Quantum Error Detection I: Statement of the Problem

A. Ashikhmin * A. Barg † E. Knill ‡ S. Litsyn §

Abstract

This paper is devoted to the problem of error detection with quantum codes.We show that it is possible to give a consistent definition of the undetected error event. To prove this, we examine possible problem settings for quantum error detection. Our goal is to derive a functional that describes the probability of undetected error under natural physical assumptions concerning transmission with error detection with quantum codes. We discuss possible transmission protocols with stabilizer and unrestricted quantum codes. The set of results proved in the paper shows that in all the cases considered the average probability of undetected error for a given code is essentially given by one and the same function of its weight enumerators.

In the final section of the paper we examine polynomial invariants of quantum codes and show that coefficients of Rains's "unitary weight enumerators" [17] are known for classical codes under the name of binomial moments of the distance distribution. As in the classical situation, these enumerators provide an alternative expression for the probability of undetected error.

In a companion paper (part II) we use the relation of the probability of undetected error and weight enumerators to derive bounds on this probability for quantum codes.

Index Terms — Quantum code, measurement, undetected error, Shor-Laflamme enumerators.

1 Introduction

The possibility of correcting decoherence errors in entangled states was discovered by Shor [20] and Steane [21]. Since then the theory of quantum codes has been a topic of intense study. Error processes in the depolarizing channel are characterized in [12] where it was shown that one can restrict attention to error operators given by Kronecker products of Pauli matrices.

*Present address: Bell Laboratories, Lucent Technologies, 600 Mountain Avenue 2C-179, Murray Hill, NJ 07974, e-mail aea@research.bell-labs.com. Previous address: Los Alamos National Laboratory, Los Alamos, NM 87545.

†Bell Laboratories, Lucent Technologies, 600 Mountain Avenue 2C-375, Murray Hill, NJ 07974. e-mail: abarg@research.bell-labs.com

‡Los Alamos National Laboratory Group CIC-3, Mail Stop P990, Los Alamos, NM 87545. e-mail: knill@c3serve.c3.lanl.gov

§Department of Electrical Engineering-Systems, Tel Aviv University, Tel Aviv 69978, Israel. e-mail: litsyn@eng.tau.ac.il

This opened the possibility of finding parallels between the theory of classical error correcting codes and their quantum counterparts.

This theory has developed simultaneously in different, often not very related directions. Mathematically one of the most interesting works on quantum codes is the paper by Calderbank et al. [5], where the authors introduce a class of so-called stabilizer quantum codes (independently found in [7]), and discovered a beautiful geometric and group-theoretic connection that shows that such codes can be studied using the well-developed theory of classical codes over $GF(4)$. Stabilizer codes share some of the properties of classical linear codes.

One of the most important concepts in classical coding theory is the notion of decoding, decoding error, and the probability of this event for a given (random) error process in the channel. In the quantum case a similar theory still awaits construction; even defining decoding does not seem an easy problem. In the classical coding theory the simplest known decoding algorithm is testing the received vector for containment in the code; if the test fails, the decoder detects an error. Clearly, the error will not be detected if the sum of the transmitted vector and the error is itself a code vector.

The focus of our paper is error detection by quantum stabilizer and nonstabilizer codes. To give an analogy, let us recall the definition of error detection for classical codes. Let D be a code of length n over an alphabet of q elements and $B_i, 0 \le i \le n$, its Hamming distance distribution given by $B_i = \frac{1}{|D|}\sum_{\mathbf{c}' \in D} |\{\mathbf{c} \in D \mid \mathrm{dist}(\mathbf{c}, \mathbf{c}') = i\}|$. Suppose that D is used for transmission over a q-ary memoryless symmetric channel in which each symbol is unchanged with probability $1-p$ and replaced by another symbol with one and the same probability $\frac{p}{q-1}$. Let $\mathbf{c} \in D$ be a vector sent over the channel. The decoder tests the received vector $\mathbf{y}$ for containment in the code; if the test fails, it detects an error. Thus, the only case when the error is not detected occurs when the received vector $\mathbf{y} \in D \setminus \mathbf{c}$. The probability to receive a vector $\mathbf{y}$ if the sent vector is $\mathbf{c}$ equals $P(\mathbf{y}|\mathbf{c}) = (\frac{p}{q-1})^{\mathrm{dist}(\mathbf{y},\mathbf{c})}(1-p)^{n-\mathrm{dist}(\mathbf{y},\mathbf{c})}$. Then the probability of undetected error for the code D equals

$$P_{ue}(D,p) = \frac{1}{|D|}\sum_{\mathbf{c}\in D}\sum_{\mathbf{y}\in D\setminus\mathbf{c}} P(\mathbf{y}|\mathbf{c}) = \frac{1}{|D|}\sum_{\mathbf{c}\in D}\sum_{\mathbf{y}\in D\setminus\mathbf{c}} \Big(\frac{p}{q-1}\Big)^{\mathrm{dist}(\mathbf{y},\mathbf{c})}(1-p)^{n-\mathrm{dist}(\mathbf{y},\mathbf{c})}$$

$$= \sum_{i=1}^{n} B_i \Big(\frac{p}{q-1}\Big)^i (1-p)^{n-i}. \qquad (1)$$

The theory of error detection for classical codes is surveyed in [10].

Observe that this (classical) concept consists of two parts, the definition of the error event and a way, (1), to compute its probability. In the quantum case both parts are not nearly as obvious. One can consider error detection with stabilizer codes; the error will not be detected if the measured transmission result is in the code and is not orthogonal or collinear to the transmitted state vector. It is not difficult to show that the probability of undetected error in this case can be computed via the weight enumerators of quantum codes in a way analogous to (1). This definition can be generalized in two different ways. First, it is desirable to extend it to cover all quantum codes; second and more importantly, from the physical point of view if the angle between the received vector and the transmitted vector is very small, it is natural to assume that no error has occurred since the measurement of the state of the system produces almost the same state as the transmitted one. On the other hand, if the received vector is a

valid code point but is orthogonal to the transmitted one, then with probability one the error is not detected. Hence it is natural to define the undetected error event as the average probability that the state received from the channel is orthogonal to the transmitted one.

A further generalization, which is physically perhaps the most important, involves transmission of completely entangled states and studying the probability of preserving the original entanglement.

The goal of our paper in the first part is to prove that in all the situations mentioned, one can introduce a consistent definition of the undetected error event, and that the actual functional on the quantum code accounting for this event is essentially the same. This enables us in the second part [2] to prove that there exist quantum codes with exponentially falling probability of undetected error and to derive bounds on this exponent.

The first part of the paper is organized as follows. In Section 2 we recall some notions of the theory of quantum codes, most importantly, the weight enumerators. In Section 3 we define and compute the probability of undetected error for stabilizer and unrestricted codes. The answers differ by a constant factor; hence their dependence on the code is the same in both cases. In Section 4 we study the event of undetected error in the case of completely entangled states and again arrive to the same functional as in the previous sections. Section 5 is devoted to the study of polynomial invariants of quantum codes. We show that "unitary weight enumerators" of [17] are known in classical coding theory under the name of binomial moments of the distance distribution. They were introduced by MacWilliams in [13]. They were studied extensively in [1] (see also related works referenced therein), partly because they are convenient for bounding below the probability of undetected error.

2 Quantum Error Correcting Codes

In this section we review basic facts of the theory of quantum codes relevant to our study, focusing on the error process in the depolarizing channel and weight enumerators of codes.

We begin by setting up basic linear-algebraic notation and reminding the reader of elementary quantum-mechanical operations performed on state vectors. General sources for the relevant aspects of quantum theory are books [8], [14]; a treatment that highlights the context of information transmission is given in [16]. Below by bold letters ($\mathbf{v}, \mathbf{w}, \dots$) we denote complex column vectors. For a given vector $\mathbf{v}$ we denote by $\mathbf{v}^*$ its conjugate transpose. Let $\mathcal{H}_n = \mathbb{C}^{2^n}$ denote the complex 2^n-dimensional space. Let us fix an orthonormal basis in this space; denote it by $\mathbf{v}_1, \dots, \mathbf{v}_{2^n}$. Observe that once the basis is fixed, a basis vector can be referred to by its number, i. This is employed when the states and operations are written in the Dirac notation, used in much of the physics literature on quantum codes. The correspondence is established as follows:

$$\mathbf{v}_i \leftrightarrow |i\rangle, \quad \mathbf{v}_i^* \leftrightarrow \langle i|, \quad \mathbf{v}_i^* B \mathbf{v}_i \leftrightarrow \langle i|B|i\rangle,$$

where B is a $2^n \times 2^n$ matrix. This correspondence is discussed from the physical perspective in [14]; mathematically oriented readers might enjoy the discussion in [11].

