Sparse-Graph Codes for Quantum Error-Correction

David J.C. MacKay
Cavendish Laboratory, Cambridge, CB3 0HE.
mackay@mrao.cam.ac.uk

Graeme Mitchison
M.R.C. Laboratory of Molecular Biology, Hills Road, Cambridge, CB2 2QH.
gjm@mrc-lmb.cam.ac.uk

Paul L. McFadden
Dept. Applied Maths and Theoretical Physics, Cambridge, CB3 0WA
p.l.mcfadden@damtp.cam.ac.uk

quant-ph/0304161 Version 7.7e

This is the extended version of a paper submitted to *IEEE Transactions on Information Theory* May 8, 2003; revised January 20th, 2004; accepted April 9th 2004; published volume 50, number 10, October 2004.

Indexing terms: Error-correction codes, probabilistic decoding, quantum error-correction.

Abstract

We present sparse-graph codes appropriate for use in quantum error-correction.

Quantum error-correcting codes based on sparse graphs are of interest for three reasons. First, the best codes currently known for classical channels are based on sparse graphs. Second, sparse-graph codes keep the number of quantum interactions associated with the quantum error-correction process small: a constant number per quantum bit, independent of the blocklength. Third, sparse-graph codes often offer great flexibility with respect to blocklength and rate.

We believe some of the codes we present are unsurpassed by previously published quantum error-correcting codes.

1 Introduction

Our aim in this paper is to create *useful* quantum error-correcting codes. To be useful, we think a quantum code must have a large blocklength, and it must be able to correct a large number of errors. From a theoretical point of view, we would especially like to find, for any rate R, a family of error-correcting codes with increasing blocklength N, such that, no matter how large N is, the number of errors that can be corrected is proportional to N. (Such codes are called 'good' codes.) From a practical point of view, however, we will settle for a lesser goal: to be able to make codes with blocklengths in the range 500–20,000 qubits and rates in the range 0.1–0.9 that can correct the largest number of errors possible.

While the existence of 'good' quantum error-correcting codes was proved by Calderbank and Shor (1996), their method of proof was non-constructive. Recently, a family of asymptotically good quantum codes based on algebraic geometry has been found by Ashikhmin *et al.* (2000) (see also Ling *et al.* (2001) and Matsumoto (2002)); however to the best of our knowledge no practical decoding algorithm (*i.e.*, an algorithm for which the decoding time is polynomial in the blocklength) exists for these codes. Thus, the task of constructing good quantum error-correcting codes for which there exists a practical decoder remains an open challenge.

This stands in contrast to the situation for classical error-correction, where practically-decodable codes exist which, when optimally decoded, achieve information rates close to the Shannon limit. Low-density parity-check codes (Gallager 1962; Gallager 1963) are an example of such codes. A regular low-density parity-check code has a parity-check matrix $\mathbf{H}$ in which each column has a small weight j (*e.g.*, $j = 3$) and the weight per row, k is also uniform (*e.g.*, $k = 6$). Recently low-density parity-check codes have been shown to have outstanding performance (MacKay and Neal 1996; MacKay 1999) and modifications to their construction have turned them into state-of-the-art codes, both at low rates and large blocklengths (Luby *et al.* 2001; Richardson *et al.* 2001; Davey and MacKay 1998) and at high rates and short blocklengths (MacKay and Davey 2000). The sparseness of the parity-check matrices makes the codes easy to encode and decode, even when communicating very close to the Shannon limit. It is worth emphasizing that the sum-product algorithm solves the decoding problem for low-density parity-check codes at noise levels far greater than the maximum noise level correctable by any code decoded by a traditional bounded-distance decoder.

This paper explores the conjecture that the best quantum error-correcting codes will be closely related to the best classical codes. By converting classical low-density parity-check codes into quantum codes, we hope to find families of excellent quantum codes.

Since the parity-check matrix is sparse, a quantum low-density parity-check code would have the additional attractive property that only a small number of interactions per qubit are required in order to determine the error that occurred. Moreover, since practical decoding algorithms have been found for classical low-density parity-check codes, it seems likely that a practical decoding algorithm will also exist for quantum low-density parity-check codes.

The Pauli matrices $\mathtt{X}$, $\mathtt{Y}$, and $\mathtt{Z}$

$$\mathtt{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathtt{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \mathtt{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{1}$$

have the actions

$$\begin{array}{rcl} \mathtt{X}(\alpha_0 |0\rangle + \alpha_1 |1\rangle) & = & \alpha_0 |1\rangle + \alpha_1 |0\rangle \\ \mathtt{Y}(\alpha_0 |0\rangle + \alpha_1 |1\rangle) & = & i(\alpha_0 |1\rangle - \alpha_1 |0\rangle) \\ \mathtt{Z}(\alpha_0 |0\rangle + \alpha_1 |1\rangle) & = & \alpha_0 |0\rangle - \alpha_1 |1\rangle ; \end{array} \tag{2}$$

thus $\mathtt{X}$ is a bit flip, $\mathtt{Z}$ is a phase flip, and $\mathtt{Y}$ (ignoring the phase factor i) is a combination of bit and phase flips. $\mathtt{X}$, $\mathtt{Y}$, and $\mathtt{Z}$ satisfy

$$\mathtt{X}^2 = \mathtt{I} \quad \mathtt{Y}^2 = \mathtt{I} \quad \mathtt{Z}^2 = \mathtt{I} \tag{3}$$

and

$$\begin{array}{ll} \mathtt{XY} = i\mathtt{Z} & \mathtt{YX} = -i\mathtt{Z} \\ \mathtt{YZ} = i\mathtt{X} & \mathtt{ZY} = -i\mathtt{X} \\ \mathtt{ZX} = i\mathtt{Y} & \mathtt{XZ} = -i\mathtt{Y}. \end{array} \tag{4}$$

Box 1. The Pauli operators.

In section 2 we review the *stabilizer formalism* for describing quantum error-correcting codes that encode a quantum state of K qubits in N qubits, and explain how a general stabilizer code is related to a classical binary code.

In section 3 we review sparse graph codes, in section 4 we discuss dual-containing sparse graph codes, and in section 4.6 we present several families of classical sparse graph codes that satisfy the constraints required to make a valid stabilizer code. The connection between graphs and quantum codes that we use is different from that explored in Schlingemann and Werner (2002) and Grassl *et al.* (2002).

In sections 5 and 6 we describe the experimental performance of our codes on three channels.

In this paper, we ignore the issue of *fault tolerance*: our codes correct errors in the encoded quantum state, assuming that the encoding and decoding circuits function perfectly.

2 Quantum Codes

We now review quantum error-correction and the connection between quantum codes and classical codes. For further reading on quantum codes, we direct the reader to the admirably clear accounts in (Lo *et al.* 2001: Chapter 5), (Preskill 2001: Chapter 7), and (Steane 2001). Boxes 1 and 2 review our notation and conventions.

The analogue of a classical bit is a *qubit*, a quantum state $|\psi\rangle$ in a two-dimensional complex

A Pauli operator on N qubits has the form $cO_1O_2\ldots O_N$, where each O_i is one of `I`, `X`, `Y`, or `Z` and $c = 1, -1, i$ or $-i$. This operator takes $|i_1 i_2 \ldots i_N\rangle$ to $cO_1 |i_1\rangle \otimes O_2 |i_2\rangle \otimes \ldots \otimes O_N |i_N\rangle$. So for instance `IXZ`$(|000\rangle + |111\rangle) = |010\rangle - |101\rangle$. For convenience, we will also sometimes employ a shorthand notation for representing Pauli operators, in which only the non-identity O_i are given; for example `IXIZI` is denoted by $\mathtt{X}_2\mathtt{Z}_4$.

Two Pauli operators *commute* if and only if there is an even number of places where they have different Pauli matrices neither of which is the identity `I`. This follows from the relations (3) and (4). Thus for example `XXI` and `IYZ` do not commute, whereas `XXI` and `ZYX` do commute. If two Pauli operators do not commute, they anticommute, since their individual Pauli matrices either commute or anticommute.

Box 2. Pauli operators on N qubits. We reserve the typewriter font (*e.g.*, `X`) for operators that act on a single qubit.

vector space H_2 which can be written

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle \tag{5}$$

with α_0, α_1 complex numbers satisfying $|\alpha_0|^2 + |\alpha_1|^2 = 1$. $|\psi\rangle$ is determined up to a phase factor $e^{i\theta}$, so $|\psi\rangle$ and $e^{i\theta} |\psi\rangle$ define the same state.

The quantum state of K qubits has the form $\sum \alpha_{\mathbf{s}} |\mathbf{s}\rangle$, where $\mathbf{s}$ runs over all binary strings of length K, so there are 2^K complex coefficients $\alpha_{\mathbf{s}}$, all independent except for the normalization constraint

$$\sum_{\mathbf{s}=000\ldots00}^{111\ldots11} |\alpha_{\mathbf{s}}|^2 = 1. \tag{6}$$

For instance, $\alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle$, with $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$ is the general 2-qubit state (where $|00\rangle$ is shorthand for the tensor product $|0\rangle \otimes |0\rangle$).

Whereas a classical binary (N, K) code protects a *discrete-valued* message $\mathbf{s}$ taking on one of 2^K values by encoding it into one of 2^K discrete codewords of length N bits, quantum error correction has a much tougher job: the quantum state of K qubits is specified by 2^K *continuous-valued* complex coefficients $\alpha_{\mathbf{s}}$, and the aim is to encode the state into a quantum state of N qubits in such a way that errors can be detected and corrected, and all 2^K complex coefficients perfectly restored, up to a phase factor.

The errors that must be corrected include continuous errors corresponding to unitary rotations in the quantum state space, and errors in which an accidental 'measurement' causes the quantum state to collapse down into a subspace. As an example of a continuous error, if one qubit is physically embodied in the spin of a particle, an environmental magnetic field might induce a rotation of the spin through some arbitrary angle. This rotation of the spin corresponds to a unitary transformation of the quantum state vector. It might seem impossible to correct such errors, but it is one of the triumphs of quantum information theory that, when the state is suitably encoded, error correction is possible.

Consider the following encoding of a single qubit in three qubits:

$$\begin{aligned} |\bar{0}\rangle &= \tfrac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \\ |\bar{1}\rangle &= \tfrac{1}{\sqrt{2}}(|000\rangle - |111\rangle), \end{aligned} \tag{7}$$

(where the bar denotes the encoded state). A general state of one qubit, $\alpha_0 |0\rangle + \alpha_1 |1\rangle$, is encoded into $\alpha_0 |\bar{0}\rangle + \alpha_1 |\bar{1}\rangle$. We will show that the receiver can detect and correct single qubit flips if he measures two diagnostic operators `ZZI` and `IZZ`, which we call the quantum syndrome. (These two observables commute, so they can both be measured simultaneously.) Imagine that the first qubit undergoes a flip $|0\rangle \leftrightarrow |1\rangle$, so $\alpha_0 |\bar{0}\rangle + \alpha_1 |\bar{1}\rangle$ becomes $\alpha_0 \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle) + \alpha_1 \frac{1}{\sqrt{2}}(|100\rangle - |011\rangle)$. Now, measuring `ZZI` gives -1, and `IZZ` gives $+1$, for any value of the coefficients α_0 and α_1. The four possible outcomes of ± 1 for the two operators correspond to the three possible bit-flips and to no flip. Thus measuring the observables `ZZI` and `IZZ` gives an error diagnosis analogous to the classical syndrome. As in the classical case, the appropriate correction can be made after syndrome measurement. In the above example, one applies the bit-flip operator `X` to the first qubit, thus restoring the state to $\alpha_0 |\bar{0}\rangle + \alpha_1 |\bar{1}\rangle$.

Now consider an error that lies in the continuum of rotations: the operator $(\cos\theta)\mathtt{I} + i(\sin\theta)\mathtt{X}$ applied to the first qubit in the encoded state. For simplicity, we assume the encoded state is $|\bar{0}\rangle$; the error operator takes $|\bar{0}\rangle$ to

$$\frac{1}{\sqrt{2}} \left[(\cos\theta |0\rangle + i \sin\theta |1\rangle) |00\rangle + (i \sin\theta |0\rangle + \cos\theta |1\rangle) |11\rangle \right]. \tag{8}$$

Measuring the syndrome operators `ZZI` and `IZZ` causes the state to collapse onto the original encoded state $|\bar{0}\rangle$ with probability $\cos^2\theta$ or onto the bit-flipped state $|100\rangle + |011\rangle$ with probability $\sin^2\theta$. In the former case we get the syndrome $(+1,+1)$, and in the latter $(-1,+1)$, so the appropriate correction can be applied. Exactly the same collapse-and-correct procedure works if one has a general encoded qubit $\alpha_0 |\bar{0}\rangle + \alpha_1 |\bar{1}\rangle$. Thus, for a cunning choice of syndrome measurement, collapse in effect 'picks' a discrete error, and allows one to think of bit flips much as one does in classical error-correction.

However, bit flips are not the only types of error that can occur in quantum states. In a 'phase flip', which corresponds to the application of `Z` to a qubit, the coefficient of $|0\rangle$ remains unchanged but the sign of the coefficient of $|1\rangle$ is switched. In the above example, the encoded state $|\bar{0}\rangle$ would be taken to $|\bar{1}\rangle$ (and vice versa) by a phase flip of any of its qubits:

$$\mathtt{Z}_n |\bar{0}\rangle = \frac{1}{\sqrt{2}} \mathtt{Z}_n (|000\rangle + |111\rangle) = \frac{1}{\sqrt{2}} (|000\rangle - |111\rangle) = |\bar{1}\rangle \quad \text{for } n = 1, 2, \text{ or } 3, \tag{9}$$

and this error could not be corrected since the corrupted state is a codeword.

