FAKULTAT FUR MATHEMATIK, INFORMATIK
UND NATURWISSENSCHAFTEN

RHEINISCH-WESTFALISCHE TECHNISCHE
HOCHSCHULE AACHEN

Bachelorarbeit in Mathematik

im September 2012

# On Weight Enumerators of Quantum Codes

Andrés Wilhelm Goens Jokisch

LEHRSTUHL D FÜR MATHEMATIK
Prof. Dr. Gabriele Nebe

Ich versichere, dass ich die Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt, sowie Zitate kenntlich gemacht habe.

Aachen, den 28. September 2012

# Contents

**Table of Contents** **1**

**Introduction** **2**

**Acknowledgements** **2**

**1 Preliminaries** **3**
1.1 On Notational Conventions in this Thesis . . . . . 3
1.2 Remarks on Linear Algebra . . . . . 4
1.3 The Pauli Group . . . . . 5
1.4 Random Unitary Matrices . . . . . 7
1.5 Physical Background: the Postulates of Quantum Mechanics . 9

**2 Qubits and Quantum Codes** **11**
2.1 Error Correction . . . . . 11
2.2 Additive Codes . . . . . 14
2.3 Logical Operators . . . . . 15
2.4 Code Distance . . . . . 16
2.5 CSS Codes . . . . . 18

**3 Quantum Weight Enumerators** **19**
3.1 The Shor-Laflamme and Rains enumerators . . . . . 19
3.2 The Relationship between the Enumerators . . . . . 22
3.3 The MacWilliams Transform . . . . . 26

**4 Applications of the Weight Enumerators: Bounds** **28**
4.1 The Relationship between the Code Distance and the Enumerators . . . . . 28
4.2 Shadow Enumerators . . . . . 35
4.3 Automorphisms of Codes . . . . . 39

**5 References** **43**

# Introduction

Coding theory has played a very important role on the development of modern computers. If large-scale quantum computing is ever going to be possible, it is only plausible to assume that quantum codes will play a similar role. In this thesis we will introduce the subject of quantum coding theory, and in an analogy to classical coding theory, we will develop the theory of quantum Weight Enumerators to get bounds for quantum error correcting codes. In Section 1 a few mathematical preliminaries will be treated: results that while are not part of the standard curriculum of mathematics, do not directly belong to quantum coding theory. As a bachelors thesis in mathematics, we will assume the reader has no prior knowledge of quantum mechanics and the physical preliminaries, these will be therefore also covered. Section two will then follow and introduce quantum codes, explaining how coding, decoding and error detection and correction should work in principle. Section 3 then goes on to introduce the quantum Weight Enumerators and a few properties of these, and Section 4 presents one of the main uses for them, which is that of finding bounds on the minimal distance or code space dimension for quantum error correcting codes.

# Acknowledgements

I want to thank Prof. Dr. Gabriele Nebe for all the patience she had with me for this thesis, and for all her help on it.

# 1 Preliminaries

The aim of this section is only to introduce the mathematical and physical preliminaries needed for the rest of the thesis, which thematically however, do not belong in the other chapters.

## 1.1 On Notational Conventions in this Thesis

Throughout this thesis we will use a few concepts for which there is not one single standard notation, or for which the notation is sometimes used elsewhere. To help clarify problems that might arise, we will here note some of the most important of these notations.

This thesis will use the so-called bra and ket notation: Let $\mathcal{H}$ be a finite-dimensional complex Hilbert space. We will denote elements of $\mathcal{H}$ as so-called kets: $|v\rangle \in \mathcal{H}$. For the scalar product of $|v\rangle, |w\rangle \in \mathcal{H}$ we will write $\langle v|w\rangle$. The dual space of $\mathcal{H}$ (the space of linear forms), we will denote by $\mathcal{H}^* := \mathrm{Hom}(\mathcal{H}, \mathbb{C})$. Through the scalar product on $\mathcal{H}$ we get a canonical isomporhism from $\mathcal{H}$ to $\mathcal{H}^*$, which maps $\mathcal{H} \ni |v\rangle \mapsto (|w\rangle \mapsto \langle v|w\rangle) \in \mathcal{H}^*$ to the linear form given by taking the scalar product. We will identify $\mathcal{H}$ with $\mathcal{H}^*$ through this isomorphism and write the image of $|v\rangle \in \mathcal{H}$ under this isomorphism as $\langle v|$. Since by definition, applying the linear form on a vector $|w\rangle \in \mathcal{H}$ coincides with the scalar product, we will write both the same, leaving one of the | characters which would correspond on the former: $\langle v|w\rangle \equiv \langle v||w\rangle := (\langle v|)(|w\rangle)$. Since we are dealing with finite dimensional vectorspace, we will often explicitly use $\mathcal{H} := \mathbb{C}^n$ for an integer $n$. In this case, we will think of the elements of $\mathcal{H}$ as column vectors, and will identify $\mathcal{H}^*$ with row vectors. The canonical isomorphism then becomes hermitian conjugation, i.e. transposition and complex conjugation. For a general complex $n \times m$ matrix $A \in \mathbb{C}^{n\times m}$ we will use the notation $A^\dagger$ to refer to the hermitian conjugate.

A few further notational conventions adopted in this thesis are the following: Let $V, W$ be vector spaces over a field $K$, and let $A$ be an endomorphism of $V$, i.e. a linear mapping $A \in \mathrm{Hom}_K(V, V)$

- By $\mathrm{Tr}(A)$ we denote the trace of the endomorphism $A$ (the same for a square matrix)
- By $V \otimes W$ we denote the tensor-product of $V$ and $W$. This will be treated as the Kronecker-Product on all finite dimensional vector spaces.

- Let $G$ be a group acting on $V$ and $W$. Through this, $V$ and $W$ become $KG$-Modules. We denote by $\mathrm{Hom}_G(V, W)$ the set of G-Homomorphisms from $V$ to $W$ (i.e., G-equivariant homomorphisms)
- We denote with $\mathrm{Im}(A)$ the image the mapping $A$, $\mathrm{Ker}(A)$ its kernel. The same notation will be used for other mappings where it makes sense.

Also, some group theoretical notational conventions we will assume: Let $G, H$ be two groups, and let $H$ act on the set $\Omega$. then we denote by $G \wr_\Omega H$ the wreath product of G and H with respect to the action of $H$ on $\Omega$. When this action is clear from the context, we will omit it. We will denote by $D_n = \langle a, b \mid a^2 b^n (ab)^2 \rangle$ the dihedral group on a regular polygon with n sides.

Further, we will work with finite fields, which we will denote by $\mathbb{F}_q$ for a prime power $q$. For $q = 4$ we will fix the construction as $\mathbb{F}_2[x]/(x^2+x+1)$ and will use $\omega \in \mathbb{F}_4$ to denote the residue class of $x$ modulo the ideal generated by $x^2 + x + 1$, i.e. $\omega^2 + \omega + 1 = 0$ in $\mathbb{F}_4$.

A list of these conventions and further ones introduced later can be found at the end of the thesis.

## 1.2 Remarks on Linear Algebra

Throughout this thesis we will focus mainly on tensor product spaces of a particular finite-dimensional complex Hilbert space. Recall that a complex Hilbert space $\mathcal{H}$ is a complete complex vector space with a complex scalar product $\langle \cdot, \cdot \rangle$, i.e. a positive-definite, hermitian, bilinear form. Every finite dimensional complex vector space with a scalar product is complete, and as we will only work with such in these thesis, we need not worry about the completeness.

**Remark 1.1.** The trace function $\mathrm{Tr} : \mathbb{C}^{n\times n} \to \mathbb{C}$ induces an associative, symmetric, bilinear form on $\mathbb{C}^{n\times n}$, the trace bilinar form: $\mathrm{Tr} : \mathbb{C}^{n\times n} \times \mathbb{C}^{n\times n} \to \mathbb{C}, (A, B) \mapsto \mathrm{Tr}(AB)$. This means the following:

- $\mathrm{Tr}(kA + B, C) = k\mathrm{Tr}(A, C) + \mathrm{Tr}(B, C)$ for all $A, B, C \in \mathbb{C}^{n\times n}, k \in \mathbb{C}$.
- $\mathrm{Tr}(A, B) = \mathrm{Tr}(B, A)$ for all $\mathbb{C}^{n\times n}$.
- $\mathrm{Tr}(AB, C) = \mathrm{Tr}(B, CA)$ for all $A, B, C \in \mathbb{C}^{n\times n}$.

All of which immediately follow from the definition.

**Definition 1.2.** Let $V, W$ be finite-dimensional Hilbert spaces, and $A \in \mathrm{End}(V), B \in \mathrm{End}(W)$ Hermitian. We define the partial trace of $A \otimes B$ over $W$ as $\mathrm{Tr}_W(A \otimes B) := \mathrm{Tr}(B)A$, and extend the definition linearly. Since the trace is linear, this is well defined.

**Proposition 1.3.** With the notation from Def. 1.2, the partial trace of $A \in \mathrm{End}(V \otimes W)$ Hermitian, is the unique Hermitian operator $\mathrm{Tr}_W(A) \in \mathrm{End}(V)$ which satisfies:

$$\mathrm{Tr}(A(B \otimes \mathrm{Id}_W)) = \mathrm{Tr}(\mathrm{Tr}_W(A)B) \text{ for all } B \in \mathrm{End}(V) \text{ Hermitian} \quad (1)$$

*Proof.* $\mathrm{Tr}_W(A)$ is hermitian since $A$ already is. Let $A = \sum_{i=1}^k V_i \otimes W_i$ with $V_i \in \mathrm{End}(V), W_i \in \mathrm{End}(W)$ Hermitian for all $i \in \underline{k}$. Then $\mathrm{Tr}_W(A) = \sum_{i=1}^k \mathrm{Tr}(W_i)V_i$ satisfies for all $B \in \mathrm{End}(W)$Herm.:

$$\mathrm{Tr}(A(B \otimes \mathrm{Id}_W)) = \mathrm{Tr}(\sum_{i=1}^k V_i B \otimes W_i)$$

$$= \sum_{i=1}^k \mathrm{Tr}(V_i B)\mathrm{Tr}(W_i) = \mathrm{Tr}(\sum_{i=1}^k V_i B \mathrm{Tr}(W_i)) = \mathrm{Tr}(\mathrm{Tr}_W(A)B)$$

Further is $\mathrm{Tr}_W(A)$ unique with this property, since the restriction of trace bilinear form to hermitian operators is non-degenerate. Assuming there is a $T \in \mathrm{End}(V)$ hermitian with $\mathrm{Tr}(TB) = Tr(A(B \otimes Id_W)) = \mathrm{Tr}(\mathrm{Tr}_W(A)B)$ for all $B \in \mathrm{End}(W)$Herm., then it follows that $\mathrm{Tr}((T - \mathrm{Tr}_W(A)), B) = 0$ for all such $B$ which implies that $T - \mathrm{Tr}_W(A) = 0$. □

**Remark 1.4.** Let $\mathcal{H}$ be a Hilbert space with a particular decomposition $\mathcal{H} = V_1 \otimes \ldots \otimes V_n$, e.g.$(\mathbb{C}^2)^{\otimes n}$with $V_i \cong \mathbb{C}^2$ for all $i \in \underline{n}$, and $S \dot{\cup} S^c = \underline{n}, S = \{s_1 < \ldots < s_j\}, S^c = \{s_1^c < \ldots < s_k^c\}$ we define $V_S := V_{s_1} \otimes \ldots \otimes V_{s_j}, V_{S^c} := V_{s_1^c} \otimes \ldots \otimes V_{s_k^c}$. And use $\mathrm{Tr}_S$ as a short notation for $\mathrm{Tr}_{V_S} : \mathrm{End}(V_1 \otimes \ldots \otimes V_n) \to \mathrm{End}(V_{S^c})$. Note that for $s_j \geq s_1^c$ this is not entirely correct, since we cannot write $V$ as $V_S \otimes V_{S^c}$, but we get a canonical isomorphism from reordering the tensor product components, and by abuse of notation we will always identify $V$ with its image under it, such that we can always write $V = V_S \otimes V_{S^c}$. With this notation, and the definition of the partial trace it is easy to see that $\mathrm{Tr}_{S \dot{\cup} S'}(A) = \mathrm{Tr}_S(\mathrm{Tr}_{S'}(A))$ for all $S, S' \subseteq \underline{n}$ disjoint.

## 1.3 The Pauli Group

**Definition 1.5.** The Pauli matrices, or Pauli operators on $\mathbb{C}^2$ are defined by:

$$\mathrm{Id}, X := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Z := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, Y := iXZ = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix} \quad (2)$$

We denote with

$$\begin{aligned}\mathcal{E}_n &:= \{\sigma_1 \otimes \ldots \otimes \sigma_n, \text{ where } \sigma_i \in \{I, X, Y, Z\} \text{ for all } i \in \underline{n}\} \\ &\subseteq \mathrm{End}((\mathbb{C}^2)^{\otimes n}) := \mathrm{End}(\underbrace{\mathbb{C}^2 \otimes \cdot \otimes \mathbb{C}^2}_{\text{n times}})\end{aligned}$$

the set of all so-called Pauli operators, and by $\mathcal{P}_n := \langle \mathcal{E} \rangle \leq \mathrm{GL}_n(\mathbb{C})$, we denote the generated subgroup, which we will call the Pauli group on n qubits.

**Remark 1.6.** The set $\{\mathrm{Id}, X, Y, Z\}$ is linearly independent and thus forms a basis of $\mathbb{C}^{2\times 2}$. A simple calculation shows that this basis is orthogonal with respect to the trace bilinear form on $\mathbb{C}^{2\times 2}$. Analogously, since $\mathrm{Tr}(A \otimes B) = \mathrm{Tr}(A)\mathrm{Tr}(B)$ for all $A \in \mathbb{C}^{m\times m}, B \in \mathbb{C}^{m'\times m'}$, $\mathcal{E}$ is an orthogonal basis of $\mathbb{C}^{2^n \times 2^n}$.

**Proposition 1.7.** Let $G = \mathcal{P}_n$ be the Pauli group on n qubits. Then the following is true:

a) $Z(G) = \{\pm\mathrm{Id}, \pm i\mathrm{Id}\}$, where $Z(G)$ denotes the center of G.

b) $G' = \pm\{\mathrm{Id}\} \leq Z(G)$, where $G'$ denotes the commutator subgroup of G.

c) $G/Z(G)$ is a $2n$-dimensional $\mathbb{F}_2$ vector space

d) The commutator $[\cdot,\cdot] : G \times G \to G$ induces a non-degenerate symplectic form on $G/Z(G)$: $[gZ(G), hZ(G)] \mapsto [g, h]$.

*Proof.* a) Let $A \in Z(G)$. Since $\langle G \rangle_{\mathbb{C}} = \mathbb{C}^{2^n \times 2^n}$ it means that $A \in \underbrace{Z(\mathbb{C}^{2^n \times 2^n})}_{\mathbb{C}\mathrm{Id}} \cap G = \{\pm\mathrm{Id}, \pm i\mathrm{Id}\}$.

b) It follows directly from the calculation for $X, Y, Z$ and by induction on $n$.

c) Since $G' \leq Z(G)$ is $G/Z(G)$ abelian. By induction on $n$ it can be easily shown that $G^2 \subseteq Z(G)$, hence $G/Z(G)$ is elementary abelian. Since $|G| = 4^n \cdot 4^n = 2^{2n+2}$ it follows that $\dim_{\mathbb{F}_2}(G/Z(G)) = 2n$.

d) Since $G' \leq Z(G)$ the induced mapping is well-defined. Since $[g, g] = 1$ for all $g \in G$ it follows that $[\cdot,\cdot]$ is alternating on $G/Z(G)$. $\mathbb{F}_2$ bilinearity follows directly from the definition.

