Quantum MacWilliams Identities

Peter Shor[1,3] and Raymond Laflamme[2,3]

[1] *AT&T Research, Room 2D-149, 600 Mountain Ave.*
Murray Hill, NJ 07974, USA
[2] *Theoretical Astrophysics, T-6, MS B288*
Los Alamos National Laboratory, Los Alamos, NM 87545, USA
[3] *Institute for Theoretical Physics*
University of California, Santa Barbara, CA 93106-4030, USA

(October 25, 1996)

We derive a relationship between two different notions of fidelity (entanglement fidelity and mean fidelity) for a completely depolarizing quantum channel. This relationship gives rise to a quantum analog of the MacWilliams identities in classical coding theory. These identities relate the weight enumerator of a code to the one of its dual and, with linear programming techniques, provided a powerful tool to investigate the possible existence of codes. The same techniques can be adapted to the quantum case. We give examples of their power.

89.70.+c,89.80.th,02.70.–c,03.65.–w

The discovery of error correcting codes [1,2] for quantum computers has revolutionized the field of quantum information. Although quantum computing holds great promise, it is plagued by the fragility of quantum information [3–5]. Quantum error correction is a technique which enables one to encode quantum information in a robust way and therefore overcome this fragility.

It is important to classify codes in order to know what is the most compact way to encode a number of qubits against a given number of errors. Various techniques have been used to discover such codes [1,6–14]. In the classical theory a very powerful technique for looking for the existence of codes is the use of MacWilliams identities [15]. They relate the weight distribution of a code to the weight distribution of its dual code. These relationships can be used with linear programming to find bounds on how good quantum codes can be and to test whether potential good codes can exist [16].

In this letter we give a quantum analog to the weight distributions which obey the (classical) MacWilliams identities. We use these identities to derive the non-existence of some codes. For example we will show that there is no degenerate 5 bit code which encodes 1 qubit of information and corrects for a general 1 bit error; this implies that the perfect code of [8,10] is the best that can attained in this respect. We will also show that there is no 9-bit code which encodes 1 qubit of information and corrects for a general 2 qubit error.

Let us first introduce a basis of operators given by the Hermitian set

$$\mathcal{E} = \{\sigma_i^1 \otimes \sigma_j^2 ... \otimes \sigma_k^n\} \tag{1}$$

for all $i, j, ...k$ and where σ_k^n is chosen from the set of Pauli matrices augmented by the identity, acting on the n^{th} qubit. Note that all elements of $\mathcal{E}$ give the identity when multiplied by their Hermitian conjugate. We define the set E_d as the subset of $\mathcal{E}$ containing exactly d Pauli matrices different from the identity, and we call it the set of distance d.

In a system interacting with an environment, errors (differences from the original state) can be classified as bit flip, sign flip or bit and sign flip [1,8] corresponding to the three Pauli matrices. The set $\mathcal{E}$ corresponds to all possible effects due to independent environments. If we assigned an equal probability of $(1-p)/3$ every time a Pauli matrix appears in a member of $\mathcal{E}$ an initial state ρ_i would therefore evolve as

$$\rho_f = \sum_{E\in\mathcal{E}} p^{d(E)} (\frac{1-p}{3})^{n-d(E)} E\rho_i E^\dagger \tag{2}$$

where ρ_f is the final state and $d(E)$ is the distance of the operator E.

We now define two weights A_d and B_d on operators $\mathcal{O}_1, \mathcal{O}_2$, where d ranges from 0 to n, as

$$A_d = \frac{1}{\mathrm{tr}\mathcal{O}_1 \mathrm{tr}\mathcal{O}_2} \sum_{E_d} \mathrm{tr}(E_d\mathcal{O}_1)\mathrm{tr}(E_d^\dagger\mathcal{O}_2) \tag{3}$$

$$B_d = \frac{1}{\mathrm{tr}\mathcal{O}_1\mathcal{O}_2} \sum_{E_d} \mathrm{tr}(E_d\mathcal{O}_1 E_d^\dagger\mathcal{O}_2) \tag{4}$$

where the sum is over all E_d of distance d.