The first quantum code able to correct both bit and phase flips was discovered by Shor (1995), and it encodes a single qubit in nine qubits:

$$\begin{aligned} |\bar{0}\rangle &= \frac{1}{\sqrt{8}} (|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle) \\ |\bar{1}\rangle &= \frac{1}{\sqrt{8}} (|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle), \end{aligned} \tag{10}$$

Here, a single bit flip in the first three qubits can be detected by measuring $\mathtt{Z}_1\mathtt{Z}_2$, $\mathtt{Z}_2\mathtt{Z}_3$ (as in the previous code we considered), and similarly $\mathtt{Z}_4\mathtt{Z}_5$, $\mathtt{Z}_5\mathtt{Z}_6$, $\mathtt{Z}_7\mathtt{Z}_8$ and $\mathtt{Z}_8\mathtt{Z}_9$ detect a bit flip in the remaining qubits. But one can also detect phase flips, by measuring `XXXXXXIII` and `IIIXXXXXX`, and these two diagnostic operators together with the six `Z`-containing ones above form a commuting set which can therefore be measured simultaneously. Note that the outcomes of the `X` measurements do not determine which of the qubits in each block of three underwent a phase flip, but this knowledge is unnecessary for correcting the state, because changing the sign of a particular qubit in the block corrects a sign change of any one of the three. Note also that a combined bit and phase flip on the same qubit, a `Y` error, can be detected and corrected. For instance, a `Y` error on the first qubit gives a -1 on measuring $\mathtt{Z}_1\mathtt{Z}_2$ and `XXXXXXIII`, and $+1$ for all the other operators.

As any unitary transformation on one qubit can be written as a weighted sum of `I`, `X`, `Y`, and `Z` (because these four operators span the space of 2×2 matrices), it follows that any error of this unitary type on one qubit can be corrected. Furthermore, more general errors, measurements for instance, can be represented as sums of these operators.

Suppose, for example, an interaction with the environment has the effect of a measurement of the observable $\mathtt{M} = (\cos\theta)\mathtt{Z} + (\sin\theta)\mathtt{X}$ on the first qubit. Let the projections corresponding to the eigenvalues $+1$ and -1 be `P` and `Q`, respectively. Then $\mathtt{P} + \mathtt{Q} = \mathtt{I}$ and $\mathtt{P} - \mathtt{Q} = \mathtt{M}$, so the projection onto the $+1$ eigenspace is $(\mathtt{I} + \mathtt{M})/2$. Thus, if the measurement outcome (which is not known to us) is $+1$, the projection takes an encoded state $|\psi\rangle$ to the state

$$\left|\tilde{\psi}\right\rangle = \mathcal{N}(\mathtt{I}_1 + \cos\theta\mathtt{Z}_1 + \sin\theta\mathtt{X}_1)\,|\psi\rangle\,, \tag{11}$$

where $\mathcal{N}$ is a normalization constant. When all eight diagnostic operators are measured, the probabilities of the various syndromes are as shown in table 3. Having diagnosed the error that is present after syndrome measurement, it can be corrected, despite the fact that the original error in this case was not even a unitary transformation.

The foregoing examples all involve an error on one qubit only. An error operator that affects several qubits can be written as a weighted sum $\sum c_\alpha P_\alpha$ of Pauli operators acting on those qubits and acting as the identity on other qubits. (A general operator on k qubits can be written as such a sum because the 4^k possible Pauli operators span the space of $2^k \times 2^k$ complex matrices.) Given such an error and a codeword $|\psi\rangle$, a suitable set of diagnostic operators will 'pick' an individual error term $P_{\tilde{\alpha}}\,|\psi\rangle$ from the sum, and an error correction procedure applied to this term will restore the original codeword.

An error may act not only on the code qubits but on the environment too. Given an initial state that is a product $|\psi\rangle\,|\phi\rangle^e$ of code qubits and environmental variables, any error acting on both the code and the environment can be written as a weighted sum $\sum c_{\alpha,\beta} P_\alpha P^e_\beta$ of Pauli operators that act on code and environment qubits. If S_i are diagnostic operators that pick the error term $P_{\tilde{\alpha}}\,|\psi\rangle$, then the operators $S_i I^e$ will pick terms $\sum_{\tilde{\beta}} c_{\tilde{\alpha},\tilde{\beta}} P_{\tilde{\alpha}}\,|\psi\rangle\,P^e_{\tilde{\beta}}\,|\phi\rangle^e$ from the corrupted state, and these terms can be written as $(P_{\tilde{\alpha}}\,|\psi\rangle)\,|\mu\rangle^e$ for some new environmental state $|\mu\rangle^e$. So measuring the syndrome restores a product state of qubits and environment, and in this sense the code and the environment evolve independently and we may ignore the

	Error:	$\mathtt{I}_1$	$\mathtt{X}_1$	$\mathtt{Z}_1$
	Probability:	$\frac{1}{2}$	$\frac{1}{2}\sin^2\theta$	$\frac{1}{2}\cos^2\theta$
Stabilizer		Syndrome		
ZZIIIIIII		+1	−1	+1
IZZIIIIII		+1	+1	+1
IIIZZIIII		+1	+1	+1
IIIIZZIII		+1	+1	+1
IIIIIIZZI		+1	+1	+1
IIIIIIIZZ		+1	+1	+1
XXXXXXIII		+1	+1	−1
IIIXXXXXX		+1	+1	+1

Table 3. The stabilizers for the Shor code and the syndromes corresponding to particular error operators, together with their probabilities.

environment in what follows.

2.1 Stabilizer codes

The scene is now set to define a general way of making quantum codes: the stabilizer framework. A stabilizer is essentially what we have been calling a 'diagnostic operator'. We now begin with a set of such operators and use it to define a code.

A stabilizer group $\mathcal{S}$ consists of a set of Pauli operators on N qubits closed under multiplication, with the property that any two operators in the set commute, so that all can be measured simultaneously. It is enough to check this commutation property on a set of generators of $\mathcal{S}$, i.e., on a set $\{S_i\}$ that generate all of $\mathcal{S}$ under multiplication. For instance, we could take the diagnostic operators associated with the Shor code (see table 3) as generators for a set of stabilizers $\mathcal{S}$. The full set $\mathcal{S}$ will include operators like ZIZIIIIII (the product of the first two generators) and YYXXXXIII (the product of the first and seventh), and so on.

Given a set of stabilizers, a codeword is defined to be a state $|\psi\rangle$ that is a +1 eigenstate of all the stabilizers, so

$$S_i |\psi\rangle = |\psi\rangle \text{ for all } i. \tag{12}$$

Consider what the codewords of the stabilizers shown in table 3 must be. If $|\psi\rangle = \sum_{\mathbf{s}} \alpha_{\mathbf{s}} |\mathbf{s}\rangle$, equation (12) applied to the first two stabilizers in the table implies that the first three bits in any binary string $\mathbf{s}$ in the sum must be 000 or 111, and the same is true for the two other groups of three. From the last two stabilizers in the table, we deduce that strings $\mathbf{s}$ with an odd number of 1s all have equal coefficients $\alpha_{\mathbf{s}}$, and similarly for those with an even number of 1s. It follows that the code is generated by $|\bar{0}\rangle$ and $|\bar{1}\rangle$ given by equation (10). Thus we recover the original Shor code.

Consider now a set of error operators $\{E_\alpha\}$, i.e. Pauli operators taking a state $|\psi\rangle$ to the corrupted state $E_\alpha |\psi\rangle$. A given operator E_α either commutes or anticommutes with each stabilizer generator S_i (see Box 2). If E_α commutes with S_i then

$$S_i E_\alpha |\psi\rangle = E_\alpha S_i |\psi\rangle = E_\alpha |\psi\rangle , \tag{13}$$

so $E_\alpha |\psi\rangle$ is a $+1$ eigenstate of S_i. Similarly, if it anticommutes, $E_\alpha |\psi\rangle$ is a -1 eigenstate of S_i. Thus $E_\alpha |\psi\rangle$ is an eigenstate of the joint measurement of all the stabilizer generators, and the outcome of this measurement – the syndrome – is completely determined by the commutation properties of E_α with the stabilizers. Thus the syndrome is determined by the error operator and is independent of the state $|\psi\rangle$, which implies that we learn nothing about the state in measuring the syndrome. This is important since, in quantum mechanics, a state is usually damaged when a measurement yields information about it.

A sufficient condition for the set of error operators $\{E_\alpha\}$ to be *correctable* is that each operator of the set should have a distinct syndrome, so the syndrome determines the index α. Correction can then be performed by applying the specific E_α to the corrupted state, since E_α^2 is the identity operator up to some phase factor. A set of error operators $\{E_\alpha\}$ is also correctable if any two operators E_α and E_β that have the same syndrome differ by a stabilizer. Thus $E_\alpha^\dagger E_\beta$ is a stabilizer, S say, so $E_\beta = E_\alpha S$. Then $E_\beta |\psi\rangle = E_\alpha S |\psi\rangle = E_\alpha |\psi\rangle$, so E_α and E_β generate the same corrupted state and can therefore be corrected by the same operator.

An error arising from any linear combination of operators from a correctable set of Pauli operators $\{E_\alpha\}$ can be corrected. Just as in the example of the Shor code, syndrome measurement collapses the state onto one of the syndrome eigenspaces, and the original state can then be restored.

Most realistic error mechanisms will generate linear combinations that include uncorrectable error operators. For instance, consider an error process $\mathcal{E}_{\mathtt{U}}$ in which each qubit experiences an independent perturbation, undergoing a unitary transformation

$$\mathtt{U} = (1 - p^2 - q^2 - r^2)^{1/2}\mathtt{I} + ip\mathtt{X} + iq\mathtt{Y} + ir\mathtt{Z}, \tag{14}$$

where p, q and r are small real numbers. Starting from an encoded state $|\psi\rangle$, the perturbed state includes terms $c_\alpha E_\alpha |\psi\rangle$ for every possible Pauli operator E_α. There will be many uncorrectable operators amongst them, but if the code is well-chosen for the given error model, the coefficients c_α will be small for these particular operators.

Suppose that p, q and r are chosen from a distribution $P(x)$ that is symmetric about zero, so $P(x) = P(-x)$. If ρ is the density matrix for the state of a single qubit, its state $\tilde{\rho}$ after $\mathtt{U}$ is applied is

$$\tilde{\rho} = \int P(p)P(q)P(r)\mathtt{U}\rho\mathtt{U}^\dagger dp\, dq\, dr. \tag{15}$$

The symmetry of P ensures that cross-terms like $\mathtt{X}\rho\mathtt{Y}$ are zero, so

$$\tilde{\rho} = (1 - 3u)\rho + u\left[\mathtt{X}\rho\mathtt{X} + \mathtt{Y}\rho\mathtt{Y} + \mathtt{Z}\rho\mathtt{Z}\right], \tag{16}$$

where $u = \int x^2 P(x)\, dx$. This noise model is known as the depolarizing channel.

Thus the error caused when U, with randomly chosen p, q and r, is applied to a qubit is indistinguishable, by any quantum mechanical measurement, from a random process that leaves the state unchanged with probability $1 - 3u$ or applies X, Y or Z with probability u.

It follows that the error process $\mathcal{E}_{\mathtt{U}}$, which applies U independently to each qubit, is indistinguishable from a process that applies one of X, Y or Z with probability u to each qubit, despite the very different characters of the two underlying mechanisms. We can either think of errors being caused by the presence of uncorrectable terms $c_\alpha E_\alpha |\psi\rangle$ when each qubit is given a small perturbation by U, or by the chance occurrence of an uncorrectable combination of bit or phase flips. The latter process closely resembles a classical bit-flip error process. We now make the analogy between quantum and classical codes more precise.

2.2 The relationship between quantum and classical codes

Given any Pauli operator on N qubits, we can write it uniquely as a product of an X-containing operator and a Z-containing operator and a phase factor ($+1$, -1, i, or $-i$). For instance,

$$\mathtt{XIYZYI} = \begin{matrix} -(\mathtt{XIXIXI})\times \\ (\mathtt{IIZZZI}). \end{matrix} \tag{17}$$

We now express the X operator as a binary string of length N, with '1' standing for X and '0' for I, and do the same for the Z operator. Thus each stabilizer can be written as the X string followed by the Z string, giving a matrix of width $2N$. We mark the boundary between the two types of strings with vertical bars, so, for instance, the set of generators in table 3 appears as the matrix $\mathbf{A}$, where

$$\mathbf{A} = \left(\begin{array}{ccccccccc|ccccccccc} & & & & \mathtt{X} & & & & & & & & & \mathtt{Z} & & & & \\ 1&1&1&1&1&1&0&0&0 & 0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&1&1&1&1&1 & 0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0 & 1&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0 & 0&1&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0 & 0&0&0&1&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0 & 0&0&0&0&1&1&0&0&0 \\ 0&0&0&0&0&0&0&0&0 & 0&0&0&0&0&0&1&1&0 \\ 0&0&0&0&0&0&0&0&0 & 0&0&0&0&0&0&0&1&1 \end{array}\right). \tag{18}$$

The commutativity of stabilizers now appears as orthogonality of rows with respect to a *twisted product* (also known as a symplectic product): if row m is $r_m = (x_m, z_m)$, where x_m is the X binary string and z_m the Z string, then the twisted product $\odot$ of rows m and m' is

$$r_m \odot r_{m'} = x_m \cdot z_{m'} + x_{m'} \cdot z_m \mod 2, \tag{19}$$

where '$\cdot$' is the usual dot product, $x_m \cdot z_{m'} = \sum_i x_{mi} z_{m'i}$. The twisted product is zero if and only if there is an even number of places where the operators corresponding to rows m and m' differ (and are neither the identity), i.e., if the operators commute. If we write $\mathbf{A}$ as $\mathbf{A} = (\mathbf{A}_1|\mathbf{A}_2)$, then the condition $r_m \odot r_{m'} = 0$ for all m and m' can be written compactly as

$$\mathbf{A}_1 \mathbf{A}_2^{\mathsf{T}} + \mathbf{A}_2 \mathbf{A}_1^{\mathsf{T}} = \mathbf{0}. \tag{20}$$

A Pauli error operator E can be interpreted as a binary string $\mathbf{e}$ of length $2N$. Our convention is that we reverse the order of the `X` and `Z` strings in the error operator, so, for instance the binary string

$$100000001 \,|\, 010000001$$

(with a '|' inserted for interpretational convenience), corresponds to the operator $\mathtt{Z}_1\mathtt{X}_2\mathtt{Y}_9$. With this convention, the ordinary dot product (mod 2) of $\mathbf{e}$ with a row of the matrix is zero if E and the stabilizer for that row commute, and 1 otherwise. Thus the quantum syndrome for the noise is exactly the classical syndrome $\mathbf{Ae}$, regarding $\mathbf{A}$ as a parity check matrix and $\mathbf{e}$ as binary noise.

