \text{poly}(\epsilon). \tag{4.5}$$

By claim 4.13 in [15],

$$\sum_{(h,a)\in V} |\widehat{\Delta_h f}(a)|^2 \geq \sum_{(h,a)\in V+y} |\widehat{\Delta_h f}(a)|^2 \geq \text{poly}(\epsilon). \tag{4.6}$$

□

5 The Darboux basis

In the previous section, we found a subspace V with high weight $\sum_{(h,a)\in V} |\widehat{\Delta_h f}(a)|^2$. Our goal in the upcoming three sections is to find a Lagrangian subspace L such that $\sum_{(h,a)\in L} |\widehat{\Delta_h f}(a)|^2$. A Lagrangian subspace is a subspace $L \subseteq \mathbb{F}_p^{2n}$ such that $\dim L = p^n$ and $[v, w] = 0$ for all $v, w \in L$, where $[v, w]$ denotes the *symplectic inner product*, which we will define below.

In the current section we prove a theorem that gives a nice basis for V, known as the Darboux basis. This basis captures the symplectic structre of V.

5.1 The symplectic inner product

Define the symplectic inner product as follows:

Definition 5.1.1. The symplectic inner product on $\mathbb{F}_p^{2n}$ is the bilinear form defined by the matrix $J \in \mathbb{F}_p^{2n\times 2n}$, $J = \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix} \in \mathbb{F}_p^{2n\times 2n}$ by

$$[x, y] = y^T Jx = \sum_{i=1}^{n} x_i y_{n+1} - \sum_{i=1}^{n} y_i x_{n+1}. \tag{5.1}$$

For the remainder of this chapter, we define the *symplectic orthogonal complement* of a set $X \subseteq \mathbb{F}_p^{2n}$ as

$$X^\perp = \{y \in \mathbb{F}_2^{2n} : [x, y] = 0 \text{ for all } x \in X\}. \tag{5.2}$$

5.2 The structure of symplectic spaces

It turns out that there exists a canonical basis for symplectic spaces that makes them easier to reason about. The following result is taken from [30] and is a standard result in symplectic geometry.

Theorem 5.2.1. *[The Darboux basis] Let V be a subspace of $\mathbb{F}_p^{2n}$. There exist vectors $u_1, \ldots, u_k, v_1, \ldots, v_k, w_1, \ldots, w_m \in \mathbb{F}_p^{2n}$ that form a basis for V such that*

1. $[u_i, u_j] = [v_i, v_j] = 0$
2. $[u_i, v_j] = \delta_{ij}$
3. $w_l \in V \cap V^\perp$

for all $i, j \in [k]$, and for all $l \in [m]$.

A basis $\{u_1, \ldots, u_k, v_1, \ldots, v_k, w_1, \ldots, w_m\}$ with the properties as in Theorem 5.2.1 is known as a *Darboux basis.*

Proof. Let $W \subseteq V$ be the subset of elements that have symplectic inner product zero with all element of V,

$$W := V^{\perp} \cap V. \tag{5.3}$$

Defined in this way, W is a subspace: if $w_1, w_2 \in W$, then for all $x \in V$, $[w_1 + w_2, x] = [w_1, x] + [w_2, x] = 0$, and clearly $w_1 + w_2 \in V$. Let $m = \dim W$.

Let $w_1, \ldots, w_m$ be a basis for W. Let U be the subspace of V such that $V = U \oplus W$. By this definition, U is the subspace of V consisting of all vectors u such that $u = 0$, or there exists at least one v with $[u, v] = 1$. We define our basis inductively:
Suppose that we have defined linearly independent vectors $u_1, \ldots, u_i, v_1, \ldots, v_i$ such that $[v_i, u_j] = \delta_{ij}$ and $[v_i, v_j] = [u_i, u_j] = 0$. We define $U_i := \langle u_1, \ldots, u_i, v_1 \ldots, v_i \rangle$. Our induction hypothesis is that U_i has the following property:

$$U = U_i \oplus (U_i^{\perp} \cap U) \tag{5.4}$$

For the base case $i = 0$, (5.4) holds since $U_0 = \{0\}$ and $U_0^{\perp} \cap U = U$.

Now take u_{i+1} any nonzero vector in $U_i^{\perp} \cap U$. If no such vector exists, then by (5.4), $U = U_i$ and we terminate the process.

Since $u_{i+1} \in U \backslash \{0\}$, there must be a vector $v \in U$ that satisfies $[u_{i+1}, v] = 0$ by the definition of U. Let $v = v' + v''$ where $v' \in U_i$ and $v'' \in U_i^{\perp} \cap U$. Since $[u_{i+1}, v'] = 0$, $[u_{i+1}, v''] = 1$. So we set $v_{i+1} = v''$.

Notice that $[v_{i+1}, v_j] = [v_{i+1}, u_j] = 0$ for all $j \in [i]$, since $u_{i+1}, v_{i+1} \in U_i^{\perp}$. It remains to check property (5.4) for U_{i+1}.

First we prove that $U_{i+1} \cap (U_{i+1}^{\perp} \cap U) = \{0\}$. Let $x \in U_{i+1} \cap U_{i+1}^{\perp}$. Suppose that $x = \sum_{j=1}^{i+1} a_j u_j + b_j v_j$. Then for all $\ell \in [i+1]$,

$$0 = [u_\ell, x] = [u_\ell, \sum_{j=1}^{i+1} a_j u_j + b_j v_j] = \sum_{j=1}^{i+1} a_j [u_\ell, u_j] + \sum_{j=1}^{i+1} b_j [u_\ell, v_j] = b_\ell \tag{5.5}$$

and similarly,

$$0 = [v_\ell, x] = [u_\ell, \sum_{j=1}^{i+1} a_j u_j + b_j v_j] = \sum_{j=1}^{i+1} a_j [v_\ell, u_j] + \sum_{j=1}^{i+1} b_j [v_\ell, v_j] = a_\ell \tag{5.6}$$

hence $x = 0$.

Next we prove $U = U_{i+1} \oplus (U_{i+1}^{\perp} \cap U)$. Let $x \in U$, and let $a_j = [x, u_j], b_j = [x, v_j]$ for $j \in [i+1]$. Then,

$$x = \sum_{j=1}^{i+1} b_j u_j + a_j v_j + x - \left(\sum_{j=1}^{i+1} b_j u_j + a_j v_j \right), \tag{5.7}$$

where $\sum_{j=1}^{i+1} b_j u_j + a_j v_j \in U_{i+1}$, and $x - \left(\sum_{j=1}^{i+1} b_j u_j + a_j v_j\right) \in U_{i+1}^{\perp}$, since for all $\ell \in [i+1]$,

$$\left[u_\ell, x - \left(\sum_{j=1}^{i+1} b_j u_j + a_j v_j\right)\right] = [u_\ell, x] - a_\ell = 0 \tag{5.8}$$

and similarly

$$\left[v_\ell, x - \left(\sum_{j=1}^{i+1} b_j u_j + a_j v_j\right)\right] = [v_\ell, x] - b_\ell = 0 \tag{5.9}$$

Since $U_{i+1} \cap (U_{i+1}^{\perp} \cap U) = \{0\}$ and $U = U_{i+1} + (U_{i+1}^{\perp} \cap U)$, this implies that $U = U_{i+1} \oplus (U_{i+1}^{\perp} \cap U)$. □

Corollary 5.2.2. *Every subspace V of $\mathbb{F}_2^{2n}$ can be decomposed as $V = V' \oplus W$ with $W = V^{\perp} \cap V$.*

Proof. Let $u_1, \ldots, u_k, v_1, \ldots, v_k, w_1, \ldots, w_m$ be a Darboux basis for V. Then let

$$V' = \langle u_1, \ldots, u_k, v_1, \ldots, v_k \rangle, \tag{5.10}$$
$$W = \langle w_1, \ldots, w_m \rangle. \tag{5.11}$$

Then $V = V' \oplus W$ and $W = V \cap V^{\perp}$ □

6 The Stone-von Neumann Theorem for finite fields

In chapter 5, we proved a result about symplectic geometry over finite fields. This allowed us to find a Darboux basis $u_1, \ldots, u_k, v_1, \ldots, v_k, w_1, \ldots, w_m$ for V. In this chapter, we define a set of matrices $g(v,t)$ for $(v,t) \in \mathbb{F}_p^{2n} \times \mathbb{Z}_4$ if $p = 2$ and $(v,t) \in \mathbb{F}_p^{2n} \times \mathbb{F}_p$ if p is uneven. The commutation relations of these matrices are governed by the symplectic inner product.

We prove a theorem that gives us a unitary U such that

$$Ug(u_i, 0)U^* = g((e_i, 0^n), 0) \tag{6.1}$$

and

$$Ug(v_i, 0)U^* = g((0^n, e_i), 0) \tag{6.2}$$

for all $i \in [k]$, where e_i is the i-th standard basis vector.

The original version of this result, for symplectic vector spaces over $\mathbb{R}$ and $\mathbb{C}$ was proven by von Neumann [31]. The version we prove here was proven in the case that p is uneven by Gross [32]. For the $p = 2$ case, we could not find a full proof in the literature, and the proof below is our own.

Throughout this chapter, we will let V be a subspace of $\mathbb{F}_p^{2n}$. We decompose V by Theorem 5.2.1 as $V = V' \oplus W$ where $W = \{w \in V : [v,w] = 0 \text{ for all } v \in V\} = \langle w_1, \ldots, w_m \rangle$ and $V' = \langle u_1, \ldots, u_k, v_1, \ldots, v_k \rangle$, by Theorem 5.2.1. Here $k, m \in \mathbb{N}$ are such that $\dim W = k$ and $\dim V' = 2k$.

6.1 The case where p is an odd prime

We will first deal with the case where p is an odd prime, which is considerably more straightforward than the case where $p = 2$.