Let V and W be two subspaces of $\mathcal{H}_n$ and A and B be linear operators on V and W, respectively. Consider the linear operator $C = A \otimes B$ on $V \otimes W$. Let $\{\mathbf{v}_1, \mathbf{v}_2, \dots\}$ be an

orthonormal basis of V and $\{\mathbf{w}_1, \mathbf{w}_2, \dots\}$ an orthonormal basis of W. The *partial trace* of C over V by definition equals

$$\mathrm{Tr}_V(C) := \mathrm{Tr}(A)B = \sum_i (\mathbf{v}_i^* A \mathbf{v}_i) B.$$

Here $\mathrm{Tr}(A) = \mathrm{Tr}_V(A) = \sum_i (\mathbf{v}_i^* A \mathbf{v}_i)$ is the trace of A. Similarly, one can define the partial trace over W as follows:

$$\mathrm{Tr}_W(C) := A\,\mathrm{Tr}(B) = \sum_i A(\mathbf{w}_i^* B \mathbf{w}_i),$$

Obviously,

$$\mathrm{Tr}_{V\otimes W}(C) = \mathrm{Tr}_V(\mathrm{Tr}_W(C)). \tag{2}$$

Any linear operator C on $V \otimes W$ can be written in the form

$$C = \sum_j A_j \otimes B_j,$$

where A_j and B_j are operators on V and W, respectively. This representation is generally not unique. However, it is not difficult to check that the partial trace

$$\mathrm{Tr}_V(C) = \sum_j \mathrm{Tr}(A_j) B_j,\ \mathrm{Tr}_W = \sum_j A_j\,\mathrm{Tr}(B_j). \tag{3}$$

is a well-defined function. (In fact, it is possible to give an invariant definition of the trace [15, p.130].)

Let us proceed to the definition of quantum codes and operations. A *qubit* is a two dimensional Hilbert space. A state (more precisely, a pure state) of a qubit is a unit vector $\mathbf{v}$ in the Hilbert space $\mathbb{C}^2$. Physically, a qubit occurs as a spin one-half particle, for example. Qubits are combined to form larger systems by taking the tensor products of the Hilbert spaces. The state of n qubits is therefore described by a unit vector in $(\mathbb{C}^2)^{\otimes n}$ (nth tensor power). A *quantum code* Q is a linear subspace of $\mathcal{H}_n$. We denote a code of dimension K by $Q((n, K))$.

Remark. There is a subtle point about this definition. Namely, although Q is a linear subspace, proportional vectors account for one and the same state, so in effect we only deal with vectors of unit norm. (Below we write $\mathbf{u} \propto \mathbf{v}$ to indicate that the vectors $\mathbf{u}$ and $\mathbf{v}$ are collinear.) Therefore, Q can be thought of as the projective space $\mathbf{P}\mathbb{C}^{K-1}$. However, defining Q in this way poses problems for tensoring it with other subspaces (systems). Therefore, we prefer the definition given above. On the other hand, averaging over the code, we integrate only over the vectors in Q of unit norm. This convention, adopted with some abuse of notation, is valid for the entire paper.

The number $R_Q = \frac{\log_2 K}{n}$ is called the *rate* of Q. A code vector (a state of n qubits) "sent" over a quantum channel is subjected to an error process that can alter the amplitude and/or the phase of some of the qubits. At the receiving end the decoder attempts to recover the state sent. The decoder is a quantum computing device; so it can perform only unitary rotations and measurements. Let us proceed to describing them in more detail.

Let $\mathbf{v} \in \mathcal{H}_n$, $||\mathbf{v}|| = 1$. A *unitary rotation* U of the state $\mathbf{v} \in \mathcal{H}_n$ produces a state $U\mathbf{v}$. A (*von Neumann*) *measurement* of $\mathbf{v}$ is a probabilistic operation performed with respect to a set of projections $P_1, P_2, \ldots, P_t$ that satisfy the properties

$$P_i P_j = \delta_{ij} P_i,$$
$$P_1 + P_2 + \ldots + P_t = \mathrm{id}.$$

Measuring $\mathbf{v}$ with respect to $P_1, P_2, \ldots, P_t$ results in projecting it by one of the operators $P_i, 1 \leq i \leq t$. The resulting state has the form

$$\frac{P_i \mathbf{v}}{\sqrt{\mathbf{v}^* P_i \mathbf{v}}}, \tag{4}$$

for some i. The probability for the ith projection is $\mathbf{v}^* P_i \mathbf{v}$. Upon performing the measurement we obtain the state (4) and observe the number i.

Suppose a code vector $\mathbf{v} \in Q$ is sent through the *depolarizing channel*. The outcome of the transmission can be written as $E\mathbf{v}$, where the error operator E has the form

$$E = \tau_1 \otimes \tau_2 \otimes \ldots \otimes \tau_n, \tag{5}$$

and each τ_i is either I_2 or one of the following (Pauli) matrices:

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \ \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \ \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}. \tag{6}$$

The *weight* of the error E is the number of nonidentity matrices in the expansion (5). Matrices of the form (5) either commute or anticommute:

$$E_1 E_2 = \pm E_2 E_1.$$

The choice of the sign is determined by either geometric [3] or algebraic considerations [5]; see (13) below. Note also that error operators are "trace-orthogonal":

$$\mathrm{Tr}(E_i E_j) = 2^n \delta_{ij} \tag{7}$$

Throughout the paper we assume that the channel is *symmetric*, i.e., the probability

$$\Pr(\tau_i) = \begin{cases} 1-p, & \tau_i = I_2 \\ \frac{p}{3}, & \tau_i \in \{\sigma_x, \sigma_y, \sigma_z\}, \end{cases}$$

where $0 \leq p \leq 3/4$. Different qubits are subjected to the error process independently. Therefore we have

$$\Pr(E) = \left(\frac{p}{3}\right)^{\mathrm{wt}(E)} (1-p)^{n - \mathrm{wt}(E)}. \tag{8}$$

Similarly to classical codes one can introduce the *weight enumerator* $B(x,y) = \sum_{i=0}^{n} B_i x^{n-i} y^i$ of a quantum $((n, K))$ code [19]. By definition,

$$B_i := \frac{1}{K^2} \sum_{wt(E)=i} \mathrm{Tr}^2(EP). \tag{9}$$

Here P is the orthogonal projection on Q. Another weight enumerator associated with Q [19] is given by $B^{\perp}(x,y) = \sum_{i=0}^{n} B_i^{\perp} x^{n-i} y^i$, where

$$B_i^{\perp} := \frac{1}{K} \sum_{wt(E)=i} \mathrm{Tr}(EPEP). \tag{10}$$

Some reflection shows that both B_i and $B_i^{\perp}$ are real. Indeed, by (6) error operators E are Hermitian. Of course, P is also Hermitian, and so is PEP. Eigenvalues of Hermitian operators are real; therefore, both $\mathrm{Tr}(EP)$ and $\mathrm{Tr}(EPEP)$ are real.

The following two theorems account for the role of the weight enumerators in the theory of quantum codes.

Theorem 1 [19]

$$B(x,y) = \frac{1}{2^n K} B^{\perp}(x+3y, x-y) \tag{11}$$

Theorem 2 [19] *Let Q be a quantum code with weight distributions B_i and $B_i^{\perp}$. Then*

i) $B_0 = B_0^{\perp} = 1$ *and* $B_i^{\perp} \geq B_i \geq 0$ $(1 \leq i \leq n)$

ii) the minimum distance of Q equals $t+1$, where t is the largest integer such that $B_i = B_i^{\perp}, 0 \leq i \leq t$.

These theorems are readily seen to be analogous to the MacWilliams transform and surrounding results in classical coding theory. A particular case of classical codes is formed by additive (or group) codes [6, p. 84]. An additive code C is a subgroup of the additive group of $\mathbf{Z}_q$. For such codes it is possible to define a dual code $C^{\perp}$, and the Hamming weight enumerators of C and $C^{\perp}$ are connected by the MacWilliams equation (11). A similar concept, stabilizer codes, was introduced in quantum coding theory in [4], [7].

To define stabilizer codes, let us provide more details on error operators (5). A natural framework to study them is that of orthogonal geometry and the theory of finite groups [3]. Matrices of the form αE, where $\alpha^2 = \pm 1$ and E is given by (5), form a group, say $\mathcal{E}_n$ of order 2^{2n+2} [3]. Its center is $Z = \{\pm I_{2^n}, \pm i I_{2^n}\}$. Let $\bar{\mathcal{E}}_n = \mathcal{E}_n / Z$ be the quotient group, formed by matrices of the form (5) with constant factors disregarded. In what follows an error operator E can be either from $\mathcal{E}_n$ or $\bar{\mathcal{E}}_n$. If $E \in \bar{\mathcal{E}}_n$ then we will assume that E is of the form (5), that is we take E as a coset representative.

Definition. A quantum code Q is called a *stabilizer* code if there exists an Abelian subgroup S of the group $\mathcal{E}_n$ such that Q is an eigenspace of S with eigenvalue 1. In other words, a code Q is a stabilizer code if

$$Q = \{\mathbf{v} \in \mathcal{H}_n \mid \forall_{E \in S}\, E\mathbf{v} = \mathbf{v}\}.$$

If the order of S is 2^{n-k}, then $\dim(Q) = 2^k$ [5], [7], and so the dimension of a stabilizer code always equals an integer power of 2. A stabilizer code of length n and dimension 2^k is denoted by $Q[[n,k]]$.

Let $F := GF(4) = \{0, 1, \omega, \omega^2\}$. In the remaining part of this section we explain a way to associate to a quantum stabilizer code two additive codes C and $C^\perp$ over F in such a manner that $B(x, y)$ and $B^\perp(x, y)$ are their respective weight enumerators. This connection is the main discovery of [5]. It is also of key importance for both parts of our study.