We can now define the conditions for error correction in this classical setting. If there is a set of binary noise vectors $\{\mathbf{e}_\alpha\}$ that have distinct syndromes, then the errors are correctable, and so are the corresponding errors in the quantum code. However, we also know the errors are correctable under the relaxed requirement that any operators E_α and E_β with the same syndrome differ by a stabilizer. Any stabilizer S_α in $\mathcal{S}$ can be written as a product of some subset of the generator set $\{S_i\}$, and S_α is equivalent to a binary string generated by adding rows of $\mathbf{A}$, in other words to an element of the dual code generated by $\mathbf{A}$.

This more lax requirement applies to the Shor code shown above. The binary strings

$$\begin{array}{r|l} 100000000 & 000000000 \\ 010000000 & 000000000 \end{array}$$

have the same syndrome, but they differ by an element of the dual code, namely the stabilizer $\mathtt{Z}_1\mathtt{Z}_2$.

In conclusion, the properties of stabilizer codes can be inferred from those of a special class of classical codes. Given any binary matrix of size $M_Q \times 2N$ that has the property that the twisted product of any two rows is zero, an equivalent quantum code can be constructed that encodes $N - M_Q$ qubits in N qubits. If there is a set of errors for the classical code that are uniquely characterized by their syndromes, or differ by an element of the dual code if they have the same syndrome, then the corresponding error operators in the quantum code can be corrected.

2.3 Examples of stabilizer codes

2.3.1 Cyclic codes

An elegant $(N, K) = (5, 1)$ quantum code is generated by the four stabilizers given below alongside their equivalent matrix:

$$\begin{array}{l} \text{Stabilizers} \\ \texttt{XZZXI} \\ \texttt{IXZZX} \\ \texttt{XIXZZ} \\ \texttt{ZXIXZ} \end{array} \qquad \mathbf{A} = \left(\begin{array}{ccccc|ccccc} & & \texttt{X} & & & & & \texttt{Z} & & \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right). \tag{21}$$

All the twisted product of rows in $\mathbf{A}$ vanish, so $\mathbf{A}$ defines a commuting set of stabilizers and hence a quantum code. A correctable set of errors consists of all operators with one non-identity term, *e.g.* `XIIII`, `IIIYI` or `IZIII`. These correspond to binary strings such as 00000|10000 for `XIIII`, 00010|00010 for `IIIYI`, and so on. There are 15 of these, and each has a distinct syndrome, thereby using up all the $2^4 - 1$ possible non-zero syndromes. This is therefore a perfect quantum code.

If one adds a fifth row 00101|11000 to $\mathbf{A}$, so that the `X` and `Z` submatrices are cyclic, the fifth row is redundant, being the sum of the other four rows (its stabilizer is the product of the other four).

2.3.2 CSS codes

An important class of codes, invented by Calderbank, Shor & Steane (Calderbank and Shor 1996; Steane 1996), has the form

$$\mathbf{A} = \left(\begin{array}{c|c} \mathbf{H} & \mathbf{0} \\ \mathbf{0} & \mathbf{G} \end{array}\right), \tag{22}$$

where $\mathbf{H}$ and $\mathbf{G}$ are $M \times N$ matrices. Requiring $\mathbf{H}\mathbf{G}^{\mathrm{T}} = \mathbf{0}$ ensures that (20) is satisfied. As there are $M_Q = 2M$ stabilizer conditions applying to N qubit states, $N - 2M$ qubits are encoded in N qubits.

2.3.3 CSS codes based on dual-containing codes.

If $\mathbf{H} = \mathbf{G}$, $\mathbf{A}$ has the particularly simple form

$$\mathbf{A} = \left(\begin{array}{c|c} \mathbf{H} & \mathbf{0} \\ \mathbf{0} & \mathbf{H} \end{array}\right). \tag{23}$$

Equation (20) is satisfied if $\mathbf{H}\mathbf{H}^{\mathsf{T}} = \mathbf{0}$. This is equivalent to $\mathcal{C}^{\perp}(\mathbf{H}) \subset \mathcal{C}(\mathbf{H})$, where $\mathcal{C}(\mathbf{H})$ is the code having $\mathbf{H}$ as its parity check matrix and $\mathcal{C}(\mathbf{H})^{\perp}$ is its dual code. We call such a code a 'dual-containing' code; it is the type of code we are most concerned with in this paper. (Dual-containing codes are also known as 'weakly self-dual codes'.)

Any state of the form

$$|\psi\rangle = \sum_{\mathbf{x}\in\mathcal{C}^{\perp}(\mathbf{H})} |\mathbf{x}+\mathbf{y}\rangle\,, \tag{24}$$

with $\mathbf{y} \in \mathcal{C}(\mathbf{H})$ and '+' denoting addition mod 2, is a codeword. This is because each X-stabilizer S permutes the terms in the sum, so $S\,|\psi\rangle = |\psi\rangle$, and the Z-stabilizers leave each term in the sum unchanged, since the dual-containing property implies that $\mathbf{x}+\mathbf{y}$ is a codeword of $\mathcal{C}(\mathbf{H})$ if $\mathbf{x} \in \mathcal{C}^{\perp}(\mathbf{H})$ and $\mathbf{y} \in \mathcal{C}(\mathbf{H})$. The most general codeword has the form

$$|\psi\rangle = \sum_{\mathbf{y}\in\mathcal{C}(\mathbf{H})} \alpha_{\mathbf{y}} \sum_{\mathbf{x}\in\mathcal{C}^{\perp}(\mathbf{H})} |\mathbf{x}+\mathbf{y}\rangle\,. \tag{25}$$

An example of a dual-containing code is Steane's 7 qubit code, defined by the Hamming code

$$\mathbf{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}. \tag{26}$$

The rows have an even number of 1s, and any two of them overlap by an even number of 1s, so $\mathcal{C}^{\perp}(\mathbf{H}) \subset \mathcal{C}(\mathbf{H})$. Here $M = 3$, $N = 7$, so $N - 2M = 1$, and thus 1 qubit is encoded in 7 qubits.

2.3.4 Codes over GF(4)

Let the elements of GF(4) be 0, 1, w and $w^2 = \bar{w} = 1 + w$. One can write a row $r_1 = a_1a_2\ldots a_n|b_1b_2\ldots b_n$ in the binary string representation as a vector over GF(4), $\rho_1 = (a_1 + b_1w, a_2 + b_2w, \ldots, a_n + b_nw)$. Given a second row $r_2 = c_1c_2\ldots c_n|d_1d_2\ldots d_n$, with $\rho_2 = (c_1 + d_1w, c_2 + d_2w, \ldots, c_n + d_nw)$, the Hermitian inner product is defined by

$$\rho_1 \cdot \rho_2 = \sum_i (a_i + b_i\bar{w})(c_i + d_iw) = \sum_i \left[(a_ic_i + b_id_i + b_ic_i) + (a_id_i + b_ic_i)w\right]. \tag{27}$$

Now the coefficient of w on the right-hand side of this equation is

$$(a_id_i + b_ic_i) = r_1 \odot r_2 \tag{28}$$

so if the Hermitian inner product of two rows is zero then $r_1 \odot r_2 = 0$ (though the converse does not hold). Thus a code over GF(4) that contains its Hermitian dual defines a stabilizer code, since we can interpret its rows as binary strings whose twisted products vanish (Calderbank *et al.* 1997). However, not all stabilizer codes can be obtained from GF(4) codes in this way, since, as we have just noted, $r_1 \odot r_2 = 0$ does not imply that the Hermitian product $\rho_1 \cdot \rho_2$ is zero.

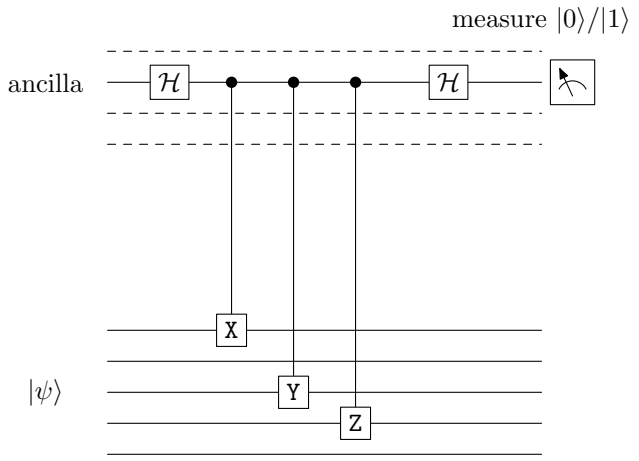


Figure 4. Measuring the syndrome of a quantum code. There is an ancilla for each stabilizer. Here the operations for an ancilla corresponding to the stabilizer $S_\alpha = \texttt{XIYZI}$ are shown. The black dot on the ancilla's line indicates that the ancilla controls the operator (e.g. `X`) in the attached box acting on the state $|\psi\rangle$ to be decoded. The boxes labelled '$\mathcal{H}$' carry out Hadamard transforms on the ancilla.

2.4 A quantum circuit for decoding

We consider decoding first as this can be carried out by circuits that are quite simple. In the circuit shown in figure 4, an extra line, corresponding to an additional ancillary qubit, controls a set of operations on the encoded qubits. Here, 'control' means that when the ancilla is $|0\rangle$, no operation is performed on the encoded qubits, and when the ancilla is $|1\rangle$ the operation shown in the box (`X`, `Y` or `Z`) is carried out. Taken together, the individual controlled operations correspond to a controlled stabilizer operator S_α^c on N qubits, and in the figure the stabilizer S_α is assumed to be `XIYZI`.

An initial and final Hadamard operation

$$\mathcal{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{29}$$

is carried out on the ancilla. The effect of this is that a final measurement of the ancilla in a $|0\rangle\,/\,|1\rangle$ basis gives outcome 0 when S_α has outcome $+1$, and 1 when S_α has outcome -1. This follows because

$$\begin{aligned}
(\texttt{I}\otimes\mathcal{H})S_\alpha^c(\texttt{I}\otimes\mathcal{H})\,|\psi\rangle\,|0\rangle &= (\texttt{I}\otimes\mathcal{H})S_\alpha^c\,|\psi\rangle\,(|0\rangle+|1\rangle)/\sqrt{2} && (30)\\
&= (\texttt{I}\otimes\mathcal{H})(|\psi\rangle\,|0\rangle + S_\alpha\,|\psi\rangle\,|1\rangle)/2 && (31)\\
&= [|\psi\rangle\,(|0\rangle+|1\rangle) + S_\alpha\,|\psi\rangle\,(|0\rangle-|1\rangle)]\,/2 && (32)\\
&= \frac{1}{2}(\texttt{I}+S_\alpha)\,|\psi\rangle\,|0\rangle + \frac{1}{2}(\texttt{I}-S_\alpha)\,|\psi\rangle\,|1\rangle\,, && (33)
\end{aligned}$$

and thus measuring the ancilla projects $|\psi\rangle$ onto the eigenstates of S_α.

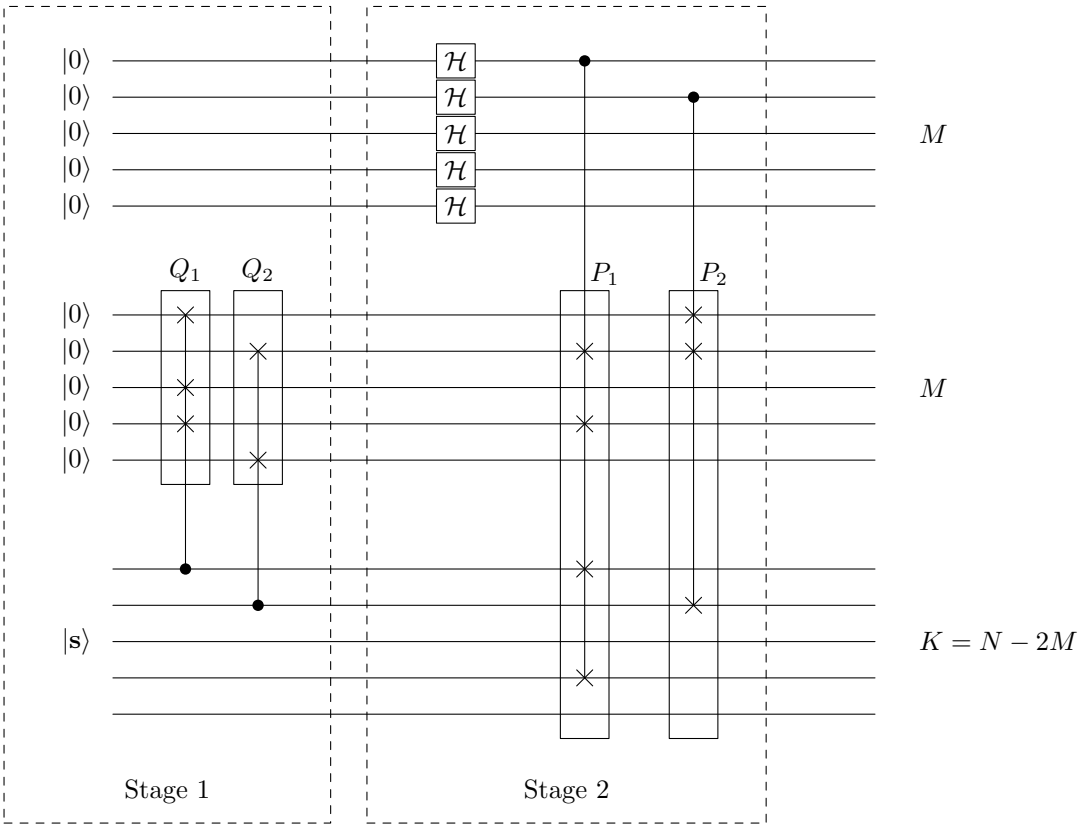


Figure 5. Encoding a quantum state. The first stage applies a series of controlled operations that carry out multiplication by the matrix $\mathbf{Q}$. This means that the kth box, Q_k, controlled by the kth qubit in the last $K = N - 2M$ qubits, has a cNOT at the mth qubit within the box if and only if the kth column of $\mathbf{Q}$ has a 1 in its mth position, i.e., $Q_{mk} = 1$. The second stage adds the *rows* of $\mathbf{P}$ to the last $N - M$ qubits by applying cNOT operations at all positions where the mth row of $\mathbf{P}$ has a 1. Thus the box labelled P_m applies cNOTs where the mth row of $\mathbf{P}$ has a 1, and is controlled by the mth qubit in the top block of M qubits.

