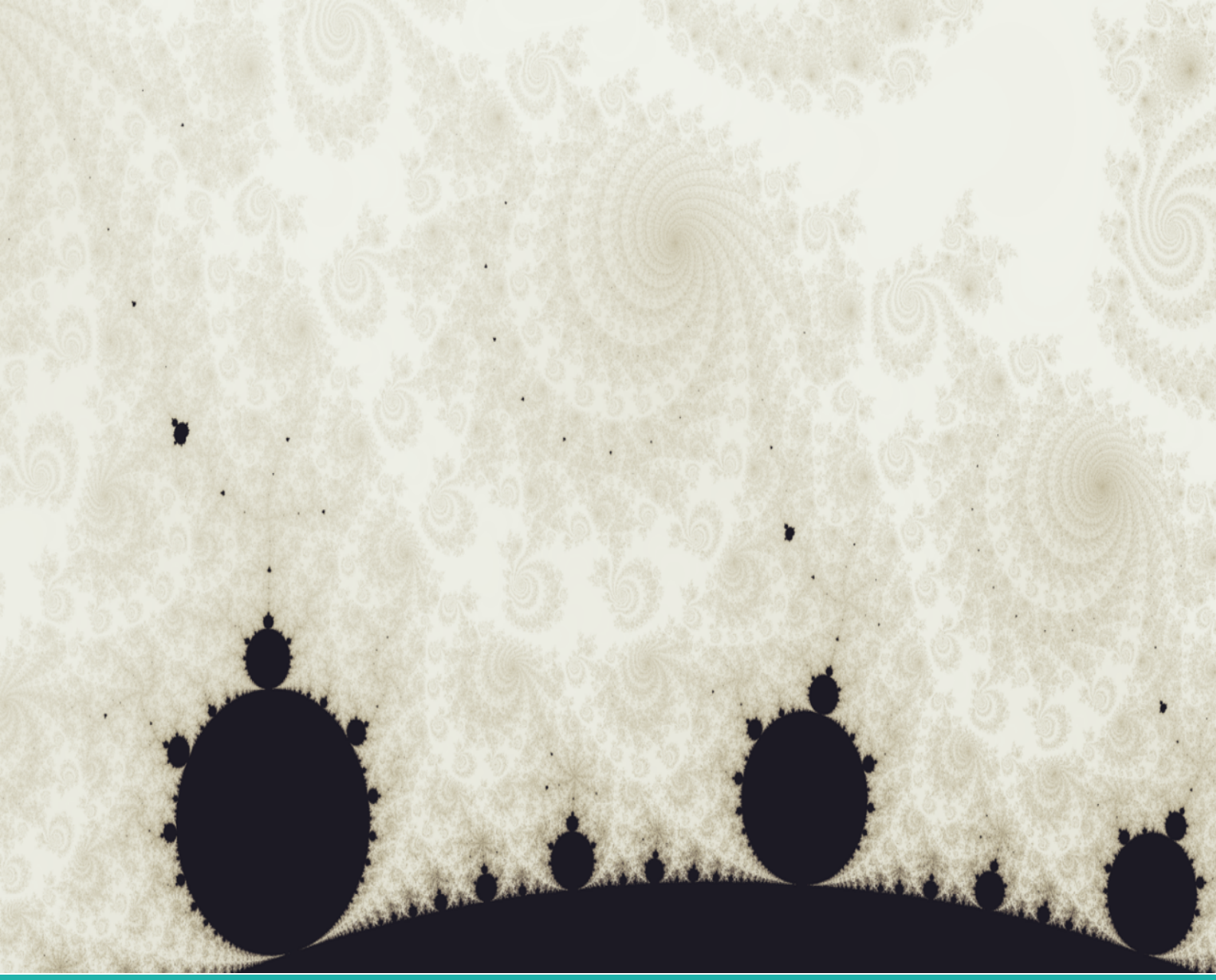

Stabilizer Codes and Quantum Error Correction

A mathematical vision

Autor: Francisco Costa Cano

Versión: 0.1

aka: podxboq

La realidad es compleja, despiertos vivimos la parte real y durmiendo la parte imaginaria.

