Notation

- $\mathcal{H}$ a complex hilbertspace
- Tr The trace of an endomorphism (or square matrix)
- $V \otimes W$ the tensor-product of V and W.
- X, Y, Z Pauli matrices (see def. 1.4)
- $\mathcal{E}_n := \{\sigma_1 \otimes \ldots \otimes \sigma_n$, 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 $x^2 + x + 1 \in \mathbb{F}_2[x]$

Contents

1 Preliminaries

1.1 Remarks on linear algebra

Throughout this thesis we will focus mainly on groups acting 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.

Remark 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:

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

Further for a Hilbert space with a particular decomposition $V_1 \otimes \ldots V_n$, e.g.$(\mathbb{C}^2)^{\otimes n}$with $V_i \cong \mathbb{C}^2 \, \forall \, i \in \underline{n}$, 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 Tr_S as a short notation for $\mathrm{Tr}_{V_S} : \mathrm{End}(V_1 \otimes \ldots \otimes V_n) \to \mathrm{End}(V_{S^c})$. 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.

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 $\forall B \in \mathrm{End}(W)$Herm.:

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

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 $T - \mathrm{Tr}_W(A) = 0$. □

1.2 The Pauli Group

Definition 1.4. The Pauli matrices, or Pauli operators on $\mathbb{C}^2$ are defined by:

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

We denote with

$$\mathcal{E}_n := \{\sigma_1 \otimes \ldots \otimes \sigma_n, \text{ where } \sigma_i \in \{I, X, Y, Z\} \text{ for all } i \in \underline{n}\} \subseteq \mathrm{End}((\mathbb{C}^2)^{\otimes n}) := \mathrm{End}(\underbrace{\mathbb{C}^2 \otimes \mathbb{C}^2}_{\text{n times}}) \tag{3}$$

the set of all so-called Pauli operators, and by $\mathcal{P}_n := \langle \mathcal{E} \rangle \leq \mathrm{GL}_n(\mathbb{C})$, called the so-called Pauli group.

Remark 1.5. 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 $\mathrm{Tr}(A \otimes B) = \mathrm{Tr}(A)\mathrm{Tr}(B) \forall A \in \mathbb{C}^{m\times m}, B \in \mathbb{C}^{m'\times m'}$, $\mathcal{E}$ is an orthogonal basis of $\mathbb{C}^{2^n\times 2^n}$.

Proposition 1.6. 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 $Z(G)$ is the centre of G.

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

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

d) The commutator $[\cdot,\cdot] : G \times G \to G$ induces a non-degenerate symmplectic product on $G/Z(G)$

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 $[,]$ is alternating on $G/Z(G)$. $\mathbb{F}_2$ bilinearity follows directly from the definition.

□

Remark 1.7. 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. 1.6 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 φ 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 $\mathbb{F}_4$: $(x \mapsto x^2)$. 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: $(a_1, \dots, a_n, b_1, \dots, b_n) \mapsto (\omega a_1 + \bar{\omega} b_1, \dots, \omega a_n + \bar{\omega} b_n)$, and call the resulting isomorphism $\tilde{\varphi}$. $\tilde{\varphi}$ is an isometry with respect to the commutator and the $\mathbb{F}_2$-symplectic form on $\mathbb{F}_4$.

1.3 Random Unitary Matrices

Theorem 1.8 (Haar Measure)**.** Let U denote the the group of unitary $n \times n$ matrices over the complex field $\mathbb{C}$. Then there exists a unique measure μ on U, called the Haar measure, which satisfies the following:

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

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

Remark 1.9. The Haar measure makes the group of unitary $n \times n$ matrices U 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 U, and thus we can interpret the indentity mapping on U as a random, uniformly distributed unitary matrix. The expected value of a measurable function f on U can thus be explicitly be calculated through a Lebesgue integral:

$$E(f) = \int_U f(x) d\mu(x) \tag{4}$$

Lemma 1.10. Let V be a finite dimensional $\mathbb{C}$ vector space and V^* its dual space. Further let G be the unitary group acting on V. Then

$$\mathrm{Hom}_G(V \otimes V^*, \mathbb{C}) \cong \mathrm{Hom}_G(V, V) \tag{5}$$

as vector spaces, where G acts diagonally on $V \otimes V^*$.