2.5 A quantum circuit for encoding

We show now how to encode, in the case of a dual-containing code defined by a full rank matrix $\mathbf{H}$, with $N > 2M$. We call the number of source qubits $K = N - 2M$. First, some algebra:

A set of row operations plus reordering of columns allows $\mathbf{H}$ to be transformed to $\tilde{\mathbf{H}} = [\mathbf{I}, \mathbf{P}]$, where the notation indicates that the $M \times M$ identity matrix $\mathbf{I}$ and an $M \times (N-M)$ binary matrix $\mathbf{P}$ are placed side by side to form the $M \times N$ matrix $\tilde{\mathbf{H}}$. We can assume that the reordering of columns was not necessary (in other words, we chose the right ordering of columns in $\mathbf{H}$ to begin with). Now, $\mathbf{P}$ has full rank, because if not, then row operations on $\tilde{\mathbf{H}}$ could create a row $\mathbf{r}$ that was zero in the last $N-M$ bits but had some non-zero bits in the first M. Since $\mathbf{r} \in \mathcal{C}^\perp(\tilde{\mathbf{H}}) = \mathcal{C}^\perp(\mathbf{H})$ and $\mathcal{C}^\perp(\mathbf{H}) \subset \mathcal{C}(\mathbf{H})$, this must be a codeword of $\mathcal{C}(\mathbf{H})$ and hence of $\mathcal{C}(\tilde{\mathbf{H}})$. But the inner product of some rows of $\tilde{\mathbf{H}}$ with this codeword must be non-zero, having a 1 bit overlap in the first M bits and no overlap elswhere, and this is a contradiction.

Thus $\mathbf{P}$ has full rank, and we can apply row operations to $\mathbf{P}$ in turn to obtain $\tilde{\mathbf{P}} = [\mathbf{I}, \mathbf{Q}]$ for some $M \times K$ matrix $\mathbf{Q}$. For any length-K binary string $\mathbf{f}$, $[\mathbf{Qf}, \mathbf{f}]$ is a codeword of $\mathcal{C}(\tilde{\mathbf{P}})$, hence of $\mathcal{C}(\mathbf{P})$, and so $[\mathbf{0}, \mathbf{Qf}, \mathbf{f}]$ is a codeword of $\mathcal{C}(\mathbf{H})$. Furthermore, if two $\mathbf{f}$s are distinct, the resulting codewords cannot differ by an element of $\mathcal{C}^\perp(\mathbf{H})$, since any non-zero element of $\mathcal{C}^\perp(\mathbf{H})$ has 1s in the first M bits whereas the codewords obtained by our construction have zeros in the first M bits. Thus each $\mathbf{f}$ gives a unique equivalence class in $\mathcal{C}$ relative to the subspace $\mathcal{C}^\perp$.

We can use this construction to encode $K = N - 2M$ qubits in N qubits by the circuit shown in figure 5. Given a K qubit state $|\mathbf{s}\rangle_K$, where $\mathbf{s}$ is a K bit string, the first stage of the circuit carries out the transformation

$$|\mathbf{0}\rangle_M |\mathbf{0}\rangle_M |\mathbf{s}\rangle_K \to |\mathbf{0}\rangle_M |\mathbf{Qs}\rangle_M |\mathbf{s}\rangle_K \tag{34}$$

using the cNOT (controlled NOT, or controlled X) operations shown in the boxes Q_1, Q_2, etc.. The next stage of the circuit ('stage 2') first applies a Hadamard transform on the first M qubits, taking the initial $|\mathbf{0}\rangle_M$ state to

$$|\mathbf{0}\rangle_M \to \prod^M \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{2^{M/2}} \sum_{\mathbf{i}} |\mathbf{i}\rangle_M \,, \tag{35}$$

where $\mathbf{i}$ runs over all 2^M binary strings of length M. Let $\mathbf{t}$ denote the binary string $[\mathbf{Qs}, \mathbf{s}]$. Let P_m^c denote the operator that is controlled by the mth qubit $|i_m\rangle$ in the first set $|\mathbf{i}\rangle_M$ of M qubits and applies cNOT operations to the remaining $N-M$ qubits $|t\rangle_{N-M}$ in positions where the mth row of $\mathbf{P}$ has a 1. Then the final part of 'stage 2' carries out all these operations for $m = 1$ to M. The effect of these operators is to add rows of $\tilde{\mathbf{H}} = [\mathbf{I}, \mathbf{P}]$ to the binary string $\mathbf{t}$. Thus the operation of the final stage is:

$$\frac{1}{2^{M/2}} \sum_{\mathbf{i}} |\mathbf{i}\rangle_M |\mathbf{t}\rangle_{N-M} \to \frac{1}{2^{M/2}} \sum_{\mathbf{i}} \left[\prod_{m=1}^{M} P_m^c \right] |\mathbf{i}\rangle_M |\mathbf{t}\rangle_{N-M} = \frac{1}{2^{M/2}} \sum_{\mathbf{r} \in \mathcal{C}^\perp(\mathbf{H})} |\mathbf{r} + \mathbf{t}\rangle_N \,, \tag{36}$$

and we have generated an encoded state of the form (24). If we start from $\sum_{\mathbf{s}} \alpha_{\mathbf{s}} |\mathbf{s}\rangle_K$ we get the right hand side of equation (25), the most general codeword.

3 Sparse-graph codes

It has been proved that there exist quantum codes with non-zero rate R and blocklength N that can correct any t errors, with $t \propto N$. However, *practical* codes with these properties have not yet been presented. To be practical, a quantum code must satisfy two properties. First, the associated classical decoding problem must be practically solvable. [To be precise, we want a decoding time polynomial in N, preferably linear in N.] And second, the M_Q measurements required to implement the error-correction mechanism must be feasible: in our view, an error-correction mechanism is much more likely to be feasible if every syndrome measurement involves only a small subset of size $k \ll N$ of the qubits, rather than a size $k \propto N$ that is required for a generic quantum code.

We therefore study quantum codes that are associated with *sparse graphs*. In a sparse-graph code, the nodes in the graph represent the transmitted bits and the constraints they satisfy. Any linear code can be described by a graph, but what makes a sparse-graph code special is that each constraint involves only a small number of variables in the graph. The sparseness has the immediate advantages that (1) the quantum syndrome can be measured with sparse interactions – for example, if the quantum syndrome is found by bringing together qubits in pairs, a quantum code with a sparse graph requires only of order N interactions, rather than N^2; and (2) there are practical decoding algorithms (in particular, the sum-product algorithm) for decoding classical codes defined on sparse graphs; indeed, codes based on sparse graphs are record-breaking codes for classical channels.

3.1 Classical sparse-graph codes

The archetypal sparse-graph code is Gallager's (1962) low-density parity-check code. A low-density parity-check code is a block code that has a parity-check matrix, $\mathbf{H}$, every row and column of which is 'sparse'.

In a *regular* low-density parity-check code, every column of $\mathbf{H}$ has the same weight j and every row has the same weight k; regular low-density parity-check codes are constructed at random subject to these constraints. A tiny low-density parity-check code with $j = 3$ and $k = 4$ is illustrated in figure 6. In spite of their simplicity and sparseness, low-density parity-check codes have excellent theoretical and practical properties. The following results are proved in Gallager (1963) and MacKay (1999). For any column weight $j \geq 3$, low-density parity-check codes are 'good' codes, *given an optimal decoder* ('good' in the technical sense that there exist sequences of codes that achieve vanishing error probability at non-zero communication

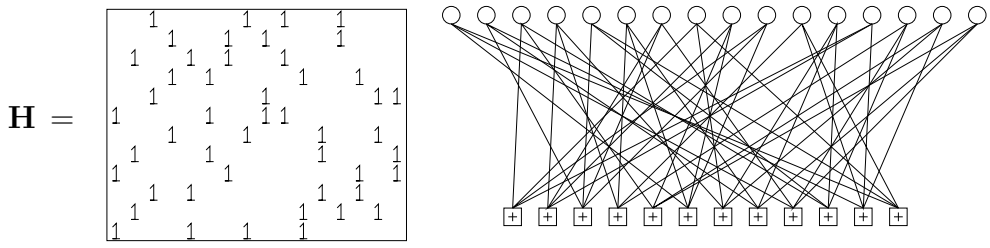


Figure 6. A low-density parity-check matrix and the corresponding graph of a rate-$1/4$ low-density parity-check code with blocklength $N = 16$, and $M = 12$ constraints. Each white circle represents a transmitted bit, corresponding to a column of $\mathbf{H}$. Each bit participates in $j = 3$ constraints, represented by $\boxplus$ squares, corresponding to the 12 rows of $\mathbf{H}$. Each constraint forces the sum of the $k = 4$ bits to which it is connected to be even. From (MacKay 2003).

rate). Furthermore, they have 'good' minimum distance (that is, there exist sequences of codes whose distance grows linearly with blocklength).

The decoding of a low-density parity-check code is an NP-complete problem (Berlekamp *et al.* 1978), but for practical purposes, as long as the graph is sparse, it has been found that simple message-passing algorithms can give excellent performance. The best such algorithm known is the sum–product algorithm, also known as iterative probabilistic decoding or belief propagation. This iterative algorithm is explained in (MacKay and Neal 1996; MacKay 1999; MacKay 2003; Frey 1998). In one iteration, each edge in the graph carries a message (a single real number) from its bit node (the circles in figure 6) to its check node (the squares), representing the relative probability of the two states of the bit node; each check node then computes the relative likelihoods of the two states of each bit node, given the incoming messages from the other nodes and the constraint enforced by the check node; these likelihood ratios are sent back up each edge; then each bit node collates the likelihoods it receives, multiplying them together appropriately in order to compute new probabilities for the next iteration.

When decoded in this way, regular low-density parity-check codes with column weight $j = 3$ or 4 are quite hard to beat. Performance even closer to the Shannon limit has been achieved by making the sparse graph irregular (Luby *et al.* 2001; Richardson and Urbanke 2001a; Richardson *et al.* 2001): if the bit nodes have a carefully chosen distribution of degrees, rather than all having the same degree j, then the effectiveness of the sum-product decoding algorithm is enhanced.

Sparse-graph codes have great flexibility: we can make low-density parity-check codes of almost any required blocklength N and rate R; and they are good codes for a wide variety of channels – for example channels with erasures, channels with a varying noise level and channels with burst noise, as well as the traditional binary symmetric channel.

The challenge that remains is to make a sparse-graph *quantum* code that can correct a good

number of errors. Our ultimate aim is to find practical codes that can correct a number of errors $\propto N$. To be precise, we'd like to find a family of codes with blocklength N that can correct *almost any* t errors, where $t \propto N$. The difference between correcting 'almost any t errors' and 'any t errors' is important – if we wish to approach the Shannon limit, we must make systems with the former property. In the present paper, we describe first steps in this direction. The codes we present do not have distance $\propto N$; nevertheless, they can achieve error-correction at substantial noise-levels, and for intermediate values of N (large, but not enormous), we believe they are the best known quantum codes.

3.2 Distance isn't everything

Perhaps we should elaborate on the perspective on code design given above. Much of coding theory, including the founding papers of quantum coding theory, emphasizes 'the number of errors that can be corrected' by a code – an emphasis which leads to one trying to make codes that have large minimum distance. However, *distance isn't everything*. The distance of a code is of little relevance to the question 'what is the maximum noise level that can be tolerated by the optimal decoder?' Let us explain, assuming that the channel in question is the standard binary symmetric channel. At large blocklength N, the Gilbert-Varshamov conjecture (widely believed true) asserts that the best binary codes of rate R have a minimum distance d that satisfies

$$R = 1 - H_2(d/N). \tag{37}$$

If we decode such a code with a bounded-distance decoder, which corrects 'up to $t \simeq d/2$ errors', then the maximum noise level that can be tolerated is

$$f_{\rm bdd}^{\rm max} \simeq \frac{d/2}{N}, \tag{38}$$

which satisfies

$$R = 1 - H_2(2f_{\rm bdd}^{\rm max}). \tag{39}$$

In contrast, Shannon's noisy channel coding theorem says that there exist codes of rate R that when optimally decoded give *negligible probability of error* at noise levels up to $f_{\rm Shannon}^{\rm max}$, which satisfies:

$$R = 1 - H_2(f_{\rm Shannon}^{\rm max}). \tag{40}$$

Comparing (39) and (40) we deduce

$$f_{\rm Shannon}^{\rm max} = 2f_{\rm bdd}^{\rm max}. \tag{41}$$

The maximum tolerable noise level according to Shannon is twice the maximum tolerable noise level for a bounded-distance decoder, even if the code has the best possible distance. In order to get close to the Shannon limit, we must tolerate a number of errors twice as great as the maximum *guaranteed* correctable, $t \simeq d/2$. Shannon's codes can (asymptotically) correct almost any $t_{\rm Shannon}$ errors, where $t_{\rm Shannon} = f_{\rm Shannon}^{\rm max} N$.