We begin by establishing a bijection $\bar{\phi}$ between the set of matrices $\{I_2, \sigma_x, \sigma_z, \sigma_y\}$ and the elements of F as follows:

$$\bar{\phi}(I_2) = 0,\ \bar{\phi}(\sigma_x) = 1,\ \bar{\phi}(\sigma_z) = \omega,\ \bar{\phi}(\sigma_y) = \omega^2,$$

where ω is a primitive element of F. This bijection naturally extends to a bijection ϕ_n between $\bar{\mathcal{E}}_n$ and F^n and defines a mapping $\phi_n : \mathcal{E}_n \to F^n$ as a composition of $\bar{\phi}_n$ and the factorization mapping. For $a \in F$ let $\bar{a}$ be its conjugate under the action of the Galois group. In particular, this action transposes ω and $\bar{\omega} = \omega^2$. Let $*$ be the inner product in F^n defined by

$$\mathbf{u} * \mathbf{v} = \mathrm{tr}(\sum_i v_i \bar{u}_i) = \sum_i (v_i u_i^2 + v_i^2 u_i), \tag{12}$$

where $\mathrm{tr}(x) := x + x^2$ is the trace from F to $GF(2)$. Key properties of error operators from $\mathcal{E}_n$ in this context are the following [4], [5]:

$$E_1 E_2 = \begin{cases} E_2 E_1 & \text{if } \mathbf{e}_1 * \mathbf{e}_2 = 0, \\ -E_2 E_1 & \text{if } \mathbf{e}_1 * \mathbf{e}_2 \neq 0, \end{cases} \tag{13}$$

where $\mathbf{e}_i = \phi_n(E_i)$, and

$$E_1 E_2 = E_3 \ \Rightarrow\ \mathbf{e}_1 + \mathbf{e}_2 = \mathbf{e}_3.$$

Thus, $\bar{\phi}_n$ establishes a group isomorphism between $\bar{\mathcal{E}}_n$ and the additive group of F^n; so $\bar{\mathcal{E}}_n$ is elementary Abelian of order 2^{2n}, and ϕ_n is a homomorphism. Another useful property of error operators is

$$\mathrm{Tr}(E_1 E_2 E_1 E_2) = (-1)^{e_1 * e_2} \mathrm{Tr}(E_1 E_2 E_2 E_1) = (-1)^{e_1 * e_2} 2^n. \tag{14}$$

Now let $S < \mathcal{E}_n$ be a subgroup. Let

$$C := \{\mathbf{c} \in F^n \mid \mathbf{c} = \phi_n(E) \text{ for some } E \in S\}.$$

Obviously, C is an additive subgroup in the group F^n. Let

$$C^\perp = \{\mathbf{c} \in F^n \mid \forall_{\mathbf{c}' \in C}(\mathbf{c} * \mathbf{c}') = 0.\}$$

Letting $\mathbf{c}$ range over the entire $C^\perp$ defines a subgroup $\bar{S}^\perp = \{\bar{\phi}_n^{-1}(\mathbf{c})\} < \bar{\mathcal{E}}_n$. By definitions of $C, C^\perp$, and (13) we see that any matrices $E \in S$, $E' \in S^\perp$ commute. Note also that S is Abelian; by (13) this implies that $\mathbf{c}' * \mathbf{c}'' = 0$ for any vectors $\mathbf{c}', \mathbf{c}'' \in C$; hence

$$C \subseteq C^\perp$$

and therefore, $S < S^\perp$ and $\bar{S} < \bar{S}^\perp$.

The following theorem completes our task.

Theorem 3 [18] *Let Q be a stabilizer code, $B(x,y)$ and $B^{\perp}(x,y)$ its weight enumerators, and let C and $C^{\perp}$ be the codes over F^n defined above. Then the Hamming weight enumerator of C (resp., $C^{\perp}$) is $B(x,y)$ ($B^{\perp}(x,y)$).*

The proof relies on the following lemma whose short proof we include for completeness.

Lemma 4 [18] *The orthogonal projection P on Q can be written in the following form:*

$$P = \frac{1}{2^{n-k}} \sum_{E \in S} E. \tag{15}$$

Proof A linear operator is a projection if and only if it is idempotent. A projection is orthogonal if and only it is self-adjoint. Self-adjointness of P follows from (6) and (5). P is also idempotent.

$$P^2 = \Big(\frac{1}{2^{n-k}}\Big)^2 \sum_{E' \in S} E' \sum_{E \in S} E = \Big(\frac{1}{2^{n-k}}\Big)^2 \sum_{E \in S} 2^{n-k} E = P.$$

Let us compute the dimension of the space $\{P\mathbf{v} \mid \mathbf{v} \in \mathcal{H}\}$. From (5) we see that $\mathrm{Tr}(E) = 0$ unless $E = I_{2^n}$. Hence $\mathrm{Tr}(P) = 2^k = \dim Q$. Finally, for any $\mathbf{v} \in Q$ we have $E\mathbf{v} = \mathbf{v}$ by definition of Q; hence also $P\mathbf{v} = \mathbf{v}$. □

The proof of Theorem 3 is now accomplished by invoking (14) and (7).

3 Quantum undetected error

In this section we study error detection with quantum codes used over the depolarizing channel. We examine a number of possible definitions of undetected error and establish their equivalence.

For a quantum code Q we denote by $Q^{\perp}$ its orthogonal code under the standard Hermitian inner product on $\mathcal{H}_n$. The orthogonal projection on $Q^{\perp}$ is denoted by $P^{\perp}$.

Let us first describe the *quantum error detection protocol.* The transmitted vector $\mathbf{v} \in Q$ is corrupted in the channel by the action of an error operator $E \in \bar{\mathcal{E}}_n$. The received vector has the form $\mathbf{w} = E\mathbf{v}$. In order to detect the error we perform the measurement of $\mathbf{w}$ with respect to the projections $(P, P^{\perp})$. If the result of this measurement is contained in $Q^{\perp}$ we detect an error. Otherwise we assume that there is no error and that the code vector $P\mathbf{w}$ was transmitted.

A. STABILIZER CODES Let us begin with the easier case of stabilizer codes. Suppose S is a stabilizer group of a code Q. Below by C we denote the code obtained by evaluating $\phi_n(E)$ on all $E \in S$.

Let $E \in \bar{\mathcal{E}}_n$ and $\mathbf{v} \in Q$. Suppose $\mathbf{z}$ is a result of the measurement of $\mathbf{w} = E\mathbf{v}$ with respect to the system $(P, P^{\perp})$. Let us introduce the indicator function $\delta(E, \mathbf{v})$ as follows:

$$\delta(E, \mathbf{v}) = \begin{cases} 1 & \mathbf{z} \in Q \text{ and } \mathbf{z} \not\propto \mathbf{v} \\ 0 & \text{otherwise.} \end{cases}$$

Note that if $\mathbf{w} \in Q$ then measuring it with respect to the system $(P, P^\perp)$ with probability 1 we obtain a code vector. As shown below, for stabilizer codes the vector $\mathbf{w}$ is contained either in Q or in $Q^\perp$; hence in this case δ is deterministic.

Definition. Let Q be a stabilizer code. Its probability of undetected error in a depolarizing channel with error probability p is defined as

$$P_{ue}^{(s)}(Q,p) = \sum_{E \in \bar{\mathcal{E}}_n} \Pr(E) \int_{\mathbf{v} \in Q} \delta(E, \mathbf{v}) d\nu(\mathbf{v}), \tag{16}$$

where $\nu(\cdot)$ is the normalized uniform measure on Q.

To compute the probability of undetected error let us first specify the error event, i.e., examine the case $\delta(E, \mathbf{v}) = 1$ in more detail. Consider a possible effect of error operators on vectors from Q. For an error operator E let $\mathbf{e} = \bar{\phi}_n(E)$. There are the following three possibilities.

1) If $E \in \bar{S}$ then $E\mathbf{v} \propto \mathbf{v}$ for any $\mathbf{v} \in Q$; so this error has no effect on the transmission.

2) Let $E \notin \bar{S}^\perp$. This means that $\mathbf{e} \notin C^\perp$ and so $\mathbf{e} * \mathbf{e}' \neq 0$ for some $\mathbf{e}' \in C$. Hence $EE' = -E'E$ and $E'E\mathbf{v} = -EE'\mathbf{v} = -E\mathbf{v}$. Thus $E\mathbf{v}$ is contained in the eigenspace of E' with eigenvalue -1. Since E is a Hermitian operator, its eigenspaces are pairwise orthogonal. Thus

$$\mathbf{w}^* E\mathbf{v} = 0$$

for any $\mathbf{w} \in Q$. In other words $\mathbf{w} \in Q^\perp$, and making measurement with respect to $(P, P^\perp)$ we will detect the presence of error with probability 1.

3) Now let $E \in \bar{S}^\perp \setminus \bar{S}$, i.e., $\mathbf{e} \in C^\perp \setminus C$. Then $\mathbf{e} * \mathbf{e}' = 0$ for all $\mathbf{e}' \in C$. Hence by (13) $EE' = E'E$ for all $E' \in S$, and so $E'E\mathbf{v} = EE'\mathbf{v}$. Hence $E\mathbf{v}$ is an eigenvector of E' with eigenvalue 1 and therefore $E\mathbf{v} \in Q$. However, $E \notin \bar{S}$; so $E\mathbf{v} \not\propto \mathbf{v}$ for some $\mathbf{v} \in Q$. Thus, E acts on Q by rotation, possibly with some invariant directions.

Note that in contrast with classical linear codes there are errors whose detection depends on the transmitted vector.

The above information enables us to compute the probability of undetected error.

Proposition 5

$$P_{ue}^{(s)}(Q,p) = \sum_{E \in \bar{S}^\perp \setminus \bar{S}} \Pr(E) \tag{17}$$

$$= \sum_{i=0}^{n} (B_i^\perp - B_i) \left(\frac{p}{3}\right)^i (1-p)^{n-i} \tag{18}$$

Proof. The proof follows the standard proof of (1), relying upon (8) and the definition of the weight distributions $\{B_i\}$ and $\{B_i^\perp\}$.