Proof. Since $End(V) \cong V \otimes V^*$ we will identify them with each-other and in particular, not distinguish between $\mathrm{Hom}(End(V), \mathbb{C})$ and $\mathrm{Hom}(V \otimes V^*, \mathbb{C})$. Let $\varphi \in \mathrm{Hom}_G(V, V)$. Then define $\eta(\varphi)(v \otimes \alpha) := \alpha(\varphi(v))$ for all $v \otimes \alpha \in V \otimes V^*$ and extend it linearly to $V \otimes V^*$. It is easy to see that η is a well-defined as a vector space homomorphism (linear mapping), since $\mathrm{Im}(\eta)$ is G-equivariant. If $\alpha(\varphi(v)) = 0$ for all $v \in V, \alpha \in V^*$ it follows that $\varphi = 0$, and hence η is injective. Let $f : V \otimes V^* \to \mathbb{C}$ be a G-equivariant linear mapping. Then f is fully characterized by the image of elements of the form $v \otimes \alpha$, $v \in V, \alpha \in V^*$... finish me...! □

Theorem 1.11. Let U be a random unitary $n \times n$ matrix over $\mathbb{C}$ and $A, B \in \mathbb{C}^{n \times n}$. 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 $W \in \mathcal{U}_n(\mathbb{C})$:

$$WE(UAU^\dagger)W^\dagger = W\int_{\mathcal{U}}(UAU^\dagger)d\mu(U)W^\dagger = \int \mathcal{U}(WU)A(WU)^\dagger d\mu(WU) = E(UAU^\dagger) \tag{8}$$

, where in the second equality we used the fact that μ 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. $\varphi \in \mathrm{Hom}_{\mathcal{U}_n}(\mathbb{C}^n \otimes (\mathbb{C}^n)^*, \mathbb{C}) \cong Hom_{\mathcal{U}_n}(V, V)$ by lemma 1.10. Since $\mathcal{U}_n$ is transitive on $V \backslash \{0\}$, $\dim_{\mathbb{C}}(Hom_{\mathcal{U}_n}(V, V)) = 1$, 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 ψ is a bilinear mapping. There are two crucial observations to complete the proof. First, $\psi(\cdot, I_n) \in \mathrm{Hom}_{\mathcal{U}_n}(\mathbb{C}^n \otimes (\mathbb{C}^n)^*, \mathbb{C})$ and, by the same argument as above, there exisits 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 $A \in C^{n \times n}, B \in \mathcal{E}$

$$\psi(A, B) = \int_{\mathcal{U}_n} \mathrm{Tr}(AU)\mathrm{Tr}(BU^\dagger)d\mu(U) = \int_{\mathcal{U}_n} \underbrace{\mathrm{Tr}(AU)}_{=\mathrm{Tr}(ABBU)} \underbrace{\mathrm{Tr}(BU^\dagger)}_{=\mathrm{Tr}((BU)^\dagger)} d\mu(BU) = \int_{\mathcal{U}_n} \mathrm{Tr}(ABU)\mathrm{Tr}(I_nU^\dagger)d\mu(U) = \psi(AB, I_n) \tag{9}$$

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 ψ. That $\lambda = \frac{1}{n}$ follows again from $\psi(I_n, I_n) = \int_{\mathcal{U}_n} \underbrace{\mathrm{Tr}(U)\mathrm{Tr}(U^\dagger)}_{=|\mathrm{Tr}(U)|^2=1} d\mu(U) = 1$. □

1.4 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.

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 $\{|\psi_t\rangle \mid t \in \mathbb{R}\}$, reletad 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 proyective space of $\mathcal{H}$ (parametrized with t as well). 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 meassuring $m \in I$, $p(m)$ 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 satisify: $\sum_{m \in I} M_m^\dagger M_m = \mathrm{Id}_{\mathcal{H}}$, 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 1.12. One does not have to think long to percieve an (appearent?) 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 meassurement has an inherent probabilistic behaviour, which is inconsistent with this. This problem is called the meassurement problem, and is in the end rather a philosophical problem, which is why we will not further pursue it in this thesis.