Capítulo 1 Introduction and preliminary material

1.1 Quantum Computers

The first quantum error-correcting codes were discovered by Shor [**?**] and Steane [**?**]. For a more complete treatment of quantum mechanics, see [**?**]. For a more complete treatment of classical error-correcting codes, see [**?**].

1.2 Introduction to Quantum Mechanics

The state of a classical computer is a string of 0s and 1s, which is a vector over the finite field $\mathbf{Z}_2$. The state of a quantum computer (or any quantum system) is instead a vector over the complex numbers $\mathbf{C}$. Actually, a quantum state lies in a Hilbert space, since there is an inner product (which I will define later). The state is usually written $|\psi\rangle$, which is called a *ket*. A classical computer with n bits has 2^n possible states, but this is only an n-dimensional vector space over $\mathbf{Z}_2$. A quantum computer with n qubits is a state in a 2^n-dimensional complex vector space. For a single qubit, the standard basis vectors are written as $|0\rangle$ and $|1\rangle$. An arbitrary single-qubit state is then

$$\alpha\,|0\rangle + \beta\,|1\rangle\,. \tag{1.1}$$

α and β are complex numbers, with $|\alpha|^2 + |\beta|^2 = 1$. This is a *normalized* state. With multiple qubits, we can have states that cannot be written as the product of single-qubit states. For instance,

$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \tag{1.2}$$

cannot be decomposed in this way. Such a state is said to be *entangled*. Entangled states are what provide a quantum computer with its power. They will also play a major role in quantum error correction. The particular state (**??**) is called an Einstein-Podalsky-Rosen pair (or EPR) pair, and serves as a useful basic unit of entanglement in many applications.

If we make a measurement on the qubit in equation (**??**), we get a classical number corresponding to one of the basis states. The measurement disturbs the original state, which collapses into the basis state corresponding to the measurement outcome. If we measure the state (**??**), the outcome will be 0 with probability $|\alpha|^2$, and it will be 1 with probability $|\beta|^2$. The normalization ensures that the probability of getting some result is exactly 1. Through most of this thesis, I will instead write down unnormalized states. These states will stand for the corresponding normalized states, which are formed by multiplying the unnormalized states by an appropriate constant. The overall phase of a state vector has no physical significance.

The measurement we made implements one of two projection operators, the projections on the basis $|0\rangle\,,\ |1\rangle$. This is not the only measurement we can make on a single qubit. In fact, we can project on any basis for the Hilbert space of the qubit. If we have multiple qubits, we can measure a number of different qubits independently, or we can measure some joint property of the qubits, which corresponds to projecting on some entangled basis of the system. Note that the projection on the basis $|0\rangle\,,\ |1\rangle$ for either qubit destroys the entanglement of the state (**??**), leaving it in a tensor product state.

A particularly fruitful way to understand a quantum system is to look at the behavior of various operators acting on the states of the system. For instance, a nice set of operators to consider for a single qubit is the set of Pauli spin matrices

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},\ \text{and } \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{1.3}$$

The original measurement I described corresponds to measuring the eigenvalue of σ_z. The corresponding projection operators are $\frac{1}{2}(I \pm \sigma_z)$. If we have a spin-1/2 particle, this measurement is performed by measuring the spin of the particle along the z axis. We could also measure along the x or y axis, which corresponds to measuring the eigenvalue of σ_x or σ_y. The projections are $\frac{1}{2}(I \pm \sigma_x)$ and $\frac{1}{2}(I \pm \sigma_y)$.

We can also make measurements of more general operators, provided they have real eigenvalues. A matrix A has real eigenvalues iff it is Hermitian: $A^\dagger = A$, where $A^\dagger$ is the *Hermitian adjoint* (or just *adjoint*), equal to the complex conjugate transpose. Note that all of the Pauli spin matrices are Hermitian.