So, does the minimum distance matter at all? Well, yes. If our aim is to make for a given channel a sequence of codes with *vanishing* error probability, then the minimum distance d

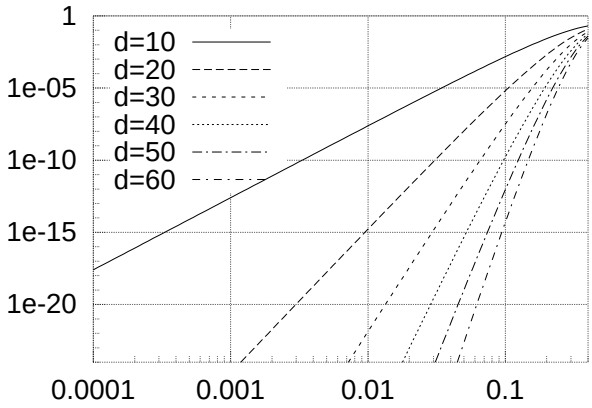


Figure 7. The error probability associated with a single codeword of weight d, $\binom{d}{d/2} f^{d/2}(1-f)^{d/2}$, as a function of f.

must increase along that sequence, since the error probability is at least β^d, where β is a property of the channel independent of blocklength N; for example, for the binary symmetric channel, $\beta(f) = 2f^{1/2}(1-f)^{1/2}$ (MacKay 2003). But the distance does not need to increase *linearly* with N in order for the code to be able to correct *almost any* $t_{\text{Shannon}} = f_{\text{Shannon}}^{\max} N$ errors. Moreover, if our goal is simply to make a code whose error probability is smaller than some figure such as 10^{-6} or 10^{-20} then there is no reason why the distance has to grow at all with blocklength.

This unimportance of the minimum distance for practical purposes is illustrated in figure 7, which shows the error probability associated with a single codeword of weight d in the case of a binary symmetric channel with noise level f. From this figure we can see for example that if the raw error probability f is about 0.001, the error probability associated with one codeword at distance $d = 20$ is smaller than 10^{-24}.

All else being equal, we might prefer a code with large distance, but for practical purposes a code with blocklength $N = 10,000$ can have codewords of weight $d = 32$ and the error probability can remain negligibly small even when the channel is creating errors of weight 320. Indeed we will demonstrate codes with exactly this property.

4 Dual-containing sparse-graph codes

In this paper, we focus on dual-containing codes, which have the property that every row of the parity-check matrix is a codeword of the code.

4.1 Some misconceptions

We initially thought we would be unable to make good quantum codes from dual-containing low-density parity-check codes, because a random low-density parity-check code is, with high probability, a *good* code having good distance (*i.e.*, distance proportional to N), whereas the dual of a low-density parity-check code is certainly a *bad* code having bad distance (its distance is at most equal to the row-weight k of the original matrix $\mathbf{H}$). So a low-density parity-check code that contains its dual would have to be a bad code. [Bad codes are ones that, for large N, cannot correct a number of errors proportional to N.] And since almost all low-density parity-check codes are good codes, low-density parity-check codes are not expected to contain their duals.

This point of view is indeed correct. The codes that we now describe are *not* good classical codes; they contain low-weight codewords. However, low-weight codewords need not necessarily harm the *quantum* code: if the low-weight codewords are themselves all contained in the dual of the code, then they do not produce quantum errors – the quantum codewords are invariant under addition of codewords contained in the dual.

Furthermore, from a practical point of view, it is not essential to have good minimum distance. As long as we have a near-optimal decoder (*i.e.*, one that works well beyond half the minimum distance of the code), the error-probability associated with low-weight codewords can be very small, as illustrated by classical turbo codes, which have good practical performance even though they typically have a few codewords of low weight. A few low-weight codewords hurt performance only a little, because the noise has so many directions it could take us in that it is unlikely to take us in the few directions that would give rise to confusion with the nearest codewords.

So while our ideal goal is to make a good dual-containing code (based on a sparse graph) that has no low-weight codewords not in the dual, we are also happy with a lesser aim: to make a dual-containing code whose low-weight codewords not in the dual are of sufficiently high weight that they contribute negligibly to the quantum code's error probability.

4.2 Do dual-containing low-density parity-check codes exist?

A code is a regular dual-containing $(j, k)(N, M)$ low-density parity-check code if it has an $M \times N$ parity check matrix $\mathbf{H}$ such that

1. every row has weight k and every column has weight j;
2. every pair of rows in $\mathbf{H}$ has an even overlap, and every row has even weight.

The speculation that motivated this research was that for small fixed j and arbitrarily large N and M, dual-containing $(j, k)(N, M)$ low-density parity-check codes exist and almost all

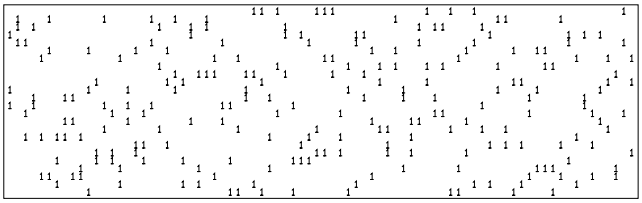


Figure 8. A regular dual-containing (3,10)(80,24) low-density parity-check code's parity check matrix, found by a Monte Carlo search.

of them define good quantum codes.

Finding such codes proved difficult however. Figure 8 shows one code found by a Monte Carlo search. If we increase either the blocklength or the column weight j, our Monte Carlo searches become ineffective. [We exclude from our search trivial solutions whose graphs are not well-connected, such as codes defined by block-diagonal matrices.]

4.3 A counting argument

We count approximately the number of regular dual-containing $(j,k)(N,M)$ low-density parity-check codes by finding the probability that a randomly created matrix $\mathbf{H}$ with column-weight j satisfies all the $\binom{M}{2}$ self-orthogonality constraints. [In defining this ensemble, we neglect the condition that the row weights should be exactly k, in order to make the calculation easier; we do not expect this omission to have any significant effect on the result (Litsyn and Shevelev 2002). Similar counting arguments for classical low-density parity-check codes give valid predictions.]

The number of matrices with column-weight j is

$$\mathcal{N}_0 = \binom{M}{j}^N. \tag{42}$$

As each column of the matrix is created, we can imagine keeping track of the $\mathcal{M} \equiv \binom{M}{2}$ inner products (modulo 2) between rows. Each column of weight j flips the parity of $\binom{j}{2}$ of the inner products. We can view this process as creating a random walk on the $\mathcal{M}$-dimensional hypercube, starting from the origin. As each column is added, $\binom{j}{2}$ individual steps are taken on the hypercube. The probability that, after all N columns are created, all $\mathcal{M}$ inner products are zero (the dual-containing condition) is the probability that the random walk on the hypercube is at the origin after $r = N\binom{j}{2}$ steps. The probability of return to zero after r steps is approximately (for $r \ll \mathcal{M}$ (MacKay 1999))

$$\frac{1}{\mathcal{M}^{r/2}} \frac{r!}{2^{r/2}(r/2)!} \simeq \left(\frac{r/2}{\mathcal{M}}\right)^{r/2}, \tag{43}$$

so with $r = N\binom{j}{2}$ and $\mathcal{M} = \binom{M}{2}$,

$$P(\text{dual-containing}) \simeq \left(\frac{N\binom{j}{2}/2}{M^2/2} \right)^{N\binom{j}{2}/2} \tag{44}$$

$$= \left(\frac{Nj(j-1)/2}{M^2} \right)^{Nj(j-1)/4} . \tag{45}$$

[Equation (43) can be motivated by imagining that $r/2$ steps are allowed to select distinct dimensions for 'outbound' steps, and the other $r/2$ steps are required to undo all these steps in a given order (which has probability $1/\mathcal{M}^{r/2}$); the number of ways of ordering these steps is $r!/(2^{r/2}(r/2)!)$.] So the number of dual-containing matrices is

$$\mathcal{N}_1 = \mathcal{N}_0 P(\text{dual-containing}) \simeq \frac{M^{jN}}{(j!)^N} \left(\frac{Nj(j-1)/2}{M^2} \right)^{Nj(j-1)/4} . \tag{46}$$

What really matters here is whether this quantity scales as $N^{+\alpha N}$ or as $N^{-\alpha N}$. Are there lots of dual-containing codes, or negligibly many? We thus drop all terms other than N and M, and we assume $N \propto M$.

$$\mathcal{N}_1 \sim N^{jN} \left(\frac{1}{N} \right)^{Nj(j-1)/4} \sim N^{N(j - j(j-1)/4)}. \tag{47}$$

This expression grows with N if

$$j - j(j-1)/4 > 0, \tag{48}$$

i.e. if $j < 5$.

4.4 Second counting argument

We give a second argument for the difficulty of making these dual-containing codes, based on a particular construction method.

A concrete method for making (j, k) low-density parity-check codes is to create $j \times k$ permutation matrices $\{\mathbf{R}_{hi}\}$ (*i.e.* square matrices with one 1 per row and one 1 per column) of size $(M/j) \times (M/j)$, and arrange them in the manner illustrated here for the case $(j, k) = (3, 4)$:

$$\mathbf{H} = \begin{bmatrix} \mathbf{R}_{11} & \mathbf{R}_{12} & \mathbf{R}_{13} & \mathbf{R}_{14} \\ \mathbf{R}_{21} & \mathbf{R}_{22} & \mathbf{R}_{23} & \mathbf{R}_{24} \\ \mathbf{R}_{31} & \mathbf{R}_{32} & \mathbf{R}_{33} & \mathbf{R}_{34} \end{bmatrix} . \tag{49}$$

[While this form of matrix might seem restrictive compared with a free choice from all matrices $\mathbf{H}$ with column-weight j and row-weight k, the information content of a matrix of the form (49) (*i.e.*, the log of the number of matrices) is to leading order equal to the information content of a freely chosen matrix with the same j and k.] We might hope to

enforce all the orthogonality rules by picking permutation matrices and picking a set of constraints which are for example of the form

$$\mathbf{R}_{11}\mathbf{R}_{12}^{\mathsf{T}}\mathbf{R}_{22}\mathbf{R}_{21}^{\mathsf{T}} = \mathbf{I}, \quad \mathbf{R}_{11}\mathbf{R}_{13}^{\mathsf{T}}\mathbf{R}_{33}\mathbf{R}_{31}^{\mathsf{T}} = \mathbf{I}, \quad \mathbf{R}_{21}\mathbf{R}_{24}^{\mathsf{T}}\mathbf{R}_{34}\mathbf{R}_{31}^{\mathsf{T}} = \mathbf{I}; \tag{50}$$

these three constraints ensure that all overlaps in the first group of columns are compensated by overlaps elsewhere in the matrix. The total number of such constraints required to enforce the dual-containing property would be $k\binom{j}{2}/2$. The number of degrees of freedom in defining a matrix like (49) (where one degree of freedom is the freedom to choose one permutation matrix) is $(k-1)(j-1)$, since without loss of generality, the top row and left column can all be set to $\mathbf{I}$. So a construction like this only has freedom to make a variety of codes if

$$(k-1)(j-1) > k\binom{j}{2}/2, \tag{51}$$

i.e.,

$$(k-1) > kj/4 \tag{52}$$

which cannot be satisfied if $j \geq 4$, and can be satisfied if $j = 3$ and $k > 4$.

These two results are bad news for our mission. We had hoped to be able to make numerous random codes with $j = 5$. We viewed $j \geq 5$ as a necessary constraint in order that the graph of the code have good expansion properties. A dual-containing code with $j = 4$ would, we believe, be bound to have low-weight codewords (rather as regular Gallager codes with $j = 2$ have low-weight codewords).

Nevertheless, we have found a few ways to make small numbers of dual-containing codes, which we now describe. Furthermore, the negative arguments are only bad news for *dual-containing* sparse-graph codes; they do not rule out the possibility of making more general sparse-graph codes that satisfy the twisted product constraint (20).

4.5 Making dual-containing low-density parity-check codes

We have tried three approaches to constructing codes satisfying the even-overlap constraint: random constructions using Monte Carlo search; constructions in which the even-overlap constraints are deliberately built into the *local* structure of the sparse graph; and constructions in which the constraints are satisfied by a deliberate choice of *global* structure. Only the third of these approaches worked out for us. The codes we make are slightly irregular in that while the row weights are all equal to k, the column weights are slightly non-uniform.

4.6 List of constructions of dual-containing sparse-graph codes

In this paper we present four constructions of sparse-graph codes, all based on sparse cyclic matrices. We call the constructions B, U, N, and M. Of these, the first is the most successful.

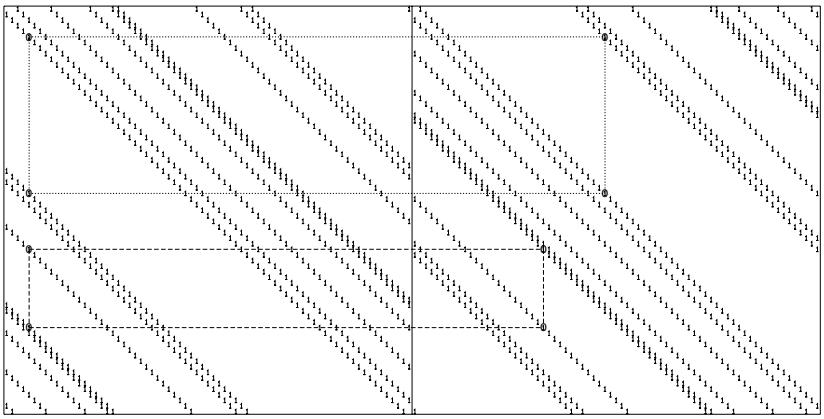


Figure 9. Example of a matrix $\mathbf{H}_0 = [\,\mathbf{C}, \mathbf{C}^{\mathsf{T}}\,]$ used in construction B. The dotted lines illustrate the way in which two vertical differences in column 5 of the left hand matrix are reproduced in the right half of the matrix.