□

**Remark 1.8.** Let $G = \mathcal{P}_n$, $G \ni g = i^k X_1^{a_1} \dots X_n^{a_n} Y_1^{b_1} \dots Y_n^{b_n}, k \in \underline{4}, a_i, b_i \in \{0,1\}$ for all $i \in \underline{n}$. Note that by Prop. 1.7 every element in G can be written than way. Then an $\mathbb{F}_2$ isomorphism $\varphi : G/G' \to \mathbb{F}_2^{2n}$ is given by:

$$\varphi(g = i^k X_1^{a_1} \dots X_n^{a_n} Y_1^{b_1} \dots Y_n^{b_n}) = (a_1, \dots, a_n, b_1, \dots, b_n) \in \mathbb{F}_2^{2n}$$

The image under $\varphi$ is sometimes referred to as symplectic notation. Further let $\mathbb{F}_4 = \mathbb{F}_2[\omega]$, with $\omega^2 + \omega + 1 = 0$, equipped with the $\mathbb{F}_2$-symplectic form $(x, y) \mapsto \mathrm{Tr}(x\bar{y})$, where $(x \mapsto \bar{x})$ denotes the Galois automorphism from $\mathbb{F}_4$: $(x \mapsto x^2)$. Note that since $\mathrm{Tr}(x\bar{y}) = (x\bar{y}) + (\bar{x}\bar{\bar{y}}) = x^2 y + xy^2 = xy^2 + x^2 y = \mathrm{Tr}(y\bar{x})(= -\mathrm{Tr}(y\bar{x}))$ this is indeed a symplectic form. Then we can identify $\mathbb{F}_2^{2n} \cong_{\mathbb{F}_2} \mathbb{F}_4^n$ in a canonical way with respect to the symplectic notation: $(a_1, \dots, a_n, b_1, \dots, b_n) \mapsto (\omega a_1 + \bar{\omega} b_1, \dots, \omega a_n + \bar{\omega} b_n)$. The isomorphism given by the composition of these two we denote by $\tilde{\varphi}$. $\tilde{\varphi}$ is an isometry with respect to the commutator and the $\mathbb{F}_2$-symplectic form on $\mathbb{F}_4$.

## 1.4 Random Unitary Matrices

**Theorem 1.9** (Haar Measure)**.** Let $\mathcal{U} := \mathcal{U}_n(\mathbb{C})$ denote the group of unitary $n \times n$ matrices over the complex field $\mathbb{C}$. With respect to the topology induced by the norm on $\mathbb{C}^{n \times n} \cong \mathbb{C}^{n^2}$, $\mathcal{U}$ becomes a (compact) topological group: the multiplication and inversion mappings are continuous. There exists a unique measure $\mu$ on $\mathcal{U}$, called the Haar measure, which satisfies the following:

- $\mu$ is a countably additive, non-trivial measure on the Borel subsets of $\mathcal{U}$ (i.e. on the $\sigma-$algebra generated by the open subsets of $\mathcal{U}$).
- $\mu(\mathcal{U}) = 1$
- $\mu(gEh) = \mu(E)$ for all Borel sets $E \subseteq \mathcal{U}$, and for all $g, h \in \mathcal{U}$.

This last property is usually referred to as (left and right) translation invariance. A proof can be found in [5].

**Remark 1.10.** The Haar measure makes the group of unitary $n \times n$ matrices $\mathcal{U} := \mathcal{U}_n(\mathbb{C})$ over $\mathbb{C}$ with its Borel sets into a measurable space, and through it, all familiar concepts of stochastics carry over. Since the Haar measure is translation invariant it is in particular uniform on $\mathcal{U}$, and thus we can interpret the identity mapping on $\mathcal{U}$ as a random, uniformly distributed unitary matrix. In the following, for simplicity, we will say "Let $U$ be a uniformly distributed random unitary matrix" as an abuse of notation for saying: Let $U : \mathcal{U} \to \mathcal{U}, u \mapsto u$ be the identity mapping on the measurable space $\mathcal{U}$ as a

random variable. The expected value of a measurable function $f$ on $\mathcal{U}$ can thus be explicitly be calculated through a Lebesgue integral:

$$E(f) = \int_{\mathcal{U}} f(x) d\mu(x) \tag{3}$$

**Lemma 1.11.** Let $G$ be a group and let $V$ be a $\mathbb{C}G$ module, finite dimensional as a $\mathbb{C}$ vector space. Further let $V^*$ be its dual space. Then

$$\mathrm{Hom}_G(V \otimes V^*, \mathbb{C}) \cong \mathrm{Hom}_G(V, V) \tag{4}$$

as vector spaces, where G acts on $V^*$ through $g \cdot f := f \circ g^{-1}$ for all $f \in V^*, g \in G$, and it acts diagonally on $V \otimes V^*$.

*Proof.* We fix a $\mathbb{C}$ basis $e_1, \ldots, e_n$ of $V$. With respect to this basis we see that both are basically just $n \times n$ matrices, and we get an isomorphism easily:

$$\mathrm{End}_G(V, V) \ni (e_i \mapsto \sum_{j=0}^{n} a_{i,j} e_j) \mapsto \sum_{i,j=0}^{n} a_{i,j} (e_i \otimes e_j^*)^* \in \mathrm{Hom}_G((V \otimes V^*), \mathbb{C}) \tag{5}$$

From Equation 5 we can immediately see the inverse mapping, which implies bijectivity. It only remains to prove that this linear mapping is well defined. This is the case since the condition of being $G$-equivariant translates to the set of linear equations on the coefficients $a_{i,j}$ given by the fact that the mapping described by $a_{i,j}$ has to commute with all representation matrices given by the action of $G$ on $V$ with respect to the basis $e_1, \ldots, e_n$. □

**Theorem 1.12.** Let $U$ be a random unitary $n \times n$ matrix over $\mathbb{C}$ (see Remark 1.10) and $A, B \in \mathbb{C}^{n \times n}$, and let $\mathcal{U} := \mathcal{U}_n(\mathbb{C})$ be the set of unitary $n \times n$ matrices. Then:

$$E(UAU^\dagger) = \frac{1}{n} \mathrm{Tr}(A) I_n \tag{6}$$

$$E(\mathrm{Tr}(AU)\mathrm{Tr}(BU^\dagger)) = \frac{1}{n} \mathrm{Tr}(AB) \tag{7}$$

Where $E$ is the expected value and $I_n$ denotes the unit matrix $\in \mathbb{C}^{n \times n}$.

*Proof.* For the first one (Eqn. 6) we note that for $W \in \mathcal{U}_n(\mathbb{C})$ :

$$\begin{aligned} WE(UAU^\dagger)W^\dagger &= W \int_{\mathcal{U}} (UAU^\dagger) d\mu(U) W^\dagger \\ &= \int_{\mathcal{U}} (WU) A (WU)^\dagger d\mu(WU) = E(UAU^\dagger), \end{aligned} \tag{8}$$

where in the second equality we used the fact that $\mu$ is translation invariant. In particular, $[E(UAU^\dagger), \mathcal{U}_n] = \{I_n\}$, and since $\mathcal{U}_n$ is an irreducible representation of itself, it contains a $\mathbb{C}$ basis for $\mathbb{C}^{n\times n}$ (for example, the set $\mathcal{E}$ of Pauli operators), which means that $E(UAU^\dagger) \in \{\lambda I_n \mid \lambda \in \mathbb{C}\}$, since it has to commute with every matrix in $\mathbb{C}^{n\times n}$.

Further we note that the mapping

$$\varphi : \mathbb{C}^{n\times n} \to \mathbb{C}I_n, A \mapsto E(UAU^\dagger)$$

is a $\mathbb{C}$-linear, $\mathcal{U}_n$-equivariant mapping, i.e. $\varphi \in \mathrm{Hom}_{\mathcal{U}_n}(\mathbb{C}^n \otimes (\mathbb{C}^n)^*, \mathbb{C}) \cong \mathrm{Hom}_{\mathcal{U}_n}(V, V)$ by Lemma 1.11. Since $\mathcal{U}_n$ is transitive on $V\backslash\{0\}$, $\dim_{\mathbb{C}}(\mathrm{Hom}_{\mathcal{U}_n}(V, V)) = 1$, and thus $\mathrm{Hom}_{\mathcal{U}_n}(\mathbb{C}^n \otimes (\mathbb{C}^n)^*, \mathbb{C})$ is also 1-dimensional. Since Tr is a $\mathcal{U}_n$-equivariant, non-trivial homomorphism, it follows that $\mathrm{Hom}_{\mathcal{U}_n}(\mathbb{C}^n \otimes (\mathbb{C}^n)^*, \mathbb{C}) = \langle \mathrm{Tr}\rangle_{\mathbb{C}}$, and in particular, $\varphi = \lambda\mathrm{Tr}$, for some $\lambda \in \mathbb{C}$. That $\lambda = \frac{1}{n}$ follows immediately from $E(UI_nU^\dagger) = I_n = \lambda\mathrm{Tr}(I_n)I_n = \lambda n I_n$.

For Equation 7 we consider the mapping

$$\psi : \mathbb{C}^{n\times n} \times \mathbb{C}^{n\times n} \to \mathbb{C}, (A, B) \mapsto E(\mathrm{Tr}(AU)\mathrm{Tr}(BU^\dagger))$$

Since both the trace and the Lebesgue integral are linear mappings, it follows that $\psi$ is a bilinear mapping. There are two crucial observations to complete the proof. First, the mapping $\psi(\cdot, I_n) : \mathbb{C} \otimes (\mathbb{C}^n)^* \to \mathbb{C}, A \mapsto \psi(A, I_n)$ is an $\mathcal{U}_n$-equivariant linear form: $\psi(\cdot, I_n) :\in \mathrm{Hom}_{\mathcal{U}_n}(\mathbb{C}^n \otimes (\mathbb{C}^n)^*, \mathbb{C})$ and, by the same argument as above, there exists a $\lambda \in \mathbb{C}$ such, that $\psi(A, I_n) = \lambda\mathrm{Tr}(A)$ for all $A \in \mathbb{C}^{n\times n}$. On the other hand, for $A \in \mathbb{C}^{n\times n}, B \in \mathcal{E}$

$$\begin{aligned}\psi(A, B) = \int_{\mathcal{U}_n} \mathrm{Tr}(AU)\mathrm{Tr}(BU^\dagger)d\mu(U) &= \int_{\mathcal{U}_n} \underbrace{\mathrm{Tr}(AU)}_{=\mathrm{Tr}(ABBU)} \underbrace{\mathrm{Tr}(BU^\dagger)}_{=\mathrm{Tr}((BU)^\dagger)} d\mu(BU) \\ &= \int_{\mathcal{U}_n} \mathrm{Tr}(ABU)\mathrm{Tr}(I_nU^\dagger)d\mu(U) = \psi(AB, I_n)\end{aligned}$$

Since $B = B^\dagger = B^{-1}$ for all $B \in \mathcal{E} \subseteq \mathcal{U}_n$. But $\langle\mathcal{E}\rangle_{\mathbb{C}} = \mathbb{C}^{n\times n}$, so it holds for all $B \in \mathbb{C}^{n\times n}$ from the bilinearity of $\psi$. That $\lambda = \frac{1}{n}$ follows again from $\psi(I_n, I_n) = \int_{\mathcal{U}_n} \mathrm{Tr}(U)\mathrm{Tr}(U^\dagger)d\mu(U) = 1$, by a generalization of the Schur orthogonality relations for characters, see for example 5.8 in [12] □

## 1.5 Physical Background: the Postulates of Quantum Mechanics

The motivation for studying quantum codes comes obviously from physics. To better understand quantum codes, it might therefore be a sensible thing to

study the basic mathematical foundations of quantum mechanics. Quantum mechanics is a mathematical framework for describing physical phenomena, and can be given an axiomatic basis: this basis is usually referred to as 'the postulates of quantum mechanics'. The following formulation is mainly based on Section 2.2. of [8].

**The postulates of Quantum Mechanics**

a) Every isolated physical system $S$ is described by a tuple $(\mathcal{H}, \varphi)$, where $\mathcal{H}$ is a complex Hilbert space, called the state space of $S$, and $\varphi : \mathbb{R} \to \mathcal{U}(\mathcal{H}), t \mapsto U_t$ a group homomorphism of $(\mathbb{R}, +)$ in the unitary group of $\mathcal{H}$ is the mapping that gives the time evolution of the system. The concrete state of the space is described by a family of unit vectors $\{|\psi_t\rangle \mid t \in \mathbb{R}\}$, related by $|\psi_t\rangle = U_t U_{t'}^{-1} |\psi_{t'}\rangle$ for all $t, t' \in \mathbb{R}$. Alternatively the system can be seen as described by the projective space of $\mathcal{H}$. In this thesis $\mathcal{H}$ will always be finite-dimensional, but the formalism does not require it to be.

b) A measurement made on the system is described by a collection $\{M_m | m \in I\} \subseteq End(\mathcal{H})$ of operators, where $I$ is some countable index set which represents the possible outcomes of the measurement. For a system in a state $|\psi\rangle$, the probability of measuring $m \in I$, $p(m)$ is given by $p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle$, and after a measurement with outcome $m \in I$ the system is in the state $\frac{1}{||M_m|\psi\rangle||} M_m |\psi\rangle$. Further, the set of measurement operators has to satisfy: $\sum_{m \in I} M_m^\dagger M_m = \mathrm{Id}_{\mathcal{H}}$, which basically means that $\sum_{m \in I} p(m) = 1$.

c) A system that is composed of various quantum systems with state spaces $\mathcal{H}_1, \ldots, \mathcal{H}_n$ has the state space $\mathcal{H} = \mathcal{H}_1 \otimes \ldots \otimes H_n$

**Remark 1.13.** One does not have to think long to perceive an (apparent?) inconsistency in the postulates. The universe itself should be a closed quantum system, which means that the time evolution of the whole universe should be uniquely determined by it's starting state by the 1. postulate. But the 2. postulate states that a measurement has an inherent probabilistic behavior, which is inconsistent with this. This problem is called the measurement problem, and is in the end rather of philosophical nature, which is why we will not further pursue it in this thesis.

# 2 Qubits and Quantum Codes

With the required mathematical and physical preliminares, we can now turn our attention to quantum coding theory. We will now introduce the subject, and a few of the more important results or families of codes.

**Definition 2.1.** A qubit is a two dimensional complex Hilbert space $\mathcal{H} = (\mathbb{C}^2, < \cdot, \cdot >)$. It is an abstraction of a two state quantum system, whose physical realization we disregard. For convention we will fix an orthonormal basis of $\mathbb{C}^2$ and call the two vectors $|0\rangle$ and $|1\rangle$ in analogy to the two states of a bit, 0 and 1.

**Remark 2.2.** A many qubit system is, as by the postulates of quantum mechanics, described by the tensor product Hilbert space of its single qubits. This is the reason why an n-qubit system is described by $\mathcal{H} = \underbrace{\mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2}_{\text{n times}} \cong \mathbb{C}^{2^n}$. The basis of this space given by the $|0\rangle, |1\rangle$ basis for each qubit can be abbreviated by binary strings: $|b_1 b_2 \ldots b_n\rangle := |b_1\rangle \otimes |b_2\rangle \ldots \otimes |b_n\rangle$. For instance $|010\rangle = |0\rangle \otimes |1\rangle \otimes |0\rangle$. This notation also makes the analogy to bits further clear, hence the name, qubits.

**Definition 2.3.** A quantum code $\mathcal{C}$ is a (linear) subspace of an n-qubit space $\mathbb{C}^{2^n}$. If the code is a $2^k$ dimensional subspace of $\mathbb{C}^{2^n}$ for some integer $k \leq n$, then we call the code $\mathcal{C}$ an $[[n, k]]$-Code. In this case there is a bijective linear mapping from a $k$-qubit system to the code $\mathcal{C}$. We say the code encodes $k$ qubits in $n$ qubits. For a general $K$-dimensional code on $n$ qubits, we say it is an $((n, K))$ code.