2 Qubits and Quantum Codes

Definition 2.1. A qubit is a two dimensional complex Hilbert space, $(\mathbb{C}^2, <\cdot,\cdot>)$. 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.

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 properties, as discussed in section **??**, we will first consider the pauli operators ($\mathcal{E}$) as errors. These are, in particular, a unitary, hermitian basis of 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:

$$P_0 := |000\rangle\langle 000| + |111\rangle\langle 111|,\ P_1 := |100\rangle\langle 100| + |011\rangle\langle 011|$$

$$P_2 := |010\rangle\langle 010| + |101\rangle\langle 101|,\ P_3 := |001\rangle\langle 001| + |110\rangle\langle 110|$$

From the operators themselves it is easy to see that a measurement in this basis will immediately identify if exactly one 'bit flip' error (but nothing else) has happened, 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 quibts. 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 in example **??**, 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 Haddamard 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 [**?**] 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 (**??**) 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, which is a linear combination of the E_i, i.e. $F_j = \sum_{i \in I} c_{i,j} E_i$ for all $j \in J$ and for some $c_{i,j} \in \mathbb{C}$, 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 quantum operations; but this goes beyond the scope of this thesis. The more general statement, along with a proof, can be found in [**?**].

2.2 Stabilizer 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. 1.7. Then C defines a quantum code on n qubits via a lifting ψ of the inverse mapping to the induced by the symplectic notation defined in rem. 1.7:

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

$S := \psi(C)$ 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 $2^{n - dim_{F_2}(C)}$.

Proof. From rem. 1.7 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 $\mathrm{Tr}(X) = \mathrm{Tr}(Y) = \mathrm{Tr}(Z) = 0$ and $\mathrm{Tr}(A \otimes B) = \mathrm{Tr}(A)\mathrm{Tr}(B)$ for all $A \in \mathbb{C}^{k_1 \times k_1}, B \in C^{k_2 \times k_2}, k_1, k_2 \in \mathbb{N}$. □

Definition 2.10. 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.[**?**]: Through symplectic notation, S defines an $\mathbb{F}_2$ vectorspace (equivalent to S being closed under multiplication) that is self orthogonal with respect to the commutator, since S is abelian.

Example 2.11. With stabilizer codes now properly defined, we can return to the previous example (**??**), the 9-qubit Shor code. The Shor code is generated by the 8 $\mathbb{F}_2$-linearly independent generators in table **??** (see [**?**]). 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 **??**). From their symplectic notation it can be immediately checked they are indeed $\mathbb{F}_2$-linearly independent generators.

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 2.12. Let $S \leq \mathcal{P}_n$ be a stabilizer group. The centralizer of S in $\mathcal{P}_n$, $C_{\mathcal{P}_n}(S)$ is defined as:

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

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 physical 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 do 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 codewords to codewords; 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. With a little more mathematics (the development of which would be too long for this thesis), logical operators can be further understood:

Remark 2.13. FIXME: prove/check this: For each operator A on k qubits, there is - of course - an operator $A^{(n)}$ on the encoding n qubits. This operator is not unique however: an equivalency class can be defined for logical operators, making two operators equivalent, when they act as the same operator on the k logical qubits. Two such equivalent operators differ actually always by an element of the stabilizer group, i.e. : $A^{(n)}$ and $B^{(n)}$ are equivalent iff $\exists T \in S$ with $A^{(n)} = B^{(n)}T$. That these is true can be made at least plausible by reminding us of the definition of the stabilizer group: it does not alter the code!