To make a code with classical rate 3/4 and quantum rate 1/2, we can take the top half of this matrix.

1. **Construction B**: 'B' is mnemonic for bicycle. To make a **Bicycle code** with row-weight k, blocklength N, and number of constraint nodes M, we take a random sparse $N/2 \times N/2$ cyclic matrix $\mathbf{C}$ with row-weight $k/2$, and define

$$\mathbf{H}_0 = [\,\mathbf{C}, \mathbf{C}^{\mathsf{T}}\,]\,. \tag{53}$$

By construction, every pair that appears in $\mathbf{C}$ appears in $\mathbf{C}^{\mathsf{T}}$ also (figure 9). Then we delete some rows from $\mathbf{H}_0$ to obtain a matrix $\mathbf{H}$ with M rows. We delete rows using the heuristic that the column weights of $\mathbf{H}$ should be as uniform as possible. We usually choose the non-zero entries in $\mathbf{C}$ using a difference set satisfying the property that every difference (modulo $N/2$) occurs at most once in the set.

This construction has the advantage that the choice of N, M, and k is completely flexible.

The disadvantage of this construction is that the deleted rows are all low-weight codewords of weight k, which are unlikely to be in the dual. Thus technically speaking we cannot make 'good' codes in this way – if we fix k and increase the blocklength, the error probability will not vanish (*cf.* section 3.2); nevertheless for useful blocklengths, we will show that the error probability associated with these low-weight codewords is negligible, for practical purposes.

2. **Construction U**: 'U' is mnemonic for unicycle. **Unicycle codes** are made with the help of a perfect difference set (box 10) over the additive group of size $\tilde{M} = 73$, 273, 1057, or 4161. For example, a perfect difference set for the group of size $\tilde{M} = 73$ is $\{2, 8, 15, 19, 20, 34, 42, 44, 72\}$. $\tilde{M}$ will be the number of rows in the code's parity-check matrix. By making a cyclic matrix $\mathbf{C}$ from a perfect difference set, we obtain

An example of a perfect difference set is the set of integers

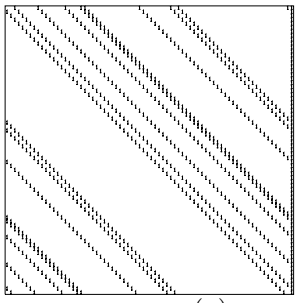
$$0, 3, 5, 12 \pmod{13}.$$

A perfect difference set on the additive group of size M has the property that every integer from 0 to $M-1$ can be written as the difference of two integers in the set (modulo M) in exactly one way.
For example, the differences between the above integers, modulo 13, are

			$3-0$	$=$	**3**	$5-0$	$=$	**5**	$12-0$	$=$	**12**
$0-3$	$=$	**10**				$5-3$	$=$	**2**	$12-3$	$=$	**9**
$0-5$	$=$	**8**	$3-5$	$=$	**11**				$12-5$	$=$	**7**
$0-12$	$=$	**1**	$3-12$	$=$	**4**	$5-12$	$=$	**6**			

Some of our constructions use plain *difference sets* in which every difference occurs either one or zero times.

Box 10. Perfect difference sets. An entertaining tutorial on difference sets by Kris Coolsaet can be found at `http://www.inference.phy.cam.ac.uk/cds/`.



(a)

DIFFERENCE-SET CYCLIC CODES

N	21	73	273	1057	4161
M	**10**	**28**	**82**	**244**	**730**
K	11	45	191	813	3431
d	**6**	**10**	**18**	34	66
k	**5**	**9**	17	33	65

(b)

Figure 11. (a) The parity check matrix of the 'Unicycle' code of blocklength $N = 74$. (b) Table of five difference-set cyclic codes from which useful unicycle codes may be derived.

a parity check matrix that defines a code with blocklength $N = \tilde{M}$ and a number of independent parity constraints M given in the table of figure 11(b), which also shows the distance d of each code and the row-weight k. The number of independent parity constraints is much smaller than the total number of rows $\tilde{M}$.

Difference set cyclic codes have been found to have impressive performance on classical channels when decoded by message-passing decoders (Karplus and Krit 1991; Lucas *et al.* 2000).

The perfect-difference-set property implies that all pairs of rows of $\mathbf{C}$ have an overlap of 1. To create a dual-containing code, we need to make these overlaps even. We do this by extending the parity check matrix, adding one extra column, all ones. Since all pairs of rows of this additional column have an overlap of 1, all rows of the new parity check matrix have overlap 2. Thus we have defined a dual-containing $(N+1, K+1)$ code

with parity check matrix $\mathbf{H}$ whose row weight is $k+1$ (for example, 10, for $\tilde{M}=73$) and whose column weights are all k except for one column with enormous weight $\tilde{M}$. When decoding, we can handle this one column in a special way. We can view the code as the union of two codes, one for each setting of the extra bit. The first code (in which the extra bit is set to zero) is the original difference set cyclic code; the second is the code obtained by adding the vector $(1\,1\,1\,1\ldots1)$ to all words of the first. We can decode each of the two codes separately by the sum-product algorithm then (if both decoders return a codeword) select the codeword that has maximum likelihood.

A disadvantage of these codes is that so few of them exist, so there is little choice of the parameters N, M, and k. Another disappointing property is that the code has codewords of weight equal to the row-weight.

3. **Construction N** also makes use of cyclic difference sets. We choose a number of rows M and an integer v such as $v=4$ and create v cyclic matrices from v cyclic difference sets over $\{0,1,2,\ldots(M-1)\}$, with the special property that every difference (modulo M) occurs zero times or twice (preferably once in one set and once in another). Such sets of difference sets are not easy to find but can be found by computer search. An example of $v=4$ sets for $M=500$ is:

$$\begin{array}{lllll}\{0 & 190 & 203 & 345 & 487\}\\ \{0 & 189 & 235 & 424 & 462\}\\ \{0 & 94 & 140 & 170 & 310\}\\ \{0 & 15 & 47 & 453 & 485\}\end{array}$$

with an illustrative pair of matched differences being $170-140=30$ (in set 3) matching $15-485=30 \pmod{500}$ (in set 4).

We turn each set into a square cyclic matrix and put the matrices alongside each other to make the parity check matrix $\mathbf{H}$. Since every difference occurs an even number of times, the overlap between any pair of rows is even.

4. **Construction M** is a special case of construction N in which all the v difference sets are derived from a single parent difference set with w elements. The parent difference set has the property that every difference (modulo M) occurs one or zero times. We select the v difference sets using a design (for example, for $v=8$ and $w=14$, a $14,7$ quasi-symmetric design) that ensures every pair appears in exactly two derived difference sets. [We thank Mike Postol for providing this quasi-symmetric design.] The v derived difference sets define v square cyclic matrices each of which is either transposed or not when they are put alongside each other to define $\mathbf{H}$.

For the codes reported here we used the $14,7$ quasi-symmetric design shown in table 12. We used parent difference sets over $M=273$ and $M=1901$.

Constructions N and M both suffer from two problems. First, a code built from v square cyclic matrices each of weight j inevitably has many codewords of weight $2j$: for any pair of square cyclic matrices associated with vectors $\mathbf{f}$ and $\mathbf{g}$ (both of weight j), the vector $(\mathbf{g},\mathbf{f})$ is a weight-$2j$ codeword, as is any vector built from cyclic shifts of $\mathbf{g}$ and $\mathbf{f}$. Second, every square cyclic matrix has 'near-codewords' associated with it.

Matrix number	Elements selected							
1 :	4	6	7	8	9	10	12	
2 :	1	5	7	9	10	11	13	T
3 :	1	2	6	10	11	12	0	
4 :	2	3	7	8	11	12	13	T
5 :	1	3	4	9	12	13	0	
6 :	2	4	5	8	10	13	0	T
7 :	3	5	6	8	9	11	0	
8 :	1	2	3	4	5	6	7	T

Table 12. The $14, 7$ quasi-symmetric design. The final column indicates by T the matrices that were transposed.

We define a (w, v) *near-codeword* of a code with parity-check matrix $\mathbf{H}$ to be a vector $\mathbf{x}$ with weight w whose syndrome $\mathbf{z}(\mathbf{x}) \equiv \mathbf{H}\mathbf{x}$ has weight v. Near-codewords with both small v and relatively small w tend to be error states from which the sum-product decoding algorithm cannot escape. A small value of w corresponds to a quite-probable error pattern, while the small value of v indicates that only a few check-sums are affected by these error patterns (MacKay and Davey 2000; MacKay and Postol 2003). If the square matrix is defined by a vector $\mathbf{g}$ of weight j, then the component-reversed vector $\tilde{\mathbf{g}}$ is a (j, j) near-codeword.

5 Channel models chosen for simulations

When comparing candidate codes for quantum error-correction, we have studied the codes' performance on three classical channels. Because of the correspondence between classical codes and stabilizer codes (section 2.2), our results will give bounds on the performance of the quantum codes defined in the previous section. To each classical channel there corresponds a quantum channel whose error operators $\{E_\alpha\}$ are related to the binary noise vectors $\{e_\alpha\}$ of the classical channel as described in section 2.2.

1. Independent binary symmetric channels. The simplest channel models `X` errors and `Z` errors as independent events, identically distributed with a flip probability f_{m}. The suffix 'm' denotes the 'marginal' flip probability. Most of our simulations have used this model because it allows easy comparison with textbook codes. For this channel, and for a quantum code based on a dual-containing classical code, the `X` errors and `Z` errors can be inferred independently with two separate classical decodings, so the probability of block error is roughly twice P_{BSC}, the probability of block error for a *single* block of the classical code on a binary symmetric channel (to be precise, it is $1 - (1 - P_{\mathrm{BSC}})^2$). When reporting results for this channel in figures 13–16, we plot P_{BSC}.

2. However, a possibly more realistic channel is the **depolarizing channel** (equation (16)). The classical analogue that is simulated here is the **4-ary symmetric channel**, which

creates X errors, Y errors, and Z errors with equal probability $f/3$. The total flip probability is f. The probability of no error is $1-f$. If we describe a Y error as the combination of an X error and a Z error then the marginal flip probability (the probability of an X error, ignoring what's happening to Z) is

$$f_{\rm m} = 2f/3. \tag{54}$$

The 4-ary symmetric channel may be treated by a decoder as if it were a pair of binary symmetric channels, but this approximation throws away information about the correlations between X errors and Y errors. The sum-product decoding algorithm can retain this information with only a small increase in complexity.

3. Diversity of qubit reliabilities. We also studied a third channel, with noise level varying from qubit to qubit, to illustrate the gains possible when the decoder can make use of known variations in noise level. We chose the standard Gaussian channel, the workhorse of communication theory, to define our classical channel. One way to describe this channel is as a binary symmetric channel where the noise level for each bit is set by drawing a random variable y from a Gaussian distribution with mean 1 and standard deviation σ, and setting the flip probability to $f_n = 1/(1+\exp(2|y|/\sigma^2))$. If this channel is treated by the decoder as a binary symmetric channel then its marginal flip probability is $f_{\rm m} = \Phi(1/\sigma)$, where $\Phi(z) = \int_z^\infty e^{-z^2/2} dz/\sqrt{2\pi}$; but neglecting the reliabilities $\{f_n\}$ in this way reduces the maximum achievable communication rate.

The corresponding quantum channel is one in which X errors and Z errors are independent events, but each bit has its own probability of X flip and Z flip; these $2N$ probabilities $\{f_n\}$ are known to the decoder, and are set afresh each time a block is received.

5.1 Benchmark communication rates for symmetric channels

We define three benchmark rates for the classical channels, and obtain benchmark quantum rates from them.

The capacity of the binary symmetric channel is

$$C_{\rm BSC}(f_{\rm m}) = 1 - H_2(f_{\rm m}). \tag{55}$$

The capacity, also known as the Shannon limit, is the maximum rate at which reliable communication can be achieved over the binary symmetric channel with flip probability $f_{\rm m}$.

The classical Gilbert rate is defined by

$$R_{\rm GV}(f_{\rm m}) = 1 - H_2(2f_{\rm m}) \quad f_{\rm m} \in (0, 1/4). \tag{56}$$

This is widely believed to be the maximum rate at which a *bounded-distance decoder* can communicate over the channel.

The capacity of the classical 4-ary symmetric channel is

$$C_4(f) = 2 - (H_2(f) + f \log_2 3). \tag{57}$$

For comparability, we rescale this function as follows:

$$C_{4B}(f_{\mathrm{m}}) \equiv \frac{1}{2} C_4(3f_{\mathrm{m}}/2). \tag{58}$$

This is the maximum rate at which reliable communication can be achieved over each half of the 4-ary symmetric channel whose marginal flip probability is f_{m}.

For each classical rate R we can define a quantum rate $R_Q(R) = 2R - 1$ (because a classical dual-containing code with M constraints and rate $(N - M)/N$ defines a quantum code with rate $(N - 2M)/N = 2R - 1$).