## 2.1 Error Correction

So, how does quantum error correction work? We will describe the basic theory of quantum error correction in analogy to the classical theory of linear codes. In particular, we will develop it in this section based on the very simple example of the [3,1,3] binary linear code $0 \mapsto 000, 1 \mapsto 111$ (repetition code).

By the postulates of quantum mechanics, errors (possible time-evolutions of the physical space) are given by elements of the Unitary group on $\mathcal{H}$, which for this case is the group $\mathcal{U}_{2^n}(\mathbb{C})$. Because of its many useful properties, we will first consider the Pauli operators $(\mathcal{E}_n)$ as errors. These are, in particular, a unitary, hermitian basis of $\mathrm{End}(\mathcal{H})$. There is also a very good physical motivation for choosing the Pauli operators, since these are closely related to the spin of the system.

**Example 2.4.** A first, naive approach for building a quantum code is just the repetition code in qubits:

$$|0\rangle \mapsto |000\rangle$$

$$|1\rangle \mapsto |111\rangle$$

It is not hard to see that this code will protect from one Pauli $X$ error, for example, $X_2$:

$$X_2|000\rangle = |010\rangle$$

And just as in the classical analog, we can see this (assuming only one $X_i$ error) can only have been $|000\rangle$. It is not difficult to see that this code will protect from a single $X_i$ error on an arbitrary qubit. Simple, right? The problem is, we have to measure in some way the state of the code in order to find out what the state is and what error happened. Fortunately, there is a way of covering all 'bit flip' ($X_i$) errors with a measurement: Define the following measurement operators:

$$P_\emptyset := |000\rangle\langle 000| + |111\rangle\langle 111|,\ P_{\{1\}} := |100\rangle\langle 100| + |011\rangle\langle 011|$$

$$P_{\{2\}} := |010\rangle\langle 010| + |101\rangle\langle 101|,\ P_{\{3\}} := |001\rangle\langle 001| + |110\rangle\langle 110|$$

These operators satisfy the requirements for the measurement postulate, so they represent a measurement of a physical quantity whose values are the indices of the measurement operators. These have been chosen to be the support of the error for simplicity, so what this means is that measuring the quantity described by this set of operators will give as a result the support of the error, assuming at most a single $X_i$ error. In our example where the recieved message is $|010\rangle$, we see that by the postulates, the result of the measurement is going to be $\{2\}$ with probability $p(\{2\}) = \langle 010|P_{\{2\}}^\dagger P_{\{2\}}|010\rangle = \langle 010|010\rangle = 1$, and all the other possibilities with probability $p(m) = 0, m \in \{\{1\}, \{3\}, \emptyset\}$. A close inspection of the operators then makes it clear that if exactly one 'bit flip' error (but nothing else) has happened, this measurement will identify the error with 100% probability and leave everything as it is.

This example also shows another point where the analogies to classical codes have its limits: any unitary operator could be an error on the qubits. Consider the state $|+\rangle := 1/\sqrt{2}(|0\rangle + |1\rangle)$. Coding this would yield $1/\sqrt{2}(|000\rangle + |111\rangle)$. Since all error operators are linear, a bit flip would still be corrected with the measurement above. But how about a phase flip? Consider the error $Z_1$, for example. $Z_1(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)) =$

$\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$, which would go undetected, but would be decoded to be $|-\rangle := 1/\sqrt{2}(|0\rangle - |1\rangle)$.

We can modify the code to detect phase flip ($Z_i$) errors: We have seen that the operator $Z$ takes $|+\rangle$ to $|-\rangle$ and vice-versa. That is, it flips both states. If we were to rename our states $|0\rangle$ and $|1\rangle$, $Z$ would act as an $X$. With this in mind, it is not difficult to see why coding $|0\rangle \mapsto |+++\rangle$, $|1\rangle \mapsto |---\rangle$ would be a good idea. If we make the same measurement as above, but in the $|+\rangle, |-\rangle$ basis instead, a phase flip would be the same as a bit flip in that basis, and would be detected. It can be immediately checked that the operator

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

also called a Hadamard gate, takes $(|0\rangle, |1\rangle) \mapsto (|+\rangle, |-\rangle)$. So the measurement operators would be $HP_iH^\dagger = HP_iH, i = 0, 1, 2, 3$.

But this code, again, would not be able to detect a bit flip. We can try combining them, on a 9 qubit code:

**Example 2.5.** This 9 qubit code, also known as Shor code (see [8]) can correct an $X$ or $Z$ error on **a single qubit**. This is achieved by combining the two codes previously mentioned. First the phase flip code, $|0\rangle \mapsto |+++\rangle$, $|1\rangle \mapsto |---\rangle$, then the bit flip code to each of the three qubits of the first encoding: $|+++\rangle = |+\rangle|+\rangle|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \mapsto \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$ and in an analogous fashion $|---\rangle \mapsto \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$

This, we have seen, can correct a single one of two different errors on a single qubit. It might seem like a lot of work for very little gain. Fortunately, as we will see, the correcting of these two errors is enough to correct an arbitrary single-qubit error! In fact, the following theorem ( 2.6) is one of the results that make quantum error correction possible in the first place, since it helps to bypass the problem of a continuous, infinite set of possible errors.

**Theorem 2.6.** Let $\{E_i \mid i \in I\}$ for some index set $I$ be a set of unitary operators, and $C$ be a quantum code that can correct errors on all these $E_i, i \in I$. Further let $\{F_j \mid j \in J\}$ for another index set $J$ be another set of unitary operators, each of which is a linear combination of the $E_i$, i.e. $F_j = \sum_{i \in I} c_{i,j} E_i$ for all $j \in J$ where $c_{i,j} \in \mathbb{C}$ for all $i \in I, j \in J$, and almost all $c_{i,j} = 0$. Then, $C$ can also correct all errors $F_j, j \in J$. This theorem actually holds for a wider class of errors, where $E_i, F_j$ are so-called quantum operations; but this goes beyond the scope of this thesis. The more general statement, along with a proof, can be found in [8].

## 2.2 Additive Codes

We will now study a very important class of quantum codes, stabilizer or additive quantum codes.

**Definition 2.7.** Let $V$ be a finite dimensional $\mathbb{F}_4$ vector space and let $(\cdot,\cdot) : V \times V \to \mathbb{F}_4$ be a symplectic, non-degenerate bilinear form on $V$. Further let $C \subset V$. We define the orthogonal complement of $C$ to be $C^\perp := \{v \in V \mid (v,c) = 0 \text{ for all } c \in C\}$. If $C \subseteq C^\perp$ we say $C$ is self-orthogonal.

**Definition 2.8.** Let $V$, $(\cdot,\cdot)$ be as above and let $C \leq_{\mathbb{F}_2} V$ be an $\mathbb{F}_2$ subspace of $V$, i.e. $C$ is an additive subset (closed under addition) of $V$. If $C \subseteq C^\perp$ we call $C$ an additive code.

**Proposition 2.9.** Let $C \leq_{\mathbb{F}_2} V = \mathbb{F}_4^n$ be an additive code, and the symplectic form $(x,y) = \mathrm{Tr}(x\bar{y})$ for all $x, y \in V$ as in Rem. 1.8. Then $C$ defines a quantum code on $n$ qubits via a lifting $\psi$ of the inverse mapping to the induced by the symplectic notation defined in Rem. 1.8:

$$\psi : V \to G, (\omega a_1 + \bar{\omega} b_1, \ldots, \omega a_n + \bar{\omega} b_n) \mapsto X_1^{a_1} Y_1^{b_1} \ldots X_n^{a_n} Y_n^{b_n}$$

$S := \psi(C)$ is an abelian subgroup of $\mathcal{P}_n$, called the stabilizer group of $C$, which defines a quantum code $\tilde{C}$ on $\mathbb{C}^{2^n}$ through $\tilde{C} := \{v \in \mathbb{C}^{2^n} \mid sv = v \text{ for all } s \in S\}$. The dimension of this code is $2^{n - dim_{\mathbb{F}_2}(C)}$.

*Proof.* From Rem. 1.8 we know that symplectic notation is an isometry to $\mathcal{P}_n/\mathcal{P}_n'$. Further since $C$ is self-orthogonal it follows that $S$ is abelian (since two elements of $\mathcal{P}_n$ commute iff their images are orthogonal over $\mathbb{F}_4$) and since $C \leq_{\mathbb{F}_2} V$ it follows that $S$ is an $\mathbb{F}_2$ vector space. Define $R_S := \frac{1}{|S|} \sum_{g \in S} g \in \mathrm{End}(\mathbb{C}^{2n})$. $R_S = R_S^2$ is a projection onto $\tilde{C}$, then for $s \in S, v \in V, c \in \tilde{C}$ it holds that:

$$sR_S(v) = \frac{1}{|S|} \sum_{g \in S} (sg)v = R_S(v), R_S(c) = \frac{1}{|S|} \sum_{g \in S} gc = \frac{1}{|S|} \sum_{g \in S} c = c$$

and in particular $c \in R_S^{-1}(c)$. It follows that

$$\dim_{\mathbb{C}}(\tilde{C}) = \mathrm{Tr}(R_S) = \frac{1}{|S|} \sum_{g \in S} \mathrm{Tr}(g) = \frac{1}{|S|} \mathrm{Tr}(\mathrm{Id}) = 2^n/|S| = 2^{n - \dim_{\mathbb{F}_2}(S)}$$

since for $\mathrm{Id} \neq g \in G : \mathrm{Tr}(g) = 0$ which follows directly from the fact that $\mathrm{Tr}(X) = \mathrm{Tr}(Y) = \mathrm{Tr}(Z) = 0$ and $\mathrm{Tr}(A \otimes B) = \mathrm{Tr}(A)\mathrm{Tr}(B)$ for all $A \in \mathbb{C}^{k_1 \times k_1}, B \in \mathbb{C}^{k_2 \times k_2}, k_1, k_2 \in \mathbb{N}$. □

**Definition 2.10.** The quantum code $\tilde{C}$ constructed on Proposition 2.9 is called an additive quantum code, and $C$ is called the associated additive code over $\mathbb{F}_4$.

**Definition 2.11.** A subgroup $S \leq \mathcal{P}_n$ is called a stabilizer group iff $-I \notin S$. Note that this implies that $S$ is abelian, since $\mathcal{P}_n' = \{\pm \mathrm{Id}\}$. This definition is also consistent with the notation introduced in Prop. 2.9: Through symplectic notation, S defines an $\mathbb{F}_2$ vector space (equivalent to S being closed under multiplication) that is self orthogonal with respect to the commutator, since S is abelian.

**Example 2.12.** With stabilizer codes now properly defined, we can return to the previous example ( 2.5), the 9-qubit Shor code. The Shor code is generated by the 8 $\mathbb{F}_2$-linearly independent generators in Table 1 (see [8]). This is, in general, a much more compact way to write down the code. We see that, of course, the code is stabilized by all operators and there is 8 of them (what is in agreement with Theorem 2.9). From their symplectic notation it can be immediately checked they are indeed $\mathbb{F}_2$-linearly independent generators. We see that it agrees with the construction: The stabilizer group has $2^8$ elements, since it is an 8-dimensional additive $\mathbb{F}_2$ code. Hence, the quantum code associated to it, the Shor code, has dimension $2^{9-1} = 2$, encoding exactly 1 qubit.

| Name | Operator |
|---|---|
| $g_1$ | $ZZIIIIIII$ |
| $g_2$ | $IZZIIIIII$ |
| $g_3$ | $IIIZZIIII$ |
| $g_4$ | $IIIIZZIII$ |
| $g_5$ | $IIIIIIZZI$ |
| $g_6$ | $IIIIIIIZZ$ |
| $g_7$ | $XXXXXXIII$ |
| $g_8$ | $IIIXXXXXX$ |

Table 1: Stabilizer Generators for the 9-Qubit Shor Code

## 2.3 Logical Operators

There is another class of operators which is very important for stabilizer codes: the so-called logical operators.

**Definition 2.13.** Let $S \leq \mathcal{P}_n$ be a stabilizer group. Let $C_{\mathcal{P}_n}(S)$ be the centralizer of S in $\mathcal{P}_n$, i.e.:

$$C_{\mathcal{P}_n}(S) = \{A \in \mathcal{P}_n \mid [A, B] = 0 \text{ for all } B \in S\}$$

Note that since $S$ is abelian, $S \leq C_{\mathcal{P}_n}(S)$. An element $L \in C_{\mathcal{P}_n}(S) \backslash S$ is called a logical operator.

Logical operators have the following interpretation: An [[n,k]] qubit code encodes $k$ qubits in $n > k$. Once encoded, we are confronted with $n$ physical qubits, but know that logically, only $k$ are represented. If we were to apply an operator $A$ on the unencoded $k$ qubits, we would obtain a different state for these $k$ qubits. But, how would this new state look like when encoded in the $n$ qubits? There has to be an operator $A^{(n)}$ on $n$ qubits that applies $A$ on the encoded qubits: $A^{(n)}$ is a logical operator, as it acts as $A$ on the logical qubits.

But why are these exactly the elements in $C_{\mathcal{P}_n}(S) \backslash S$? Well, for a logical operator to act on the logical, encoded qubits, it has to map code words to code words; after all, the new encoded state is part of the code as well. It is precisely the elements of $C_{\mathcal{P}_n}(S)$ that do that. On the other hand, the elements of $S$, per definition, act as the identity on the code, leaving it unchanged. We want to define only non-trivial logical operators as such, and leave therefore $S$ out.

**Remark 2.14.** Let $f : \mathbb{C}^{2^k} \to \mathbb{C}^{2^n}$ be a $\mathbb{C}$-linear, injective mapping that encodes $k$ qubits in $n$ qubits, i.e. $f(\mathbb{C}^{2^k}) =: C$ is an additive quantum code. Then, $\mathrm{Aut}_{\mathbb{C}}(C)$ acts on $\mathbb{C}^{2^k}$ via $\sigma v := f^{-1}(\sigma f(v))$, and the stabilizer group S is the stabilizer of this action. Note that this is well defined since $\mathrm{Im}(\sigma) = C$. Hence, for an operator $A \in \mathrm{End}(\mathbb{C}^{2^n})$ and $A^{(n)}, B^{(n)}$ such, that both act as $A$ on $k$ qubits (as described above), there exists a $T \in S$ such, that $A^{(n)} = TB^{(n)}$.

**Example 2.15.** Again, the 9-qubit Shor code (Ex. 2.5): It encodes only one qubit, so we will only search for the two logical operators $X^{(9)}$ and $Z^{(9)}$. These are given by $X^{(9)} = ZZZZZZZZZ$ and $Z^{(9)} = XXXXXXXXX$, as can be checked with a simple calculation. Note that it is not as one might naively expect at first, but exactly the opposite instead.

## 2.4 Code Distance

There is an easy way of quantifying how many errors a code can correct: the code distance. It is analogous to what is used in classical coding theory. It is also a good reason for studying logical operators. Before introducing it however, we need a further definition:

**Definition 2.16.** Let $V = (\mathbb{C}^2)^{\otimes n}$, and $\sigma = i^k \sigma_1 \otimes \ldots \otimes \sigma_n \in \mathcal{P}_n$. We define the support of $\sigma$ to be $\mathrm{Supp}(\sigma) = \{i \in \underline{n} \mid \sigma_i \neq \mathrm{Id}\}$ and its weight as $\mathrm{wt}(\sigma) = |\mathrm{Supp}(\sigma)|$.

Similarly, we define a weight on $\mathbb{F}_2^{2n} = (e_1, \ldots, e_n, f_1, \ldots, f_n)$ through

$$|\sum_{i=1}^{n} a_i e_i + b_i f_i| := |\{i \in \underline{n} \mid a_i \neq 0 \text{ or } b_i \neq 0\}, a_i, b_i \in \mathbb{F}_2 \text{ for all } i \in \underline{n} \quad (9)$$

This coincides with the Hamming-weight on $\mathbb{F}_4$ with the identification from Remark 1.8.