Definition 6.1.1 (Heisenberg group over $\mathbb{F}_p$)**.** Let $\mathbb{H}_{2n+1}(p)$ be the group with element set $\mathbb{F}_p^{2n} \times \mathbb{F}_p$ and operation

$$(v,t) \bullet (w,t') = (v + w, t + t' + \frac{1}{2}[v,w]) \tag{6.3}$$

This is indeed a group. Clearly, the set $\mathbb{F}_p^{2n} \times \mathbb{F}_p$ is closed under the operation. Associativity is straightforward to verify, and the neutral element is $(0,0)$. The inverse of an element (v,t) is $(-v,-t)$ since $[v,v] = 0$ for all $v \in \mathbb{F}_p^{2n}$.

Next, we define the Weyl representation $g : H_{2n+1}(p) \to \mathrm{GL}_{p^n}(\mathbb{C})$, after Hermann Weyl, defined by

$$(g(v,t)f)(x) = \omega_p^{t+\frac{1}{2}\langle v_1,v_2\rangle+\langle v_1,x\rangle} f(x+v_2), \tag{6.4}$$

where we write $v = (v_1, v_2) \in \mathbb{F}_p^n \times \mathbb{F}_p^n$.

This is indeed a representation:

$$\begin{aligned}
g(w,t')g(v,t)f(x) &= \omega_p^{t'+\frac{1}{2}\langle w_1,w_2\rangle+\langle x,w_1\rangle}(g(v,t)f)(x+w_2) && (6.5)\\
&= \omega_p^{t'+\frac{1}{2}\langle w_1,w_2\rangle+\langle x,w_1\rangle}\omega_p^{t+\frac{1}{2}\langle v_1,v_2\rangle+\langle x+w_2,v_1\rangle} f(x+w_2+v_2) && (6.6)\\
&= \omega_p^{t'+t+\langle x,w_1+v_1\rangle+\frac{1}{2}(\langle v_1,v_2\rangle+\langle w_1,w_2\rangle+2\langle w_2,v_1\rangle)} f(x+w_2+v_2) && (6.7)\\
&= \omega_p^{t'+t+\langle x,w_1+v_1\rangle+\frac{1}{2}(\langle v_1+w_1,v_2+w_2\rangle+[v,w])} f(x+w_2+v_2) && (6.8)\\
&= g(w+v, t'+t+\frac{1}{2}[v,w])f(x) && (6.9)\\
&= g((w,t)\bullet(v,t'))f(x). && (6.10)
\end{aligned}$$

In fact, g is a unitary representation, which we can show by verifying that for all $a, b \in \mathbb{F}_p^n$ we have $\langle g(v,t)e_a, g(v,t)e_b\rangle = \langle e_a, e_b\rangle = \delta_{ab}$, where e_a is the function $e_a : \mathbb{F}_p^n \to \mathbb{C}$ with $e_a(x) = \delta_{ax}$. Indeed,

$$\begin{aligned}
\langle g(v,t)e_a, g(v,t)e_b\rangle &= \sum_x \overline{g(v,t)e_a(x)}g(v,t)e_b(x) && (6.11)\\
&= \sum_x \overline{\omega_p^{t+\frac{1}{2}\langle v_1,v_2\rangle+\langle x,v_1\rangle}}\omega_p^{t+\frac{1}{2}\langle v_1,v_2\rangle+\langle x,v_1\rangle} e_a(x+v_2)e_b(x+v_2) && (6.12)\\
&= \overline{\omega_p^{t+\frac{1}{2}\langle v_1,v_2\rangle+\langle a-v_2,v_1\rangle}}\omega_p^{t+\frac{1}{2}\langle v_1,v_2\rangle+\langle b-v_2,v_1\rangle}\delta_{ab} && (6.13)\\
&= \delta_{ab}. && (6.14)
\end{aligned}$$

Lemma 6.1.2. *The trace of $g(v,t)$ is equal to $\omega_p^t p^n \mathbb{1}[v=0]$*

Proof. We calculate the trace of the matrix $g(v,t)$:

$$\begin{aligned}
\mathrm{tr}[g(v,t)] &= \sum_x g(v,t)_{xx} && (6.15)\\
&= \sum_x g(v,t)e_x(x) && (6.16)\\
&= \sum_x \omega_p^{t+\frac{1}{2}\langle v_1,v_2\rangle+\langle x,v_1\rangle} e_x(x+v_2) && (6.17)\\
&= \sum_x \omega_p^{t+\frac{1}{2}\langle v_1,v_2\rangle+\langle x,v_1\rangle}\mathbb{1}[v_2=0] && (6.18)\\
&= \omega_p^t \sum_x \omega_p^{\langle x,v_1\rangle}\mathbb{1}[v_2=0] && (6.19)\\
&= \omega_p^t p^n \mathbb{1}[v_1=v_2=0] && (6.20)
\end{aligned}$$

□

We consider the subgroup G of $\mathbb{H}_{2n+1}(p)$ defined as

$$G = \{(v,t) : v \in V', t \in \mathbb{F}_p\}. \tag{6.21}$$

We define the Pauli group on k qubits as a subgroup of $\mathbb{H}_{2n+1}(p)$ as follows:

$$P_{p,k} = \{(v,t) : v \in \mathbb{F}_p^k \times \{0^{n-k}\} \times \mathbb{F}_p^k \times \{0^{n-k}\}, t \in \mathbb{F}_p\}. \tag{6.22}$$

When it is clear from context, we leave out the dependence on p and k and write P instead of $P_{p,k}$. We can define the matrix $S \in \mathbb{F}_p^{2n\times 2n}$ that maps u_i to e_i and v_i to e_{n+i} for all $i \in [k]$. Note that $[Su_i, Sv_j] = [e_i, e_{n+j}] = [u_i, v_j]$ and $[Su_i, Su_j] = [e_i, e_j] = [u_i, u_j]$ and $[Sv_i, Sv_j] = [e_{n+i}, e_{n+j}] = [v_i, v_j]$.

This matrix induces a function ϕ from G to P with $\phi(v,t) = (Sv,t)$.

That this is an isomorphism can be readily verified:

$$\phi(v,t) \bullet \phi(w,t) = (Sv,t) \bullet (Sw,t') = (Sv + Sw, t + t' + \frac{1}{2}[Sv, Sw]) = \tag{6.23}$$

$$(S(v+w), t + t' + \frac{1}{2}[v,w]) = \phi((v,t) \bullet (w,t')). \tag{6.24}$$

This gives us two representations of G, namely g and $g \circ \phi$. The characters of these representations are equal:

$$\begin{aligned} \mathrm{tr}[g(v,t)] &= \omega_p^t p^n \mathbb{1}[v = 0] && (6.25)\\ &= \omega_p^t p^n \mathbb{1}[Sv = 0] && (6.26)\\ &= \mathrm{tr}[g(Sv,t)] && (6.27)\\ &= \mathrm{tr}[g(\phi(v,t))] && (6.28) \end{aligned}$$

by Lemma 6.1.2 and the fact that S is injective on V'.

These representations are equivalent by the following lemma, [33, Corollary 2, section 2.3]:

Lemma 6.1.3. *If two representations $g, g' : G \to GL_{p^n}(\mathbb{C})$ have the same character, then they are equivalent.*

In fact, they are unitarily equivalent by the next lemma, [34, page 11]. We include the proof for completeness.

Lemma 6.1.4. *If we have two unitary representations $g, g' : G \to GL_{p^n}(\mathbb{C})$ that are equivalent, then they are unitarily equivalent. To be precise, there exists a unitary such that for all group elements $h \in G$, $U^* g(h) U = g'(h)$*

Proof. Since g, g' are equivalent, there exists a matrix $A \in \mathrm{GL}_{p^n}(\mathbb{C})$ such that for any $x \in G$,

$$g(x) = A^{-1} g'(x) A. \tag{6.29}$$

We can take adjoints on both sides, to get

$$g(x)^* = A^* g'(x)^* (A^{-1})^*. \tag{6.30}$$

Since g, g' are a unitary representations, $g(x)^* = g(x^{-1})$ and $g'(x)^* = g'(x^{-1})$. So,

$$g(x^{-1}) = A^* g'(x^{-1})(A^{-1})^* \tag{6.31}$$

for all $x \in G$, so also $g(x) = A^* g'(x)(A^{-1})^*$, which can be rearragned to

$$.g'(x) = (A^{-1})^* g(x) A^*. \tag{6.32}$$

If we fill this in into equation (6.29), we get

$$g(x) = A^{-1}(A^{-1})^* g(x) A^* A = (A^* A)^{-1} g(x) A^* A. \tag{6.33}$$

Now A^*A is positive definite with inverse $A^{-1}(A^{-1})^*$, so it has a unique positive definite square root B, by [35, Lemma 2.18]. We call this root B. Since $g(x)^{-1}(A^*A)g(x) = A^*A$ by equation (6.33), $g(x)^{-1}Bg(x)$ is also a square root of A^*A, for all $x \in G$. If we fill in x^{-1}, we get that $g(x)Bg(x)^{-1}$ is a square root of A^*A.

Because $g(x)^{-1} = g(x)^*$, $g(x)Bg(x)^{-1} = g(x)Bg(x)^*$. The matrix $g(x)Bg(x)^*$ is again positive semi-definite and even positive definite because $g(x)$ is unitary and therefore has full rank.

Therefore, because B is the unique positive definite square root of A^*A, we have that $g(x)Bg(x)^{-1} = B$. We rewrite this to

$$Bg(x)B^{-1} = g(x). \tag{6.34}$$

Next, we define $U = AB^{-1}$. Then $A = UB$. Also, U is a unitary:

$$U^*U = (B^{-1})^* A^* A B^{-1} = (A^*A)^{-1/2}(A^*A)(A^*A)^{-1/2} = I \tag{6.35}$$

using that B is positive definite so $(B^{-1})^* = B^{-1}$. By equations (6.29) and (6.34)

$$g'(x) = UBg(x)(UB)^{-1} \tag{6.36}$$

$$= Ug(x)U^{-1}. \tag{6.37}$$

Therefore, g and g' are equivalent through the unitary U. □

Now we are ready to prove the Stone-von Neumann theorem over $\mathbb{F}_p$ with p uneven. Recall that P is the Pauli group as defined in equation (6.22).