The Pauli matrices also satisfy an important algebraic property — they *anticommute* with each other. That is,

$$\{\sigma_i, \sigma_j\} = \sigma_i\sigma_j + \sigma_j\sigma_i = 0 \tag{1.4}$$

whenever $i \neq j$ (with $i, j \in \{x, y, z\}$). Another possible relationship between two operators A and B is for them to *commute*. That is,

$$[A, B] = AB - BA = 0. \tag{1.5}$$

It is possible for two matrices to neither commute nor anticommute, and, in fact, this is the generic case. Two commuting matrices can be simultaneously diagonalized. This means that we can measure the eigenvalue of one of them without disturbing the eigenvectors of the other. Conversely, if two operators do not commute, measuring one will disturb the eigenvectors of the other, so we cannot simultaneously measure non-commuting operators.

There is a natural complex inner product on quantum states. Given an orthonormal basis $|\psi_i\rangle$, the inner product between $|\alpha\rangle = \sum c_i |\psi_i\rangle$ and $|\beta\rangle = \sum d_i |\psi_i\rangle$ is

$$\langle\alpha|\beta\rangle = \sum c_i^* d_j \langle\psi_i|\psi_j\rangle = \sum c_i^* d_i. \tag{1.6}$$

Each ket $|\psi\rangle$ corresponds to a *bra* $\langle\psi|$ and the Hermitian adjoint is the adjoint with respect to this inner product, so $U|\psi\rangle$ corresponds to $\langle\psi|U^\dagger$. The operator $\sum |\psi\rangle\langle\phi|$ acts on the Hilbert space as follows:

$$\left(\sum |\psi\rangle\langle\phi|\right)|\alpha\rangle = \sum \langle\phi|\alpha\rangle\ |\psi\rangle\,. \tag{1.7}$$

The inner product can reveal a great deal of information about the structure of a set of states. For instance, $\langle\psi|\phi\rangle = 1$ if and only if $|\psi\rangle = |\phi\rangle$.

Eigenvectors of a Hermitian operator A with different eigenvalues are automatically orthogonal:

$$\langle\psi|A|\phi\rangle = \langle\psi|\left(A|\phi\rangle\right) = \lambda_\phi\langle\psi|\phi\rangle \tag{1.8}$$

$$= \left(\langle\psi|A\right)|\phi\rangle = \lambda_\psi^*\langle\psi|\phi\rangle\,. \tag{1.9}$$

Since the eigenvalues of A are real, it follows that $\langle\psi|\phi\rangle = 0$ whenever $\lambda_\phi \neq \lambda_\psi$. Conversely, if $\langle\psi|\phi\rangle = 0$, there exists a Hermitian operator for which $|\psi\rangle$ and $|\phi\rangle$ are eigenvectors with different eigenvalues.

We often want to consider a subsystem $\mathcal{A}$ of a quantum system $\mathcal{B}$. Since $\mathcal{A}$ may be entangled with the rest of the system, it is not meaningful to speak of the "state" of $\mathcal{A}$. If we write the state of $\mathcal{B}$ as $\sum |\psi_i\rangle|\phi_i\rangle$, where $|\psi_i\rangle$ is an orthonormal basis for $\mathcal{B}-\mathcal{A}$, and $|\phi_i\rangle$ are possible states for $\mathcal{A}$, then to an observer who only interacts with the subsystem $\mathcal{A}$, the subsystem appears to be in just one of the states $|\phi_i\rangle$ with some probability. $\mathcal{A}$ is said to be in a *mixed state* as opposed to the *pure state* of a closed system in a definite state.

We can extend the formalism to cover mixed states by introducing the *density matrix* ρ. For a pure system in the state $|\psi\rangle$, the density matrix is $|\psi\rangle\langle\psi|$. The density matrix for the subsystem for the entangled state above is $\sum |\phi_i\rangle\langle\phi_i|$. Density matrices are always positive and have $\operatorname{tr}\rho = 1$. To find the density matrix of a subsystem given the density matrix of the full system, simply trace over the degrees of freedom of the rest of the system.