**Definition 2.17.** Let $S \leq \mathcal{P}_n$ be a stabilizer group with corresponding code $C$. Then, the minimal distance (or code distance) $\rho$ of $C$ is defined as:

$$\rho := \min\{|A| \in \mathcal{P}_n | A \text{ is a logical operator}\} = \min\{|A| \mid A \in C_{\mathcal{P}_n}(S) \backslash S\} \quad (10)$$

An [[n,k]] code with minimal distance $\rho$ is also called an [[n,k,$\rho$]] code, and similarily for an $((n, K))$ code with minimal distance $\rho$ we say it is an $((n, K, \rho))$ code.

The basic idea for the definition of $\rho$ is that it marks the number of qubits an operator has to minimally affect for it to change one code word to another. An argument similar to that of the classical coding theory (see [11]) can be made to prove that a code with distance $\rho$ can correct all errors $E$ which satisfy $|E| < \frac{\rho}{2}$. A direct proof for quantum coding theory can be found in [7].

**Example 2.18.** We can calculate the code distance of Ex. 2.5. We know two logical operators, $\overline{X} := ZZZZZZZZZ$ and $\overline{Z} := XXXXXXXXX$, and know that they represent the only two equivalency classes of logical operators, since the Shor code encodes a single qubit. This means we can get all logical operators this way, by going through the equivalency classes:

$$C_{\mathcal{P}_n}(S) = \{A\overline{X} \mid A \in S\} \cup \{A\overline{Z} \mid A \in S\} \quad (11)$$

From Table 1 we get the generators of S, so we know in principle all logical operators. We can look at, for example $\overline{Z} g_8 = ZZZIIIIII$, or $g_2 g_3 g_6 \overline{X} = ZIIIIZZII$. It is not hard to see that these operators are of minimal weight in the two classes from Eqn. 11. This means that $\rho = 3$, and hence, the Shor code corrects $1 < \frac{3}{2}$ errors.

Definition 2.17 can be generalized for any quantum code, and it will have the same properties as it has for additive codes, as well as in classical coding theory.

**Definition 2.19.** For a quantum code $C$ on $n$ qubits, define $C$ to have minimal distance of at least $d$ iff $\langle v|U_d|v\rangle = \langle v'|U_d|v'\rangle$ for all unit vectors $|v\rangle, |v'\rangle \in C$, where $U_d$ ranges over all unitary operators with support on exactly $d$ qubits. Since for $\dim_{\mathbb{C}} C = 1$ this always holds trivially, we define $C$ in that case to have minimal distance $\geq d$ iff there exisits an $a \in \mathbb{C}$ such that $\mathrm{Tr}_{S^c}(|u\rangle\langle u|) = a\mathrm{Id}$ for the (here, unique) unit vector $|u\rangle \in C$ and $S^c \subseteq \underline{n}, |S^c| = n - d$. This condition is usually called purity, for a more detailed discussion see 13.1 of [9].

## 2.5 CSS Codes

A class of codes worth mentioning, a subclass of stabilizer codes, are CSS codes. CSS codes are named after their inventors: A. R. Calderbank, Peter Shor and Andrew Steane. The original construction actually uses classical codes, and is one of the advantages of CSS codes, since you can derive much information about the code from the classical codes used on its construction.

**Definition 2.20.** Let $D_1, D_2 \leq \mathbb{F}_2^n$ be two (classical) linear codes, which encode $k_1$ and $k_2$ bits respectively, i.e. one is an $[n, k_1]$ code and the other one $[n, k_2]$, such that $D_2 \subseteq D_1$ . Further let $D_1$ and $D_2^\perp$ have both minimal distance $d \geq 2t + 1$ for some positive integer $t$. For $x \in \mathbb{F}_2^n$ let $|x\rangle \in \mathbb{C}^{2^n}$ be the $n$-qubit state indexed by the bit string $x$, and define $|x + D_2\rangle := \frac{1}{\sqrt{|D_2|}} \sum_{y \in D_2} |x+y\rangle$ for all $x \in D_1$. Now define $C := C(D_1, D_2) := \{|x+D_2\rangle \mid x \in D_1\}$ as the CSS code from $D_1$ over $D_2$.

**Remark 2.21.** The above defined $C = C(D_1, D_2)$ is an $[[n, k_1 - k_2, d]]$ code, with $d \geq 2t + 1$. A proof can be found in [8].

# 3 Quantum Weight Enumerators

Having now seen what quantum error correcting codes are, and how they should work in principle, one of the first questions that it invites is that of how good a code can be. How many qubits can a code on a given number of qubits and with a given distance maximally encode? What about a fix code space dimension, what the maximal distance is. To anwser these types of questions we will use a concept which is again inspired on classical coding theory, nameley Weight Enumerators.

## 3.1 The Shor-Laflamme and Rains enumerators

**Definition 3.1.** Let $V = (\mathbb{C}^2)^{\otimes n}$, and $\mathcal{E} = \{\sigma_1 \otimes \ldots \otimes \sigma_n \mid \sigma_i \in \{X, Y, Z, \mathrm{Id}\}$ for all $i \in \underline{n}\}$ (generating set for the Pauli group on V). Further let $S \subseteq \underline{n}$ and $M_1, M_2 \in \mathbb{C}^{2^n \times 2^n} (\cong \mathrm{End}(V))$, with $\mathrm{Tr}(M_1) \neq 0 \neq \mathrm{Tr}(M_2)$. Then we define the coefficients of the Shor-Laflamme enumerators [2] of $M_1, M_2$ as follows:

$$A_S(M_1, M_2) := \frac{1}{\mathrm{Tr}(M_1)\mathrm{Tr}(M_2)} \sum_{\substack{E \in \mathcal{E} \\ \mathrm{Supp}(E) = S}} (\mathrm{Tr}(EM_1)\mathrm{Tr}(EM_2)) \tag{12}$$

$$B_S(M_1, M_2) := \frac{1}{\mathrm{Tr}(M_1 M_2)} \sum_{\substack{E \in \mathcal{E} \\ \mathrm{Supp}(E) = S}} (\mathrm{Tr}(EM_1 EM_2)) \tag{13}$$

And for $d \in \underline{n}$ we define

$$A_d(M_1, M_2) := \sum_{\substack{S \subseteq \underline{n} \\ |S| = d}} A_S(M_1, M_2); B_d(M_1, M_2) := \sum_{\substack{S \subseteq \underline{n} \\ |S| = d}} B_S(M_1, M_2) \tag{14}$$

**Definition 3.2.** Again let $V = (\mathbb{C}^2)^{\otimes n}$, and $\mathcal{E} = \{\sigma_1 \otimes \ldots \otimes \sigma_n \mid \sigma_i \in \{X, Y, Z, \mathrm{Id}\}$ for all $i \in \underline{n}\}$. Further let $S \subseteq \underline{n}, S^c = \underline{n} \backslash S$ and $M_1, M_2 \in \mathbb{C}^{2^n \times 2^n}$ with $\mathrm{Tr}(M_1) \neq 0 \neq \mathrm{Tr}(M_2)$. We define the coefficient of the Rains enumerators [1] of $M_1, M_2$ as follows:

$$A'_S(M_1, M_2) := \frac{1}{\mathrm{Tr}(M_1)\mathrm{Tr}(M_2)} \mathrm{Tr}(\mathrm{Tr}_{S^c}(M_1)\mathrm{Tr}_{S^c}(M_2)) \tag{15}$$

$$B'_S(M_1, M_2) := \frac{1}{\mathrm{Tr}(M_1 M_2)} \mathrm{Tr}(\mathrm{Tr}_S(M_1)\mathrm{Tr}_S(M_2)) \tag{16}$$

As well as for a $d \in \underline{n}$:

$$A'_d(M_1, M_2) := \sum_{\substack{S \subseteq \underline{n} \\ |S| = d}} A'_S(M_1, M_2); B'_d(M_1, M_2) := \sum_{\substack{S \subseteq \underline{n} \\ |S| = d}} B'_S(M_1, M_2) \tag{17}$$

Note that these definitions differ by a normalization factor from those in the original paper [1].

**Definition 3.3.** Let $C \leq (\mathbb{C}^{2^n})$ be a quantum code, and $P : \mathbb{C}^{2^n} \to C$ be the orthogonal projection onto $C$. The Shor-Laflamme enumerator polynomial of $C$ is defined as $\sum_{i=0}^{n} A_i(P,P)x^{n-i}y^i$, and the Rains enumerator polynomial similarly as $\sum_{i=0}^{n} A'_i(P,P)x^{n-i}y^i$

**Lemma 3.4.** Let $C \leq (C^2)^{\otimes n} =: V$ be an additive quantum code and $G \subseteq \mathcal{E}$ be its stabilizer group (i.e. $C = V^G$). and $E, E' \in \mathcal{E} = \{\sigma_1 \otimes \ldots \otimes \sigma_n \mid \sigma_i \in \{X, Y, Z, \mathrm{Id}\}$ for all $i \in \underline{n}\}$. Then

a) The orthogonal projection operator on $C$ is given by $P_C = \frac{1}{|G|}\sum_{\sigma\in G}\sigma$

b) $\mathrm{Tr}(EP_c) = \frac{1}{|G|} \cdot \begin{cases} 2^n = \dim(V) & \text{if } E \in G \\ 0 & \text{if } E \notin G \end{cases}$

c) $\mathrm{Tr}(\mathrm{Tr}_S(E)\mathrm{Tr}_S(E')) = 0$ if $E \neq E'$ or if there exists an $i \in S$ which satisfies that for $E = \sigma_1 \otimes \ldots \otimes \sigma_n$, $\sigma_i \neq \mathrm{Id}$, otherwise $\mathrm{Tr}(\mathrm{Tr}_S(E)\mathrm{Tr}_S(E)) = 2^{n+|S|}$.

d) $\mathrm{Tr}(EP_CEP_C) = \begin{cases} \frac{2^n}{|G|} & \text{for } E \in G^\perp \\ 0 & \text{otherwise} \end{cases}$

*Proof.* a) From a simple calculation it follows that $\sigma P_c(v) = P_c(v)$ for all $v \in V, \sigma \in G$ and $P_c(v) = v$ for all $v \in V^G$. From this it follows immediately that $\mathrm{Im}(P_C) = V^G$ and $P_C^2 = P_C$, and hence that it is the orthogonal projection onto $V^G$.

b) Since $\mathrm{Tr}(X) = \mathrm{Tr}(Z) = \mathrm{Tr}(Y) = 0$ and $\mathrm{Tr}(\sigma_1 \otimes \sigma_2) = \mathrm{Tr}(\sigma_1)\mathrm{Tr}(\sigma_2)$ it follows immediately that $\mathcal{E}$ is an orthogonal basis with respect to the trace bilinear form (since $< \mathcal{E} >_{\mathbb{C}} = \mathbb{C}^{2^n \times 2^n}$), and for all $E \in \mathcal{E}$ we have $E^2 = \mathrm{Id}_V$, hence $\mathrm{Tr}(E^2) = \dim(V) = 2^n$. From a) we get:

$$\mathrm{Tr}(EP_c) = \frac{1}{|G|}\sum_{\sigma\in G}\mathrm{Tr}(\sigma E) = \frac{1}{|G|} \cdot \begin{cases} 2^n = \dim(V) & \text{if } E \in G \\ 0 & \text{if } E \notin G \end{cases} \quad (18)$$

c) Since $\mathrm{Tr}(X) = \mathrm{Tr}(Y) = \mathrm{Tr}(Z) = 0$, as soon as $S \cap \mathrm{Supp}(E) \neq \emptyset$, it follows that $\mathrm{Tr}_S(E) = 0$, and hence $\mathrm{Tr}_S(E)\mathrm{Tr}_S(E') = 0$. The same applies obviously for $E'$. Now if $E \neq E'$ and $S \cap \mathrm{Supp}(E) = \emptyset$, then $\mathrm{Tr}_S(E) \neq \mathrm{Tr}_S(E')$ and thus $\mathrm{Tr}_S(E)\mathrm{Tr}_S(E') \neq 2^{|S|}\mathrm{Id}$, which in turn implies that $\mathrm{Supp}(\mathrm{Tr}_S(E)\mathrm{Tr}_S(E')) \neq \emptyset$ and so its trace vanishes. On the other hand, if $E = E'$ and $\mathrm{Supp}(E) \cap S = \emptyset$, then $\mathrm{Tr}_S(E)\mathrm{Tr}_S(E) = (2^{|S|})^2\mathrm{Id}_{S^c}$ and $2^{2|S|}\mathrm{Tr}(\mathrm{Id}_{S^c}) = 2^{2|S|}\dim(V_{S^c}) = 2^{n+|S|}$.

d) First note that $E = E^{-1}$ for all $E \in \mathcal{E}$ and that $\mathcal{P}'_n = \{\pm \mathrm{Id}\}$. This means that for $D \in \mathcal{E} \subseteq \mathcal{P}_n$: $EDE = EDE^{-1} = [E, D]D = \pm \mathrm{Id}D$. It follows that

$$\mathrm{Tr}(EP_CEP_C) = \frac{1}{|G|^2} \sum_{\sigma,\sigma' \in G} \mathrm{Tr}(\underbrace{E\sigma E}_{=[E,\sigma]\sigma} \sigma') \tag{19}$$

$$= \frac{1}{|G|^2} \sum_{\sigma,\sigma' \in G} < E, \sigma > \mathrm{Tr}(\sigma\sigma') = \frac{2^n}{|G|^2} \sum_{\sigma \in G} < E, \sigma > \tag{20}$$

where $< \cdot, \cdot >$ denotes the symplectic form onto $\{\pm 1\}$ induced by the commutator. For $E \in G^\perp$, per definition, $< E, \sigma >= 1$ for all $\sigma \in G$, hence $\sum_{\sigma \in G} < E, \sigma >= |G|$. On the other hand, if $E \notin G^\perp$, there exists a $\sigma_0 \in G :< E, \sigma_0 >= -1$. The mapping $\epsilon : G \to \{\pm 1\}, \sigma \mapsto < E, \sigma >$ is an epimorphism of groups and in particular yields that the cosets $\mathrm{Ker}(\epsilon)$, $\sigma_0\ \mathrm{Ker}(\epsilon)$ have the same size and give a partition of G in classes of elements with $< \sigma, E >= 1$ and $< \sigma, E >= -1$, which implies that $\sum_{\sigma \in G} < E, \sigma >= 0$.

□

**Theorem 3.5.** Let $C \leq (C^2)^{\otimes n} =: V$ be an additive quantum code and $G \subseteq \mathcal{E}$ be its stabilizer group (i.e. $C = V^G$); let $P_C$ be the orthogonal projection onto $C$, and let $S \subseteq \underline{n}$. Then the coefficients of the weight enumerators are given as follows:

$$A_S(P_C, P_C) = \#\{E \in G \mid \mathrm{Supp}(E) = S\} \tag{21}$$

$$B_S(P_C, P_C) = \#\{E \in G^\perp \mid \mathrm{Supp}(E) = S\} \tag{22}$$

$$A'_S(P_C, P_C) = 2^{-|S|} \#\{\sigma \in G \mid \sigma_{\big|_{S^c}} = \mathrm{Id}\} \tag{23}$$

$$B'_S(P_C, P_C) = \frac{2^{|S|}}{|G|} \#\{\sigma \in G \mid \sigma_{\big|_S} = \mathrm{Id}\} \tag{24}$$

Where for $\sigma = \sigma_1 \otimes \ldots \otimes \sigma_n$ and $S = \{s_1 < \ldots < s_k\}$, $\sigma_{\big|_S}$ denotes $\sigma_{s_1} \otimes \ldots \otimes \sigma_{s_k}$.