Example 2.14. Again, the 9-qubit Shor code (ex. **??**): It encodes only one qubit, so we will only search for the two logical operators $\overline{X}$ and $\overline{Z}$. These are given by $\overline{X} = ZZZZZZZZZ$ and $\overline{Z} = XXXXXXXXX$, 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 2.15. Let $E \in \mathcal{P}_n$ be an arbitrary Pauli operator. The weight of E, $|E|$, is defined as the number of qubits on which E is supported, i.e. the number of qubits on which E acts non-trivially, while disregarding an overall phase (factor). Similarly, we define a weight on $\mathbb{F}_2^{2n} = (e_1, \ldots, e_n, f_1, \ldots, f_n)$ through

$$|\sum_{i=1}^{n} a_i e_i + b_i f_i| := |\{i \in \underline{n} \mid a_i \neq 0 \text{ or } b_i \neq 0\}, a_i, b_i \in \mathbb{F}_2 \text{ for all } i \in \underline{n} \tag{10}$$

This coincides with the Hamming-weight on $\mathbb{F}_4$ with the identification from remark 1.7.

Definition 2.16. Let $S \leq \mathcal{P}_n$ be a stabilizer group with corresponding code C. Then, the minimal distance (or code distance) ρ of C is defined as:

$$\rho := \min\{|A| \in \mathcal{P}_n | A \text{ is a logical operator}\} = \min\{|A| \mid A \in C_{\mathcal{P}_n}(S) \backslash S\} \tag{11}$$

An [[n,k]] code with distance ρ is also called an [[n,k,ρ]] code.

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

Example 2.17. We can calculate the code distance of ex. **??**. 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:

$$C_{\mathcal{P}_n}(S) = \{A\overline{X} \mid A \in S\} \cup \{A\overline{Z} \mid A \in S\} \tag{12}$$

From table **??** 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. **??**. This means that $\rho = 3$, and hence, the Shor code corrects $1 < \frac{3}{2}$ errors.

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 2.18. 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 2.19. The above defined $C = C(D_1, D_2)$ is an $[[n, k_1 - k_2, d]]$ code, with $d \geq 2t + 1$. FIXME: proof!! A proof can be found in [**?**].

3 Quantum Weight Enumerators

3.1 The Shor-laflamme and Rains enumerators

Definition 3.1. 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 σ to be $\mathrm{Supp}(\sigma) = \{i \in \underline{n} \mid \sigma_i \neq \mathrm{Id}\}$ and its weight as $\mathrm{wt}(\sigma) = |\mathrm{Supp}(\sigma)|$.

This definition is consistent with the weight on $\mathbb{F}_4^n$.

Definition 3.2. Let $V = (\mathbb{C}^2)^{\otimes n}$, and $\mathcal{E} = \{\sigma_1 \otimes \ldots \otimes \sigma_n \mid \sigma_i \in \{X, Y, Z, \mathrm{Id}\} \forall i \in \underline{n}\}$ (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 [**?**] of M_1, M_2 as follows:

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

$$B_S(M_1, M_2) = \frac{1}{\mathrm{Tr}(M_1 M_2)} \sum_{\substack{E \in \mathcal{E} \\ \mathrm{Supp}(E) = S}} (\mathrm{Tr}(EM_1 EM_2)) \tag{14}$$

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

$$A_d(M_1, M_2) = \sum_{\substack{S \subseteq \underline{n} \\ |S| = d}} A_S(M_1, M_2); B_d(M_1, M_2) = \sum_{\substack{S \subseteq \underline{n} \\ |S| = d}} B_S(M_1, M_2) \tag{15}$$

Definition 3.3. Again let $V = (\mathbb{C}^2)^{\otimes n}$, and $\mathcal{E} = \{\sigma_1 \otimes \ldots \otimes \sigma_n \mid \sigma_i \in \{X, Y, Z, \mathrm{Id}\} \forall i \in \underline{n}\}$. Further let $S \subseteq \underline{n}, S^c = \underline{n} \backslash S$ and $M_1, M_2 \in \mathbb{C}^{2^n \times 2^n}$. We define the coefficient of the Rains enumerators [**?**] of M_1, M_2 as follows:

$$A'_S(M_1, M_2) = \mathrm{Tr}(\mathrm{Tr}_{S^c}(M_1)\mathrm{Tr}_{S^c}(M_2)) \tag{16}$$

$$B'_S(M_1, M_2) = \mathrm{Tr}(\mathrm{Tr}_S(M_1)\mathrm{Tr}_S(M_2)) \tag{17}$$

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

$$A'_d(M_1, M_2) = \sum_{\substack{S \subseteq \underline{n} \\ |S| = d}} A'_S(M_1, M_2); B'_d(M_1, M_2) = \sum_{\substack{S \subseteq \underline{n} \\ |S| = d}} B'_S(M_1, M_2) \tag{18}$$

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 $E, E' \in \mathcal{E} = \{\sigma_1 \otimes \ldots \otimes \sigma_n \mid \sigma_i \in \{X, Y, Z, \mathrm{Id}\} \forall i \in \underline{n}\}$. Then

a) The 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 $E = \sigma_1 \otimes \ldots \sigma_n$, $\sigma_i \neq \mathrm{Id}$, otherwise $\mathrm{Tr}(\mathrm{Tr}_S(E)\mathrm{Tr}_S(E)) = 2^n$.

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

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 $P_c(v) = v \, forall \, v \in V^G$. From this it follows immediately that $\mathrm{Im}(P_C) = V^G$ and $P_C^2 = P_C$, and hence that it is the 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 $E^2 = Id_V$, hence $\mathrm{Tr}(E^2) = \dim(V) = 2^n$. From a) we get:

$$\mathrm{Tr}(EP_c) = \frac{1}{|G|} \sum_{\sigma \in G} \mathrm{Tr}(\sigma E) = \frac{1}{|G|} \cdot \begin{cases} 2^n = \dim(V) & \text{if } E \in G \\ 0 & \text{if } E \notin G \end{cases} \tag{19}$$

(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 $E \neq E'$, 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 $\mathrm{Tr}_S(E)\mathrm{Tr}_S(E) = 2^{|S|}\mathrm{Id}_{S^c}$ and $2^{|S|}\mathrm{Tr}(\mathrm{Id}_{S^c}) = 2^{|S|}\dim(V_{S^c}) = 2^n$.

(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

$$\mathrm{Tr}(EP_CEP_C) = \frac{1}{|G|^2} \sum_{\sigma,\sigma' \in G} \mathrm{Tr}(\underbrace{E\sigma E}_{=[E,\sigma]\sigma} \sigma') \tag{20}$$

$$= \frac{1}{|G|^2} \sum_{\sigma,\sigma' \in G} < E, \sigma > \mathrm{Tr}(\sigma\sigma') = \frac{2^n}{|G|^2} \sum_{\sigma \in G} < E, \sigma > \tag{21}$$

, 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 paritition 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. $C = V^G$), and let P_C be the projection onto C, and let $S \subseteq \underline{n}$. Then the coefficients are given as follows:

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

$$B_S(P_C, P_C) = \#\{E \in G^\perp \mid \mathrm{Supp}(E) = S\} \tag{23}$$

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

$$B'_S(P_C, P_C) = \frac{2^n}{|G|^2}\#\{\sigma \in G \mid \sigma_{\big|_{S}} = \mathrm{Id}\} \tag{25}$$

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.

$$\text{First } A_S(P_c, P_c) = \frac{1}{\dim(C)^2} \sum_{\substack{E \in \mathcal{E} \\ \mathrm{Supp}(E) = S}} Tr(P_cE)^2 = \frac{1}{(\dim(C)|G|)^2} \sum_{\substack{E \in \mathcal{E} \\ \mathrm{Supp}(E) = S}} \sum_{\sigma,\sigma' \in G} \underbrace{\mathrm{Tr}(\sigma E)\mathrm{Tr}(\sigma' E)}_{\substack{=0, \sigma \neq E \text{ or } \sigma' \neq E \\ =2^{2n}, \sigma = \sigma' = E}} \tag{26}$$

$$= \underbrace{(\frac{2^n}{|G|\dim C})^2}_{=1, \text{see lemma on dim C}} \quad \#\{E \in G \mid \mathrm{Supp}(E) = S\} \tag{27}$$