Suppose $E \in \bar{S}^\perp \setminus \bar{S}$ and $\mathbf{e} = \bar{\phi}_n(E)$. Let

$$\widehat{Q}(E) := \{\mathbf{v} \in Q \mid E\mathbf{v} = \mathbf{v}\}.$$

Let us construct the code $C_{\mathbf{e}}$ by adjoining $\mathbf{e}$ to the basis of C. Since $\mathbf{e} * \mathbf{e} = 0$ for any $\mathbf{e} \in \mathbb{C}^{2^n}$, the new code is self-orthogonal. Hence we can construct an $[[n, k-1]]$ quantum stabilizer code $Q(E)$ associated with $C_{\mathbf{e}}$. Obviously $Q(E) \subset Q$ and any $\mathbf{v} \in Q(E)$ is stabilized by E. It also follows from the definition of stabilizer codes that all vectors of $\mathbb{C}^{2^n}$ stabilized by both S and E belong to $Q(E)$. Hence $\widehat{Q}(E) = Q(E)$. Therefore, the size of $\widehat{Q}(E)$ does not depend on E, and for every E the set $\widehat{Q}(E)$ is a $K-1$-dimensional subspace. Therefore $\nu(\widehat{Q}(E)) = 0$. This implies our claim since

$$\begin{aligned} P_{ue}^{(n)}(Q,p) &= \sum_E \Pr(E) \int_{\mathbf{v}\in Q} \delta(E,\mathbf{v}) d\nu(\mathbf{v}) \\ &= \sum_{E \in \bar{S}^\perp \setminus \bar{S}} \Pr(E)\nu(Q \setminus \widehat{Q}(E)) = \sum_{E \in \bar{S}^\perp \setminus \bar{S}} \Pr(E)\nu(Q) \\ &= \sum_{E \in \bar{S}^\perp \setminus \bar{S}} \Pr(E). \end{aligned}$$

This proves (17). To prove the final part, note that $|\{E : \mathrm{wt}(E) = i, E \in \bar{S}^\perp \setminus \bar{S}\}| = B_i^\perp - B_i$. □

This proposition shows that if, speaking loosely, we assume that the error E is not detectable whenever $E \in \bar{S}^\perp \setminus \bar{S}$, ignoring vectors from $\hat{Q}$, the probability of undetected error will be still given by (17)-(18). This might motivate another definition of undetected error for stabilizer codes, namely, assuming the uniform distribution on Q, let us call an error E undetectable if $E \in \bar{S}^\perp \setminus \bar{S}$.

B. NONSTABILIZER CODES. In this part we consider a more general situation of Q an arbitrary quantum code. Moreover, we take a viewpoint more natural in the physical perspective, namely if a "received" vector is close to the transmitted vector then we assume that little error has occurred despite the fact that formally they are not equal. This assumption is justified since a physical measurement in this case will not exhibit any difference between the transmitted and the received vectors.

More specifically, let $\mathbf{v} \in Q$ and $\mathbf{w} = E\mathbf{v}$ for some error operator E. If as a result of the measurement with respect to $(P, P^\perp)$, $\mathbf{w}$ is projected on $Q^\perp$, the error is detected. Let us examine more closely the situation of $\mathbf{w}$ projected on Q. Let

$$\mathbf{z} = \frac{P\mathbf{w}}{\sqrt{\mathbf{w}^* P \mathbf{w}}} = \frac{PE\mathbf{v}}{\sqrt{\mathbf{v}^* EPE\mathbf{v}}} \tag{19}$$

be this projection, which occurs with probability $\mathbf{v}^* EPE\mathbf{v}$. A natural proximity measure of $\mathbf{z}$ and $\mathbf{v}$ is the absolute value of the angle $\angle(\mathbf{z}, \mathbf{v})$ between them. If $\mathbf{z}$ is sufficiently close to $\mathbf{v}$, we assume that no error has occurred. By way of thought experiment suppose that for a given code vector $\mathbf{v}$ we measure $\mathbf{z}$ with respect to the system $(\mathbf{v}\mathbf{v}^*, P - \mathbf{v}\mathbf{v}^*)$. Denote the result of this measurement by $\mathbf{y}_{\mathbf{z}}$. In other words, we represent Q as a direct sum of $\mathbf{v}$ and a $K-1$-dimensional orthogonal subspace $Q_{\mathbf{v}}$ and create a pair of projections, on the line given by $\mathbf{v}$ and on $Q_{\mathbf{v}}$. The probability that after this measurement $\mathbf{z} \in Q$ projects on $\mathbf{v}$ equals $\mathbf{z}^* \mathbf{v}\mathbf{v}^* \mathbf{z} = cos^2 \angle(\mathbf{z}, \mathbf{v})$; the probability of the complementary event is $\mathbf{z}^*(P - \mathbf{v}\mathbf{v}^*)\mathbf{z}$. In the former case we assume that the error has no effect on transmission; in the latter that the error is undetectable.

The overall probability that if $\mathbf{v} \in Q$ is subjected to an error operator E, then $\mathbf{y_z}$ is a code vector orthogonal to $\mathbf{v}$ equals $||(I - \mathbf{v}\mathbf{v}^*)PE\mathbf{v}||^2$. Indeed, it equals

$$\begin{aligned}\Pr\{\mathbf{z} \in Q\} \Pr\{\mathbf{y_z} \perp \mathbf{v} | \mathbf{z} \in Q\} &= (\mathbf{v}^* EPE\mathbf{v})(\mathbf{z}^*(P - \mathbf{v}\mathbf{v}^*)\mathbf{z}) \\ &\stackrel{(a)}{=} \mathbf{v}^* EP(I_{2^n} - \mathbf{v}\mathbf{v}^*)PE\mathbf{v} \\ &\stackrel{(b)}{=} \mathbf{v}^* EP(I_{2^n} - \mathbf{v}\mathbf{v}^*)(I_{2^n} - \mathbf{v}\mathbf{v}^*)PE\mathbf{v} \\ &= ||(I - \mathbf{v}\mathbf{v}^*)PE\mathbf{v}||^2,\end{aligned}$$

where (a) follows upon substituting $\mathbf{z}$ from (19) and recalling that P is a projection on Q and (b) uses the fact that $I_{2^n} - \mathbf{v}\mathbf{v}^*$ is a projection. Concluding, we arrive at the following general definition of the probability of undetected error.

Definition. Let Q be a quantum code used over a depolarizing channel with error probability p. Then

$$P_{ue}^{(n)}(Q, p) = \sum_E \Pr(E) \int_{\mathbf{v} \in Q} ||(I - \mathbf{v}\mathbf{v}^*)PE\mathbf{v}||^2 d\nu(\mathbf{v}), \tag{20}$$

where ν is a normalized uniform measure on Q.

This definition is more general than the one given for stabilizer codes.

The main result that we prove regarding $P_{ue}^{(n)}(Q, p)$ is given in the following theorem, which shows that $P_{ue}^{(n)}(Q, p)$ differs from $P_{ue}^{(s)}(Q, p)$ only by a constant factor.

Theorem 6 *Let Q be an $((n, K))$ quantum code with weight distributions B_i and $B_i^\perp$, $0 \leq i \leq n$. Then*

$$P_{ue}^{(n)}(Q, p) = \frac{K}{K+1} \sum_{i=0}^{n} (B_i^\perp - B_i) \Big(\frac{p}{3}\Big)^i (1-p)^{n-i}. \tag{21}$$

PROOF. The proof is accomplished by computing the integral in (20). It is clear that

$$\begin{aligned}&\int_{\mathbf{v} \in Q} ||(I - \mathbf{v}\mathbf{v}^*)PE\mathbf{v}||^2 d\nu(\mathbf{v}) \\ &= \int_{\mathbf{v} \in Q} \mathbf{v}^* EP(I - \mathbf{v}\mathbf{v}^*)(I - \mathbf{v}\mathbf{v}^*)PE\mathbf{v} d\nu(\mathbf{v}) \\ &= \int_{\mathbf{v} \in Q} \mathbf{v}^* EPE\mathbf{v} d\nu(\mathbf{v}) - \int_{\mathbf{v} \in Q} (\mathbf{v}^* EP\mathbf{v})(\mathbf{v}^* PE\mathbf{v}) d\nu(\mathbf{v}).\end{aligned} \tag{22}$$

To compute the integrals in (22) we need the following lemmas proved in the appendix.

Lemma 7 *Let Q be an (n, K) quantum code. Let P be the orthogonal projection on Q, and let $\mu(\mathbf{v})$ be the normalized uniform measure on Q. Then*

$$\int_{\mathbf{v} \in Q} \mathbf{v}\mathbf{v}^* d\mu(\mathbf{v}) = \frac{P}{K}$$

Lemma 8

$$\int_{\mathbf{v}\in Q} \mathbf{v}\mathbf{v}^* \otimes \mathbf{v}\mathbf{v}^* d\mu(\mathbf{v}) = \frac{1}{K(K+1)} \left(\sum_{i,j} \mathbf{v}_i\mathbf{v}_i^* \otimes \mathbf{v}_j\mathbf{v}_j^* + \mathbf{v}_i\mathbf{v}_j^* \otimes \mathbf{v}_j\mathbf{v}_i^* \right) \tag{23}$$

Using these lemmas, let us compute the integrals in (22). By Lemma 7 we have for the first term

$$\begin{aligned} \int_{\mathbf{v}\in Q} \mathbf{v}^* EPE\mathbf{v} d\mu(\mathbf{v}) &\overset{(a)}{=} \int_{\mathbf{v}\in Q} \mathrm{Tr}(EPE\mathbf{v}\mathbf{v}^*) d\mu(\mathbf{v}) \\ &= \mathrm{Tr}\left(EPE \int_{\mathbf{v}\in Q} \mathbf{v}\mathbf{v}^* d\mu(\mathbf{v}) \right) \\ &= \frac{1}{K} \mathrm{Tr}(EPEP), \end{aligned} \tag{24}$$

where (a) is obtained by replacing a scalar by its trace.