*Proof.*

$$\text{First } A_S(P_c,P_c) = \frac{1}{\dim(C)^2}\sum_{\substack{E\in\mathcal{E}\\ \text{Supp}(E)=S}} Tr(P_cE)^2$$

$$= \frac{1}{(\dim(C)|G|)^2}\sum_{\substack{E\in\mathcal{E}\\ \text{Supp}(E)=S}}\sum_{\sigma,\sigma'\in G}\underbrace{\text{Tr}(\sigma E)\text{Tr}(\sigma' E)}_{\substack{=0,\sigma\neq E \text{ or } \sigma'\neq E\\ =2^{2n},\sigma=\sigma'=E}}$$

$$= \underbrace{(\frac{2^n}{|G|\dim(C)})^2}_{=1,\text{see Prop. 2.9}}\#\{E\in G \mid \text{Supp}(E)=S\}$$

Where the second and third equalities follow from Lemma 3.4. The calculation for $B_S(P_C,P_c)$ is completely analogous.

Now, for the Rains enumerators:

$$A'_S(P_C,P_C) = \frac{1}{\text{Tr}(P_c)}\text{Tr}(\text{Tr}_{S^c}(P_C)\text{Tr}_{S^c}(P_C))$$

$$= \frac{1}{\dim(C)^2}\frac{1}{|G|^2}\sum_{\sigma,\sigma'\in G}\text{Tr}(\text{Tr}_{S^c}(\sigma)\text{Tr}_{S^c}(\sigma'))$$

$$= \frac{1}{\dim(C)^2}\frac{1}{|G|^2}\sum_{\sigma\in G}\text{Tr}(\text{Tr}_{S^c}(\sigma)\text{Tr}_{S^c}(\sigma))$$

$$= \underbrace{\frac{1}{\dim(C)^2}\frac{2^{n+|S^c|}}{|G|^2}}_{=2^{|S^c|-n}=2^{-|S|}}\#\{\sigma\in G \mid \sigma_{\big|_{S^c}} = \text{Id}\}$$

Again, the 2. and 3. equalities follow from Lemma 3.4. For $B'_S$ it is enough to see that $B'_S = \dim(C)A'_{S^c}$, which follows directly from their definitions. □

## 3.2 The Relationship between the Enumerators

There is a characterization of the Rains enumerators, which also sheds some light to the motivation for defining $A'$ and $B'$. They are basically the Shor-Laflamme enumerators, but "averaged over" the whole unitary group, instead of over $\mathcal{E}$.

**Theorem 3.6.** Let V be a finite-dimensional complex vector space, $n = \dim V, S \subseteq \underline{n}$, $M_1, M_2 \in \text{End}(V)$ hermitian, and let $U_S$ be a random , uniformly distributed unitary matrix on $V_S$, and $U_S \otimes \text{Id}_{S^c}$ its embedding on the full $\text{End}(V)$. Then:

$$A'_S(M_1,M_2) = 2^{|S|}E(\text{Tr}(M_1(U_S\otimes \text{Id}_{S^c}))\text{Tr}(M_2(U_S\otimes \text{Id}_{S^c})^\dagger)) \tag{25}$$

$$B'_S(M_1, M_2) = 2^{|S|} E(\mathrm{Tr}(M_1(U_S \otimes \mathrm{Id}_{S^c}) M_2 (U_S \otimes \mathrm{Id}_{S^c})^\dagger)) \tag{26}$$

*Proof.* With Equation 7 we have:

$$A'_S(M_1, M_2) = \mathrm{Tr}(\mathrm{Tr}_{S^c}(M_1)\mathrm{Tr}_{S^c}(M_2)) = 2^{|S|} E(\mathrm{Tr}(\mathrm{Tr}_{S^c}(M_1)U_S)\mathrm{Tr}(\mathrm{Tr}_{S^c}(M_2)U_S^\dagger))$$

$$= 2^{|S|} E(\mathrm{Tr}(M_1(U_S \otimes \mathrm{Id}_{S^c}))\mathrm{Tr}(M_2(U_S \otimes \mathrm{Id}_{S^c})^\dagger))$$

Where the last equality follows from Remark 1.4. Now for the $B'$, define $\tilde{B}_S(M_1, M_2) := 2^{|S|} E(\mathrm{Tr}(M_1(U_S \otimes \mathrm{Id}_{S^c}) M_2 (U_S \otimes \mathrm{Id}_{S^c})^\dagger))$. Then it follows with Equation 6:

$$\begin{aligned} \tilde{B}_S(M_1, M_2) &= \tilde{B}_S(E(U_S M_1 U_S^\dagger), E(U_s M_2 U_S^\dagger)) \\ &= 2^{-2|S|} \tilde{B}_S(\mathrm{Tr}_S(M_1) \otimes \mathrm{Id}_S, \mathrm{Tr}_S(M_2) \otimes \mathrm{Id}_S) \\ = 2^{-|S|} \mathrm{Tr}((\mathrm{Tr}_S(M_1) \otimes \mathrm{Id}_S)(\mathrm{Tr}_S(M_2) \otimes \mathrm{Id}_S)) &= B'_S(M_1, M_2) \end{aligned}$$

□

For the remainder of this section let $C \leq \mathbb{C}^{2^n}$ be an additive quantum code, $G$ its stabilizer group, and for $S \subseteq \underline{n}$ let $A_S := A_S(P_C, P_C)$, and similarly for $A'_S, B_S, B'_S$. The results of this section have been proved by Eric Rains [1] for non-additive codes as well, and the proof is in fact, not harder. We focus here on additive codes for purely didactical reasons.

**Proposition 3.7.** Let $S \subseteq \underline{n}$. Then the Rains and Shor-Laflamme enumerators are related by the following:

$$A'_S = 2^{-|S|} \sum_{T \subseteq S} A_T \text{ and } B'_S = 2^{-|S|} \sum_{T \subseteq S} B_T \tag{27}$$

*Proof.* For $A'_S$ The crucial observation here is that for $\sigma \in G$, $\sigma_{\big|S} = \mathrm{Id} \Leftrightarrow \mathrm{Supp}(\sigma) \subseteq S^c$. It follows that

$$\{\sigma \in G \mid \sigma_{\big|S} = \mathrm{Id}\} = \dot{\bigcup}_{T \subseteq S^c} \{\sigma \in G \mid \mathrm{Supp}(\sigma) = T\}$$

And this in turn implies:

$$\begin{aligned} A'_S &= 2^{-|S|} \#\{\sigma \in G \mid \sigma_{\big|S^c} = \mathrm{Id}\} \\ = 2^{-|S|} \sum_{T \subseteq S} \underbrace{\#\{\sigma \in G \mid \mathrm{Supp}(\sigma) = T\}}_{=A_T} &= 2^{-|S|} \sum_{T \subseteq S} A_T \end{aligned}$$

Now for $B'_S$ we use Theorem 3.6:

$$B'_S = \frac{2^{-|S|}}{\dim(C)} E(\mathrm{Tr}(P_C(U_s \otimes \mathrm{Id}_{S^c}) P_C(U_S \otimes \mathrm{Id}_{S^c})))$$
$$= \frac{2^{-|S|}}{\dim(C)|G|^2} \sum_{g,g' \in G} E(\mathrm{Tr}[g(U_S \otimes \mathrm{Id}_{S^c}) g'(U_S^\dagger \otimes \mathrm{Id}_{S^c})])$$

Using the expansion in the orthogonal basis $\mathcal{E} : U_S \otimes \mathrm{Id}_{S^c}$
$= \sum_{\sigma \in \mathcal{E}} 2^{-n} \mathrm{Tr}((U_S \otimes \mathrm{Id}_{S^c})\sigma)\sigma$ yields:

$$B'_S = \frac{2^{|S|-2n}}{\dim(C)|G|^2} \sum_{g,g' \in G} \sum_{\sigma,\sigma' \in \mathcal{E}} E(\mathrm{Tr}[g\mathrm{Tr}(\sigma(U_S \otimes \mathrm{Id}_{S^c}))\sigma g' \mathrm{Tr}(\sigma'(U_S^\dagger \otimes \mathrm{Id}_{S^c}))\sigma'])$$

$$= \frac{2^{|S|-2n}}{\dim(C)|G|^2} \sum_{g,g' \in G} \sum_{\sigma,\sigma' \in \mathcal{E}} \mathrm{Tr}(g\sigma g'\sigma') E[\mathrm{Tr}(\sigma(U_S \otimes \mathrm{Id}_{S^c}))\mathrm{Tr}(\sigma'(U_S^\dagger \otimes \mathrm{Id}_{S^c}))]$$

Lemma 3.4 together with Equation 7 yield

$$E[\mathrm{Tr}((U_S \otimes \mathrm{Id}_{S^c})\sigma)\mathrm{Tr}((U_S^\dagger \otimes \mathrm{Id}_S^c)\sigma')] = 2^{-|S|}\mathrm{Tr}(\sigma_{\big|S}\sigma'_{\big|S})\mathrm{Tr}(\sigma_{\big|S^c})\mathrm{Tr}(\sigma'_{\big|S^c})$$
$$= \begin{cases} 2^{2n-2|S|}\delta_{\sigma,\sigma'} & \text{if } \mathrm{Supp}(\sigma) \subseteq S \\ 0 & \text{otherwise} \end{cases}$$

from which in turn follows that:

$$B'_S = \frac{2^{-|S|}}{\dim(C)} \sum_{\sigma \in \mathcal{E}, \mathrm{Supp}(\sigma) \subseteq S} \frac{1}{|G|^2} \sum_{g,g' \in G} \mathrm{Tr}(g\sigma g'\sigma)$$
$$= \frac{2^{-|S|}}{\dim(C)} \sum_{\sigma \in \mathcal{E}, \mathrm{Supp}(\sigma) \subseteq S} \underbrace{\mathrm{Tr}(P_C \sigma P_C \sigma)}_{=\mathrm{Tr}(\sigma P_C \sigma P_C)} = 2^{-|S|} \sum_{T \subseteq S} B_T$$

□

**Corollary 3.8.** For $d \in \underline{n}$ we get thus:

$$A'_d = 2^{-d} \sum_{i=0}^{d} \binom{n-i}{n-d} A_i \text{ and } B'_d = 2^{-d} \sum_{i=0}^{d} \binom{n-i}{n-d} B_i \tag{28}$$

*Proof.*

$$A'_d = \sum_{S \subseteq \underline{n}, |S|=d} A'_S = 2^{-d} \sum_{S \subseteq \underline{n}, |S|=d} \sum_{T \subseteq S} A_T = 2^{-d} \sum i = 0^d \sum_{T \subseteq \underline{n}, |T|=i} \sum_{T \subseteq S, |S|=d} A_T \tag{29}$$

$$= 2^{-d} \sum_{i=0}^{d} \sum_{T \subseteq \underline{n}, |T|=i} \binom{n-i}{n-d} A_T = 2^{-d} \sum_{i=0}^{d} \binom{n-i}{n-d} A_i \tag{30}$$

The same proof works for $B'_d$. □

**Corollary 3.9.** For $S \subseteq \underline{n}$, the enumerators $A_S(M_1, M_2), A'_S(M_1, M_2)$, $B_S(M_1, M_2), B'_S(M_1, M_2)$ are invariant under the equivalence of codes given by the action of $\mathcal{U}_2(\mathbb{C}) \wr S_S$, where $S_S$ is the symmetric group on the tensor product components given by $S$.

*Proof.* For the Rains enumerators it is immediately clear from Theorem 3.6: Since an element $\sigma \in \mathcal{U}_2(\mathbb{C}) \wr S_d$ would not change the support, and the unitary operators do not change the enumerator coefficients because of the tranlation invariance of the haar measure. For the Shor-Laflamme enumerators it follows from Proposition 3.7 as we can explicitly write $A_S(M_1, M_2)$ in terms of $A'_S(M_1, M_2)$ and the same for the $B$'s. □

**Example 3.10.** We can return to the example of the Shor code, the associated additive code has the $(\mathbb{F}_2)$-Generator matrix:

$$M := \begin{pmatrix} \omega^2 & \omega^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \omega^2 & \omega^2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega^2 & \omega^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \omega^2 & \omega^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \omega^2 & \omega^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^2 & \omega^2 \\ \omega & \omega & \omega & \omega & \omega & \omega & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega & \omega & \omega & \omega & \omega & \omega \end{pmatrix}$$

Using this we can easily get the Shor-Laflamme enumerator polynomials for this code, as it is the Hamming Weight Enumerator of the additive code

$$A(x, y) = x^9 + 9x^7y^2 + 27x^5y^4 + 75x^3y^6 + 144xy^8 \tag{31}$$

The Rains enumerator polynomial is a little bit harder to calculate. It is:

$$A'(x, y) = x^9 + \frac{9}{2}x^8y + \frac{45}{4}x^7y^2 + \frac{147}{8}x^6y^3 + \frac{171}{8}x^5y^4 + 18x^4y^5 + \frac{93}{8}x^3y^6 + \frac{45}{8}x^2y^7 + \frac{9}{4}xy^8 + \frac{1}{2}y^9 \tag{32}$$

This is obtained using Cor. 3.8, or equivalently, a relationship between both enumerator polynomials which follows from it, as will be seen in 3.11. Note that the coefficients of the rains enumerator polynomial need not be integers, the reason for this becomes clear after examining Theorem 3.5

## 3.3 The MacWilliams Transform

**Lemma 3.11.** Let $C$ be a quantum code on $n$ qubits and let $A(x,y), B(x,y)$, $A'(x,y), B(x,y)$ be its Short-Laflamme and Rains enumerator polynomials respectively. Then they are related by the following:

$$A'(x,y) = A(x + \frac{y}{2}, \frac{y}{2}) \tag{33}$$

$$B'(x,y) = B(x + \frac{y}{2}, \frac{y}{2}) \tag{34}$$

*Proof.* Using Cor. 3.8 we get:

$$A'(x,y) = \sum_{d=0}^{n} A'_d x^{n-d} y^d = \sum_{d=0}^{n} \sum_{i=0}^{d} 2^{-d} \binom{n-i}{n-d} A_i x^{n-d} y^d$$

$$= \sum_{i=0}^{n} \sum_{d=i}^{n} 2^{-d} \binom{n-i}{n-d} A_i x^{n-d} y^d \underbrace{=}_{j:=n-d} \sum_{i=0}^{n} \sum_{j=0}^{n-i} 2^{-(n-j)} \binom{n-i}{j} A_i x^j y^{n-j}$$

$$= \sum_{i=0}^{n} y^i 2^{-i} \sum_{j=0}^{n-i} 2^{-(n-i-j)} \binom{n-i}{j} A_i x^j y^{n-i-j}$$

$$= \sum_{i=0}^{n} A_i (\frac{y}{2})^i (x + \frac{y}{2})^{n-i} = A(x + \frac{y}{2}, \frac{y}{2})$$

The calculation for $B'$ is literally the same, replacing $A$ with $B$. □

**Theorem 3.12.** We get analogies of the MacWilliams Identity for Quantum codes: Let $C \leq \mathbb{C}^{2^n}$ be a an additive quantum code on $n$ qubits, and $A(x,y), B(x,y)$ be the corresponding Shor-Laflamme enumerator polynomials, $A'(x,y), B'(x,y)$ the Rains enumerator polynomials. Then:

$$\dim(C) A'(x,y) = B'(y,x) \tag{35}$$

$$\dim(C) A(x,y) = B(\frac{x+3y}{2}, \frac{x-y}{2}) \tag{36}$$

*Proof.* For the first one we again note that immediately from its definition it is clear that $\dim(C) A'_i = B'_{n-i}$. It follows then

$$\dim(C) A'(x,y) = \dim(C) \sum_{d=0}^{n} A_d x^{n-d} y^d = \sum_{d=0}^{n} B_{n-d} x^{n-d} y^d = B'(y,x)$$

Using Lemma 3.11 we can translate this identity to the Shor-Laflamme enumerators:

$$\begin{aligned}\dim(C)A(x,y) &= \dim(C)A'(x-y,2y) = B'(2y,x-y)\\ &= B(2y+\frac{x-y}{2},\frac{x-y}{2}) = B(\frac{x+3y}{2},\frac{x-y}{2})\end{aligned}$$

□

**Example 3.13.** Knowing the enumerator polynomials of the Shor code, Ex. 3.10, we immediately get the enumerator polynomials for the dual codes through the MacWilliams Transform:

$$\begin{aligned}B(x,y) = 9x^7y^2 + 27x^5y^4 + 75x^3y^6 + 144xy^8 + 39x^6y^3 +\\ 207x^4y^5 + 333x^2y^7 + x^9 + 189y^9 \qquad (37)\\ B'(x,y) = 2y^9 + 9y^8x + \frac{45}{2}y^7x^2 + \frac{147}{4}y^6x^3 + \frac{171}{4}y^5x^4\\ +36y^4x^5 + \frac{93}{4}y^3x^6 + \frac{45}{4}y^2x^7 + \frac{9}{2}yx^8 + x^9 \qquad (38)\end{aligned}$$

# 4 Applications of the Weight Enumerators: Bounds

Having introduced Weight Enumerators for quantum error correcting codes, and having found out a few properties of these, we can go on to see one of the most important applications of the Weight Enumerators, namely that of finding bounds for the distance or dimension of codes with specific parameters. This is analogous to classical coding theory and is the reason why these enumerators for quantum codes were introduced in the first place by Shor and Laflamme. To do this, we first have to find out what the relationship is between the code distance and the Weight Enumerators.