Thus we define

$$C^Q_{\mathrm{BSC}}(f_{\mathrm{m}}) = 1 - 2H_2(f_{\mathrm{m}}); \tag{59}$$

$$R^Q_{\mathrm{GV}}(f_{\mathrm{m}}) = 1 - 2H_2(2f_{\mathrm{m}}); \tag{60}$$

and

$$C^Q_4(f_{\mathrm{m}}) = 1 - (H_2(3f_{\mathrm{m}}/2) + (3f_{\mathrm{m}}/2) \log_2 3). \tag{61}$$

C^Q_{BSC}, defined in equation (59), should not be confused with the quantum channel capacity. It is the maximum rate attainable by stabilizer codes constructed from dual-containing codes, and therefore provides an upper bound (and ideal goal) for this particular class of code. R^Q_{GV} and C^Q_4 have similar meanings. We also define the quantum GV bound for stabilizer codes; this is labelled the stabilizer rate in figures that follow:

$$R^Q_{GV4}(f_{\mathrm{m}}) = 1 - (H_2(2f_{\mathrm{m}}) + (2f_{\mathrm{m}}) \log_2 3), \quad f_{\mathrm{m}} \in (0, 1/6). \tag{62}$$

6 Results

We measured the block error probability of each code as a function of noise level by empirical experiments involving many simulated decodings. We simulated the classical channel then attempted to solve the resulting decoding problem using the standard decoding algorithm for low-density parity-check codes, the sum-product algorithm (Gallager 1963; MacKay and Neal 1996). The outcome of each decoding is either the correct decoding, or a block error. Each block error is classified as a detected error if the decoder itself identifies the block as one that is known to be in error, and otherwise as an undetected error (if the decoder finds a valid decoding that is not the correct decoding). In the figures we graph the performance of a code by showing its total block error probability, with two-sigma error bars. The caption of each figure notes whether the block errors were entirely detected errors.

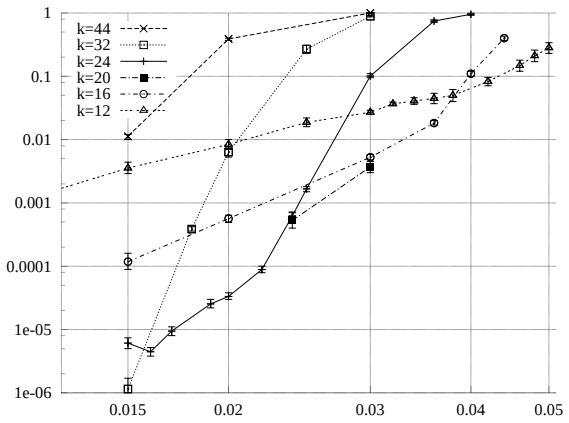


Figure 13. Performance of dual-containing binary codes of construction B with parameters $N = 3786$, $M = 1420$, and row weights ranging from $k = 88$ to $k = 12$, on the binary symmetric channel, as a function of the flip probability $f_{\rm m}$. The vertical axis shows the block error probability. All errors were detected errors, that is, the decoder reported the fact that it had failed. The quantum codes obtained from these codes have quantum rate $R_Q = 1/4$.

6.1 Construction B

Figures 13–15 show results for some codes of construction B. In each figure the blocklength and rate are fixed, and the different codes have different row-weights k.

By comparing figure 13 and figure 14 one may see the effect of increasing the blocklength from $N = 3786$ to $N = 19\,014$ while keeping the quantum rate fixed at $R_Q = 1/4$. Notice that while the minimum distance of the code with $N = 3786$ and $k = 24$ is known to be at most 24, this code is able to correct almost any 80 errors with a block error probability smaller than 10^{-4}; similarly the code with $N = 19\,014$ and $k = 32$ has minimum distance at most 32 yet it can correct almost any 380 errors with a block error probability smaller than 10^{-5}.

Figure 15 shows codes with blocklength $N = 3786$ and a larger rate of $R_Q = 3/4$.

For each blocklength and rate there is an optimum row-weight k for the codes of construction B. For a blocklength of $N = 3786$ the optimum was about $k = 24$; for the larger blocklength of 19 014, the optimum was about $k = 32$.

6.2 Constructions U, N, and M

Figure 16 shows performance curves for the unicycle code with $N = 274$. Whereas the codes of construction B presented thus far made no undetected errors, the codes of construction U sometimes gave undetected errors. To put it positively, the decoder for the code with $N = 274$ performs almost as well as the maximum likelihood decoder for the code (all the

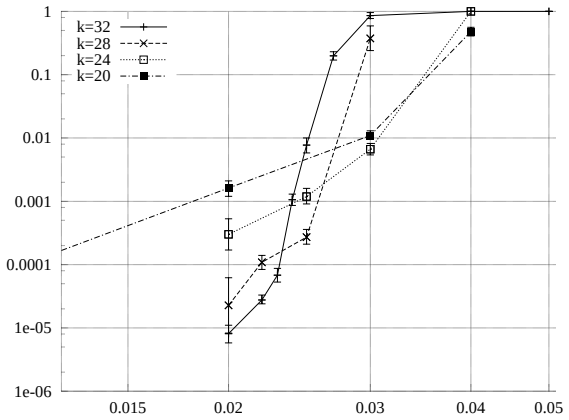


Figure 14. Performance of dual-containing binary codes of construction B with parameters $N = 19\,014$, $M = 7131$, and row weights ranging from $k = 32$ to $k = 20$, on the binary symmetric channel, as a function of the flip probability f_{m}. The vertical axis shows the block error probability. All errors were detected errors, that is, the decoder reported the fact that it had failed. The quantum codes obtained from these codes have quantum rate $R_Q = 1/4$.

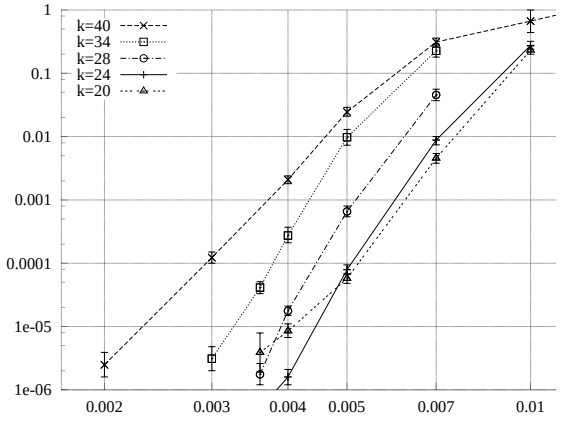


Figure 15. Performance of dual-containing binary codes of construction B with parameters $N = 3786$, $M = 473$, and row weights ranging from $k = 40$ to $k = 20$, on the binary symmetric channel, as a function of the flip probability f_{m}. The vertical axis shows the block error probability. All errors were detected errors, that is, the decoder reported the fact that it had failed. The quantum codes obtained from these codes have quantum rate $R_Q = 3/4$.

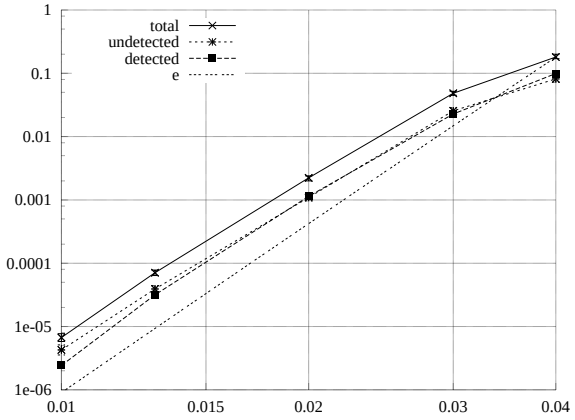


Figure 16. Performance of the construction-U code with $N = 274$ and $M = 82$ on the binary symmetric channel, as a function of the flip probability $f_{\rm m}$. The vertical axis shows the block error probability. Roughly half the errors were detected and half undetected. The three curves with error bars show the total block error rate, the detected error rate, and the undetected error rate. Also shown is an estimate $e = A \binom{d}{d/2} f^{d/2}(1-f)^{d/2}$ of the error rate of the maximum likelihood decoder, assuming that the code has $A = 273^3$ words of weight $d = 18$.

errors made by a maximum likelihood decoder are undetected errors). The decoder also made detected errors, the frequencies of errors of each type being roughly equal. Most of the undetected errors do not lie in the dual (so they are not admissible errors for the quantum code).

To make it easy to compare many quantum codes simultaneously, we summarise each code's performance by finding the noise level $f_{\rm m}$ at which its block error probability is 10^{-4}. In the case of a quantum code based on a dual-containing classical code, decoded by treating the channel as if it were a pair of independent binary symmetric channels, the value plotted is the noise level at which the block error probability of one constituent classical code is 0.5×10^{-4}. Figure 17 compares these performance summaries for a selection of codes. The right-hand vertical axis shows the quantum rate of the codes. The left-hand vertical axis shows the classical rate of the underlying classical code, where this concept is applicable. The figure shows the performance of four Unicycle codes, two rate-$^3/_4$ codes of construction M and one rate-$^1/_2$ code of construction N. And it includes the performance of some algebraically-defined codes, CSS codes based on BCH codes, Reed-Muller codes, and the Golay code.

6.3 Exploiting channel knowledge when decoding

We can improve the performance of all the sparse-graph codes presented here by putting knowledge about the channel properties into the decoding algorithm. For example, if the channel is the 4–ary symmetric channel with error probability q, then instead of treating this channel as if it consisted of two independent binary symmetric channels with flip probability $f_{\rm m} = 2q/3$ (as is normal practice with CSS codes), we can build knowledge of the correlations

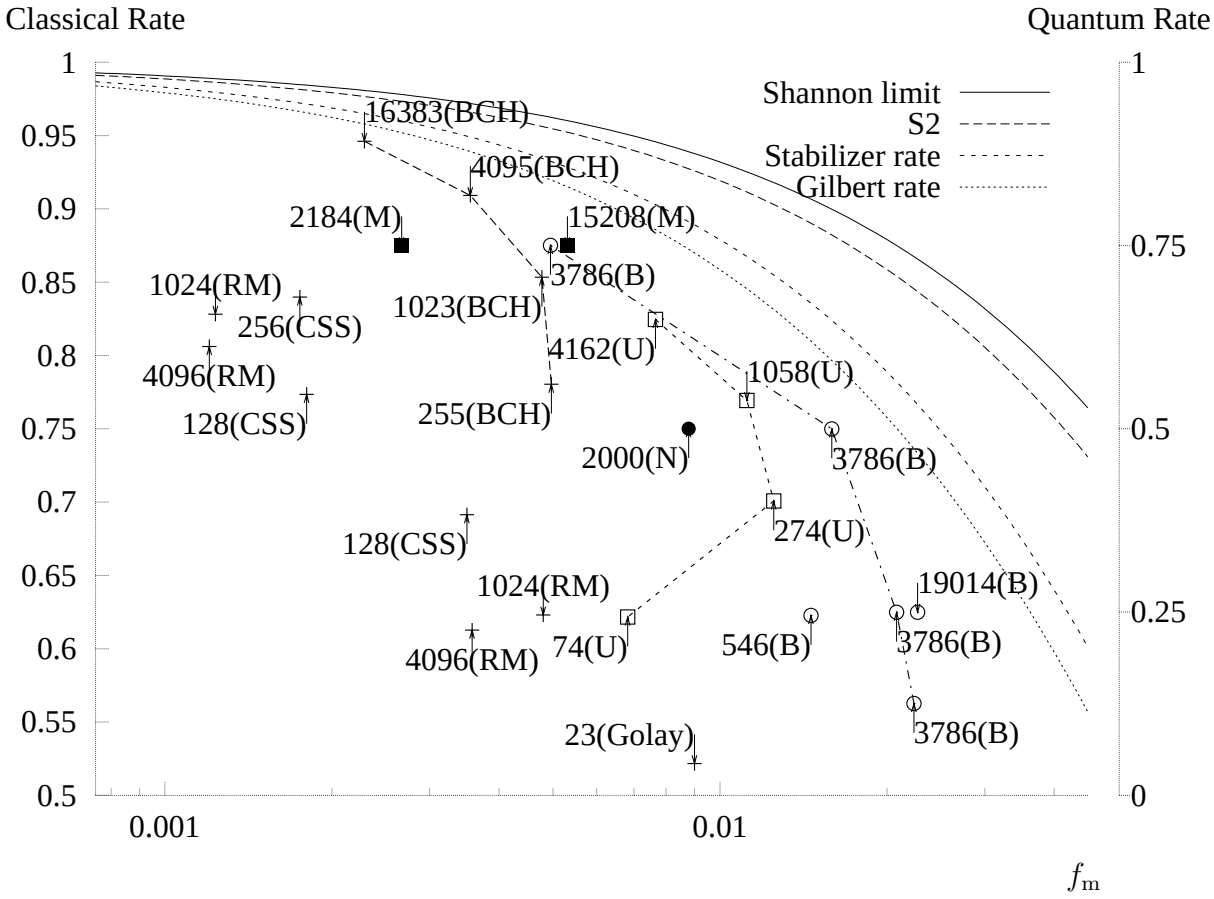


Figure 17. Summary of performances of several quantum codes on the 4-ary symmetric channel (depolarizing channel), treated (by all decoding algorithms shown in this figure) as if the channel were a pair of independent binary symmetric channels. Each point shows the marginal noise level f_{m} at which the block error probability is 10^{-4}. In the case of dual-containing codes, this is the noise level at which each of the two identical constituent codes (see equation (23)) has an error probability of 5×10^{-5}.

As an aid to the eye, lines have been added between the four unicycle codes (U); between a sequence of bicycle codes (B) all of blocklength $N = 3786$ with different rates; and between a sequence of of BCH codes with increasing blocklength.

The curve labelled S2 is the Shannon limit if the correlations between `X` errors and `Z` errors are neglected, (59).

Points '+' are codes invented elsewhere. All other point styles denote codes presented for the first time in this paper.

between `X` errors and `Z` errors into the sum-product decoding algorithm.