Let us compute the second term in (22). The code Q is a K-dimensional linear space; so it is isomorphic to the complex space $\mathbb{C}^K$. The following calculations are simplified by performing them on $\mathbb{C}^K$ instead of Q.

Note that for any operators

$$\mathrm{Tr}(ABC) = \mathrm{Tr}(BCA). \tag{25}$$

Therefore, we can rewrite our integral as

$$\int_{\mathbf{v}\in\mathbb{C}^K} \mathbf{v}^* EP\mathbf{v}\mathbf{v}^* PE\mathbf{v} d\mu(\mathbf{v}) = \int_{\mathbf{v}\in\mathbb{C}^K} \mathrm{Tr}(EP\mathbf{v}\mathbf{v}^* PE\mathbf{v}\mathbf{v}^*) d\mu(\mathbf{v}). \tag{26}$$

Let L_n be the space of linear operators on $\mathcal{H}_n$. Consider the bilinear functional

$$\begin{aligned} \Phi_1 : L_n \times L_n &\to \mathbb{C} \\ (A, B) &\mapsto \mathrm{Tr}(CAC^*B). \end{aligned}$$

By the definition of the tensor product [11], there exists a (universal) bilinear map $t : L_n \times L_n \to L_n \otimes L_n$ such that $\Phi_1 = \Phi_2 \circ t$, where Φ_2 is a *linear* functional defined by

$$\begin{aligned} \Phi_2 : L_n \otimes L_n &\to \mathcal{H}_n \\ A \otimes B &\mapsto \mathrm{Tr}(CAC^*B). \end{aligned}$$

Now we have

$$\begin{aligned}
\int_{\mathbf{v}\in\mathbb{C}^K} \mathbf{v}^* EP\mathbf{v}\mathbf{v}^* PE\mathbf{v} d\mu(\mathbf{v}) &\stackrel{(a)}{=} \int_{\mathbf{v}\in\mathbb{C}^K} \Phi_2(\mathbf{v}\mathbf{v}^* \otimes \mathbf{v}\mathbf{v}^*) d\mu(\mathbf{v}) \\
&\stackrel{(b)}{=} \Phi_2\Big(\int_{\mathbf{v}\in\mathbb{C}^K} \mathbf{v}\mathbf{v}^* \otimes \mathbf{v}\mathbf{v}^* d\mu(\mathbf{v})\Big) \\
&\stackrel{(c)}{=} \frac{1}{K(K+1)} \Phi_2\Big(\sum_{i,j=1}^{K} \mathbf{v}_i\mathbf{v}_i^* \otimes \mathbf{v}_j\mathbf{v}_j^* + \mathbf{v}_i\mathbf{v}_j^* \otimes \mathbf{v}_j\mathbf{v}_i^*\Big) \\
&\stackrel{(d)}{=} \frac{1}{K(K+1)} \Big[\sum_i \mathrm{Tr}(EP\mathbf{v}_i\mathbf{v}_i^* PE \sum_j \mathbf{v}_j\mathbf{v}_j^*) + \sum_{i,j} \mathrm{Tr}(EP\mathbf{v}_i\mathbf{v}_j^* PE\mathbf{v}_j\mathbf{v}_i^*)\Big] \\
&\stackrel{(e)}{=} \frac{1}{K(K+1)} \Big[\sum_i \mathrm{Tr}(EP\mathbf{v}_i\mathbf{v}_i^* PEP) + \sum_{i,j} \mathrm{Tr}(\mathbf{v}_i^* EP\mathbf{v}_i)\,\mathrm{Tr}(\mathbf{v}_j^* PE\mathbf{v}_j)\Big] \\
&\stackrel{(f)}{=} \frac{1}{K(K+1)} \Big[\mathrm{Tr}(PEPEP \sum_i \mathbf{v}_i\mathbf{v}_i^*) + \mathrm{Tr}(EP \sum_i \mathbf{v}_i\mathbf{v}_i^*)\,\mathrm{Tr}(PE \sum_j \mathbf{v}_j\mathbf{v}_j^*)\Big] \\
&\stackrel{(g)}{=} \frac{1}{K(K+1)} \Big[\mathrm{Tr}(PEPE) + \mathrm{Tr}(EP)^2\Big] \qquad (27)
\end{aligned}$$

Here (a) follows by (26) and the definition of Φ_2, (b) holds true by linearity of Φ_2, (c) follows by Lemma 8, (d) is by definition of Φ_2, (e) uses the fact that $P = \sum_i \mathbf{v}_i\mathbf{v}_i^*$, (f) uses (25) and the additivity of trace, and (g) follows by (25) and the fact that P is idempotent.

Substitution of (24) and (27) in (22) gives

$$\int_{\mathbf{v}\in Q} ||(I - \mathbf{v}\mathbf{v}^*)PE\mathbf{v}||^2 d\nu(\mathbf{v}) = \frac{K}{K+1}\Big[\frac{1}{K}\,\mathrm{Tr}(EPEP) - \frac{1}{K^2}\,\mathrm{Tr}(EP)^2\Big];$$

by (9)-(10) this proves the theorem. □

4 Composite systems

In this section we study the most general problem setting for quantum error detection. The general idea is to take into account not only the error process but also the relationship of the current code vector with states of other quantum systems. More specifically, the qubits of the current vector can be entangled with other qubits that may not even take part in the transmission. We would like to study error detection that takes into account not only the error process but also this entanglement. The overall goal is to evaluate how well the original entanglement is preserved under the action of errors. Somewhat surprisingly, though this definition of undetected error is more broad, the actual functional is again the same as studied above.

This problem has no direct analogy in classical information transmission where typically one can study the effect of the error process on the transmitted vector without considering the influence on it of other parts of the message.

Let Q be a quantum code that is a part of a combined system $QR = Q \otimes R$, where R is another K-dimensional subspace. A generic element of QR can be written as $\sum_{i=1}^{K} \mathbf{v}_i \otimes \mathbf{w}_i$,

where $\mathbf{v}_i$ and $\mathbf{w}_i$ are basis vectors of space Q and R respectively. Upon normalization we obtain a *completely entangled state* of the composite system,

$$\mathbf{b}_{QR} = \frac{1}{\sqrt{K}} \sum_{i=1}^{K} \mathbf{v}_i \otimes \mathbf{w}_i.$$

Let us assume that we transmit or store in quantum memory only qubits of Q. These qubits are subjected to the error process described above; so qubits of R remain error-free. The "received" state has the form

$$\widehat{\mathbf{b}}_{QR} = \frac{1}{\sqrt{K}} \sum_{i=1}^{K} (E_Q \otimes I_R)\mathbf{v}_i \otimes \mathbf{w}_i,$$

where E_Q is an error operator on Q and I_R is the identity operator on R. At the "receiving end" we again apply the same decoding, namely, measure the state with respect to $(P_Q, P_Q^{\perp})$. As above, the error is not detected if after this measurement we obtain a code vector that is orthogonal to the transmitted vector $\mathbf{v}$. Therefore, in analogy with (20) let us define the probability of undetected error for the case of composite systems as follows

$$P_{ue}^{(c)}(Q,p) := \sum_{E_Q} \Pr(E_Q) ||(I_R \otimes I_R - \mathbf{b}_{QR}\mathbf{b}_{QR}^*)(P_Q \otimes I_R)(E_Q \otimes I_R)\mathbf{b}_{QR}||^2 \tag{28}$$

The main result of this section is given by the following theorem.

Theorem 9 *Suppose we transmit completely entangled states $\mathbf{b}_{QR}$ over a depolarizing channel with error probability p. Then*

$$P_{ue}^{(c)}(Q,p) = \sum_{i=0}^{n} (B_i^{\perp} - B_i) \left(\frac{p}{3}\right)^i (1-p)^{n-i},$$

where $B_i, B_i^{\perp}$ are the weight enumerators of the code Q.