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

Now, for the Rains enumerators:

$$A'_S(P_C, P_C) = \mathrm{Tr}(\mathrm{Tr}_{S^c}(P_C)\mathrm{Tr}_{S^c}(P_C)) = \frac{1}{|G|^2} \sum_{\sigma,\sigma' \in G} \mathrm{Tr}(\mathrm{Tr}_{S^c}(\sigma)\mathrm{Tr}_{S^c}(\sigma')) \tag{28}$$

$$= \frac{1}{|G|^2} \sum_{\sigma \in G} \mathrm{Tr}(\mathrm{Tr}_{S^c}(\sigma)\mathrm{Tr}_{S^c}(\sigma)) = \frac{2^n}{|G|^2}\#\{\sigma \in G \mid \sigma_{\big|_{S^c}} = \mathrm{Id}\} \tag{29}$$

Again, the 2. and 3. equalities follow from lemma **??**. For B'_S it is enough to see that $B'_{S^c}(M_1, M_2) = A'_S(M_1, M_2)$ for all M_1, M_2 hermitian directly from its definition. □

3.2 The relationship between the enumerators

There is an equivalent definition of the Rains enummerators, which also sheds some light to the motivation for defining A' and B'.

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

$$A'_S(M_1, M_2) = 2^{|S|} E(\mathrm{Tr}(M_1(U_S \otimes \mathrm{Id}_{S^c}))\mathrm{Tr}(M_2(U_S \otimes \mathrm{Id}_{S^c})^\dagger)) \tag{30}$$

$$B'_S(M_1, M_2) = 2^{|S|} E(\mathrm{Tr}(M_1(U_S \otimes \mathrm{Id}_{S^c}) M_2(U_S \otimes \mathrm{Id}_{S^c})^\dagger)) \tag{31}$$

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 **??**. 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:

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

□

From here on, we will focus exclusevely on the enumerators in the case of additive/stabilizer codes. 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 similarily for A'_S, B_S, B'_S. The results of this section have been proved by Eric Rains [**?**] for non-additive codes as well.

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

$$A'_S = 2^{-|S|} \sum_{T \subseteq S} A_T \text{ and } B'_S = 2^{-|S|} \sum_{T \subseteq S} B_T \tag{32}$$

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:

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

Now for B'_S we use theorem **??**:

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

Using the expansion for 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:

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

Lemma **??** together with equation 7 yield $E[\mathrm{Tr}((U_S \otimes \mathrm{Id}_S^c)\sigma)\mathrm{Tr}((U_S^\dagger \otimes \mathrm{Id}_S^c)\sigma')] = 2^{n-|S|}\delta_{\sigma,\sigma'}$, from which in turn follows that:

$$B'_S = 2^{-n} \sum_{\sigma \in \mathcal{E}} \frac{1}{|G|^2} \sum_{g,g' \in G} \mathrm{Tr}(g\sigma g'\sigma) = 2^{-n} \sum_{\sigma \in \mathcal{E}} \mathrm{Tr}(P_C \sigma P_C \sigma) = 2^{|S|-n} B_S$$

□

Corollary 3.8. for the d's and mcwilliams 1.

Corollary 3.9. The enumerators $A_d(M_1, M_2), A'_d(M_1, M_2), B_d(M_1, M_2), B'_d(M_1, M_2)$ are invariant under equivalence of codes, i.e., under the action of $\mathcal{U}_2(\mathbb{C}) \wr S_n$, where S_n is the symmetric group on the tensor product components.

Proof. For the Rains enumerators it is immediately clear from theorem **??**. For the Shor-Laflamme enumerators it follows from cor. **??** as we can explicitly write $A_d(M_1, M_2)$ in terms of $A'_d(M_1, M_2)$ and the same for the B's. □

3.3 Code distance and the McWilliams transform

Theorem 3.10. $KA \geq B$, minimal distance (=)

Theorem 3.11. McWilliams