Theorem 6.1.5 (Stone-von Neumann Theorem, version for uneven primes)**.** *Let p be an uneven prime. Let V be a subspace of $\mathbb{F}_p^{2n}$ such that $V = V' \oplus W$ where $W = \{w \in V : [v, w] = 0 \text{ for all } v \in V\}$. Let $G = \{g(v, t) : v \in V', t \in \mathbb{F}_p\}$, where g is the Weyl representation. Then there exists a unitary $U \in \mathbb{C}^{p^n \times p^n}$ such that*

$$UGU^* = P \tag{6.38}$$

Proof. Since $g \circ \phi$ and g are unitarily equivalent representations, there exists a unitary U such that for all $(v, t) \in V'$,

$$Ug(v, t)U^* = g(\phi(v, t)). \tag{6.39}$$

Since $\phi : G \to P$ is a bijection, $UGU^* = P$. □

6.2 The case where $p = 2$

Let the map $g : V' \times \mathbb{Z}_4 \to \mathrm{GL}_{2^n}(\mathbb{C})$ be defined by

$$g(v,t)f(x) = i^t(-1)^{\langle v_1,x\rangle}f(x+v_2) \tag{6.40}$$

If we multiply two matrices $g(v,t)$ and $g(w,t')$, we get

$$\begin{aligned} g(w,t')g(v,t)f(x) &= i^{t'}(-1)^{\langle x,w_1\rangle}(g(v,t)f)(x+w_2) && (6.41)\\ &= i^{t'+t}(-1)^{\langle x,w_1\rangle+\langle x+w_2,v_1\rangle}f(x+w_2+v_2) && (6.42)\\ &= i^{t'+t+2\langle w_2,v_1\rangle}(-1)^{\langle x,v_1+w_1\rangle}f(x+w_2+v_2)) && (6.43)\\ &= g(w+v,t'+t+2\langle v_1,w_2\rangle)f(x), && (6.44) \end{aligned}$$

so

$$g(w,t')g(v,t) = g(w+v,t'+t+2\langle v_1,w_2\rangle) \tag{6.45}$$

Then we define the following subgroup G of $\mathrm{GL}_{2^n}(\mathbb{C})$:

$$G := \langle g(u_i,0), g(v_i,0), g(0,1) : i \in [k]\rangle = \{g(v,t) : v \in V', t \in \mathbb{Z}_4\}, \tag{6.46}$$

where the equality holds by equation (6.45).

These matrices are unitary. Some of them are Hermitian, and some are antihermitian:

Proposition 6.2.1.

1. $|G| = 2^{2k+2}$
2. *G is a group of unitary matrices such that for all $g(v,t) \in G$, $g(v,t)^* = g(v,t)^{-1} = (-1)^{t+\langle v_1,v_2\rangle}g(v,t)$.*
3. $g(v_i,0)^2 = (-1)^{\langle v_{i1},v_{i2}\rangle}\mathbb{I}_{2^n}$, *and* $g(u_i,0)^2 = (-1)^{\langle u_{i1},u_{i2}\rangle}\mathbb{I}_{2^n}$
4. *The commutators satisfy* $[g(u_i,0),g(u_j,0)] = [g(v_i,0),g(v_j,0)] = [g(u_i,0),g(0,1)] = [g(v_i,0),g(0,1)] = \mathbb{I}_{2^n}$ *and* $[g(u_i,0),g(v_j,0)] = (-1)^{\delta_{ij}}\mathbb{I}_{2^n}$.
5. *The trace of $g(v,t)$ is* $tr[g(v,t)] = i^t 2^n \mathbb{1}[v=0]$.

Proof. The first property holds because $G = \{g(v,t) : v \in V', t \in \mathbb{Z}_4\}$ and this set has size $4|V'| = 2^{2k+2}$.

The inverse of $g(v,t)$ is $(-1)^{t+\langle v_1,v_2\rangle}g(v,t)$ since by equation (6.45),

$$g(v,t)^2 = g(0,2(t+\langle v_1,v_2\rangle)) = \mathrm{id}_{2^n}(-1)^{t+\langle v_1,v_2\rangle}. \tag{6.47}$$

Next we calculate the adjoint of $g(v,t)$. To do this, we note that the yx-entry of the matrix $g(v,t)$ is equal to $g(v,t)e_y(x)$ where $e_y(x) = \mathbb{1}[x=y]$. Then,

$$\begin{aligned}
\overline{g(v,t)_{yx}} &= \overline{g(v,t)e_y(x)} && (6.48)\\
&= (-1)^t i^t (-1)^{\langle x, v_1\rangle} e_y(x+v_2) && (6.49)\\
&= (-1)^t i^t (-1)^{\langle x, v_1\rangle} e_x(y+v_2) && (6.50)\\
&= (-1)^t i^t (-1)^{\langle y+v_2, v_1\rangle} e_x(y+v_2) && (6.51)\\
&= (-1)^{t+\langle v_1, v_2\rangle} i^t (-1)^{\langle y, v_1\rangle} e_x(y+v_2) && (6.52)\\
&= (-1)^{t+\langle v_1, v_2\rangle} g(v,t) e_x(y) && (6.53)\\
&= (-1)^{t+\langle v_1, v_2\rangle} g(v,t)_{xy}. && (6.54)
\end{aligned}$$

Therefore, $g(v,t)^* = (-1)^{t+\langle v_1, v_2\rangle} g(v,t)$. Therefore $g(v,t)^* = g(v,t)^{-1}$ and so $g(v,t)$ is unitary. This proves property (2).

By equation (6.45),

$$g(v,0)g(v,0) = g(0, 2\langle v_1, v_2\rangle) \tag{6.55}$$

which proves property (3).

We can calculate the commutator of $g(v,t)$ and $g(w,t')$ by writing $g(v+w, t+t')$ in two ways using equation (6.45):

$$g(v+w, t+t') = (-1)^{\langle w_1, v_2\rangle} g(v,t)g(w,t') \tag{6.56}$$

while at the same time,

$$g(v+w, t+t') = (-1)^{\langle v_1, w_2\rangle} g(w,t')g(v,t). \tag{6.57}$$

Therefore,

$$[g(v,t), g(w,t')] = (-1)^{[v,w]}, \tag{6.58}$$

from which property (4) follows.

The trace of $g(v,t)$ is given by

$$\begin{aligned}
\operatorname{tr}(g(v,t)) &= \sum_{x\in\mathbb{F}_2^n} g(v,t)_{xx} && (6.59)\\
&= i^t \sum_{x\in\mathbb{F}_2^n} (-1)^{\langle x, v_2\rangle} e_x(x+v_1) && (6.60)\\
&= i^t \sum_{x\in\mathbb{F}_2^n} (-1)^{\langle x, v_2\rangle} \mathbb{1}[v_1 = 0] && (6.61)\\
&= i^t 2^n \mathbb{1}[v_1, v_2 = 0]. && (6.62)
\end{aligned}$$

□

We will define two groups, and they will turn out to be isomorphic.

Definition 6.2.2 (Pauli group on k qubits)**.** Let $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Let

$$X_i = \mathbb{I}_2 \otimes \cdots \otimes X \otimes \cdots \otimes \mathbb{I}_2 \in \mathbb{C}^{2^k \times 2^k} \tag{6.63}$$

where the X is in the i-th position. Similarly define

$$Z_i = \mathbb{I}_2 \otimes \cdots \otimes Z \otimes \cdots \otimes \mathbb{I}_2 \in \mathbb{C}^{2^k \times 2^k} \tag{6.64}$$

where the Z is in the i-th position.

We will define the Pauli group on k qubits $\mathcal{P}_k$ as the subgroup of $\mathrm{GL}_{2^k}(\mathbb{C})$ generated by $\{X_j, Z_j, i\mathbb{I}_{2^k} : j \in [k]\}$.

We will be working with the group $P_{2,k}$ which is defined as

$$P_{2,k} = \{Q \otimes \mathbb{I}_{2^{n-k}} : Q \in \mathcal{P}_k\}, \tag{6.65}$$

which is a subgroup of $\mathrm{GL}_{2^n}(\mathbb{C})$.

When p and k are clear from context, we will leave out the dependence on p and k and write P instead of $P_{p,k}$.

Proposition 6.2.3. *The following are true of P:*

1. *The size of the Pauli group on k qubits is 2^{2k+2}.*
2. *Every matrix in P is unitary.*
3. *The commutators satisfy $[X_i, Z_j] = (-1)^{\delta_{ij}}$, $[X_i, X_j] = [Z_i, Z_j] = \mathbb{I}_{2^n}$, $[X_i, i\mathbb{I}_{2^n}] = [Z_i, i\mathbb{I}_{2^n}] = \mathbb{I}_{2^n}$.*
4. *$X_i^2 = Z_i^2 = \mathbb{I}_{2^n}$.*
5. *The trace of $Q \in P$ is nonzero if and only if Q is a multiple of the identity, and $tr(i^t \mathbb{I}_{2^n}) = i^t 2^n$.*

Next, define the group $\mathcal{G}$ by giving a presentation of it.

Definition 6.2.4. Let $S = \{\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_k, \lambda\}$. Define the set

$$R = \bigcup_{i,j \in [k]} \{\lambda^4, \alpha_i^2 \lambda^{2\langle u_{i1}, u_{i2} \rangle}, \beta_i^2 \lambda^{2\langle v_{i1}, v_{i2} \rangle}, \tag{6.66}$$

$$[\alpha_i, \alpha_j], [\beta_i, \beta_j], [\alpha_i, \beta_j] \lambda^{2\delta_{ij}}, \tag{6.67}$$

$$[\lambda, \alpha_i], [\lambda, \beta_i]\}. \tag{6.68}$$

Then we let $\mathcal{F}$ be the free group on S, and let $\mathcal{R}$ be the normal subgroup of $\mathcal{F}$ generated by R.

Define $\mathcal{G} = \mathcal{F}/\mathcal{R}$.