PROOF. Let us compute the summation term in (28). We have

$$\begin{aligned}
&||(I_R \otimes I_R - \mathbf{b}_{QR}\mathbf{b}_{QR}^*)(P_Q \otimes I_R)(E_Q \otimes I_R)\mathbf{b}_{QR}||^2 \\
&\quad = \mathbf{b}_{QR}^* \Big[(E_Q \otimes I_R)(P_Q \otimes I_R)(I_Q \otimes I_R - b_{QR}\mathbf{b}_{QR}^*)(I_Q \otimes I_R - \mathbf{b}_{QR}\mathbf{b}_{QR}^*) \\
&\qquad \times (I_Q \otimes I_R - \mathbf{b}_{QR}\mathbf{b}_{QR}^*)(P_Q \otimes I_R)(E_Q \otimes I_R) \Big] \mathbf{b}_{QR} \\
&\quad = \mathbf{b}_{QR}^*(E_Q \otimes I_R)(P_Q \otimes I_R)(E_Q \otimes I_R)\mathbf{b}_{QR} \\
&\qquad - (\mathbf{b}_{QR}^*(E_Q \otimes I_R)(P_Q \otimes I_R)\mathbf{b}_{QR})(\mathbf{b}_{QR}^*(P_Q \otimes I_R)(E_Q \otimes I_R)\mathbf{b}_{QR}).
\end{aligned} \tag{29}$$

The first term in this expression can be computed as follows

$$\begin{aligned}
&\mathbf{b}_{QR}^*(E_Q\otimes I_R)(P_Q\otimes I_R)(E_Q\otimes I_R)\mathbf{b}_{QR}\\
&\qquad\overset{(a)}{=}\mathrm{Tr}_{QR}((E_Q\otimes I_R)(P_Q\otimes I_R)(E_Q\otimes I_R)\mathbf{b}_{QR}\mathbf{b}_{QR}^*)\\
&\qquad\overset{(b)}{=}\mathrm{Tr}_Q\left(\mathrm{Tr}_R\left((E_Q\otimes I_R)(P_Q\otimes I_R)(E_Q\otimes I_R)\mathbf{b}_{QR}\mathbf{b}_{QR}^*\right)\right)\\
&\qquad\overset{(c)}{=}\mathrm{Tr}_Q\left(\mathrm{Tr}_R\left(\frac{1}{K}\sum_{i,j}E_QP_QE_Q\mathbf{v}_i\mathbf{v}_j^*\otimes\mathbf{w}_i\mathbf{w}_j^*\right)\right)\\
&\qquad\overset{(d)}{=}\frac{1}{K}\mathrm{Tr}_Q\left(\sum_{i,j,l}E_QP_QE_Q\mathbf{v}_i\mathbf{v}_j^*\otimes\mathbf{w}_l^*\mathbf{w}_i\mathbf{w}_j^*\mathbf{w}_l\right) \qquad (30)\\
&\qquad\overset{(e)}{=}\frac{1}{K}\mathrm{Tr}_Q\left(E_QP_QE_Q\sum_l\mathbf{v}_l\mathbf{v}_l^*\right)\\
&\qquad=\frac{1}{K}\mathrm{Tr}_Q\left(E_QP_QE_QP_Q\right), \qquad (31)
\end{aligned}$$

where (a) is obtained upon replacing a scalar by its trace and using (25), (b) follows by property (2) of partial traces, in (c) we substitute the definition of $\mathbf{b}_{QR}$, in (d) we compute the trace over R and use (25), and in (e) we convolve over the dumb indices i,j.

Let us compute the second term in (29). Proceeding as above, we obtain

$$\begin{aligned}
&(\mathbf{b}_{QR}^*(E_Q\otimes I_R)(P_Q\otimes I_R)\mathbf{b}_{QR})(\mathbf{b}_{QR}^*(P_Q\otimes I_R)(E_Q\otimes I_R)\mathbf{b}_{QR})\\
&\quad=\mathrm{Tr}_{QR}((E_Q\otimes I_R)(P_Q\otimes I_R)\mathbf{b}_{QR}\mathbf{b}_{QR}^*)\\
&\qquad\times\mathrm{Tr}_{QR}[(P_Q\otimes I_R)(E_Q\otimes I_R)\mathbf{b}_{QR}\mathbf{b}_{QR}^*]\\
&\quad=\frac{1}{K^2}\mathrm{Tr}_Q(E_QP_QP_Q)\,\mathrm{Tr}_Q(P_QE_QP_Q)\\
&\quad=\frac{1}{K^2}\mathrm{Tr}_Q(P_QE_Q)^2. \qquad (32)
\end{aligned}$$

Substitution of (31) and (32) in (29) together with (9)-(10) completes the proof. □

This concludes our main task for the first part of the paper. We have proved that there exists a consistent definition of the probability of undetected error for quantum codes that can be given in the general case under natural physical assumptions and in the case of stabilizer codes analogously to the classical error detection. The functional of undetected error on Q in all the cases considered is the same, up to a constant factor. Therefore, as in classical coding theory, we can study performance of quantum codes under error detection. The most important question in this context is to prove that the probability of undetected error for the best possible codes falls exponentially with code length n and to exhibit specific bounds on this exponent. Namely, let

$$P_{ue}(n,K,p)=\min_{\substack{Q\in\mathcal{H}_n\\ \dim(Q)=K}}P_{ue}(Q,p).$$

The second part of the paper is devoted to the study of this function. We answer the main question in positive by proving the existence of families of stabilizer codes with exponential decline of $P_{ue}(K,n,p)$, and establish upper bounds on this function for all quantum codes.

5 Quantum weight enumerators

In this section we focus on different forms of quantum weight enumerators. We begin with a short digression on classical enumerators. Let $D \subset \mathbb{F}_q^n$ be a linear code, $\mathrm{supp}(\mathbf{x}) = \{e \in \{1,2,\ldots,n\} | \mathbf{x}_e \neq 0\}$ the support of a vector $\mathbf{x}$ (so $\mathrm{wt}(\mathbf{x}) = |\mathrm{supp}(\mathbf{x})|$) and $\mathrm{supp}(\mathcal{D}) = \cup_{\mathbf{x}\in\mathcal{D}} \mathrm{supp}(\mathbf{x})$ for a subset $\mathcal{D} \in \mathbb{F}_q^n$. Let $(B_i, 0 \leq i \leq n)$ be the weight distribution of D. The following fact, proved by MacWilliams [13], underlies the combinatorial duality of coding theory:

$$\sum_{i=0}^{w} B_i \binom{n-i}{n-w} = \sum_{\substack{F\subseteq\{1,\ldots,n\} \\ |F|=w}} \sum_{\substack{\mathcal{D} \text{ linear subcode of } D \\ \mathrm{supp}(\mathcal{D})\subseteq F}} |\mathcal{D}| \quad (0 \leq w \leq n). \tag{33}$$

In particular, this immediately implies the MacWilliams identities [13]. Denoting $\mathcal{B}_w = \sum_{i=0}^{w} B_i \binom{n-i}{n-w}$, we obtain

$$\sum_{i=0}^{n} B_i x^{n-i} y^i = \sum_{w=0}^{n} \mathcal{B}_w (x-y)^{n-w} y^w.$$

Binomial moments of the weight distribution of codes were studied extensively in [1] and some other related works (see [1] for a discussion and complete bibliography). One of the reasons for this interest is that while any particular weight component B_i can be small relative to the code size, the numbers $\mathcal{B}_i$ can not. The probability of undetected error (1) can be written in the form

$$P_{ue}(C,p) = \sum_{w=1}^{n} (\mathcal{B}_w - 1)\Big(1 - \frac{qp}{q-1}\Big)^{n-w}\Big(\frac{p}{q-1}\Big)^{w};$$

thus lower bounds on $\mathcal{B}_w$ are helpful for bounding $P_{ue}(C,p)$ below.

For a quantum code Q one can generalize definition (33) by looking at error operators E whose supports are of restricted size, the support $\mathrm{supp}(E)$ being the subset $\{e \in \{1,2,\ldots,n\} | \tau_e \neq I_2\}$. Then we arrive at the following weight enumerators for Q:

$$\begin{aligned} \mathcal{B}_w &= \frac{1}{K^2} \sum_{\substack{F\subseteq\{1,\ldots,n\} \\ |F|=w}} \sum_{\substack{E\in\mathcal{E}_n \\ \mathrm{supp}(E)\subseteq F}} \mathrm{Tr}^2(EP) \\ \mathcal{B}_w^{\perp} &= \frac{1}{K} \sum_{\substack{F\subseteq\{1,\ldots,n\} \\ |F|=w}} \sum_{\substack{E\in\mathcal{E}_n \\ \mathrm{supp}(E)\subseteq F}} \mathrm{Tr}(EPEP). \end{aligned}$$

Let $\mathcal{B}(x,y)$ and $\mathcal{B}^{\perp}(x,y)$ be the generating functions of $\mathcal{B}_w$ and $\mathcal{B}_w$, respectively. Note that up to constant factors these polynomials are the same as the unitary weight enumerators studied in [17]. As in (33), it is immediate that

$$\mathcal{B}_w = \sum_{i=0}^{w} B_i \binom{n-i}{n-w} \quad \mathcal{B}_w^{\perp} = \sum_{i=0}^{w} B_i^{\perp} \binom{n-i}{n-w},$$

which is a result in [17]. The MacWilliams equation (11) also follows immediately by the original proof in [13]. Also,

$$B(x,y) = \mathcal{B}(x-y,y) \quad B^{\perp}(x,y) = \mathcal{B}^{\perp}(x-y,y);$$

thus the probability of undetected error equals

$$P_{ue}(Q,p) = \sum_{i=0}^{n} (\mathcal{B}_i - \mathcal{B}_i^{\perp}) \Big(\frac{p}{3}\Big)^i \Big(1 - \frac{4p}{3}\Big)^{n-i}.$$

So to bound $P_{ue}(Q,p)$ below we could first derive lower estimates on $(\mathcal{B}_i - \mathcal{B}_i^{\perp})$ following the ideas of [1]. However, in part 2 we choose to work with the functions (18), (21) as a whole.

A Appendix

We precede the proofs of Lemmas 7 and 8 with two results from representation theory, in the form and on a level of generality that suits our needs.

Lemma 10 [9, p. 133] *Let G be a compact group and π be a unitary representation with operators acting on a linear space W. Let μ be the Haar measure on G. Then*

$$P := \int_{g \in G} \pi_g d\mu(g)$$

is an orthogonal projection onto the G-invariant subspace of W.