Given a closed quantum system, time evolution preserves the inner product, so the time evolution operator U must be unitary. That is, $U^\dagger U = UU^\dagger = I$. An open system can be described as a subsystem of a larger closed system, so the evolution of the open system descends from the global evolution of the full system. Time evolution of the subsystem is described by some *superoperator* acting on the density matrix of the subsystem.

One fact about quantum states that has profound implications for quantum computation is that it is impossible to make a copy of an arbitrary unknown quantum state. This is known as the "No Cloning Theorem," [**?**] and is a consequence of the linearity of quantum mechanics. The proof is straightforward: Suppose we wish to have an operation that maps an arbitrary state

$$|\psi\rangle \to |\psi\rangle \otimes |\psi\rangle\,. \tag{1.10}$$

Then arbitrary $|\phi\rangle$ is mapped by

$$|\phi\rangle \to |\phi\rangle \otimes |\phi\rangle \tag{1.11}$$

as well. Because the transformation must be linear, it follows that

$$|\psi\rangle + |\phi\rangle \to |\psi\rangle \otimes |\psi\rangle + |\phi\rangle \otimes |\phi\rangle\,. \tag{1.12}$$

However,

$$|\psi\rangle \otimes |\psi\rangle + |\phi\rangle \otimes |\phi\rangle \neq (|\psi\rangle + |\phi\rangle) \otimes (|\psi\rangle + |\phi\rangle), \tag{1.13}$$

so we have failed to copy $|\psi\rangle + |\phi\rangle$. In general, if we pick an orthonormal basis, we can copy the basis states, but we will not have correctly copied superpositions of those basis states. We will instead have either measured the original system and therefore destroyed the superposition, or we will have produced a state that is entangled between the original and the "copy." This means that to perform quantum error correction, we cannot simply make backup copies of the quantum state to be preserved. Instead, we must protect the original from any likely error.

1.3 Introduction to Classical Coding Theory

Classical coding theory tends to concentrate on *linear codes*, a subclass of all possible codes with a particular relation between codewords. Suppose we wish to encode k bits using n bits. The data can be represented as a k-dimensional binary vector v. Because we are dealing with binary vectors, all the arithmetic is mod two. For a linear code, the encoded data is then Gv for some $n \times k$ matrix G (with entries from $\mathbf{Z}_2$), which is independent of v. G is called the *generator matrix* for the code. Its columns form a basis for the k-dimensional coding subspace of the n-dimensional binary vector space, and represent basis codewords. The most general possible codeword is an arbitrary linear combination of the basis codewords; thus the name "linear code."

Given a generator matrix G, we can calculate the dual matrix P, which is an $(n-k) \times n$ matrix of 0s and 1s of maximal rank $n-k$ with $PG = 0$. Since any codeword s has the form Gv, $Ps = PGv = 0v = 0$, and P annihilates any codeword. Conversely, suppose $Ps = 0$. Since P has rank $n-k$, it only annihilates a k-dimensional space spanned by the columns of G, and s must be a linear combination of these columns. Thus, $s = Gv$ for some v, and s is a valid codeword. The matrix P is called the *parity check matrix* for the code. It can be used to test if a given vector is a valid codeword, since $Ps = 0$ iff s is a codeword. The *dual code* is defined to be the code with generator matrix P^T and parity matrix G^T.

In order to consider the error-correcting properties of a code, it is useful to look at the *Hamming distance* between codewords. The Hamming distance between two vectors is the minimum number of bits that must be flipped to convert one vector to the other. The distance between a and b is equal to the *weight* (the number of 1s in the vector) of $a+b$. For a code to correct t single-bit errors, it must have distance at least $2t+1$ between any two codewords. A t bit error will take a codeword exactly distance t away from its original value, so when the distance between codewords is at least $2t+1$, we can distinguish errors on different codewords and correct them to the proper codewords. A code to encode k bits in n bits with minimum distance d is said to be an $[n, k, d]$ code.