Lemma 6.2.5. *The size of $\mathcal{G}$ is at most 2^{2k+2}.*

Proof. For $(a,b,t) \in \mathbb{F}_2^k \times \mathbb{F}_2^k \times \mathbb{Z}_4$, we define the element $C(a,b,t) = \lambda^t \alpha_1^{a_1} \dots \alpha_k^{a_k} \beta_1^{n_1} \dots \beta_k^{n_k} \in \mathcal{F}$. Now we show that for every $f \in \mathcal{F}$,there exists an $r \in \mathcal{R}$, and $(a,b,t) \in \mathbb{F}_2^k \times \mathbb{F}_2^k \times \mathbb{Z}_4$ such that $fr = C(a,b,t)$. In other words, the number of cosets of $\mathcal{R}$ in $\mathcal{F}$ is at most $|\mathbb{F}_2^k \times \mathbb{F}_2^k \times \mathbb{Z}_4| = 2^{2k+2}$.

Suppose that f is of the form $f_1\beta_i\alpha_j f_2$. Then $(f_1\beta_i\alpha_j f_2)(f_2^{-1}[\alpha_j,\beta_i]\lambda^{2\delta_{ij}} f_2) = f_1\alpha_j\beta_i f_2$. Since $f_2^{-1}\lambda^{2\delta_{ij}}[\alpha_j,\beta_i]f_2 \in \mathcal{R}$, we have that

$$f_1\beta_i\alpha_j f_2 = f_1\alpha_j\beta_i f_2 \mod \mathcal{R} \tag{6.69}$$

If we keep doing this whenever there is an α to the left of a β, we can see that $f = f' \mod \mathcal{R}$ where f' is an element of $\mathcal{F}$ with all the α's on the left and the β's on the right. In a similar way, we can put the α's in ascending order, and the β's also in ascending order. Any occurence of α_i^2 we can replace with $\lambda^{2\langle u_{i1},u_{i2}\rangle}$ and similarly we replace β_i^2 with $\lambda^{2\langle v_{i1},v_{i2}\rangle}$. Finally, we bring all the λ's to the front. This will give us an element $f'' = f \mod \mathcal{R}$ such that $f'' = C(a,b,t)$ for some $(a,b,t) \in \mathbb{F}_2^k \times \mathbb{F}_2^k \times \mathbb{Z}_4$. Therefore, $|\mathcal{F}/\mathcal{R}| \leq 2^{2k+2}$. □

Lemma 6.2.6. *$\mathcal{G}$ is isomorphic to P.*

Proof. We can rewrite elements of $\mathcal{F}$ with the mapping $\phi : \mathcal{F} \to P$ that does the following:

$$\phi : \alpha_i \mapsto i^{\langle u_{i1},u_{i2}\rangle} X_i \tag{6.70}$$

$$\phi : \beta_i \mapsto i^{\langle v_{i1},v_{i2}\rangle} Z_i \tag{6.71}$$

$$\phi : \lambda \mapsto i\mathbb{I} \tag{6.72}$$

and $\phi(c_1c_2) = \phi(c_1)\phi(c_2)$ for $c_1, c_2 \in \mathcal{F}$. By Corollary 7.10.14 of [36], this map extends to a homomorphism $\phi : \mathcal{G} \to P$. This homomorphism is surjective, since $\phi(S)$ generates P. Since $|\mathcal{G}| \leq 2^{2k+2} = |P|$ by Lemma 6.2.5 and ϕ is surjvective, ϕ must be injective. Therefore, ϕ is an isomorphism. □

In the same way, we can prove the following lemma:

Lemma 6.2.7. *$\mathcal{G}$ is isomorphic to G, the group defined in equation* (6.46)*.*

Proof. We can rewrite elements of $\mathcal{F}$ with the mapping $\psi : \mathcal{F} \to G$ that does the following:

$$\psi : \alpha_i \mapsto g(u_i, 0) \tag{6.73}$$

$$\psi : \beta_i \mapsto g(v_i, 0) \tag{6.74}$$

$$\psi : \lambda \mapsto g(0, 1) \tag{6.75}$$

and $\psi(c_1c_2) = \psi(c_1)\psi(c_2)$ for $c_1, c_2 \in \mathcal{F}$. By Proposition 6.2.1, $\psi(r) = \mathrm{id}_{2^n}$ for all $r \in R$. By corollary 7.10.14 of [36], this map extends to a homomorphism $\psi : \mathcal{G} \to G$. This homomorphism is surjective, since $\psi(S)$ generates G. Since $|\mathcal{G}| \leq 2^{2k+2} = |G|$ by Lemma 6.2.5 and ψ is surjvective, ψ must be injective. Therefore, ψ is an isomorphism. □

Corollary 6.2.8. *G is isomorphic to P, and this isomorphism maps $g(0,1)$ to $i\mathbb{I}_{2^n}$*

Proof. Since $\phi \circ \psi^{-1}$ is a composition of isomorphisms, $\phi \circ \psi^{-1}$ is an isomorphism from G to P. Also, $\phi(\psi(g(0,1)) = \phi(\lambda) = i\mathbb{I}_{2^n}$ □

Theorem 6.2.9 (Stone-von Neumann Theorem, version for $p = 2$)**.** *Let V be a subspace of $\mathbb{F}_2^{2n}$ such that $V = V' \oplus W$ where $W = \{w \in V : [v, w] = 0$ for all $v \in V\}$. Let $G = \{g(v,t) : v \in V', t \in \mathbb{Z}_4\}$. There exists a unitary $U \in \mathbb{C}^{2^n \times 2^n}$ such that*

$$UGU^* = P \tag{6.76}$$

Proof. We have the two unitary subgroups of $\mathrm{GL}_{2^n}(\mathbb{C})$ that are isomorphic, P and G. let $\rho : G \to P$ be an isomorphism that maps $g(0,1)$ to $i\mathbb{I}_{2^n}$. We can view the identity map $\mathrm{id} : G \to \mathrm{GL}_{2^n}(\mathbb{C})$ and $\rho : G \to \mathrm{GL}_{2^n}(\mathbb{C})$ as representations of G. The trace of $g(v,t) \in G$ is equal to $2^n i^t \mathbb{1}[v = 0]$ by Proposition 6.2.1. The trace of $Q = \rho(g(v,t))$ is nonzero if and only if Q is a multiple of the identity if and only if $\rho^{-1}(Q) = g(0,t)$ for some $t \in \mathbb{Z}_4$. Since $\rho(g(0,t)) = i^t \mathbb{I}_{2^n}$, $\mathrm{tr}[\rho(g(v,t))] = 2^n i^t \mathbb{1}[v = 0]$. Therefore, the characters of these two representations are equal.

By Lemma 6.1.3, id and ρ must be equivalent representations of G. Since they are unitary representations by Propositions 6.2.1 and 6.2.3, they are unitarily equivalent, by Lemma 6.1.4. Therefore, there exists a unitary U such that $UGU^* = P$. □

7 From high weight subspace to a Lagrangian subspace

At the end of Chapter 4, we found a space $V \subseteq \mathbb{F}_p^{2n}$ with the following property:

$$\sum_{(h,a)\in V} |\widehat{\Delta_h f}(a)|^2 \geq \text{poly}(\epsilon) \tag{7.1}$$

while V is not too big: $|V| \leq \text{poly}(\frac{1}{\epsilon})p^n$.

Like before, we decompose $V = V' \oplus W$ where $W = \{w \in V : [v, w] = 0 \text{ for all } v \in V\}$ using Theorem 5.2.1, and we let m, k be such that $\dim W = m$ and $\dim V' = 2k$.

In this chapter we apply Theorems 6.2.9 and 6.1.5 in order to prove that k is not too large, specifically, $k = O(\log(\frac{1}{\epsilon}))$. This allows us to find a y such that the set $W + y$ satisfies

$$\sum_{(h,a)\in W+y} |\widehat{\Delta_h f}(a)|^2 \geq \text{poly}(\epsilon). \tag{7.2}$$

Then we extend $W + y$ to a Lagrangian subspace L.

Remark 7.0.1. *In chapter 6, we defined g in a different way for p even and uneven. In this chapter, we don't make this distinction, but we do reference g. We can fix p and define g accordingly, and the proof will work both ways.*

7.1 Bounding the non-commutativity of V

Our goal in this chapter is to prove that the dimension of V' is not too large, specifically, we prove that $k = O(\log(\frac{1}{\epsilon}))$. We show this by proving the following lemma:

Lemma 7.1.1. *Let $f : \mathbb{F}_p^n \to \mathbb{C}$ be a function with $||f||_2 = 1$. Let $V = V' \oplus W$ a subspace of $\mathbb{F}_p^n$ where $W = \{w \in V : [v, w] = 0 \text{ for all } v \in V\}$ and $\dim V' = 2k$, $\dim W = m$. Suppose that*

$$\sum_{(h,a)\in V} |\widehat{\Delta_h f}(a)|^2 = \delta. \tag{7.3}$$

Then $p^k \leq \frac{1}{\delta}\frac{|V|}{p^n}$

Proof. We unfold δ as follows.

$$\delta = \sum_{(h,a)\in V} |\widehat{\Delta_h f}(a)|^2 \tag{7.4}$$

$$= \frac{1}{p^n} \sum_{(h,a)\in V} \left| \sum_{x\in\mathbb{F}_p^n} f(x)\overline{f(x+h)}\omega_p^{-\langle a,x\rangle} \right|^2 \tag{7.5}$$

$$= \frac{1}{p^n} \sum_{h,a\in V} \sum_{x,y\in G} \overline{f(y)} f(y+h) f(x) \overline{f(x+h)} \omega_p^{-\langle a,x-y\rangle} \tag{7.6}$$

$$= \frac{1}{p^n} \sum_{x,y} \overline{f(y)} \left(\sum_{(h,a)\in V} \overline{f(x+h)} f(y+h) \omega_p^{-\langle a,x-y\rangle} \right) f(x) \tag{7.7}$$

$$= \frac{1}{p^n} f^* N f, \tag{7.8}$$

where $N := \sum_{(h,a)\in V} g((h,a),0) f f^* g((h,a),0)^*$.

We can rewrite N as

$$N = \sum_{(h,a)\in V} g((h,a),0) f f^* g((h,a),0)^* \tag{7.9}$$

$$= \sum_{w\in W} \sum_{(h,a)\in V'} g((h,a)+w,0) f f^* g((h,a)+w,0)^* \tag{7.10}$$

$$= \sum_{w\in W} g(w,0) \left(\sum_{(h,a)\in V'} g((h,a),0) f f^* g((h,a),0)^* \right) g(w,0)^* \tag{7.11}$$

$$= \sum_{w\in W} g(w,0) M g(w,0)^*, \tag{7.12}$$

where we define the matrix $M := \sum_{(h,a)\in V'} g((h,a),0) f f^* g((h,a),0)^*$.