We define the weight enumerator as

$$A(z) = \sum_{d=0}^{n} A_d z^d \tag{5}$$

and a similar equation for B. The MacWilliams identities are relationships between the weight enumerators $A(z)$ and $B(z)$ given by

$$B(z) = \frac{\mathrm{tr}\mathcal{O}_1 \mathrm{tr}\mathcal{O}_2}{2^n \mathrm{tr}\mathcal{O}_1\mathcal{O}_2} (1+3z)^n A(\frac{1-z}{1+3z}) \tag{6}$$

[These are MacWilliams identities for codes over for GF(4)]. The proof uses the expansion $\mathcal{O}_i$ in term of the set $\mathcal{E}$ as

$$\mathcal{O}_i = \sum_{D\in\mathcal{E}} \frac{\mathrm{tr}(D^\dagger \mathcal{O}_i)}{2^n} D \tag{7}$$

We can rewrite B_d as

$$B_d = \frac{1}{\mathrm{tr}\mathcal{O}_1\mathcal{O}_2} \sum_{D,E_d,D'} \mathrm{tr}(E_d D E^\dagger{}_d D') \frac{\mathrm{tr}(D^\dagger \mathcal{O}_1)}{2^n} \frac{\mathrm{tr}(D'^\dagger \mathcal{O}_2)}{2^n} \tag{8}$$

It is easy to convince yourself that we must have $D = D'$ for the trace $\mathrm{tr}(E_d D E^\dagger{}_d D')$ to be non-zero as otherwise there would be a Pauli matrix operating on at least one qubit. We can now see how to relate B_d to a sum of $A_{d'}$ by deriving the coefficient for every D of weight d' which is equal to

$$\alpha_{dd'} = \frac{\mathrm{tr}(\mathcal{O}_1\mathcal{O}_2)}{2^{2n}} \sum_{E_d} \mathrm{tr}(E_d D E^\dagger{}_d D) \tag{9}$$

for $D \in \mathcal{E}$. To prove the relationship we need to prove it for only one element D of distance d' as all the others can be reached by permutations of the qubits and transformations which are tensor products of 1-qubit unitary transformations. Eqs. (3-4) are invariant under these transformations.

We will be interested in the case where $\mathcal{O}_1 = \mathcal{O}_2 = P_c$, where P_c is a projection operator defining a quantum code. For 2 qubits the coefficient are given by

$$\begin{aligned} &\alpha_{00} = 2^n \;;\; \alpha_{01} = 2^n \;;\; \alpha_{02} = 2^n \\ &\alpha_{10} = 6*2^n \;;\; \alpha_{11} = -2*2^n \;;\; \alpha_{12} = 2^n \\ &\alpha_{20} = 9*2^n \;;\; \alpha_{21} = -3*2^n \;;\; \alpha_{22} = 2^n \end{aligned} \tag{10}$$

from which we deduce the relationship

$$B_0 = \frac{1}{2^{2-k}}(A_0 + A_1 + A_2) \tag{11}$$

$$B_1 = \frac{1}{2^{2-k}}(6A_0 + 2A_1 - 2A_2) \tag{12}$$

$$B_2 = \frac{1}{2^{2-k}}(9A_0 - 3A_1 + A_2) \tag{13}$$

where $\mathrm{tr}(P_c) = 2^k$.

In general,

$$\alpha_{dd'} = 2^n \sum_{s=0}^{d} (-1)^s 3^{d-s} \binom{d'}{s} \binom{n-d'}{d-s}, \tag{14}$$

where the s'th term in the sum comes from considering the case in Eq(9) where there are exactly s qubits on which Pauli matrices act in E_d and in D simultaneously. Eq. (14) is the standard expansion of the MacWilliams identity in terms of Krawtchouk polynomials [15] and the MacWilliams identity (6) then follows from this expansion.