Now suppose we consider a t bit error. We can write down a vector e to describe this vector by putting ones in the places where bits are flipped and zeros elsewhere. Then if the original codeword is s, after the error it is $s' = s + e$. If we apply the parity check matrix, we get

$$Ps' = P(s+e) = Ps + Pe = 0 + Pe = Pe, \tag{1.14}$$

so the value of Ps' does not depend on the value of s, only on e. If Pe is different for all possible errors e, we will be able to determine precisely what error occurred and fix it. Pe is called the *error syndrome*, since it tells us what the error is. Since $Pe = Pf$ iff $P(e-f) = 0$, to have a code of distance d, we need $Pe \neq 0$ for all vectors e of weight $d-1$ or less. Equivalently, any $d-1$ columns of P must be linearly independent.

We can place upper and lower bounds on the existence of linear codes to correct t errors. Each of the 2^k codewords has a *Hamming sphere* of radius t. All the words inside the Hamming sphere come from errors acting on the same codeword. For a code on n bits, there are n one-bit errors, $\binom{n}{2}$ two-bit errors, and in general $\binom{n}{j}$ j-bit errors. The Hamming spheres cannot overlap, but they must all fit inside the vector space, which only has 2^n elements. Thus,

$$\sum_{j=0}^{t} \binom{n}{j} 2^k \leq 2^n. \tag{1.15}$$

This is called the *Hamming bound* on $[n, k, 2t+1]$ codes. As n, k, and t get large, this bound approaches the asymptotic form

$$\frac{k}{n} \leq 1 - H\left(\frac{t}{n}\right), \tag{1.16}$$

where $H(x)$ is the *Hamming entropy*

$$H(x) = -x \log_2 x - (1-x)\log_2(1-x). \tag{1.17}$$

We can set a lower bound on the existence of $[n, k, 2t+1]$ linear codes as well, called the *Gilbert-Varshamov* bound. Suppose we have such a code (if necessary with $k = 0$) with

$$\sum_{j=0}^{2t} \binom{n}{j} 2^k < 2^n. \tag{1.18}$$

Then the spheres of distance $2t$ around each codeword do not fill the space, so there is some vector v that is at least distance $2t+1$ from each of the other codewords. In addition, $v+s$ (for any codeword s) is at least distance $2t+1$ from any other codeword s', since the distance is just $(v+s)+s' = v+(s+s')$, which is the

distance between v and the codeword $s + s'$. This means that we can add v and all the vectors $v + s$ to the code without dropping the distance below $2t + 1$. This gives us an $[n, k + 1, 2t + 1]$ code. We can continue this process until

$$\sum_{j=0}^{2t} \binom{n}{j} 2^k \geq 2^n. \tag{1.19}$$

Asymptotically, this becomes

$$\frac{k}{n} \geq 1 - H\left(\frac{2t}{n}\right). \tag{1.20}$$

Another case of great interest is the capacity of a classical channel. This is equal to the *efficiency* k/n of the most efficient code on an asymptotically large block that corrects measure one of the errors occuring. For instance, a common channel is the *binary symmetric channel*, where an error occurs independently on each bit with probability p for both 0 and 1. Shannon showed that channel capacity is just equal to one minus the entropy introduced by the channel [**?**]. For the binary symmetric channel, the entropy is just the Hamming entropy $H(p)$, so the capacity is $1 - H(p)$, coinciding with the Hamming bound for the expected number of errors $t = pn$. Shannon also showed that the capacity of a channel can be achieved by choosing codewords at random, then discarding only a few of them (measure zero asymptotically).

Bibliografía

[1] A. Church, "An unsolvable problem of elementary number theory," Amer. J. Math **58**, 345 (1936); A. M. Turing, "On computable numbers, with an application to the Entscheidungsproblem," Proc. Lond. Math. Soc. (2) **42**, 230 (1936) and Proc. Lond. Math. Soc. (2) **43**, 544 (1937).