Claim 7.1.2. *The operator norm of M is at most p^k.*

Proof of Claim : By the Stone-von Neumann Theorem there exists a unitary $U \in \mathbb{C}^{p^n\times p^n}$ such that $UGU^* = P$ where $G = \{g(v,t) : v \in V', t \in \mathbb{Z}_4\}$ and P is the Pauli group on the first k qubits. Define $K = \{(h, 0^{n-k}) : h \in \mathbb{F}_p^k\} \subseteq \mathbb{F}_p^n$. Note that $P = \{g(w,0) : w \in K \times K\}$. Let us write M in the basis defined by U:

$$UMU^* = \sum_{v\in V'} U g(v,0) f f^* g(v,0)^* U^* \tag{7.13}$$

$$= \sum_{v\in V'} U g(v,0) U^* U f f^* U^* U g(v,0)^* U^* \tag{7.14}$$

$$= \sum_{v\in K\times K} g(v,0) f' f'^* g(v,0)^* \tag{7.15}$$

We define $M' := UMU^*$.

The entries of M' are the following, for $x, y \in \mathbb{F}_p^n$

$$M'_{yx} = \sum_{h,a \in K} \overline{f'(x+h)} f'(y+h) \omega_p^{\langle a, y-x \rangle} \tag{7.16}$$

$$= \sum_{h \in K} \overline{f'(x+h)} f'(y+h) \sum_{a \in K} \omega_p^{\langle a, y-x \rangle} \tag{7.17}$$

$$= \sum_{h \in K} \overline{f'(x+h)} f'(y+h) \mathbb{1}[x_i = y_i : i \in [k]] p^k \tag{7.18}$$

Let $\overline{K}$ be the space $\{(0^k, b), b \in \mathbb{F}_p^{n-k}\}$, so that $K \oplus \overline{K} = \mathbb{F}_p^n$. Let $f'_h : \overline{K} \to \mathbb{C}$ be the function defined by $f'_h(x) = f'(h+x)$ We define the following matrix $B \in \mathbb{C}^{\overline{K} \times \overline{K}}$, with entries $(s, r) \in \overline{K} \times \overline{K}$

$$B_{sr} := \sum_{h \in K} f'_h(s) \overline{f'_h(r)}. \tag{7.19}$$

So B is the sum of outer products:

$$B = \sum_{h \in K} f'_h f'^*_h, \tag{7.20}$$

and that implies that B is positive semidefinite.

The trace of B is equal to

$$\mathrm{tr}[B] = \sum_{h \in K} \mathrm{tr} f'_h f'^*_h \tag{7.21}$$

$$= \sum_{h \in K, r \in \overline{K}} f'_h(r) \overline{f'_h}(r) \tag{7.22}$$

$$= \sum_{x \in \mathbb{F}_p^n} |f'(x)|^2 \tag{7.23}$$

$$= ||Uf||_2^2 \tag{7.24}$$

$$= 1 \tag{7.25}$$

Therefore, the sum of the eigenvalues of B is 1. Since all the eigenvalues of B are nonnegative, this implies that the largest eigenvalue of B is at most 1. Since B is Hermitian, this also implies that the operator norm of B is at most 1, because for Hermitian matrices, the operator norm is equal to the largest eigenvalue.

The matrix $p^k \mathbb{I}_{2^k} \otimes B$ is equal to M'. We can prove this by comparing the entries. Let $(h, s), (h', r) \in K \times \overline{K}$:

$$p^k (\mathbb{I}_{2^k} \otimes B)_{(h,s),(h',r)} = p^k \mathbb{1}[h = h'] B_{sr} \tag{7.26}$$

$$= M_{(h,s),(h',r)} \tag{7.27}$$

by equation (7.18).

Let $g : \mathbb{F}_p^n \to \mathbb{C}$ be a function. By Pythagoras' Theorem,

$$||M'g||_2 = p^k \sqrt{\sum_{h \in K} ||Bg_h||_2^2} \leq p^k \sqrt{\sum_{h \in K} ||g_h||_2^2} = p^k ||g||_2 \tag{7.28}$$

This implies that $||M'||_{op} \leq 1$.

Since $M' = UMU^*$, where U is unitary, M' and M have the same operator norm, and so $||M||_{op} \leq p^k$. ♦

Continuing from equation 7.8, by Cauchy-Schwarz and claim 7.1.2

$$\begin{aligned} f^*Nf &= \sum_{w \in W} f^*g(w,0)Mg(w,0)^*f && (7.29)\\ &\leq \sum_{w \in W} ||g(w,0)^*f||_2 ||Mg(w,0)^*f||_2 && (7.30)\\ &\leq \sum_{w \in W} p^k ||g(w,0)^*f||_2 ||g(w,0)^*f||_2 && (7.31)\\ &= p^{k+m}, && (7.32) \end{aligned}$$

where we have used the fact that $g(w,0)$ is unitary and $||f||_2 = 1$ in the last equality.

This implies that $\delta \leq \frac{1}{p^n} f^*Nf \leq \frac{p^{k+m}}{p^n}$. Since $|V| = p^{2k+m}$, we get that $\delta \leq \frac{|V|}{p^{n+k}}$ so $p^k \leq \frac{1}{\delta} \frac{|V|}{p^n}$ □

7.2 Obtaining the Lagrangian

Definition 7.2.1. A subspace $L \subseteq \mathbb{F}_p^{2n}$ is called *isotropic* if $[v, w] = 0$ for all $v, w \in L$. If, in addition, the dimension of L is p^n, then we call L *Lagrangian.*

Lemma 7.2.2. *Every isotropic subspace of $\mathbb{F}_p^{2n}$ is contained in a Lagrangian subspace of $\mathbb{F}_p^{2n}$.*

Proof. Suppose that $V \subseteq \mathbb{F}_p^{2n}$ is an isotropic subspace. Suppose that $\dim V = d < n$. Set $V_d = V$. We will inductively define $V_{d+1}, \ldots, V_n$ as follows.

Suppose we have defined V_j, with $\dim V = j < n$. Let $w_1, \ldots, w_j$ be a basis for V_j. Then the space $Z = \{v \in \mathbb{F}_p^{2n} : [w_i, v] = \langle J^T w_i, v \rangle = 0 \text{ for all } i \in [j]\}$ has dimension $2n - j$. Because $j < n$, $\dim Z > \dim V_j$ and so there must exist a vector v^* in $Z \backslash V_j$. We will define V_{j+1} as $V_j + \{v^*\}$. □

Lemma 7.2.3. *Suppose that $V \subseteq \mathbb{F}_p^{2n}$ is a subspace of $\mathbb{F}_p^{2n}$ such that*

- $\text{poly}(\epsilon)p^n \leq |V| \leq \text{poly}(\frac{1}{\epsilon})p^n$
- $\sum_{(h,a) \in V} |\widehat{\Delta_h f}(a)|^2 \geq \text{poly}(\epsilon)$.

Then there exists a Lagrangian $L \subseteq \mathbb{F}_p^{2n}$ such that

$$\sum_{(h,a)\in L} |\widehat{\Delta_h f}(a)|^2 \geq \text{poly}(\epsilon) \tag{7.33}$$

Proof. We decompose V using Theorem 5.2.1 as $V = V' \oplus W$, where $V' = \langle u_1, \ldots, u_k, v_1, \ldots, v_k \rangle$, and $W = \langle w_1, \ldots, w_m \rangle$. This decomposition induces a partition of V by isotropic affine subspaces in the following way:

$$V = \bigcup_{v \in V'} W + v. \tag{7.34}$$

For all $v \in V'$, $W + v$ is isotropic, since for all $w, w' \in W$,

$$[v + w, v + w'] = [v, v] + [v, w'] + [w, v] + [w', w] = 0. \tag{7.35}$$

The size of V satsifes $|V| \leq \text{poly}(\frac{1}{\epsilon})p^n$, and $\sum_{(h,a)\in V} |\widehat{\Delta_h f}(a)|^2 \geq \text{poly}(\epsilon)$. By Lemma 7.1.1, $p^k \leq \frac{1}{\text{poly}(\epsilon)} \frac{|V|}{p^n} = \text{poly}(\frac{1}{\epsilon})$. Now the size of V' is equal to $p^{2k} = \text{poly}(\frac{1}{\epsilon})$.

$$\sum_{v\in V'} \sum_{(h,a)\in W+v} |\widehat{\Delta_h f}(a)|^2 = \sum_{(h,a)\in V} |\widehat{\Delta_h f}(a)|^2 \geq \text{poly}(\epsilon) \tag{7.36}$$

so by the pidgeonhole principle there must exist a $v \in V'$ such that

$$\sum_{(h,a)\in W+v} |\widehat{\Delta_h f}(a)|^2 \geq \frac{\text{poly}(\epsilon)}{|V'|} \geq \text{poly}(\epsilon) \tag{7.37}$$

Since $L' = \bigcup_{a\in\mathbb{F}_p} W + av$ is an isotropic subspace that contains $W + v$, we can extend L' to a Lagrangian subspace $L \subseteq \mathbb{F}_p^{2n}$ using Lemma 7.2.2.

□

8 From a Lagrangian subspace to correlation with a stabilizer

In this section, we prove the final step to prove Theorem 1.2.5. So far, we have found a Lagrangian subspace of $\mathbb{F}_p^{2n}$ with $\sum_{(h,a)\in L} |\widehat{\Delta_h f}(a)|^2 \geq \text{poly}(\epsilon)$. Now we will need to turn this Lagrangian into a stabilizer state with high inner product with f.

8.1 Turning the Lagrangian into a stabilizer

Lemma 8.1.1. *Let $L \subseteq \mathbb{F}_p^{2n}$ be a Lagrangian subspace, and $f : \mathbb{F}_p^n \to \mathbb{C}$ a function with $||f||_2 = 1$, such that*

$$\sum_{(h,a)\in L} |\widehat{\Delta_h f}(a)|^2 \geq \delta. \tag{8.1}$$

Then there exists a function $s \in \mathcal{S}$ such that $|\langle f, s\rangle|^2 \geq \delta$.