## 4.1 The Relationship between the Code Distance and the Enumerators

**Lemma 4.1.** Let $C$ be a quantum code on $n$ qubits, and let $v$ be a random unit vector of $C$, uniformly distributed. Further let $P$ be the orthogonal projection onto $C$, and $K$ be the dimension of $C$, $K = \dim_{\mathbb{C}} C$. Then

$$E_{v\in C}(|v\rangle\langle v|) = \int_C |v\rangle\langle v| dv = \frac{P}{K} \tag{39}$$

*Proof.* We start by identifying that the left hand side is well defined. This is the case since the unit sphere on $\mathbb{C}^K$ is compact (with respect to the natural topology), and is a sub manifold of $\mathbb{R}^{2K}$, which allows us to define an finite integral on $C$, which can be chosen to be normed, see [6]. Now, an integral of an operator can be defined using the scalar product - see Appendix 3 in [12], and thus the integral is well defined. Now, since $C$ is isometric to $\mathbb{C}^K$, we will assume without loss of generality that $C = \mathbb{C}^K$ and thus it suffices to show that for $\tilde{P} := \int_C |v\rangle\langle v| dv$ it holds that $\tilde{P} = \frac{1}{K}\mathrm{Id}_{\mathbb{C}^K}$. To show this we note that the unitary group $\mathcal{U}_K(\mathbb{C})$ acts on $\mathrm{End}(\mathbb{C}^K)$ via conjugation, and this action defines a representation of $\mathcal{U}_K(\mathbb{C})$, which we will denote by $\pi$. Now, let $\mu$ denote the measure induced on $\mathbb{C}^K$ by the probability measure of $v$ and the isometry between $C$ and $\mathbb{C}^K$, and let $dU$ denote the Haar-measure on the unitary group $\mathcal{U}_K(\mathbb{C})$. It follows that

$$\tilde{P} = \int_{\mathbb{C}^K} |v\rangle\langle v| d\mu(v) = \int_{\mathbb{C}^K} U^\dagger|v\rangle\langle v|U d\mu(v) = \int_{\mathcal{U}_K(\mathbb{C})}\int_{\mathbb{C}^K} U^\dagger|v\rangle\langle v|U d\mu(v) dU \tag{40}$$

Where in the first equality we used the uniformity of the probability measure on $v$ and on the second one we used the normalization of the Haar measure.

Let $|v_0\rangle \in C^K, \langle v_0|v_0\rangle = 1$. Then because of the normalization of the $\mu$ measure it holds that

$$\tilde{P} = \int_{\mathcal{U}_K(\mathbb{C})} \int_{\mathbb{C}^K} U^\dagger |v\rangle\langle v| U d\mu(v) dU$$

$$= \int_{\mathcal{U}_K(\mathbb{C})} U^\dagger |v_0\rangle\langle v_0| U dU = \int_{\mathcal{U}_K(\mathbb{C})} (\pi(U))(|v_0\rangle\langle v_0|) dU \tag{41}$$

Since the only fix point of the representation $\pi$ is $I_K$, and the mapping $A \mapsto \int_{\mathcal{U}_K(\mathbb{C})} (\pi(U))(A) dU$ is an orthogonal projection to an invariant subspace of the representation $\pi$ (Reynolds operator), it follows that $\tilde{P} \in \mathbb{C} I_K$. That $\tilde{P} = \frac{1}{K} I_K$ can be seen by explicitly calculating the orthogonal projection:

$$\tilde{P} = \frac{\langle |v_0\rangle\langle v_0|, I_K\rangle}{\langle I_K, I_K\rangle} I_K = \frac{1}{K} I_K$$

□

**Lemma 4.2.** Let $C$ be a Quantum Code on $n$ qubits, $M \in \mathrm{End}(\mathbb{C}^{2^n})$ be any operator on those $n$ qubits, and let $v$ be a random unit vector of $C$, uniformly distributed. Further let $K := \dim_{\mathbb{C}} C$ and $P$ be the orthogonal projection onto $C$. Then

$$E[|\mathrm{Tr}(M|v\rangle\langle v|) - \frac{1}{K}\mathrm{Tr}(MP)|^2] = \frac{1}{K^2(K+1)}(K\mathrm{Tr}(MPM^\dagger P) - |\mathrm{Tr}(MP)|^2) \tag{42}$$

*Proof.* Since for any $a \in \mathbb{C}$ it holds that $|a|^2 = aa^*$, multiplying out yields:

$$E[|\mathrm{Tr}(M|v\rangle\langle v|) - \frac{1}{K}\mathrm{Tr}(MP)|^2]$$

$$= E[|\mathrm{Tr}(\langle v|M|v\rangle)|^2 + \frac{1}{K^2}|\mathrm{Tr}(MP)|^2$$

$$-\frac{1}{K}\mathrm{Tr}(M|v\rangle\langle)^*\mathrm{Tr}(MP) - \frac{1}{K}\mathrm{Tr}(M|v\rangle\langle v|)\mathrm{Tr}(MP)^*]$$

$$\underbrace{=}_{\text{Lemma 4.1}} E[|\mathrm{Tr}(\langle v|M|v\rangle)|^2 - \frac{1}{K^2}|\mathrm{Tr}(MP)|^2]$$

Now consider only the first integral, and from the isometry $C \cong \mathbb{C}^K$ we assume $C = \mathbb{C}^K$ without loss of generality:

$$\int_{\mathbb{C}^K} |\mathrm{Tr}(\langle v|M|v\rangle)|^2 dv = \int_{\mathbb{C}^K} |\langle v|M|v\rangle|^2 dv$$

$$= \int_{\mathbb{C}^K} \langle v|M|v\rangle\langle v|M^\dagger|v\rangle = \int_{\mathbb{C}^K} \mathrm{Tr}(\langle v|M|v\rangle\langle v|M^\dagger|v\rangle)$$

$$= \int_{\mathbb{C}^K} \mathrm{Tr}(|v\rangle\langle v|M|v\rangle\langle v|M^\dagger) =: \int_{\mathbb{C}^K} \varphi_M(|v\rangle\langle v|, |v\rangle\langle v|) dv$$

Where the mapping $\varphi_M$ is the bi-linear functional defined by $\varphi_M(A,B) := \mathrm{Tr}(AMBM^\dagger)$. Using the universal property of the tensor product, there exists exactly one linear mapping $\psi_M : \mathrm{End}(\mathbb{C}^K) \otimes \mathrm{End}(\mathbb{C}^K) \to \mathbb{C}$, so that $\varphi_M(A,B) = \psi_M(A \otimes B)$ for all $A, B \in \mathrm{End}(\mathbb{C}^K)$.

Now, with respect to the diagonal operation of the unitary group $\mathcal{U}_K(\mathbb{C})$ on the tensor product $\mathrm{End}(\mathbb{C}^K) \otimes \mathrm{End}(\mathbb{C}^K)$ we can proceed as in Lemma 4.1 and rewrite the integral as follows:

$$\begin{aligned}\psi_M(\int_{\mathbb{C}^K} |v\rangle\langle v| \otimes |v\rangle\langle v| dvv &= \psi_M(\int_{\mathcal{U}_K(\mathbb{C})} U^\dagger|v_0\rangle\langle v_0|U \otimes U^\dagger|v_0\rangle\langle v_0|U) dU \\ &= \psi_M(\int_{\mathcal{U}_K(\mathbb{C})} ((\pi \otimes \pi)(U))(|v_0\rangle\langle v_0| \otimes |v_0\rangle\langle v_0|)) dU\end{aligned}$$

Where $|v_0\rangle \in \mathbb{C}^K$ is some (fixed) unit vector ($\langle v_0|v_0\rangle = 1$), and $\pi$ is the same representation as in Lemma 4.1. With the same reasoning, it means that the image of this orthogonal projection has to be in the subspace fixed by the diagonal action of $\mathcal{U}_K(\mathbb{C})$. Let $|v_1\rangle, \ldots, |v_K\rangle$ be an orthonormal basis of $\mathbb{C}^K$. It is straightforward to see that the subspace spanned by $\sum_{i,j=1}^K (|v_i\rangle\langle v_i|) \otimes (|v_j\rangle\langle v_j|)$, $\sum_{i,j=1}^K (|v_i\rangle\langle v_j|) \otimes (|v_j\rangle\langle v_i|)$ is independent of the basis, and is in fact, the spaced fixed by the diagonal action of $\mathcal{U}_K(\mathbb{C})$. Similarly to the proof of Lemma 4.1 we retrieve the exact projection again through the scalar product, though we have to make the basis an orthonormal-one (Gram-Schmidt), which yields

$$\begin{aligned}&\psi_M(\int_{\mathcal{U}_K(\mathbb{C})} ((\pi \otimes \pi)(U))(|v_0\rangle\langle v_0| \otimes |v_0\rangle\langle v_0|)) dU \\ = \psi_M(\frac{1}{K(K+1)} &\sum_{i,j=1}^K (|v_i\rangle\langle v_i|) \otimes (|v_j\rangle\langle v_j|) + (|v_i\rangle\langle v_j|) \otimes (|v_j\rangle\langle v_i|)) \\ = \frac{1}{K(K+1)} &\sum_{i,j=1}^K \varphi_M(|v_i\rangle\langle v_i|, |v_j\rangle\langle v_j|) + \varphi_M(|v_i\rangle\langle v_j|, |v_j\rangle\langle v_i|) \\ = \frac{1}{K(K+1)} &\sum_{i,j=1}^K \mathrm{Tr}(|v_i\rangle\langle v_i|M|v_j\rangle\langle v_j|M^\dagger) + \mathrm{Tr}(|v_i\rangle\langle v_j|M|v_j\rangle\langle v_i|M^\dagger) \\ &= \frac{1}{K(K+1)}(\mathrm{Tr}(PMPM^\dagger) + |\mathrm{Tr}(PM)|^2)\end{aligned}$$

□

**Theorem 4.3.** Let $A'_i, B'_i, A_i, B_i$ be the Rains and Shor-Laflamme enumerators of a quantum Code $C$ of dimension $K$ respectively. Then it holds that

$B'_i \geq A'_i \geq 0$ for all $i \in \underline{n}$, where equality $B'_i = A'_i$ holds for all $i \in \underline{d}$ if and only if $C$ has minimal distance $d$. Similarily, for the Shor-Laflamme enumerators it holds that $B_i \geq A_i \geq 0$ for all $i \in \underline{n}$, where equality $B_i = A_i$ holds for all $i \in \underline{d}$ if and only if $C$ has minimal distance $d$. In other words we can read the minimal distance $d$ from the enumerator: $d = \max\{j \in \underline{n} \mid B'_i = A'_i \text{ for all } i \leq j\} = \max\{j \in \underline{n} \mid B_i = A_i \text{ for all } i \leq j\}$.

*Proof.* First for the Shor-Laflamme enumerators $A_i, B_i$: Consider that by definition, for any hermitian operator $M$, it holds that $A_i(M, M) = A_i(M, M^\dagger) = \sum_{\substack{E \in \mathcal{E} \\ \mathrm{wt}(E)=i}} |\mathrm{Tr}(EM)|^2$. Since the orthogonal projection $P$ onto $C$ is hermitian, it follows immediately that $A_i \geq 0$. Now for the relationship between $A_i, B_i$ consider the hermitian operator $M_v$ for any normed $|v\rangle \in C$: $M_v := |v\rangle\langle v| - \frac{1}{K}P$. Now let $v$ be a uniformly distributed, random unit vector from $C$. From our previous observation, and Lemma 4.2, we get that

$$\begin{aligned}
0 \leq E[A_i(M_v, M_v)] &\underbrace{=}_{\text{def.}} E[\frac{1}{K^2} \sum_{\substack{\sigma \in \mathcal{E} \\ \mathrm{wt}(\sigma)=i}} \mathrm{Tr}(\sigma M_v)^2] \\
&= \frac{1}{K^2} \sum_{\substack{\sigma \in \mathcal{E} \\ \mathrm{wt}(\sigma)=i}} E[\mathrm{Tr}(\sigma|v\rangle\langle v| - \frac{1}{K}\sigma P)^2] \\
= \frac{1}{K^2(K+1)}(\frac{1}{K} \sum_{\substack{\sigma \in \mathcal{E} \\ \mathrm{wt}(\sigma)=i}} \mathrm{Tr}(\sigma P \sigma^\dagger P) &- \frac{1}{K^2} \sum_{\substack{\sigma \in \mathcal{E} \\ \mathrm{wt}(\sigma)=i}} |\mathrm{Tr}(\sigma P)|^2) \\
&= \frac{1}{K^2(K+1)}(B_i(P, P) - A_i(P, P))
\end{aligned}$$

Where in order to use Lemma 4.2 we examine, that the expressions under the modulus are real, since the operators are hermitian. Further we note that $A_i = B_i$ iff $E[\mathrm{Tr}(\langle v|\sigma|v\rangle) - \frac{1}{K}\mathrm{Tr}(\sigma P)] = 0$ for all $\sigma \in \mathcal{E}$ with $\mathrm{wt}(\sigma) = i$. Since this condition is linear, it holds for the span of $\{\sigma \in \mathcal{E} \mid \mathrm{wt}(\sigma) = i\}$ which includes all $i$-qubit errors, i.e. all unitary operators whose support is exactly $i$ qubits. The condition $E(\langle v|U_i|v\rangle - \frac{1}{K}\mathrm{Tr}(U_i P)) = 0$ for all $i$-qubit errors $U_i$ can be seen, using Lemma 4.1, as the variance of the random variable given by $|v\rangle \mapsto \langle v|U_i|v\rangle = \mathrm{Tr}(\langle v|U_i|v\rangle) = \mathrm{Tr}(U_i|v\rangle\langle v|)$. Thus, this variance is zero if and only if the random variable is constant, which means that for all $|v_0\rangle, |v'_0\rangle \in C$ with $\langle v_0|v_0\rangle = \langle v'_0|v'_0\rangle = 1$ it holds that $\langle v_0|U_i|v_0\rangle = \langle v'_0|U_i|v'_0\rangle$. But this is exactly Definition 2.19. This proof transfers to the rains enumerators directly thanks to Theorem 3.6.