[2] R. P. Feynman, "Simulating physics with computers," Int. J. Theor. Phys. **21**, 467 (1982).

[3] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," Proceedings, 35th Annual Symposium on Fundamentals of Computer Science, (1994).

[4] L. K. Grover, "A fast quantum mechanical algorithm for database search," Proceedings, 28th ACM Symposium on Theory of Computation, 212 (1996).

[5] C. B. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, "Strengths and weaknesses of quantum computing," quant-ph/9701001 (1997).

[6] J. I. Cirac and P. Zoller, "Quantum computations with cold trapped ions," Phys. Rev. Lett. **74**, 4091 (1995).

[7] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland, "Demonstration of a fundamental quantum logic gate," Phys. Rev. Lett. **75**, 4714 (1995).

[8] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble, "Measurement of conditional phase shifts for quantum logic," Phys. Rev. Lett. **75**, 4710 (1995).

[9] N. Gershenfeld and I. Chuang, "Bulk spin resonance quantum computation," Science **275**, 350 (1997).

[10] P. Shor, "Scheme for reducing decoherence in quantum memory," Phys. Rev. A **52**, 2493 (1995).

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

[12] C. Cohen-Tannoudji, *Quantum Mechanics*, Wiley, New York (1977).

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

[14] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nature **299**, 802 (1982).

[15] C. E. Shannon, "A mathematical theory of communication," Bell Sys. Tech. J. **27**, 379, 623 (1948).

[16] E. Knill and R. Laflamme, "A theory of quantum error-correcting codes," Phys. Rev. A **55**, 900 (1997).

[17] C. Bennett, D. DiVincenzo, J. Smolin, and W. Wootters, "Mixed state entanglement and quantum error correction," Phys. Rev. A **54**, 3824 (1996).

[18] L. Vaidman, L. Goldenberg, and S. Wiesner, "Error prevention scheme with four particles," Phys. Rev. A **54**, 1745R (1996).

[19] M. Grassl, Th. Beth, and T. Pellizzari, "Codes for the quantum erasure channel," quant-ph/9610042 (1996).

[20] D. W. Leung, M. A. Nielsen, I. L. Chuang, Y. Yamamoto, "Approximate quantum error correction can lead to better codes," quant-ph/9704002 (1997).

[21] D. Gottesman, "Class of quantum error-correcting codes saturating the quantum Hamming bound," Phys. Rev. A **54**, 1862 (1996).

[22] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction and orthogonal geometry," Phys. Rev. Lett. **78**, 405 (1997).

[23] E. Rains, "Quantum shadow enumerators," quant-ph/9611001 (1996).

[24] R. Laflamme, C. Miquel, J. P. Paz, and W. Zurek, "Pefect quantum error correction code," Phys. Rev. Lett. **77**, 198 (1996).

[25] D. Gottesman, "Pasting quantum codes," quant-ph/9607027 (1996).

[26] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," quant-ph/9608006 (1996).

[27] A. Steane, "Simple quantum error correcting codes," Phys. Rev. A **54**, 4741 (1996).

[28] A. Steane, "Quantum Reed-Muller codes, " quant-ph/9608026 (1996).

[29] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," Phys. Rev. A **54**, 1098 (1996).

[30] A. Steane, "Multiple particle interference and quantum error correction," Proc. Roy. Soc. Lond. A **452**, 2551 (1996).

[31] E. Knill, "Non-binary error bases and quantum codes," quant-ph/9608048 (1996); E. Knill, "Group representations, error bases and quantum codes," quant-ph/9608049 (1996).

[32] H. F. Chau, "Correcting quantum errors in higher spin systems," quant-ph/9610023 (1996)

[33] H. F. Chau, "Five quantum register error correction code for higher spin systems," quant-ph/9702033 (1997).

[34] D. Aharonov and M. Ben-Or, "Fault-tolerant quantum computation with constant error," quant-ph/9611025 (1996).