Proof. Let $\pi : L \to \mathbb{F}_p^{2n}$ be the projection to the first n coordinates: $\pi(h, a) = (h, 0)$. Since π is linear, $\ker(\pi)$ is a subspace of L. Let T be the subspace of L such that $T \oplus \ker(\pi) = L$. We define the space $S = \{h : (h, a) \in T\}$, which is a subspace of $\mathbb{F}_p^n$ since S is isomorphic to $\pi(L)$.

Claim 8.1.2. *There exists a symmetric matrix $M \in \mathbb{F}_p^{n\times n}$ such that*

$$T = \{(h, Mh) : h \in S\}. \tag{8.2}$$

Proof of Claim : First we show that if we have $(h, a), (h, a') \in T$ then $a = a'$, that is to say, T is a graph.

If $(h, a), (h, a') \in T$, then $(0, a - a') \in T$, but this is an element of $\ker(\pi)$. since $L = T \oplus \ker(\pi)$, $\ker(\pi) \cap T = \{(0, 0)\}$, so $(0, a - a')$ must be $(0, 0)$.

So we define the function $P : S \to \mathbb{F}_p^n$ such that $T = \{(h, Mh) : h \in \pi(L)\}$. Next we show that P is linear:

$$(h, Ph) + (h', Ph') = (h + h', Ph + Ph') = (h + h', P(h + h')). \tag{8.3}$$

Let $r = \dim S$, and let $s_1, \ldots, s_r$ be a basis for S. Then we define $s_{r+1}, \ldots, s_n$ such that $\{s_1, \ldots, s_n\}$ is a basis for $\mathbb{F}_p^n$. We define $t_i = Ps_i$ for $i \in [r]$. Now we want to define $t_{r+1}, \ldots, t_n$ in such a way that

$$[(s_i, t_i), (s_j, t_j)] = \langle s_i, t_j\rangle - \langle s_j, t_i\rangle = 0 \tag{8.4}$$

for all $i, j \in [n]$. Because L is Lagrangian, equation (8.4) already holds for $i, j \in [r]$. Note that (8.4) holds trivially for $i = j$, and by the symmetry of equation (8.4), it is enough to prove that the equation holds for $i \leq j$.

So we suppose that $t_1, \ldots, t_k$ have been defined for some $k \in [n]$, such that (8.4) holds for $i, j \in [k]$. We must define a t_{k+1} that satisfies

$$\langle s_i, t_{k+1} \rangle - \langle s_{k+1}, t_i \rangle = 0 \tag{8.5}$$

for $i \in [k]$. This is equivalent to finding a solution for the following set of linear equalities

$$\begin{pmatrix} s_1^T \\ \vdots \\ s_k^T \end{pmatrix} t_{k+1} = \begin{pmatrix} \langle s_{k+1}, t_1 \rangle \\ \vdots \\ \langle s_{k+1}, t_k \rangle \end{pmatrix} \tag{8.6}$$

Since all the rows of the matrix $\begin{pmatrix} s_1^T \\ \vdots \\ s_k^T \end{pmatrix}$ are linearly independent, its rank is equal to k. Therefore, its image is $\mathbb{F}_p^k$ and there must exist a vector t_{k+1} satisfying equation (8.6).

Now that we have found vectors $t_1, \ldots, t_n$ we can define the matrix $M \in \mathbb{F}_p^{n \times n}$ by

$$M : \sum_{i=1}^{n} \alpha_i s_i \mapsto \sum_{i=1}^{n} \alpha_i t_i \tag{8.7}$$

It is still left to verify that M is symmetric. By equation (8.4), for any $i < j$ $s_i^T M s_j = s_j^T M s_i$. By symmetry, $s_i^T M s_j = s_j^T M s_i$ for any $i, j \in [n]$. For $x, y \in [n]$, let e_x, e_y be the x-th and y-th standard basis vector. Let $\alpha_i, \beta_j \in \mathbb{F}_p$ for $i, j \in [n]$ be such that $e_x = \sum_{i=1}^{n} \alpha_i s_i$ and $e_y = \sum_{j=1}^{n} \beta_j s_j$. Then,

$$\begin{aligned}
M_{yx} &= e_y^T M e_x && (8.8)\\
&= \left(\sum_{i=1}^{n} \alpha_i s_i^T \right) M \left(\sum_{j=1}^{n} \beta_j s_j \right) && (8.9)\\
&= \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_i \beta_j s_i^T M s_j && (8.10)\\
&= \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_i \beta_j s_j^T M s_i && (8.11)\\
&= \left(\sum_{j=1}^{n} \beta_j s_j^T \right) M \left(\sum_{i=1}^{n} \alpha_i s_i \right) && (8.12)\\
&= e_x^T M e_y && (8.13)\\
&= M_{xy}. && (8.14)
\end{aligned}$$

So $M^T = M$ and M is symmetric. ♦

Define $R = \{a : (0, a) \in L\}$ and $S = \{h : (h, Mh) \in T\}$. Note that $\dim R + \dim S = n$, so $\dim S = n - \dim R = \dim R^\perp$ Since L is isotropic, $\langle a, h\rangle = 0$ for all $a \in R$, $h \in S$, and thus $S \subseteq R^\perp$, and their dimensions match, so $S = R^\perp$.

This means that $L = \{(h, Mh + a) : h \in S, a \in R\}$. Now we can write

$$\sum_{(h,a)\in L} |\widehat{\Delta_h f}(a)|^2 = \sum_{a\in R}\sum_{h\in S} |\widehat{\Delta_h f}(Mh + a)|^2 \tag{8.15}$$

We can expand the right hand side as follows:

$$\sum_{a\in R}\sum_{h\in S} |\widehat{\Delta_h f}(Mh + a)|^2 = \sum_{a\in R}\sum_{h\in S} \left| \frac{1}{\sqrt{p^n}} \sum_{x\in\mathbb{F}_p^n} \Delta_h f(x)\omega_p^{\langle x, Mh+a\rangle} \right|^2 \tag{8.16}$$

$$= \frac{1}{p^n} \sum_{a\in R}\sum_{h\in S}\sum_{x,x'\in\mathbb{F}_p^n} \Delta_h f(x)\overline{\Delta_h f(x')}\omega_p^{\langle x-x', Mh+a\rangle} \tag{8.17}$$

$$= \frac{1}{p^n} \sum_{h\in S}\sum_{x,x'\in\mathbb{F}_p^n} \Delta_h f(x)\overline{\Delta_h f(x')}\omega_p^{\langle x-x', Mh\rangle} \left(\sum_{a\in R} \omega_p^{\langle x-x', a\rangle} \right) \tag{8.18}$$

$$= \frac{|R|}{p^n} \sum_{h\in S}\sum_{x,x'\in\mathbb{F}_p^n} \Delta_h f(x)\overline{\Delta_h f(x')}\omega_p^{\langle x-x', Mh\rangle} \mathbb{1}[x - x' \in R^\perp] \tag{8.19}$$

$$\tag{8.20}$$

Now we can make the variable substitution where we leave x as x and substitute x' with $x + h'$ for $h' \in R^\perp = S$. Also, since $\dim R + \dim S = n$, we get $\frac{|R|}{p^n} = \frac{1}{|S|}$,

$$\frac{|R|}{p^n} \sum_{h\in S}\sum_{x,x'\in\mathbb{F}_p^n} \Delta_h f(x)\overline{\Delta_h f(x')}\omega_p^{\langle x-x', Mh\rangle} \mathbb{1}[x - x' \in R^\perp] \tag{8.21}$$

$$= \frac{1}{|S|} \sum_{h,h'\in S}\sum_{x\in\mathbb{F}_p^n} \Delta_h f(x)\overline{\Delta_h f(x + h')}\omega_p^{-\langle h', Mh\rangle} \tag{8.22}$$

$$\tag{8.23}$$

Define the bilinear form $\beta(y, y') = \langle y', My\rangle$, and the induced quadratic form $Q(y) = \beta(y, y)$. For uneven characteristic, we have the following identity:

$$Q(x) - Q(x + h) - Q(x + h') + Q(x + h + h') = 2\beta(h, h') \mod p \tag{8.24}$$

This can be verified by direct computation using the bilinearity of β and the definition of Q.

Then we can define $g(x) = f(x)\omega_p^{-\frac{1}{2}Q(x)}$. This allows us to rewrite the right hand side of equation (8.22) as

$$\frac{1}{|S|} \sum_{h,h'\in S}\sum_{x\in\mathbb{F}_p^n} g(x)\overline{g(x + h)g(x + h')}g(x + h + h') \tag{8.25}$$

For even characteristic, the same equality holds $\mod 4$:

$$Q(x) - Q(x+h) - Q(x+h') + Q(x+h+h') = 2\beta(h,h') \mod 4 \tag{8.26}$$

We can take the exponent with base i on both sides of the equation,

$$i^{Q(x)}\overline{i^{Q(x+h)}i^{Q(x+h')}}i^{Q(x+h+h')} = (-1)^{\beta(h,h')} \tag{8.27}$$

So in this case we can define $g(x) := f(x)i^{Q(x)}$ and get, like in the uneven characteristic, (8.22) equals

$$\frac{1}{|S|}\sum_{h,h'\in S}\sum_{x\in\mathbb{F}_p^n} g(x)\overline{g(x+h)g(x+h')}g(x+h+h'). \tag{8.28}$$

We let $\mathbb{F}_p^n = S \oplus \overline{S}$, and define for all $y \in \overline{S}$ $g_y : S \to \mathbb{C}$ by $g_y(x) = g(x+y)$. Let $\widehat{S} : S \to \mathbb{C}$ be the character group of S and define the Fourier transform $\widehat{g_y} : \widehat{S} \to \mathbb{C}$ as

$$\widehat{g_y}(\chi) = \frac{1}{\sqrt{|S|}}\sum_{x\in S} g_y(x)\overline{\chi(x)} \tag{8.29}$$