As in the proof of Theorem 6, in the following lemmas we perform calculations in $\mathbb{C}^K$ instead of Q. Define the inner product of matrices A and B as follows

$$\langle A, B \rangle = \mathrm{Tr}(A^* B). \tag{34}$$

Lemma 11 *Let L be the space of linear operators on $\mathbb{C}^K$ and U be a unitary matrix. Then the equality*

$$A \otimes B = U^* A U \otimes U^* B U \qquad (A, B \in L)$$

holds true for any unitary matrix U if and only if $A \otimes B$ is contained in the subspace $W \subset L \otimes L$ generated by

$$\widehat{I} = I \otimes I = \sum_{i,j=1}^{K} \mathbf{v}_i \mathbf{v}_i^* \otimes \mathbf{v}_j \mathbf{v}_j^* \text{ and } J = \sum_{i,j=1}^{K} \mathbf{v}_i \mathbf{v}_j^* \otimes \mathbf{v}_j \mathbf{v}_i^*.$$

Proof. The proof is at times sketchy, however we only omit routine calculations. Let π be the representation of $U(K)$ acting on $L \otimes L$ as follows

$$\pi_U(A \otimes B) = U^* A U \otimes U^* B U.$$

We need to prove that $\pi_U(A \otimes B) = A \otimes B$ for all $U \in U(K)$ if and only if $A \otimes B \in W$.

Let us begin with the "if" part. It suffices to prove that π_U acts identically on $\widehat{I}$ and J. The first of these is obvious. For the second, let us introduce the canonical isomorphism

$$\begin{aligned} \phi: \qquad & L \otimes L \to L \otimes L \\ & A \otimes B \mapsto B \otimes A. \end{aligned}$$

Let us compute $\pi_U(J)$ as follows:

$$\begin{aligned}
\pi_U(J) &= \sum_{i,j} U^*\mathbf{v}_i\mathbf{v}_j^*U \otimes U^*\mathbf{v}_j\mathbf{v}_i^*U \\
&= \sum_{i,j} U^*\mathbf{v}_i \otimes \mathbf{v}_j^*U \otimes U^*\mathbf{v}_j \otimes \mathbf{v}_i^*U \\
&\xrightarrow{\phi} \sum_{i,j} U^*\mathbf{v}_i \otimes \mathbf{v}_i^*U \otimes U^*\mathbf{v}_j \otimes \mathbf{v}_j^*U \\
&= \sum_{i} U^*\mathbf{v}_i\mathbf{v}_i^*U \otimes \sum_{j} U^*\mathbf{v}_j\mathbf{v}_j^*U \\
&= \sum_{i,j} \mathbf{v}_i\mathbf{v}_i^* \otimes \mathbf{v}_j\mathbf{v}_j^* \\
&\xrightarrow{\phi^{-1}} \sum_{i,j} \mathbf{v}_i\mathbf{v}_j^* \otimes \mathbf{v}_j\mathbf{v}_i^*.
\end{aligned}$$

Let us prove the "only if" part. Consider the group $G = DS_K$ where D is the group of all diagonal matrices with diagonal elements from the set $\{\pm 1, \pm i\}$ and S_K is the symmetric group. Clearly, $G < U(K)$. Let

$$\chi = \frac{1}{|G|}\sum_{g\in G} \pi_g.$$

By Lemma 10, χ is an orthogonal projection on G. We will prove that the dimension of its image is 3. After that we will present an operator $\mathbf{w} \in \operatorname{im}\chi$ that is invariant under the action of G but is not fixed by $U(K)$. This will imply that the dimension of the subspace of $L \otimes L$ fixed by $U(K)$ equals 2; hence by the above this subspace is W.

Let us find $\dim\operatorname{im}(\chi) = \operatorname{Tr}(\chi) = \mathbf{u}_i^*\chi\mathbf{u}_i$, where $(\mathbf{u}_i,\, i = 1, \ldots, K^4)$ is any orthonormal basis of $L \otimes L$. For instance, take

$$\mathbf{u}_{ijkl} = \mathbf{v}_i\mathbf{v}_j^* \otimes \mathbf{v}_k\mathbf{v}_l^*.$$

Then

$$\operatorname{Tr}\Big(\frac{1}{|G|}\sum_{g\in G}\pi_g\Big) = \frac{1}{|G|}\sum_{i,j,k,l}\Big\langle \mathbf{v}_i\mathbf{v}_j^* \otimes \mathbf{v}_k\mathbf{v}_l^*, \sum_{g\in G}\pi_g(\mathbf{v}_i\mathbf{v}_j^* \otimes \mathbf{v}_k\mathbf{v}_l^*)\Big\rangle,$$

where $\langle\cdot,\cdot\rangle$ is the Hermitian inner product on $L \otimes L$,

$$\langle A \otimes B, C \otimes D\rangle = \operatorname{Tr}(AC^* \otimes BD^*). \tag{35}$$

Consider an element $g \in G$, $g = \operatorname{diag}(\mathbf{s})\sigma$, where $\mathbf{s} \in \{\pm 1, \pm i\}^K$ and $\sigma \in S_K$. It is easy to see that

$$\pi_g(\mathbf{v}_i\mathbf{v}_j^* \otimes \mathbf{v}_k\mathbf{v}_l^*) = s_is_j^*s_ks_l^*\mathbf{v}_{\sigma(i)}\mathbf{v}_{\sigma(j)}^* \otimes \mathbf{v}_{\sigma(k)}\mathbf{v}_{\sigma(l)}^*.$$

Since the basis is orthogonal, we have

$$\operatorname{Tr}\Big(\frac{1}{|G|}\sum_{g\in G}\pi_g\Big) = \frac{1}{|G|}\sum_{i,j,k,l}\Big\langle \mathbf{v}_i\mathbf{v}_j^* \otimes \mathbf{v}_k\mathbf{v}_l^*, \sum_{g\in \widehat{G}(i,j,k,l)}\pi_g(\mathbf{v}_i\mathbf{v}_j^* \otimes \mathbf{v}_k\mathbf{v}_l^*)\Big\rangle,$$

where $\widehat{G}(i,j,k,l) < G$ is a subgroup formed by the elements $g = \operatorname{diag}(\mathbf{s})\,\sigma$, where σ has fixed points i, j, k, l as fixed points. The inner product under the sum is nonzero only in the following

three cases:

a) $i = j, k = l, i \neq k$
b) $i = l, j = k, i \neq k$
c) $i = j = k = l$.

It is easy to check that in each of these cases the sum equals $|G|$. Thus we have

$$\mathrm{Tr}\Big(\frac{1}{|G|}\sum_{g\in G}\pi_g\Big) = 3.$$

To complete the proof notice that the element

$$\mathbf{w} = \sum_i \mathbf{v}_i\mathbf{v}_i^* \otimes \mathbf{v}_i\mathbf{v}_i^* \in W$$

is invariant under the action of G but not of $U(K)$. Indeed

$$\pi_g(V) = \sum_{i=1}^{K} \mathbf{v}_{\sigma(i)}\mathbf{v}_{\sigma(i)}^* \otimes \mathbf{v}_{\sigma(i)}\mathbf{v}_{\sigma(i)}^* = V.$$

It is easy to check that V is not fixed under the action of the unitary $K \times K$ matrix

$$U = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 & 0 & \dots & 0 \\ 1 & -1 & 0 & \dots & 0 \\ 0 & 0 & \sqrt{2} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \sqrt{2} \end{bmatrix}$$

For instance for $K = 2$ we have

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

and it is straightforward to see that

$$\begin{aligned} U\mathbf{v}_1\mathbf{v}_1^*U \otimes U\mathbf{v}_1\mathbf{v}_1^*U + U\mathbf{v}_2\mathbf{v}_2^*U \otimes U\mathbf{v}_2\mathbf{v}_2^*U & \\ = (\mathbf{v}_1+\mathbf{v}_2)(\mathbf{v}_1+\mathbf{v}_2)^* \otimes (\mathbf{v}_1+\mathbf{v}_2)(\mathbf{v}_1+\mathbf{v}_2)^* & \\ + (\mathbf{v}_1-\mathbf{v}_2)(\mathbf{v}_1-\mathbf{v}_2)^* \otimes (\mathbf{v}_1-\mathbf{v}_2)(\mathbf{v}_1-\mathbf{v}_2)^* & \\ \neq \mathbf{v}_1\mathbf{v}_1^* \otimes \mathbf{v}_1\mathbf{v}_1^* + \mathbf{v}_2\mathbf{v}_2^* \otimes \mathbf{v}_2\mathbf{v}_2^*. & \end{aligned}$$

□

Proof of Lemma 7.

Let $\mathbf{w}_i$ and $\mathbf{v}_i$ be orthonormal bases of Q and $\mathbb{C}^K$, respectively. Let $\phi : Q \to \mathbb{C}^K$ be the natural isomorphism given by $\phi(\mathbf{w}_i) = \mathbf{v}_i$. Denote by $\rho(U)$ the Haar measure on the unitary group $U(K)$. Applying ϕ, we can rewrite the integral in question as follows

$$\begin{aligned} \int_{\mathbf{v}\in Q} \mathbf{w}\mathbf{w}^* d\mu(\mathbf{v}) \xrightarrow{\phi} & \int_{\mathbf{v}\in\mathbb{C}^K} \mathbf{v}\mathbf{v}^* d\mu(\mathbf{v}) \\ &= \int_{\mathbf{v}\in\mathbb{C}^K} U^*\mathbf{v}\mathbf{v}^*U d\mu(\mathbf{v}) \\ &= \int_{U\in U(K)} d\rho(U) \int_{\mathbf{v}\in\mathbb{C}^K} U^*\mathbf{v}\mathbf{v}^*U d\mu(\mathbf{v}) \\ &= \int_{U\in U(K)} U^*\mathbf{v}\mathbf{v}^*U d\rho(U), \end{aligned}$$

where in the last expression $\mathbf{v}$ is an arbitrary fixed basis vector. We need to compute the last integral.