□

With this results we can see the usefulness of the Weight Enumerators. Since any quantum code must have a Weight Enumerator, and we have conditions it has to follow, we can get bounds on the minimal distance or on the dimension for a given number of qubits using these conditions. This proceeding is inspired by classical coding theory, which also gives a theorem for additive codes:

**Definition 4.4.** Let $n \in \mathbb{N}, j \in \underline{n}$. We define the Krawtchouk numbers $P_j(x,n)$ as follows:

$$P_j(x,n) := \sum_{s=0}^{j} (-1)^s 3^{j-s} \binom{x}{s} \binom{n-x}{j-s} \tag{43}$$

**Theorem 4.5** (LP bounds for additive codes)**.** Let $C$ be an additive $[[n,k,d]]$ code and $A_i, i = 0 \dots n$ be the coefficients of the Shor-Laflamme Weight Enumerator of $C$. Further let the associated $\mathbb{F}_4$ code have no vectors of weight 1, and let $P_j(x,n)$ denote the Krawtchouk number. Then, the coefficients of the Weight Enumerator have to satisfy the following equations and inequalities

$$A_0 = 1, A_1 = 0, A_j \geq 0 \text{ for all } j \in \{2,3,\dots,n\} \tag{44}$$

$$A_0 + A_1 + \dots + A_n = 2^{n-k} \tag{45}$$

$$A'_j := \frac{1}{2^{n-k}} \sum_{r=0}^{n} P_j(r,n) A_r \text{ for all } j \in \{0,1,\dots,n\} \tag{46}$$

$$A_j := A'_j \text{ for all } j \in \{0,\dots,d-1\}, A_j \leq A'_j \text{ for all } j \in \{d,\dots,n\} \tag{47}$$

$$\sum_{j=0}^{\lfloor \frac{n}{2} } A_{2j} = 2^{n-k-1} \text{ or } 2^{n-k} \tag{48}$$

$$\frac{1}{2^{n-k-1}} \sum_{r=0}^{n} P_j(2r,n) A_{2r} \geq A'_j \text{ for all } j \in \underline{n} \tag{49}$$

A proof of this can be found in [10], and can be proved with classical coding theory. It will be omitted here since an analogous result for general quantum codes will be proven later. Note that the requirement of no vectors of weight 1 is not really much of a restriction: It can be proved (see [10]) that if an $[[n,k,d]]$ code with vectors of weight 1 in the associated $\mathbb{F}_4$ exists, then also an $[[n-1,k,d]]$ code exists. In particular, for finding bounds we can safely make this assumption.

With this we can get bounds on the distance $d$ for a given pair $n,k$ (the maximal number for which the system of equations on Theorem 4.5 have

a solution), or bounds on the number of encoded qubits $k$, by maximizing $2^k = \sum_{i=0}^{n} A_i$ with the rest of the constraints given by Theorem 4.5 - a problem which falls under what is known as linear programming, and can also easily be solved. This bounds hold for additive codes, but they are not strict for general quantum error correcting codes. The following is an example of a non-additive code that is strictly better than any additive code.

**Example 4.6.** According to Theorem 4.5 there is no additive $[[5, k, 2]]$ code for $k > 2$, which means that code space dimension for an additive code with $n = 5$ qubits and minimal distance $d = 2$ is bounded by $2^2 = 4$. There is, however, a $((5, 6, 2))$ code (found in [4]), which means there is strictly better than the $((5, 4, 2))$ bound for additive codes. This code can be given explicitly, for example, by giving a projection operator onto it:

$$\begin{aligned} P := \frac{1}{16}[3(I_2 \otimes I_2 \otimes I_2 \otimes I_2 \otimes I_2) + (I_2 \otimes Z \otimes Y \otimes Y \otimes Z)_{\text{cyc}} \\ +(I_2 \otimes X \otimes Z \otimes Z \otimes X)_{\text{cyc}} - (I_2 \otimes Y \otimes X \otimes X \otimes Y)_{\text{cyc}} \\ +2(Z \otimes X \otimes Y \otimes Y \otimes X)_{\text{cyc}} - 2(Z \otimes Z \otimes Z \otimes Z \otimes Z)_{\text{cyc}}] \end{aligned}$$

Here, the subscript cyc denotes that it is the sum of all cyclic shifts of that element. A simple calculation lets us see that this is indeed a projection operator ($P^2 = P$) and since $\text{Tr}(P) = \frac{3 \cdot 2^5}{16} = 6$ it does project onto a 6-dimensional subspace of $\mathbb{C}^{2^5}$. That it has minimal distance two can be seen from its Weight Enumerator, $A(x, y) = x^5 + \frac{10}{6}xy^4 + \frac{8}{3}y^5$ using Theorem 4.3.

The main reason for introducing the Shor-Laflamme/Rains enumerators is generalizing the Hamming Weight Enumerator from additive codes to general quantum codes. In this way, we can get a result analogous to Theorem 4.5 which holds for any quantum code.

**Theorem 4.7** (LP bound for general quantum codes)**.** Let $C$ be a quantum $((n, K, d))$ code and let $\sum_{i=0}^{n} A_i x^{n-i} y^i$ be its (Shor-Laflamme) Weight Enumerator. Then the $A_i$ satisfy the following set of linear equations and inequalities:

$$A_0 = 1, A_i \geq 0 \text{ for all } i \in \underline{n} \tag{50}$$

$$B_i := \frac{K}{2^n} \sum_{r=0}^{n} P_i(r, n) A_r \tag{51}$$

$$A_i = B_i \text{ for all } i \in \{0, \ldots, d-1\} \tag{52}$$

$$A_i \leq B_i \text{ for all } i \in \{d, \ldots, n\} \tag{53}$$

*Proof.* $A_0 = 1$ follows directly from the definition. Equations 50, 52 and 53 all follow from Theorem 4.3. Equation 51 is, of course, the MacWilliams Transform (Theorem 3.12). This can be seen immediately if we expand the terms on the MacWilliams Transform:

$$\dim(C)A(x,y) = B(\frac{x+3y}{2}, \frac{x-y}{2}) \Leftrightarrow B(x,y) = KA(\frac{x+3y}{2}, \frac{x-y}{2}) \quad (54)$$

As can be seen with a simple variable substitution. Now, expanding the right hand side of the last equation yields:

$$\begin{aligned}
& KA(\frac{x+3y}{2}, \frac{x-y}{2}) \\
&= K\sum_{r=0}^{n}(\frac{x+3y}{2})^{n-r}(\frac{x-y}{2})^{r}A_i \\
&= \frac{K}{2^n}\sum_{r=0}^{n}(x+3y)^{n-r}(x-y)^{r}A_r \\
&= \frac{K}{2^n}\sum_{r=0}^{n}\sum_{j=0}^{n-r}\binom{n-r}{j}x^j(3y)^{n-r-j}\sum_{i=0}^{r}\binom{r}{i}(-1)^i x^i y^{r-i}A_r \\
&= \frac{K}{2^n}\sum_{r=0}^{n}\sum_{i=0}^{r}\sum_{j=0}^{n-r}\binom{r}{i}\binom{n-r}{j}(-1)^i 3^{n-r-j}x^{i+j}y^{n-(i+j)}A_r \qquad (55)
\end{aligned}$$

From this we can read $B_d$ as the coefficient of $x^{n-d}y^d$ to be the Krawtchouk number. □

**Example 4.8.** We get bounds on the minimal distance/code space dimension for example, for $n = 1, \ldots, 7$ by searching for a solution of 50-53 for each $d$ in $1, \ldots, n$ and each $K$ in $1, \ldots, 2^n \leq 128$. This yields Table 4.8.

Table 4.8 was calculated using [14] on an amd64 GNU/Linux PC. The bounds that are known to be sharp were all obtained from [15].

**Example 4.9.** When the solution is unique, we actually get a candidate for the weight enumerator. For example, the coefficients for a $((5,8,2))$ code are unique, this means, that if a $((5,8,2))$ code exists, it has to have the following enumerator:

$$A(x,y) = x^5 + 3y^5 \quad (56)$$

We will see later (Table 4.17), that this is in fact not the case, there is no such code.

| n | d=1 | d=2 | d=3 | d=4 | d=5 | d=6 | d=7 |
|---|---|---|---|---|---|---|---|
| 1 | 2* | - | - | - | - | - | - |
| 2 | 4* | 1* | - | - | - | - | - |
| 3 | 8* | 2 | 1 | - | - | - | - |
| 4 | 16* | 4* | 1 | 1 | - | - | - |
| 5 | 32* | 8 | 2* | 1 | 1 | - | - |
| 6 | 64* | 16* | 2* | 1* | 1 | 1 | - |
| 7 | 128* | 32 | 4 | 1 | 1 | 1 | 1 |

Table 2: Bounds on the code space dimension for all possible minimal distances of $n = 1, \ldots, 7$. An asterisk denotes a bound that is known to be sharp, i.e. for which a code is known to exist

## 4.2 Shadow Enumerators

Theorem 4.7 gives us a good start on finding bounds on the minimal distance or code space dimension for general quantum error correcting codes. The motivation for this theorem came from the hamming Weight Enumerators of classical coding theory. There is another enumerator on binary codes which has not been discussed, that (as we will see) can also be generalized for quantum error correcting codes and gives even tighter bounds, namely, the Shadow Enumerator. This was originally done by Eric Rains on [3].

**Definition 4.10.** Let $C$ be an additive quantum code on $n$ qubits, and $S$ be the associated stabilizer group. We define the shadow of $C$ to be the set $S(C)$ of all $\sigma \in \mathcal{E}$ with $\langle \sigma, \sigma' \rangle \equiv wt(\sigma')(\text{mod } 2)$ for all $\sigma' \in S$, where $\langle \cdot, \cdot \rangle$ denotes the trace inner product. The (hamming) Weight Enumerator of $S(C)$ we call the Shadow Enumerator of $C$, and denote it by $S(x, y)$.

Just as for the enumerator of the dual code, there is a simple relationship relating the Weight Enumerator to the Shadow Enumerator, as the MacWilliams Identity. For additive codes this is also very simple:

**Proposition 4.11.** Let $C$ be an [[n,k]] additive quantum code with associated stabilizer group $G$, then the (Shor-Laflamme) Weight Enumerator is related to the Shadow Enumerator in the following way:

$$S(x, y) = 2^k A(\frac{x + 3y}{2}, \frac{y - x}{2}) \tag{57}$$

*Proof.* If $S$ has no elements of odd weight, then the assertion follows from the fact that $S(C) = G^{\perp}$ in this case, as can be seen from the definition of both. Since for a code with only even-weighted elements, the Weight Enumerator

fulfills $A(x,y) = A(x,-y)$ we get the required identity from the MacWilliams Transform. Hence, we assume $G$ has elements of odd weight.

Define $G_0 \subset G$ as the subset of all elements of even weight. We know that $G$ is self-orthogonal with respect to the symplectic form given by the commutator. Applying this we get the following inclusions:

$$G_0 \subset G \subset G^{\perp} \subset G_0^{\perp} \tag{58}$$

From the self-orthogonality we also get that $G_0$ is in fact subspace of $G$. Let $A^{(0)}, B^{(0)}$ be the (Shor-Laflamme) Weight Enumerators of $G_0$. Now, consider $S(C) = \{\sigma \in \mathcal{E} \mid \langle \sigma, \sigma' \rangle \equiv wt(\sigma') (\text{mod } 2) \text{ for all } \sigma' \in G\} \subseteq G_0^{\perp}$. In fact, since for any $\sigma \in S(C), \sigma' \in G$ it has to hold that $\langle \sigma, \sigma' \rangle = 0$ if and only if $\sigma' \in G_0$, it turns out that $S(C)$ is exactly $G_0^{\perp} \backslash G^{\perp}$. Using the combinatorial interpretation of the Weight Enumerators (as hamming Weight Enumerators), we can thus express the Shadow Enumerator:

$$S(x,y) = B^{(0)}(x,y) - B(x,y) = 2^k (A^{(0)}(\frac{x+3y}{2}, \frac{x-y}{2}) - A(\frac{x+3y}{2}, \frac{x-y}{2})) \tag{59}$$

On the other hand we see that $A(x,y) + A(x,-y) = 2A^{(0)}(x,y)$, as exactly the elements of even weight cancel out like this. This yields the required identity. □

As already mentioned, Shadow Enumerators can be generalized for any quantum code, just as the hamming Weight Enumerators were. The original article in which these were introduced, [3], includes a detailed discussion of the steps taken to do this generalization, and the rationale behind it. Here, we will just present the finished generalization along with the important accompanying results.

**Definition 4.12.** Let $M$ be a hermitian operator acting on $\mathbb{C}^{2^n}$, and let $M = \sum_{\sigma \in \mathcal{E}} c_\sigma \sigma$ be the decomposition in the basis $\mathcal{E}$. We define

$$M^{(-)} := \sum_{\sigma \in \mathcal{E}} (-1)^{\text{wt}(\sigma)} c_\sigma \sigma \tag{60}$$

**Definition 4.13.** Let $C$ be a quantum code on $n$ qubits and $P$ be the orthogonal projection operator onto $C$. We define the Shadow Enumerator coefficients

$$S_d := B_d(P, P^{(-)}) \tag{61}$$

and similarly the Shadow Enumerator polynomial as

$$S(x,y) := \sum_{d=0}^{n} S_d x^{n-d} y^d \tag{62}$$

Note that for any hermitian operator $M$, $M^{(-)}$ is also hermitian, and thus, the Shadow Enumerator is well defined.

We also get a theorem analogous to Prop. 4.11.

**Theorem 4.14.** Let $C$ be a $K$-dimensional quantum code on $n$ qubits, $P$ be the orthogonal projection operator onto $C$, and $A(x,y), S(x,y)$ be the (Shor-Laflamme) Weight Enumerator and Shadow Enumerator respectively. Then they are related by the following MacWilliams Transform:

$$S(x,y) = KA(\frac{x+3y}{2}, \frac{y-x}{2}) \tag{63}$$

*Proof.* Consider the polynomial $W(x,y) := \sum_{d=0}^{n} A_d(P, P^{(-)})$. Note that though the MacWilliams Transform, Theorem 3.12, was stated explicitly for the projection operator onto a quantum code, the proof does holds the same for the enumerator coefficients with respect to any two hermitian operators. Thus, by the MacWilliams Transform we get that $S(x,y) = KW(\frac{x+3y}{2}, \frac{x-y}{2})$. It is therefore sufficient to prove that $W(x,y) = A(x,-y)$. Writing the coefficients explicitly we get the desired result:

$$A_d(P, P^{(-)}) = \frac{1}{\mathrm{Tr}(P)\mathrm{Tr}(P^{(-)})} \sum_{\substack{\sigma \in \mathcal{E} \\ \mathrm{wt}(\sigma)=d}} \mathrm{Tr}(P\sigma)\mathrm{Tr}(P^{(-)}\sigma)$$

$$= \frac{1}{\mathrm{Tr}(P)\mathrm{Tr}(P^{(-)})} \sum_{\substack{\sigma \in \mathcal{E} \\ \mathrm{wt}(\sigma)=d}} (-1)^d \mathrm{Tr}(P\sigma)\mathrm{Tr}(P\sigma) = (-1)^d A_d(P,P)$$

□

In the case of stabilizer codes we defined the Shadow Enumerators via a combinatorial identity, which also restricted many of their properties. Now we have properly generalized shadow codes and identified the relationship to the (Shor-Laflamme) Weight Enumerators via a MacWilliams transform. We still have, however, no new information from these in the general case. While these do not have to be integers in the general case, we can prove that they have to be non-negative, which adds indeed new restrictions to the set of equations and inequalities. This is proven in the following theorem:

**Theorem 4.15.** Let $C$ be a quantum code on $n$ qubits, and let $S(x,y) = \sum_{d=0}^{n} S_d x^{n-d} y^d$ be its Shadow Enumerator polynomial. Then

$$S_d \geq 0 \text{ for all } d \in \{0, \ldots, \underline{n}\} \tag{64}$$

*Proof.* It suffices to show that for the orthogonal projection operator $P$ onto $C$, $P^{(-)}$ is positive semi-definite. Indeed, for two hermitian, positive semi-definite operators $M, N$ with $\mathrm{Tr}(MN) \neq 0$ we always have that

$$B_d(M,N) = \frac{1}{\mathrm{Tr}(MN)} \sum_{\substack{E \in \mathcal{E} \\ \mathrm{wt}(E)=d}} \underbrace{(\mathrm{Tr}(MENE^{-1}))}_{\geq 0} \geq 0 \tag{65}$$

Now, to show that $P^{(-)}$ is positive definite, we can use the fact that for any hermitian operator $M$, $M^{(-)} = Y^{\otimes n}\bar{M}Y^{\otimes n}$, where $\bar{\cdot}$ denotes the complex conjugate. Since $M$ is hermitian as are all $E \in \mathcal{E}$, the coefficients $c_E$ of the basis decomposition $M = \sum_{E\in\mathcal{E}} c_E E$ are all real, and thus it suffices to show this holds for $M \in \mathcal{E}$. For $M \in \mathcal{E}$, we have $M^{(-)} = (-1)^{\mathrm{wt}M} M$. Since the products of elements in $\mathcal{E}$ can be computed 'qubit-wise', i.e. diagonally on the tensor product components, we can see what happens for each of $I_2, X, Y, Z$: $YI_2Y = Y^2 = I_2, YYY = Y^2Y = Y$, so $I_2$ and $Y$ are invariant under conjugation with $Y$. $YXY = i^2XZXXZ = -X, YZY = i^2XZZXZ = -Z$, so $X$ and $Z$ have both change signs with the conjugation. On the other hand, $X = \bar{X}$ and $Z = \bar{Z}$, but $Y = -\bar{Y}$, so that the equality holds for all cases. Since $Y^{\otimes n}$ is unitary, this means that $P^{(-)}$ is positive semi-definite, since $P$ is as a projection, which completes the proof. □

With this result we can now refine Theorem 4.7 to include the new inequalities, giving tighter bounds.