Then by Lemma 2.2.4, equation 8.28 is equal to

$$\frac{1}{|S|}\sum_{h,h'\in S}\sum_{x\in\mathbb{F}_p^n} g(x)\overline{g(x+h)g(x+h')}g(x+h+h') \tag{8.30}$$

$$= \frac{1}{|S|}\sum_{y\in\overline{S}}\sum_{x,h,h'\in S} g_y(x)\overline{g_y(x+h)g_y(x+h')}g_y(x+h+h') \tag{8.31}$$

$$= \sum_{y\in\overline{S}}\sum_{\chi\in\widehat{S}}\widehat{|g_y(\chi)|}^4. \tag{8.32}$$

By Parseval (Lemma 2.1.8) we have

$$\sum_{y\in\overline{S}}\sum_{\chi\in\widehat{S}}|\widehat{g_y}(\chi)|^2 = \sum_{y\in\overline{S}}\sum_{x\in S}|g_y(x)|^2 \tag{8.33}$$

$$= \sum_{x\in\mathbb{F}_p^n}|f(x)|^2 \tag{8.34}$$

$$= 1. \tag{8.35}$$

If we take $y' \in \overline{S}$ and $\chi' \in \widehat{S}$ such that $|\widehat{g_{y'}}(\chi')|^2 = \max_{(y,\chi)\in(\overline{S},\widehat{S})}|\widehat{g_y}(\chi)|^2$, we get

$$\sum_{(h,a)\in L}|\widehat{\Delta_h f}(a)|^2 = \sum_{y\in\overline{S}}\sum_{\chi\in\widehat{S}}\widehat{|g_y(\chi)|}^4 \tag{8.36}$$

$$\leq |\widehat{g_{y'}}(\chi')|^2\sum_{y\in\overline{S}}\sum_{\chi\in\widehat{S}}\widehat{|g_y(\chi)|}^2 \tag{8.37}$$

$$= |\widehat{g_{y'}}(\chi')|^2 \tag{8.38}$$

Let $\alpha \in S$ such that $\chi'(x) = \omega_p^{\langle \alpha, x \rangle}$. For uneven p, we can unfold $|\widehat{g_{y'}}(\chi')|^2$ as follows:

$$|\widehat{g_{y'}}(\chi')|^2 = \left| \frac{1}{\sqrt{|S|}} \sum_{x \in S} g(x+y) \omega_p^{-\langle \alpha, x \rangle} \right|^2 \tag{8.39}$$

$$= \left| \frac{1}{\sqrt{|S|}} \sum_{x \in S+y'} f(x) \omega_p^{-\frac{1}{2}\langle x, Mx \rangle} \omega_p^{-\langle \alpha, x-y' \rangle} \right|^2 \tag{8.40}$$

$$= \left| \frac{1}{\sqrt{|S|}} \sum_{x \in \mathbb{F}_p^n} f(x) \overline{s(x)} \right|^2 \tag{8.41}$$

where we define $s : \mathbb{F}_p^n \to \mathbb{C}$ as

$$s(x) = \frac{1}{\sqrt{|S|}} \omega_p^{\frac{1}{2}\langle x, Mx \rangle + \langle \alpha, x \rangle} \mathbb{1}[x \in S + y']. \tag{8.42}$$

For $p = 2$, let $A \in \mathbb{F}_2^{n \times n}$ be the matrix with entries $A_{ij} = \mathbb{1}[i < j] M_{ij}$ for $i, j \in [n]$, and let $D \in \mathbb{F}_2^{n \times n}$ be the diagonal of M. Let $\beta \in \mathbb{F}_2^n$ such that $D_{ii} = \beta_i$. Then $M = A + A^T + D$. Then

$$\langle x, Mx \rangle = 2\langle x, Ax \rangle + \langle x, Dx \rangle = 2\langle x, Ax \rangle + \langle \beta, x \rangle \tag{8.43}$$

where in the second equality we use $x_i^2 = x_i$ for $i \in [n]$ since we are working over $\mathbb{F}_2$. This means that $i^{-\langle x, Mx \rangle} = i^{-\langle \beta, x \rangle} (-1)^{\langle x, Ax \rangle}$. Similar to the case where p is uneven, we can write out $|\widehat{g_{y'}}(\chi')|^2$ as follows:

$$|\widehat{g_{y'}}(\chi')|^2 = \left| \frac{1}{\sqrt{|S|}} \sum_{x \in S} g(x+y) (-1)^{\langle \alpha, x \rangle} \right|^2 \tag{8.44}$$

$$= \left| \frac{1}{\sqrt{|S|}} \sum_{x \in S+y'} f(x) i^{-\langle \beta, x \rangle} (-1)^{\langle x, Ax \rangle} (-1)^{\langle \alpha, x-y' \rangle} \right|^2 \tag{8.45}$$

$$= \left| \frac{1}{\sqrt{|S|}} \sum_{x \in \mathbb{F}_p^n} f(x) \overline{s(x)} \right|^2 \tag{8.46}$$

where we define

$$s(x) = \frac{1}{\sqrt{|S|}} i^{2\langle \alpha, x \rangle + \langle \beta, x \rangle} (-1)^{\langle x, Ax \rangle} \mathbb{1}[x \in S + y']. \tag{8.47}$$

□

9 Proof of Theorem 1.2.5

We are now ready to prove the main theorem.

of Theorem 1.2.5. By Lemma 4.2.4 there exists a subspace $V \subseteq \mathbb{F}_p^{2n}$ such that

- $\sum_{(h,a)\in V} |\widehat{\Delta_h f}(a)|^2 \geq \text{poly}(\epsilon)$
- $|V| \leq \text{poly}(\epsilon) p^n$
- $|V| \geq \text{poly}(\frac{1}{\epsilon}) p^n$

Then from Lemma 7.2.3 we get a Lagrangian $L \subseteq \mathbb{F}_p^{2n}$ such that $\sum_{(h,a)\in L} |\widehat{\Delta_h f}(a)|^2 \geq \text{poly}(\epsilon)$. Now by Lemma 8.1.1 there exists a stabilizer s such that $|\langle s, f\rangle|^2 \geq \text{poly}(\epsilon)$. $\square$

10 The U^3-norm in a quantum setting

In this section we will talk about a state $|\psi\rangle$ defined by a function $f : \mathbb{F}_p^n \to \mathbb{C}$ by

$$|\psi\rangle = \sum_{x \in \mathbb{F}_p^n} f(x)|x\rangle. \tag{10.1}$$

10.1 Stabilizer states

In Definition 2.2.7 we defined the set of stabilizer states $\mathcal{S}$ as

$$\mathcal{S} = \{f : \mathbb{F}_p^n \to \mathbb{C} \text{ such that } ||f||_2 = 1 \text{ and } ||f||_{U^3} = 1\}. \tag{10.2}$$

As we saw in Propositions 2.2.8, 2.2.9, the functions $s \in \mathcal{S}$ are of a specific form.

Stabilizers are of interest in quantum computing and quantum information theory for a number of reasons, some of which we mention here. Stabilizer states can equivalently be defined as the set of states reachable from the state $|0\rangle$ by a Clifford circuit. A Clifford circuit is a quantum circuit using only the gates $CNOT, H$ and S, that are defined as

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}. \tag{10.3}$$

By the Gottesman-Knill theorem, any Clifford circuit is efficiently simulatable on a classical computer [37]. This means that any quantum computer running only on stabilizer states does not have a fundamental advantage over a classical computer.

Stabilizer states and the Clifford group are also of interest in quantum error correction [16, 17]. For more background on stabilizer states, we refer the reader to [2, 12, 1].

10.2 Tolerant testing algorithm

The Gowers U^3-norm is in fact a quantum testable property, by a procedure called Bell difference sampling [22]. We define the charactersistic distribution of a state as $p_\psi(h, a) = |\widehat{\Delta_h f}(a)|^2$. This is indeed a distribution, by Propoisition 2.2.3. Then we define the distribution $q_\psi(h, a) = (p_\psi * p_\psi)(h, a) = \sum_{(h',a')} p_\psi(h', a')p_\psi(h - h', a - a')$. Then we have the following

$$||f||_{U^3}^8 = \sum_{h,a} p^n |\widehat{\Delta_h f}(a)|^4 = \mathbb{E}_{(h,a)\sim p_\psi}[p^n p_\psi(h, a)] \tag{10.4}$$

By [15, Lemma 3.3],

$$\mathbb{E}_{(h,a)\sim p_\psi}[p^n p_\psi(h,a)] \geq \mathbb{E}_{(h,a)\sim q_\psi}[p^n p_\psi(h,a)] \geq \left(\mathbb{E}_{(h,a)\sim p_\psi}[p^n p_\psi(h,a)]\right)^2. \tag{10.5}$$

If we perform Bell difference sampling, we are essentially sampling from a Bernoulli distribution B where $\mathbb{P}(B=1) = p_{accept} = \frac{1}{2} + \frac{1}{2}\mathbb{E}_{x\sim q_\psi}[p^n p_\psi(h,a)]$.

What this means is that given enough copies of a quantum state $|\psi\rangle = \sum_{x\in\mathbb{F}_p^n} f(x)|x\rangle$ we can estimate $\mathbb{E}_{(h,a)\sim q_\psi}[p^n p_\psi(h,a)]$, which is a good estimate for $||f||_{U^3}^8$ by equations (10.5) and (10.4).

We can turn this into a tolerant testing algorithm. In tolerant testing, we are given a state $|\psi\rangle$ with the promise that $\mathcal{F}_{\mathcal{S}}(|\psi\rangle)$ is either larger than ϵ_1 or smaller than ϵ_2, and the task is to find out which is the case. If the outcome of Bell difference sampling is that $||f||_{U^3}$ is high, then we can use Theorem 1.2.5 to conclude that the stabilizer fidelity is high.

1. Estimate $||f||_{U^3}$ with Bell difference sampling
2. If $||f||_{U^3}$ is larger than some threshold $D = D(\epsilon_1, \epsilon_2)$, output $\mathcal{F}_{\mathcal{S}}(|\psi\rangle) \geq \epsilon_1$. Otherwise, output $\mathcal{F}_{\mathcal{S}}(|\psi\rangle) \leq \epsilon_2$.