The origin of this relationship can be traced back to the fact that the matrix $H_{ij} = \mathrm{tr} E_i E_j E_i E_j$ is proportional to a Hadamard matrix. As in the classical case, it is a "coarse grained" version of H_{ij} which enters Eq.(9).

In the case where P_c is a projection operators in the subspace defined by the set of states $\{c_i\}$ we can rewrite the weights as

$$A_d = \frac{1}{2^{2k}} \sum_{E_d} \Big| \sum_i \langle c_i|E_d|c_i\rangle \Big|^2 \tag{15}$$

$$B_d = \frac{1}{2^k} \sum_{E_d} \sum_{ij} |\langle c_i|E_d|c_j\rangle|^2 \tag{16}$$

¿From the Cauchy-Schwartz inequality we deduce that these are non-negative numbers with $B_d \geq A_d$. This is because the B's are defined as a sum of the modulus squared of every element of the operators of weight d projected on the code while the A's are the squared modulus of a sum.

For a depolarizing channel with probability of distance 1 error being $(1-p)$, the weight enumerator A has the physical interpretation that $p^n A((1-p)/3p)$ is the fidelity of entanglement [17]. This is the probability that a completely entangled state constructed from the basis states of the code remains intact after going through the channel. The physical interpretation of B is that $p^n B((1-p)/3p)/\mathrm{tr}(P_c)$ is the average fidelity [17], i.e., the average fidelity over the states of an incoherehnt ensemble given by P_c going through the channel and giving the same states.

Necessary and sufficient condition for the quantum code $\mathcal{C}$ to correct $\lfloor d/2 \rfloor$ errors are [9] that for all basis elements $|c_a\rangle$, $|c_b\rangle$ $(a \neq b)$ of P_c

$$\langle c_a|E_{d'}|c_a\rangle = \langle c_b|E_{d'}|c_b\rangle \tag{17}$$

and

$$\langle c_a|E_{d'}|c_b\rangle = 0. \tag{18}$$

for all elements $E_{d'}$ of distance less or equal to d. For a degenerate code [i.e. when (17) is non-zero], we can deduce from Eqs. (15,16) that $A_{d'} = B_{d'}$ for $1 \leq d' \leq d$, and these quantities are zero for a non-degenerate code. Thus the property of error correction restricts the possible form of the weights. The existence of non-negative weights is a necessary condition for a quantum error correcting code to exist.

As a first example of the power of these inequalities, we look for the possible existence of a degenerate 5-bit code which protects 1 qubit of information against a general 1 qubit error. This implies we are looking for a code with $n = 5$ and $k = 2$ which satisfies the equations and inequalities

$$B_0 = \frac{A_0 + A_1 + A_2 + A_3 + A_4 + A_5}{16} = A_0 = 1$$
$$B_1 = \frac{15A_0 + 11A_1 + 7A_2 + 3A_3 - A_4 - 5A_5}{16} = A_1$$
$$B_2 = \frac{45A_0 + 21A_1 + 5A_2 - 3A_3 - 3A_4 + 5A_5}{8} = A_2$$
$$B_3 = \frac{135A_0 + 27A_1 - 9A_2 - 5A_3 + 7A_4 - 5A_5}{8} \geq A_3$$
$$B_4 = \frac{405A_0 - 27A_1 - 27A_2 + 21A_3 - 11A_4 + 5A_5}{16} \geq A_4$$
$$B_5 = \frac{243A_0 - 81A_1 + 27A_2 - 9A_3 + 3A_4 - A_5}{16} \geq A_5.$$

This is a set of linear equations and inequalities in the A_i, which can easily be solved using linear programming techniques. We find that the only solution is given by $A_i = (1,0,0,0,15,0)$ and therefore $B_i = (1,0,0,30,15,18)$. This is the unique solution and since $A_1 = A_2 = 0$ it corresponds to a non-degenerate code. Thus no degenerate code exists for 5 bits. An explicit code with this weight enumerator was found in [8,10].