**Theorem 4.16** (tighter LP bound for general quantum codes)**.** Let $C$ be a quantum $((n, K, d))$ code and let $\sum_{i=0}^{n} A_i x^{n-i} y^i$ be its (Shor-Laflamme) Weight Enumerator. Then the $A_i$ satisfy the following set of linear equations and inequalities:

$$A_0 = 1, A_i \geq 0 \text{ for all } i \in \underline{n} \tag{66}$$

$$B_i := \frac{K}{2^n} \sum_{r=0}^{n} P_i(r,n) A_r \tag{67}$$

$$A_i = B_i \text{ for all } i \in \{0, \ldots, d-1\} \tag{68}$$

$$A_i \leq B_i \text{ for all } i \in \{d, \ldots, n\} \tag{69}$$

$$S_i := \frac{K}{2^n} \sum_{r=0}^{n} (-1)^r P_i(r,n) A_r \tag{70}$$

$$S_i \geq 0 \text{ for all } i \in \{0, \ldots, n\} \tag{71}$$

*Proof.* This is just Theorem 4.7 enhanced by Theorems 4.14 and 4.15. □

| n | d=1 | d=2 | d=3 | d=4 | d=5 | d=6 | d=7 |
|---|---|---|---|---|---|---|---|
| 1 | $2^*$ | - | - | - | - | - | - |
| 2 | $4^*$ | $1^*$ | - | - | - | - | - |
| 3 | $8^*$ | $\mathbf{1}^*$ | 1 | - | - | - | - |
| 4 | $16^*$ | $4^*$ | 1 | 1 | - | - | - |
| 5 | $32^*$ | $\mathbf{6}^*$ | $2^*$ | 1 | 1 | - | - |
| 6 | 64 | 16 | 2 | 1 | 1 | 1 | - |
| 7 | 128 | **26** | **3** | 1 | 1 | 1 | 1 |

Table 3: Refined Bounds for $n = 1, \ldots, 7$ using Shadow Enumerators, values that differ from Table 4.17 (without the Shadow Enumerator) are marked in boldface, values known to be sharp are marked with an asterisk

**Example 4.17.** We can now refine the bounds gotten in Example 4.8, using Theorem 4.16. This yields the Table 4.17

Table 4.17 was calculated using [14] on an amd64 GNU/Linux PC. The bounds that are known to be sharp were all obtained from [15] and Example 4.6. A comparison for these few numbers already shows the usefulness of Shadow Enumerators.

**Example 4.18.** As we can see from Table 4.17, the tentative $((5, 8, 2))$ code in Example 4.9 cannot exist. We can see this explicitly from its Shadow Enumerator:

$$S(x, y) = 8A(\frac{x + 3y}{2}, \frac{y - x}{2})$$
$$= -\frac{1}{2}x^5 + \frac{15}{2}x^4y + 15x^3y^2 + 75x^2y^3 + \frac{195}{2}xy^4 + \frac{123}{2}y^5 \qquad (72)$$

The coefficient for $x^5$ is negative, which is in contradiction with Theorem 4.15: this means that there is no $((5, 8, 2))$ code.

## 4.3 Automorphisms of Codes

Sometimes there are some codes, or families of codes, for which we know something about their automorphism groups (that is, the groups of bijective linear mappings that send the code to itself). This information can be used to further refine the equations we have from Theorem 4.16. In this section we will limit ourselves to a particular class of codes with nice automorphism groups, which are inspired from physical considerations. The principles we will use, however, can of course be used similarly for other classes with similar characteristics on their automorphism groups.

**Definition 4.19.** Let $C \leq V$ be a linear code over a finite field or a quantum code. An automorphism of $C$ is an Element $\sigma \in \mathrm{GL}(V)$ that satisfies: $\sigma C \subseteq C$, i.e., the code (as a set) is invariant under $\sigma$. The set of all automorphisms of set is called the automorphism group $\mathrm{Aut}(C)$, and is a subgroup of $\mathrm{GL}(V)$.

**Definition 4.20.** Let $G$ be a finite abelian group and $n = |G|$, and let $C$ be an additive quantum code on $n$ qubits and $S$ its stabilizer group. We will index the qubits on $S$ with the elements of $G$:

$$\sigma = \bigotimes_{i=1}^{n} \sigma_{g_i} \in \mathcal{E}_n \text{ for } G = \{g_1, \ldots, g_n\}$$

Then we get an action of $G$ on $S$ via $g_j \cdot \bigotimes_{i=1}^{n} \sigma_{g_i} := \bigotimes_{i=1}^{n} |v_{g_j g_i}$. We call the tuple $(G, C)$ with respect to this action a geometric quantum code on the lattice $G$. If the image of $G$ under the homomorphism defined by the action is part of the automorphism group of the associated $\mathbb{F}_4$ code, i.e. when $S$ is invariant under the action of $G$, then we call $C$ a translation-invariant additive quantum code.

Geometric quantum codes on a lattice are a very important model from the physical standpoint, as in a realization, the qubits will have to be ordered in some way to another. Translation-invariance is also a very plausible physical assumption.

**Definition 4.21.** Let $G$ be a finite abelian group, $n = |G|$ and $s_1, \ldots, s_k \in \mathcal{E}_n$ be Pauli Operators. Further let $G$ act on $\mathcal{E}_n$ as described in Definition 4.20. If the group $S$ generated by the orbits of $s_1, \ldots, s_k$, $S := \langle Gs_1, \ldots, Gs_k \rangle$ is an abelian group, then we call the corresponding translation-invariant additive code on the lattice $G$ the translation-invariant additive code generated by $s_1, \ldots, s_k$.

**Remark 4.22.** Let $(G, C)$ be a translation-invariant additive code on the lattice $G$ generated by $s_1, \ldots, s_k$. The action of $G$ on $S$ respects the weight, as it only permutes the support of the elements of $\mathcal{E}_n$. For the (Shor-Laflamme) Weight Enumerators $A_i$ this means that each coefficient has to be larger than the union of all orbits of elements of their order:

$$A_i \geq |\bigcup_{\mathrm{wt}(s_j)=i} Gs_j| \text{ for all } i \in \underline{n}$$

**Theorem 4.23** (bound for translation-invariant additive codes)**.** Let $(C, G)$ be a translation-invariant $[[n, k, d]]$ code generated by $s_1, \ldots, s_l$ and let

$\sum_{i=0}^{n} A_i x^{n-i} y^i$ be its (Shor-Laflamme) Weight Enumerator. Then the $A_i$ satisfy the following set of equations and inequalities:

$$A_0 = 1, A_i \geq 0 \text{ for all } i \in \underline{n} \tag{73}$$

$$B_i := \frac{K}{2^n} \sum_{r=0}^{n} P_i(r,n) A_r \tag{74}$$

$$A_i = B_i \text{ for all } i \in \{0, \ldots, d-1\} \tag{75}$$

$$A_i \leq B_i \text{ for all } i \in \{d, \ldots, n\} \tag{76}$$

$$S_i := \frac{K}{2^n} \sum_{r=0}^{n} (-1)^r P_i(r,n) A_r \tag{77}$$

$$S_i \geq 0 \text{ for all } i \in \{0, \ldots, n\} \tag{78}$$

$$A_i \geq |\bigcup_{\mathrm{wt}(s_j)=i} G s_j| \text{ for all } i \in \underline{n} \tag{79}$$

*Proof.* This is just Theorem 4.16 enhanced by Remark 4.22. □

**Example 4.24.** Let $G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $C$ be the translation-invariant code on $G$ generated by $\sigma := X_{(0,0)} \otimes \mathrm{Id}_{(0,1)} \otimes X_{(1,0)} \otimes X_{(1,1)} \otimes \mathrm{Id}_{(2,0)} \otimes X_{(2,1)} \in \mathcal{E}_6$. This generates a stabilizer group $S$ of $\mathbb{F}_2$-Dimension 4, which can be calculated easily. We will use Theorem 4.23 to try and find out the code distance of this code: Recall that this means that the associated additive quantum code has $\mathbb{C}$ dimension $K = 2^{6-4} = 4$ (See Theroem 2.9).Since we already know from Table 4.17 that an $((6,2,d))$ code can have minimal distance of at most $d = 3$, we only need to look up to there. From an examination of the generator $\sigma$ it is obvious that the acion of $G$ on the orbit of $\sigma$ is faithful, which means that $|G\sigma| = 6$, so that for the (Shor-Laflamme) enumerator $A$ of $C$ it has to be that $A_4 \geq 6$ and $6 \mid A_4$, since $\sigma$ has weight 4. Adding this constraints to the get the form of the problem in Theorem 4.23 rules out many solutions, but there is still too many to decide anything about the code. So, we can take another (redundant) generator of the code of different weight:

$$\sigma' := ((1,1)\sigma)(\sigma) = X_{(0,0)} \otimes X_{(0,1)} \otimes \mathrm{Id}_{(1,0)} \otimes \mathrm{Id}_{(1,1)} \otimes \mathrm{Id}_{(2,0)} \otimes \mathrm{Id}_{(2,1)}.$$

Here it is again obvious that the orbit has full length $6 = |G\sigma'|$. Adding the constraints from $\sigma'$: $A_2 \geq 6$ and $6 \mid A_2$, we still have many different solutions to the problem from Theorem 4.23, however, all of them are of minimial distance 1 - we have found the minimal distance, even though we did not get the weight enumerator. A little more thought lets us find three more

elements of $S$ of weight 4, but with this, in fact, we already have calculated the whole weight enumerator, and don't need LP anymore. It is

$$A(x, y) = x^6 + 6x^2y^4 + 9x^4y^2 \tag{80}$$

Note that the minimal weight of the $\mathbb{F}_4$ code is 2, but the minimal distance of the associated quantum code $C$ is 1, so they do not have to coincide. This example was calculated using [13] on an amd64 GNU/Linux PC via the C/C++ API and compiled with GCC (Debian 4.7.2-2) 4.7.2.

While in the last example it seemed we had to almost find out the weight of the complete code to get the minimal distance, these kind of process can scale very good: If the lattice becomes much bigger, but the generators are still supported only on a few qubits, we can do pretty much the same, and the constraints we gain scale with the lattice while our effort to get them does not.

# 5 References


[1] Eric M. Rains, *Quantum Weight Enumerators*, arXiv:quant-ph/9612015

[2] Peter Shor, Raymond Laflamme, *Quantum MacWilliams Identities*, arXiv:quant-ph/9610040

[3] Eric M. Rains, *Quantum Shadow Enumerators*, arXiv:quant-ph/9611001

[4] E. Rains, R. Hardin, P. Shor, N. Sloane *A Nonadditive Quantum Code*, arXiv:quant-ph/9703002

[5] Paul R. Halmos, *Measure Theory*, 1968, Van Nostrand, Princeton, N. J.

[6] Otto Forster, *Analysis 3* ,(6. Edition), 2011, Vieweg+Teubner Verlag, Germany

[7] Bernhard Leemhuis, *Geometrical Quantum Codes*(Master thesis), University of Amsterdam, 2010, available at `http://www.science.uva.nl/onderwijs/thesis/centraal/files/f2140130669.pdf`

[8] Michael Nielsen, Isaac Chuang, *Quantum Computation and Quantum Information*, $10^{\text{th}}$ Annniversary Edition (2010), Cambridge University Press

[9] Gabriele Nebe, Eric M. Rains, Neil J. A. Sloane, *Self-dual codes and invariant theory*, Springer, 2006

[10] A. R. Calderbank, E. M. Rains, P. W. Shor, N. J. A. Sloane, *Quantum Error Correction Via Codes Over GF(4)*, arXiv:quant-ph/9608006v5, 1997

[11] Wolfgang Ebeling, *Lattices and Codes*, Vieweg Wiesbaden Braunschweig, 2002

[12] Gerald B. Folland, *A Course in Abstract Harmonic Analysis*, CRC Press, 2000

[13] Lpsolve Development Team, *lpsolve-5.5 (Software)*, `http://sourceforge.net/projects/lpsolve/`

[14] Waterloo Maple Inc., *Maple 13.0 (Software)*

[15] Grassl, Markus, *Bounds on the minimum distance of linear codes and quantum codes*, Online available at `http://www.codetables.de`. Accessed on 2012-09-27.

# Notational conventions

This emphasis of this section is to summarize notational conventions used throughout the thesis, and has therefore not the aim to be complete, but rather fast to read. For this, see Section 1.1 or the part of the text where the particular notation was introduced.

- $\mathcal{H}$ a complex Hilbert space
- $A^\dagger$ the hermitian conjugate of the complex matrix $A$.
- Tr The trace of an endomorphism (or square matrix)
- $V \otimes W$ the tensor-product of $V$ and $W$. This will be treated as the Kronecker-Product on all finite dimensional vector spaces.
- $X, Y, Z$ Pauli matrices (see Def. 1.5)
- $\mathcal{E}_n := \{\sigma_1 \otimes \ldots \otimes \sigma_n$, where $\sigma_i \in \{I, X, Y, Z\}$ for all $i \in \underline{n}\}$.
- $D_n = \langle a, b \mid a^2 b^n (ab)^2 \rangle$ the dihedral group on a regular polygon with n sides.
- $V^*$: the dual space to $V$.
- $\mathrm{Hom}_G(A, B)$ the set of G-Homomorphisms from A to B (i.e., G-equivariant homomorphisms)
- $G \wr H$ the wreath product of G and H
- $\omega \in \mathbb{F}_4$ a root of $x^2 + x + 1 \in \mathbb{F}_2[x]$
- Im the image a mapping, Ker the kernel of a homomorphisms
- $\sigma_{\big|_S}$ denotes $\sigma_{s_1} \otimes \ldots \otimes \sigma_{s_k}$, where $S = \{s_1, \ldots, s_k\} \subseteq \underline{n}$ .
- $[[n, k, d]]$ code is a quantum code encoding $k$ qubits on $n$ qubits, and with minimal distance $d$.
- $((n, K, d))$ code is a quantum code on $n$ qubits which has dimension $K$ and minimal distance $d$.