Let π be a unitary representation of $U(K)$ acting on the vector space of complex $K \times K$ matrices as follows

$$\pi_U(\mathbf{v}\mathbf{v}^*) = U^*\mathbf{v}\mathbf{v}^*U.$$

Consider the operator

$$\int_{U\in U(K)} U^*\mathbf{v}\mathbf{v}^*U d\rho(U) = \int_{U\in U(K)} \pi_U(\mathbf{v}\mathbf{v}^*) d\rho(U)$$

by Lemma 10 it is an orthogonal projection. Next we show that it projects on the one-dimensional subspace generated by I_K; then the last integral becomes easy to compute.

Note that π is unitary with respect to the inner product (34). Indeed,

$$\langle \pi_U(A), \pi_U(B)\rangle = \mathrm{Tr}(U^*AUU^*BU) = \mathrm{Tr}(A^*B) = \langle A, B\rangle.$$

From the standard fact that any matrix A' can be represented in the form $A' = UAW$, where U and W are unitary matrices and A is diagonal, it is easy to see that the identity $U^*AU = A$ can hold for any unitary matrix U if and only if $A = I_K$ (this is a particular case of Lemma 11). Therefore

$$\int_{U\in U(K)} U^*\mathbf{v}\mathbf{v}^*U d\rho(U)$$

equals the projection of $\mathbf{v}^*\mathbf{v}$ on the one-dimensional subspace of W generated by I_K. Recalling that the projection of a vector $\mathbf{x}$ on a vector $\mathbf{y}$ equals $\frac{\langle \mathbf{x},\mathbf{y}\rangle}{\langle \mathbf{y},\mathbf{y}\rangle}\mathbf{y}$, we have

$$\int_{U\in U(K)} U^*\mathbf{v}\mathbf{v}^*U d\rho(U) = \frac{\langle \mathbf{v}^*\mathbf{v}, I_K\rangle}{\langle I_K, I_K\rangle} I_K = \frac{1}{K} I_K = \frac{1}{K}\sum_{i=1}^{K} \mathbf{w}_i\mathbf{w}_i^*.$$

Finally, since

$$\phi^{-1}\Big(\sum_{i=1}^{K} \mathbf{w}_i\mathbf{w}_i^*\Big) = \sum_{i=1}^{K} \mathbf{v}_i\mathbf{v}_i^* = P,$$

we are done. □

Proof of Lemma 8.

Let L be the space of linear operators on $\mathbb{C}^K$. Similarly to the proof of Lemma 7 it can be seen that

$$\int_{\mathbf{v}\in\mathbb{C}^K} \mathbf{v}\mathbf{v}^* \otimes \mathbf{v}\mathbf{v}^* d\mu(\mathbf{v}) = \int_{U\in U(K)} U^*\tilde{\mathbf{v}}\tilde{\mathbf{v}}^*U \otimes U^*\tilde{\mathbf{v}}\tilde{\mathbf{v}}^*U d\rho(U), \tag{36}$$

where $\tilde{\mathbf{v}}$ is an arbitrary fixed basis vector. By Lemma 11 the integral in (36) is a projector, with respect to the inner product (35), on the subspace $W \subset L \otimes L$ generated by $\widehat{I}$ and J. The lemma will be proved if we evaluate the projection on this subspace of $\mathbf{u} := \tilde{\mathbf{v}}\tilde{\mathbf{v}}^* \otimes \tilde{\mathbf{v}}\tilde{\mathbf{v}}^*$.

To do this, we need an orthogonal basis of W (note that $\widehat{I}$ and J are not orthogonal; indeed, it is easy to check that

$$\langle \widehat{I}, \widehat{I}\rangle = K^2, \langle J, J\rangle = K^2, \text{ and } \langle \widehat{I}, J\rangle = K.)$$

Therefore, let us consider the basis $\widehat{I}, \widehat{J}$, where

$$\widehat{J} = J - \frac{1}{K} J.$$

Again it is easy to see that

$$\langle \widehat{J}, \widehat{J} \rangle = K^2 - 1 \text{ and } \langle \widehat{I}, \widehat{J} \rangle = 0.$$

Thus, $\widehat{I}$ and $\widehat{J}$ form an orthogonal basis of W. To compute the projection of $\mathbf{u}$ on W, let us first project it on the basis directions:

$$\begin{aligned}
\langle \widehat{I}, \mathbf{u} \rangle &= \mathrm{Tr}\Big(\sum_{i,j} (\mathbf{v}_i \mathbf{v}_j^* \otimes \mathbf{v}_i \mathbf{v}_j^*)(\tilde{\mathbf{v}} \tilde{\mathbf{v}}^* \otimes \tilde{\mathbf{v}} \tilde{\mathbf{v}}^*) \Big) \\
&= \sum_{i,j} \mathrm{Tr}(\mathbf{v}_i \mathbf{v}_j^* \tilde{\mathbf{v}} \tilde{\mathbf{v}}^*) \, \mathrm{Tr}(\mathbf{v}_i \mathbf{v}_j^* \tilde{\mathbf{v}} \tilde{\mathbf{v}}^*) \\
&= 1; \\
\langle \widehat{J}, \mathbf{u} \rangle &= \Big(1 - \frac{1}{K}\Big).
\end{aligned}$$

Thus, the projection of $\mathbf{u}$ on W equals

$$\int_{\mathbf{v} \in \mathbb{C}^K} \mathbf{v}\mathbf{v}^* \otimes \mathbf{v}\mathbf{v}^* d\mu(\mathbf{v}) = \frac{\langle \widehat{I}, \mathbf{u} \rangle}{\langle \widehat{I}, \widehat{I} \rangle} \widehat{I} + \frac{\langle \widehat{J}, \mathbf{u} \rangle}{\langle \widehat{J}, \widehat{J} \rangle} \widehat{J} = \frac{1}{K(K+1)} (\widehat{I} + J).$$

This completes the proof. □

References

[1] A. Ashikhmin and A. Barg, "Binomial moments of the distance distribution: Bounds and applications," IEEE Trans. Inform. Theory, vol. 45, number 2, pp. 438–452, 1999.

[2] A. Ashikhmin, A. Barg, E. Knill, and S. Litsyn, "Quantum error detection, II: Bounds", *IEEE Trans. Inform. Theory*, submitted.

[3] A. R. Calderbank, P. J. Cameron, W. M. Kantor, and J. J. Seidel, "$\mathbb{Z}_4$-Kerdock codes, orthogonal spreads, and extremal euclidean line-sets," *Proc. London Math. Soc.*, vol. 75, no. 3, pp. 436–480, 1997.

[4] A.R. Calderbank, E.M. Rains, P.W. Shor and N.J.A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett.*, vol. 78, pp. 405-409, 1997.

[5] A.R. Calderbank, E.M. Rains, P.W. Shor and N.J.A. Sloane, "Quantum errors correction via codes over $GF(4)$," *IEEE Trans. Info. Theory*, vol. 44, no. 4, pp.1369 –1387, 1998.

[6] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Research Reports Supplements, No. 10, 1973.

[7] D. Gottesman, "A class of quantum error-correcting codes saturating the quantum Hamming bound," *Phys. Rev. A*, vol.54, pp. 1862-1868, 1996.

[8] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory*, Amsterdam: North Holland Publ. Co., 1982.

[9] A. A. Kirillov, *Elements of the Theory of Representations*, Berlin: Springer-Verlag, 1976.

[10] T.Kløve and V. Korzhik, *Error Detecting Codes*, Dordrecht: Kluwer, 1995.

[11] A. I. Kostrikin and Yu. I. Manin, *Linear Algebra and Geometry*, Gordon and Breach Science Pub., 1989.

[12] E. Knill and R. Laflamme, "A theory of quantum error correcting codes," *Phys. Rev. A*, vol. 55, pp. 900-911, 1997.

[13] F. J. MacWilliams, "A theorem in the distribution of weights in a systematic code", *Bell Syst. Techn. Journ.*, vol. 42 pp. 79–94, 1963.

[14] A. Peres, *Quantum Theory: Concepts and Methods*, Dordrecht: Kluwer, 1995.

[15] V. V. Prasolov, *Problems and Theorems in Linear Algebra*, Providence, RI: Amer Math. Soc., 1994.

[16] J. Preskill, *Quantum Information and Computation*, Lecture Notes for Physics 229, available from http://www.theory.caltech.edu/ preskill/ph229.

[17] E.M. Rains, "Quantum weight enumerators," *IEEE Trans. Info. Theory*, vol. 44, no. 4, pp.1388–1394, 1998.

[18] E.M. Rains, "Quantum shadow enumerators," *IEEE Trans. Info. Theory*, vol. 45, no. 7, pp.2361–2366, 1999.

[19] P.W. Shor and R. Laflamme, "Quantum analog of the MacWilliams identities in classical coding theory," *Phys. Rev. Lett.*, vol. 78, pp. 1600-1602, 1997.

[20] P.W. Shor, "Scheme for reducing decoherence in quantum memory," Phys. Rev. A, **52**, no. 4, pp. 2493–2496, 1995.

[21] A. M. Steane, "Simple quantum error correcting codes," *Phys. Rev. Lett.*, vol. 77, pp. 793-797, 1996.