[35] E. Rains, "Nonbinary quantum codes," quant-ph/9703048 (1997).

[36] R. Cleve and D. Gottesman, "Efficient computations of encodings for quantum error correction," quant-ph/9607030 (1996).

[37] D. P. DiVincenzo, "Quantum gates and circuits," quant-ph/9705009 (1997).

[38] P. Shor, "Fault-tolerant quantum computation," quant-ph/9605011 (1996).

[39] D. DiVincenzo and P. Shor, "Fault-tolerant error correction with efficient quantum codes," Phys. Rev. Lett. **77**, 3260 (1996).

[40] D. Gottesman, "A theory of fault-tolerant quantum computation," quant-ph/9702029 (1997).

[41] C. H. Bennett, G. Brassard, C. Crepeau, R. Josza, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podalsky-Rosen channels," Phys. Rev. Lett. **70**, 1895 (1993).

[42] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels," Phys. Rev. Lett. **76**, 722 (1996).

[43] E. Knill, R. Laflamme, and D. Gottesman, in preparation.

[44] E. Knill, personal communication.

[45] E. Knill, R. Laflamme, and W. Zurek, "Accuracy threshold for quantum computation," quant-ph/9610011 (1996); E. Knill, R. Laflamme, and W. Zurek, "Resilient quantum computation: error models and thresholds," quant-ph/9702058 (1997).

[46] J. Evslin, S. Kakade, and J. P. Preskill, unpublished.

[47] A. M. Steane, "Active stabilization, quantum computation and quantum state synthesis," Phys. Rev. Lett. **78**, 2252 (1997).

[48] E. Knill and R. Laflamme, "Concatenated quantum codes," quant-ph/ 9608012 (1996).

[49] C. Zalka, "Threshold estimate for fault tolerant quantum computing," quant-ph/9612028 (1996).

[50] S. Lloyd, "The capacity of a noisy quantum channel," Phys. Rev. A **55**, 1613 (1997).

[51] B. Schumacher and M. A. Nielsen, "Quantum data processing and error correction," Phys. Rev. A **54**, 2629 (1996).

[52] H. Barnum, M. A. Nielsen, and B. Schumacher, "Information transmission through a noisy quantum channel," quant-ph/9702049 (1997).

[53] A. Ekert and C. Macchiavello, "Error correction in quantum communication," Phys. Rev. Lett. **77**, 2585 (1996).

[54] N. J. Cerf and R. Cleve, "Information-theoretic interpretation of quantum error-correcting codes," quant-ph/9702031 (1997).

[55] P. Shor and R. Laflamme, "Quantum analog of the MacWilliams identities for classical coding theory," Phys. Rev. Lett. **78**, 1600 (1997).

[56] E. M. Rains, "Quantum weight enumerators," quant-ph/9612015 (1996).

[57] E. M. Rains, "Polynomial invariants of quantum codes," quant-ph/9704042 (1997).

[58] R. Cleve, "Quantum stabilizer codes and classical linear vodes," quant-ph/9612048 (1996).

[59] C. H. Bennett, D. P. DiVincenzo, and J. A. Smolin, "Capacities of quantum erasure channels," quant-ph/9701015 (1997).

[60] C. Fuchs and J. Smolin, unpublished.

[61] P. Shor and J. Smolin, "Quantum error-correcting codes need not completely reveal the error syndrome," quant-ph/9604006 (1996).

[62] E. M. Rains, "Quantum codes of minimum distance two," quant-ph/ 9704043 (1997).

[63] E. M. Rains, R. H. Hardin, P. W. Shor, and N. J. A. Sloane, "A nonadditive quantum code," quant-ph/9703002 (1997).

[64] S. Lloyd, "Almost any quantum logic gate is universal," Phys. Rev. Lett. **75**, 346 (1995).

[65] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, "Elementary gates for quantum computation," Phys. Rev. A **52**, 3457 (1995).