The following theorem is proven in [5]:

Theorem 10.2.1. *Let $\epsilon_1, \epsilon_2 \in [0,1]$ and let $|\psi\rangle$ be a state with stabilizer fidelity*

$$\mathcal{F}_S(|\psi\rangle) := \max_{|S\rangle\in \mathrm{STAB_n}} |\langle\psi|S\rangle|^2, \tag{10.6}$$

either (1) larger than ϵ_1 or (2) smaller than ϵ_2. If $\epsilon_2 \leq C'\epsilon_1^{6534}$ for some constant C', then $O\big(\epsilon_1^{-12}\big)$ rounds of Bell difference sampling can distinguish between case (1) and case (2) with probability greater than $2/3$.

11 Conclusion and Discussion

The main result in this thesis is Theorem 1.2.5. In order to prove this theorem, we have used techniques from higher order Fourier analysis, additive combinatorics, symplectic geometry and quantum information theory.

We have seen that this theorem implies a tolerant testing algorithm for stabilizer states. Because the dependence on ϵ in Theorem 1.2.5is polynomial, this algorithm runs in polynomial time, and the gap between ϵ_1 and ϵ_2 in Theorem 10.2.1 is polynomial.

Although a proof of this theorem was already given in [5], our proof uses only Theorems 4.1.4, 4.2.3 as a black box. The rest of the proof is self-contained.

In this thesis, we did not calculate an explicit exponent, but the exponent in [5] is 1089. However, for a fair comparison we should still multiply this with 16, since in [5], the authors have a different assumption about f, see also [15, Lemma 3.3].

11.1 Further research

It is quite unlikely that either this thesis or [5] gives an optimal exponent C_1 in Theorem 1.2.5. For practical applications, it is of interest to minimize C_1.

We have said nothing about how hard it is to find a stabilizer for which the inner product with a given function f is high. Whether or not it is possible to come up with an algorithm that gives a stabilizer, is up to future research. If we wanted to adapt our proof to an algorithmic version, we would need to know what the set X, defined in Section 3.1 looks like, and the naïve calculation takes exponential time. Also, we use Theorems 4.1.4, 4.2.3 as a black box, and we use the pidgeonhole principle in section 7.2, which further complicate adapting our proof to an algorithmic proof.

It is our hope that this proof paves the way for a U^4 inverse theorem with the L^2 normalization assumption. We can get an expression like Proposition 2.2.5, which gives

$$||f||_{U^4}^{16} = \sum_{h,h' \in \mathbb{F}_p^n} ||\Delta_h \Delta_{h'} f||_{U^2}^4 \sum_{h,h',a \in \mathbb{F}_p^n} |\widehat{\Delta_h \Delta_{h'}} f(a)|^4. \tag{11.1}$$

It is possible that the techniques applied in this thesis can be applied.

To our knowledge, there is no direct quantum analog of the U^4-norm. This line of research would be motivated from higher order Fourier analysis.

It could also be interesting to see if the same techniques we used in the proof of Theorem 1.2.5, particularly those in chapter 7, can be applied in the L^∞ setting of Theorem 1.2.3.

Popular summary

A classical computer does operations on states consisting of a specific string of zeroes and ones, called bitstrings. In contrast, a quantum computer does operations on a superposition of bitstrings. These superpositions are known as quantum states. These superposition can be seen as a combination or mixture of bitstrings. Each bitstring has a complex number, known as an amplitude, associated with it. Since there are 2^n possible bitstrings of length n, writing down the entire quantum state explicitly would require us to write down 2^n complex numbers. For most states we are interested in, this number will be much too large.

There is another problem that we run into. By the nature of quantum mechanics, if we measure the state to get some information about it, we destroy the state. The outcome of a measurement will be a bitstring of length n, which is very little information compared to the full 2^n-dimensional complex vector that describes the whole quantum state.

For the reasons mentioned above, we are interested in a certain class of quantum states that have a short description. Examples of these states can be states that have amplitude 1 on a bitstring $x \in \{0,1\}^n$ and 0 on all other bitstrings. Another example would be states for which the amplitude is a relatively simple function of the bitstring.

An example of a simple function could be a polynomial, specifically a quadratic polynomial. A state could have amplitudes $c_x = \frac{1}{\sqrt{2^n}}(-1)^{q(x)}$ for $x \in \{0,1\}^n$, where q is a polynomial of degree 2 in variables $X_1, \ldots, X_n$. In order to give a complete description of this state we only have to give the polynomial q. States like this are called stabilizer states.

Consider the following problem: we are given a quantum state $|\psi\rangle$, that has been calculated by a quantum computer. We can repeat this calculation, but it takes some time to do. If we want a complete description of the state, up to a small error margin, we need to run an exponential amount of tests. In order to make things easier, we adjust the question. What if we only have to find a description of a state $|\phi\rangle$ that is sufficiently close $|\psi\rangle$, such that $|\phi\rangle$ has a short description? Can we do this in a manageable timeframe?

In this thesis, we prove a theorem that puts a step in this direction. The theorem tells us that we can run some tests on $|\psi\rangle$, and according to the outcome of these tests, we can decide if $|\psi\rangle$ is close to one of the stabilizer states. If the answer is yes, we would also like to know which stabilizer state $|\psi\rangle$ is close to. This is something the theorem does not tell us, but hopefully, in future research, we will be able to answer this question.

Bibliography

[1] Daniel Gottesman. Stabilizer codes and quantum error correction, 1997.

[2] Maarten Van den Nest. Local equivalence of stabilizer states and codes. 2005.

[3] W. T. Gowers, Ben Green, Freddie Manners, and Terence Tao. On a conjecture of Marton, 2023.

[4] W. T. Gowers, Ben Green, Freddie Manners, and Terence Tao. Marton's conjecture in Abelian groups with bounded torsion, 2024.

[5] Zongbo Bao, Philippe van Dordrecht, and Jonas Helsen. Tolerant testing of stabilizer states with a polynomial gap via a generalized uncertainty relation, 2024. `https://arxiv.org/abs/2410.21811`.

[6] Terence Tao and Van H. Vu. *Additive Combinatorics*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2006.

[7] Yufei Zhao. *Graph Theory and Additive Combinatorics: Exploring Structure and Randomness*. Cambridge University Press, 2023.

[8] Endre Szemerédi. On sets of integers containing k elements in arithmetic progression. *Acta Arithmetica*, 27:199–245, 1975.

[9] W. T. Gowers. A new proof of Szemerédi's theorem. *Geometric & Functional Analysis GAFA*, 11(3):465–588, Aug 2001.

[10] T. Tao. *Higher Order Fourier Analysis*. Graduate studies in mathematics. American Mathematical Society, 2012.

[11] Ben Green and Terence Tao. The primes contain arbitrarily long arithmetic progressions, 2007.

[12] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[13] Scott Aaronson. *Quantum Computing since Democritus*. Cambridge University Press, 2013.

[14] Martin Ringbauer. *Exploring Quantum Foundations with Single Photons*. Imprint: Springer, Cham, 2017.

[15] Srinivasan Arunachalam and Arkopal Dutt. Polynomial-time tolerant testing stabilizer states, 2024. https://arxiv.org/abs/2408.06289.

[16] A. R. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, Aug 1996.

[17] Peter W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52:R2493–R2496, Oct 1995.

[18] Héctor J. García, Igor L. Markov, and Andrew W. Cross. On the geometry of stabilizer states, 2017.

[19] Ben Green and Terence Tao. An inverse theorem for the gowers U^3-norm, 2023.

[20] Alex Samorodnitsky. Low-degree tests at large distances. In *Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing*, STOC '07, page 506–515, New York, NY, USA, 2007. Association for Computing Machinery.

[21] Ashley Montanaro. Learning stabilizer states by bell sampling, 2017.

[22] David Gross, Sepehr Nezami, and Michael Walter. Schur–Weyl duality for the Clifford group with applications: Property testing, a robust Hudson theorem, and de Finetti representations. *Communications in Mathematical Physics*, 385(3):1325–1393, June 2021.

[23] Jeroen Dehaene and Bart De Moor. Clifford group, stabilizer states, and linear and quadratic operations over GF(2). *Physical Review A*, 68(4), October 2003.

[24] Erik Hostens, Jeroen Dehaene, and Bart De Moor. Stabilizer states and Clifford operations for systems of arbitrary dimensions and modular arithmetic. *Physical Review A*, 71(4), April 2005.

[25] Ben Green. Montreal lecture notes on quadratic Fourier analysis, 2007.

[26] R. Wheeden, R.L. Wheeden, and A. Zygmund. *Measure and Integral: An Introduction to Real Analysis*. Chapman & Hall/CRC Pure and Applied Mathematics. Taylor & Francis, 1977.

[27] Antal Balog and Endre Szemerédi. A statistical theorem of set addition. *Combinatorica*, 14(3):263–268, Sep 1994.

[28] G.A. Freĭman. *Foundations of a Structural Theory of Set Addition*. Translations of mathematical monographs. American Mathematical Society, 1973.

[29] Imre Z. Ruzsa. An analog of Freĭman's theorem in groups. 1993.

[30] A.C. da Silva. *Lectures on Symplectic Geometry*. Number nr. 1764 in Lecture Notes in Mathematics. Springer, 2001.

[31] J. v. Neumann. Die Eindeutigkeit der Schrödingerschen Operatoren. *Mathematische Annalen*, 104(1):570–578, Dec 1931.

[32] D. Gross. Hudson's theorem for finite-dimensional quantum systems. *Journal of Mathematical Physics*, 47(12), December 2006.

[33] L.L. Scott and J.P. Serre. *Linear Representations of Finite Groups*. Graduate Texts in Mathematics. Springer New York, 1996.

[34] Fiona Murnaghan. Lecture notes introduction to representation theory. `https://www.math.utoronto.ca/fiona/courses/mat445/notes.pdf`.

[35] B. Hall. *Lie Groups, Lie Algebras, and Representations: An Elementary Introduction*. Graduate Texts in Mathematics. Springer International Publishing, 2015.

[36] M. Artin. *Algebra*. Pearson Education, 2011.

[37] Daniel Gottesman. The Heisenberg representation of quantum computers, 1998.