In a similar way, we can also show that it is not possible to find a code which protects 1 qubit of information against 2 errors using $n = 9$ qubits. A solution of the Macwilliams identities exists for codes mapping 1 qubit into $n = 10$ qubits; however an extension of the techniques in this paper based on classical shadow code techniques rules this possibility out as well [18]. The smallest possible code protecting against two errors thus would map 1 qubit into $n = 11$ qubits; such a code was constructed in [13].

Both possibilities eliminated above would have required degenerate quantum codes. These might have allowed to find more compact codes than would have been expected from an analogy to classical codes. A systematic study of the MacWilliams identities for $n \leq 30$ [18] shows that this is not the case. The most compact codes appear not to be degenerate. It will be interesting to know if this holds as $n \to \infty$.

In conclusion, we have derived the quantum analog of the MacWilliams identities which give necessary conditions for the existence of codes. We have demonstrated the power of these identities by showing the non-existence of certain degenerate codes using linear programming techniques. The quantum Macwilliams identities will lead to a strong bound on the existence of quantum codes as the number of qubits grows large. This will be important to understand the capacity of noisy quantum channels [19,17]

We would like to thank E. Knill for useful comments. We are also grateful to D. DiVincenzo and W. Zurek for the invitation to participate to the the Quantum Coherence and Decoherence workshop in Santa-Barbara. This research was supported in part by the National Science Foundation under Grant No. PHY94-07194.

[1] P.W. Shor *Phys.Rev. A* 52, p.2493, 1995.

[2] A. M. Steane, "Error correcting codes in quantum theory," *Phys. Rev. Lett.*, 77, 793, 1996.

[3] R. Landauer. Is Quantum Mechanically Coherent Computation Useful? In D.H.Feng and B-L. Hu, editors, *Proc. of the Drexel-4 Symposium on quantum Nonintegrability – Quantum Classical Correspondence*, 1996. Also, private communication (1996).

[4] W. G. Unruh. Maintaining coherence in Quantum Computers. *hep-th/9406058; Phys. Rev. A*, 51:992, 1995.

[5] I.L.Chuang, R.Laflamme, P.Shor and W.H.Zurek. Quantum Computers, Factoring and Decoherence, quant-ph/9503007, Science 270, 1633, 1995.

[6] A.R. Calderbank and P.W. Shor, Good quantum error-correcting codes exist, quant-ph/9512032, *Phys. Rev. A*, 52, p. 1098, 1996.

[7] A. Steane, Multiple particle interference and quantum error correction, preprint quant-ph/9601029, to be published in Proc.Roy.Soc. London.

[8] R. Laflamme, C. Miquel, J.-P Paz and W. H. Zurek. Perfect Quantum Error Correcting Code. Physical Review Letters, 98, 77, 1996.

[9] E. Knill and R. Laflamme, A theory of quantum error correcting codes, Los Alamos National Laboratory preprint LA-UR-96-1300, and quant-ph/9604034.

[10] C.H.Bennett, D.P. DiVincenzo, J.A. Smolin and W.K. Wootters; Mixed state entanglement and quantum error correction, preprint quant-ph/9604006.

[11] D. Gottesman; A class of quantum error-correcting codes saturating the quantum Hamming bound" Phys. Rev. A54, 1844, 1996.

[12] A. Steane; Simple quantum error correcting codes, LANL e-print quant-ph/9605021.

[13] A.R. Calderbank, E.M. Rains, P.W. Shor and N.J.A. Sloane; Quantum error correction via codes over GF(4), LANL e-print quantu-ph/9608006.

[14] A. Steane; Quantum Reed-Muller Codes, LANL e-print quant-ph/9608026.

[15] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland Publishing Company, New-York, 1977.

[16] R.J. McEliece, E.R. Rodemich, H.C. Rumsey, Jr and L.R. Welch IEEE Trans.Info.Theory, 23, 157, 1977.

[17] M.A.Nielsen and B.Schumacher. Quantum Data Processing and Error Correction, LANL e-print quant-ph/9604022.

[18] E. Rains, private communication.

[19] S. Lloyd, The capacity of the noisy quantum channel, e-print quant-ph/9604023.