$P(e_x, e_z)$	$e_x = 0$	$e_x = 1$
$e_z = 0$	$1-q$	$q/3$
$e_z = 1$	$q/3$	$q/3$

We illustrate the benefits of building this knowledge into the sparse graph's decoder by giving the results for one code in figure 18. There, we show the performance of a rate-$1/2$ bicycle code (classical rate 0.75) of length $N = 3786$ before (left point) and after inclusion of correlation knowledge (right point, marked '4SC'). This code's performance is beyond the Gilbert rate and is therefore better than any performance that could be achieved by a traditional CSS code (that is, a CSS code composed of two binary codes each separately decoded by a bounded-distance decoder).

The opportunity to build in channel knowledge gives sparse-graph codes a second major advantage if the decoder knows that certain bits are more reliable than others. It is well known in communication theory that the ability to exploit such soft channel information can improve decoder performance by a couple of decibels, on standard benchmark channels. To illustrate this benefit, we took a classical rate-0.625 bicycle code of blocklength $N = 3786$ and simulated its decoding with the channel likelihoods being generated using a Gaussian noise model as described in section 5. We show the performance of the decoder (by the point marked 3786(B,D)) in figure 18 at a horizontal coordinate f_{m} corresponding to the mean flip probability of the channel.

Figure 18 also shows the performance of a small quantum code drawn from (Grassl 2003). As new quantum codes are invented, we intend to maintain a graph summarising the best performances on the depolarizing channel on the web at `www.inference.phy.cam.ac.uk/qecc/`. Authors of quantum codes are encouraged to simulate their decoders and submit the results.

7 Discussion

We have presented four families of dual-containing codes that are sparse-graph codes, all based on cyclic matrices.

The only parameter regimes in which we are aware of quantum codes of comparable blocklength that can surpass the sparse-graph codes presented here are the large-rate regime and the very small-rate regime: there exist sequences of dual-containing BCH codes with increasing blocklength N and rate R_Q tending to 1 (Steane 1999), which, as illustrated in figure 17, dominate at rates above $R_Q = 0.8$; and sequences of surface codes, with rates tending to zero, can cope with noise levels up to $f_{\mathrm{m}} \simeq 0.11$ under the two-binary-symmetric-channels noise model (Dennis *et al.* 2002). These surface codes are sparse-graph codes with very low-weight interactions.

We have estimated the performance of some of Steane's 'enlarged' codes (Steane 1999) and,

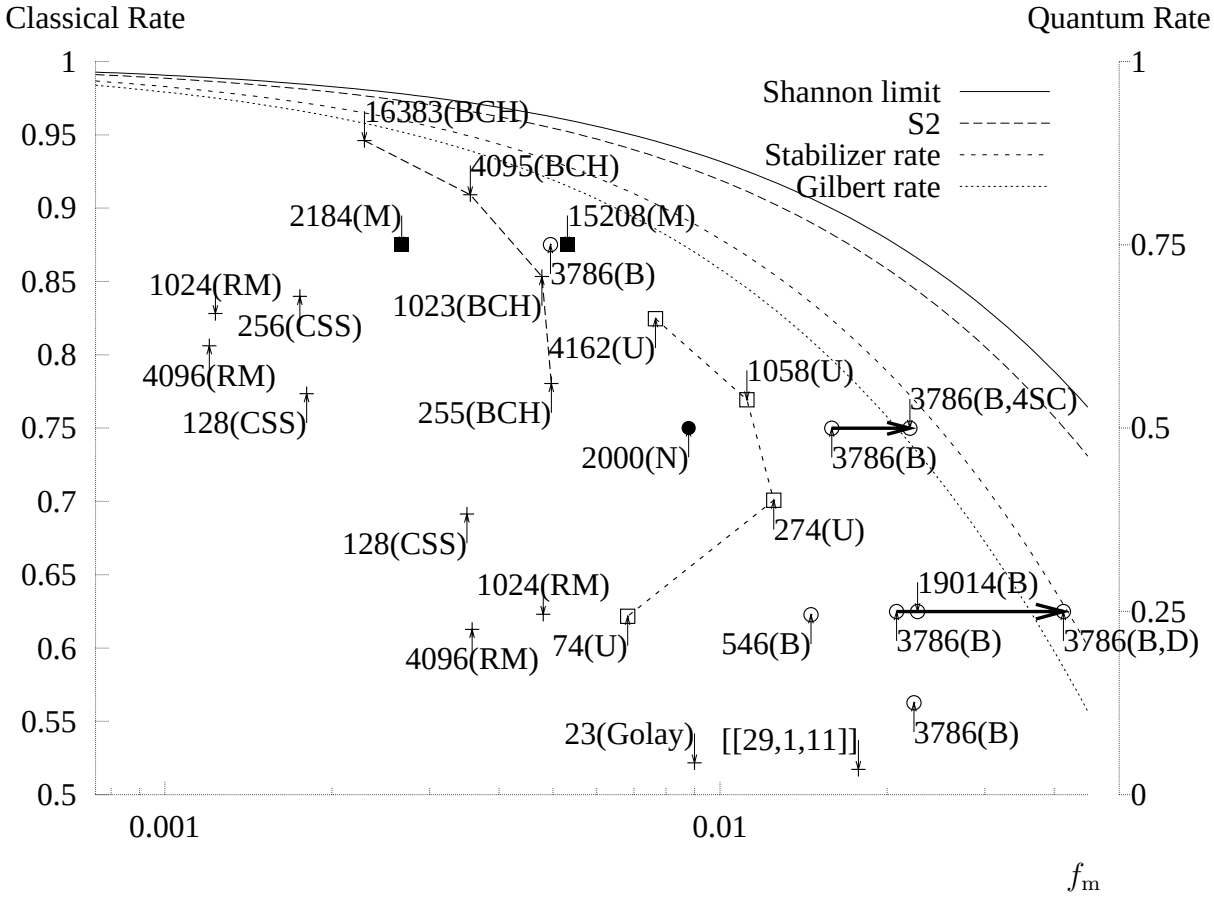


Figure 18. Summary of performances of several codes on the 4-ary symmetric channel (depolarizing channel). The additional points at the right and bottom are as follows.

3786(B,4SC): a code of construction B (the same code as its neighbour in the figure) decoded with a decoder that exploits the known correlations between `X` errors and `Z` errors.

3786(B,D): the same code as the $N = 3786$ code to its left in the figure, simulated with a channel where the qubits have a diversity of known reliabilities; `X` errors and `Z` errors occur independently with probabilities determined from a Gaussian distribution; the channel in this case is not the 4-ary symmetric channel, but we plot the performance at the equivalent value of f_{m}.

[[29,1,11]]: an algebraically constructed quantum code (not a sparse-graph code) from (Grassl 2003).

although these have somewhat higher rate than the BCH codes they are derived from, they do not surpass the codes shown here.

7.1 Encoding complexity

While all the sparse-graph codes presented have low *decoding* complexity, both in terms of the number of quantum interactions required and the number of classical operations required to infer the noise from the syndrome, we have said nothing so far about their *encoding* complexities. The worst case is that the encoding complexity will scale as N^2, if we follow the recipe in section 2.5 without exploiting the structure of the sparse graph. However, in the case of constructions U, N, and M, all of which directly involve sparse cyclic matrices, we think it is likely that the cyclic structure can be exploited to yield encoders of lower complexity. For all four constructions B, U, N, and M, another option would be to try the methods of Richardson and Urbanke (2001b) for lowering the complexity of encoding. We are not addressing the details of encoding at present as we are still hunting for even better codes; we will return to encoding when we have reached the limits of our ability to generate promising sparse-graph codes.

7.2 Concerning dual-containing codes

We hope that it is possible to find other constructions that might surpass these codes in terms of the parameters R (rate), $f_{\rm m}$ (noise level), or k (sparseness of parity check matrix).

Since finding pseudorandom dual-containing codes seems so difficult, it might be worthwhile to explore algebraically constructed sparse-graph codes. We examined a dual-containing Euclidean Geometry code with blocklength $N = 511$, kindly supplied by Shu Lin. This code's classical rate was 0.875 and it achieved a block error probability of 0.5×10^{-4} at $f_{\rm m} \simeq 0.00133$, a disappointing result; the code has low-weight codewords and at least one tenth of the decoding errors were associated with these codewords.

The decoding algorithm that we have used for all these codes is the plain sum-product algorithm. It is known this algorithm becomes increasingly suspect as the number of short cycles in the graph increases; and for dual-containing codes, the graph has an enormous number of cycles of length four. In the case of constructions B, N, and M, our decoder ignores these four cycles. It seems highly likely that a decoding algorithm that took these four-cycles into account would perform significantly better (Yedidia *et al.* 2000; Yedidia *et al.* 2002). Our attempts to make such an improved algorithm have so far yielded only algorithms whose complexity scales as 2^k, where k is the row-weight of the parity-check matrix. Given that our preferred codes have $k \simeq 20$, these algorithms are regrettably not feasible. Construction U has an advantage here: while the code has four cycles as required, our decoder works by separately searching for decodings within two subcodes, both defined by graphs with no four-cycles.

7.3 Prior work on sparse-graph codes for quantum error correction

Several constructions and decoding algorithms have been proposed for quantum codes that are associated with sparse graphs (Kitaev 2003; Dennis 2000; Dennis *et al.* 2002; Postol 2001). The major differences in our work are that we present codes with large blocklengths and with a wide variety of rates, and our codes can correct hundreds of errors; every sparse-graph code in the references listed above either has vanishing rate ($K/N \simeq 0$ for large N) or cannot correct more than a tiny number of errors.

7.4 Theoretical questions remaining

We think it would be very interesting to resolve a query about the distance properties of dual-containing codes with sparse parity check matrix. All the dual-containing codes we have found so far have the disappointing property that they have codewords (not in the dual) of weight $\leq k$, where k is the row-weight of the parity check matrix.

We offer two mutually exclusive conjectures about binary codes, one pessimistic and one optimistic, identified by the initials of the author of each conjecture.

Conjecture G: Any dual-containing code defined by an $M \times N$ parity check matrix $\mathbf{H}$ with $M < N/2$, all of whose rows have weight $\leq k$, has codewords of weight $\leq k$ that are not in the dual.

Conjecture D: There exist dual-containing codes with sparse parity-check matrix and good distance. To be precise, such codes would have a parity-check matrix with maximum row weight k, and for increasing blocklength N the minimum distance d of codewords not in the dual would satisfy $d \propto N$.

If both these conjectures are false, we will be happy, because the middle-ground – dual-containing sparse-graph codes with minimum distance $> k$ – would be sufficient to give excellent practical performance.

7.5 Beyond dual-containing codes

While we think the constructions reported here – especially construction B – are very promising and flexible, we hope to find even better practical quantum codes.

Having found the dual-containing constraint to be quite a severe one, we are now working on less-constrained sparse-graph codes, namely ones that satisfy the twisted product constraint (20) only.

Acknowledgments

We thank Shu Lin, Marc Fossorier, Mike Postol, and Andrew Landahl for helpful discussions. DJCM is supported by the Gatsby Charitable Foundation and by a partnership award from IBM Zürich Research Laboratory.

References

Ashikhmin, A., Litsyn, S., and Tsfasman, M. A., (2000) Asymptotically good quantum codes. `quant-ph/0006061`.

Berlekamp, E. R., McEliece, R. J., and van Tilborg, H. C. A. (1978) On the intractability of certain coding problems. *IEEE Trans. on Info. Theory* **24** (3): 384–386.

Calderbank, A. R., Rains, E. M., Shor, P. W., and Sloane, N. J. A., (1997) Quantum error correction via codes over GF(4). `quant-ph/9608006`.

Calderbank, A. R. and Shor, P. W. (1996) Good quantum error-correcting codes exist. *Phys. Rev. A* **54**: 1098. `quant-ph/9512032`.

Davey, M. C. and MacKay, D. J. C. (1998) Low density parity check codes over GF(q). In *Proceedings of the 1998 IEEE Info. Theory Workshop*, pp. 70–71. IEEE.

Dennis, E., (2000) Quantum codes on high-genus surfaces. `quant-ph/0007072`.

Dennis, E., Kitaev, A., Landahl, A., and Preskill, J. (2002) Topological quantum memory. *J. Math. Phys.* **43**: 4452–4505. `quant-ph/0110143`.

Frey, B. J. (1998) *Graphical Models for Machine Learning and Digital Communication*. MIT Press.

Gallager, R. G. (1962) Low density parity check codes. *IRE Trans. Info. Theory* **IT-8**: 21–28.

Gallager, R. G. (1963) *Low Density Parity Check Codes*. Number 21 in MIT Research monograph series. MIT Press. Available from `http://www.inference.phy.cam.ac.uk/mackay/gallager/papers/`.

Grassl, M., (2003) Table of quantum error-correcting codes. `http://avalon.ira.uka.de/home/grassl/QECC/`.

Grassl, M., Klappenecker, A., and Rötteler, M. (2002) Graphs, quadratic forms and quantum codes. In *Proc. IEEE Int. Symp. Inf. Th. 2002*. IEEE Inf. Th. Soc.

Karplus, K. and Krit, H. (1991) A semi-systolic decoder for the PDSC–73 error-correcting code. *Discrete Applied Mathematics* **33**: 109–128.

Kitaev, A. Y. (2003) Fault-tolerant quantum computation by anyons. *Annals Phys.* **303**: 2–30. `quant-ph/9707021`.

Ling, S., Chen, H., and Xing, C. (2001) Asymptotically good quantum codes exceeding the Ashikhmin–Litsyn–Tsfasman bound. *IEEE Trans. on Info. Theory* **47**: 2055–2058.

Litsyn, S. and Shevelev, V. (2002) On ensembles of low-density parity-check codes: asymptotic distance distributions. *IEEE Trans. on Info. Theory* **48** (4): 887–908.

Lo, H.-K., Popescu, S., and Spiller, T. (2001) *Introduction to quantum computation and information*. World Scientific.

Luby, M. G., Mitzenmacher, M., Shokrollahi, M. A., and Spielman, D. A. (2001) Improved low-density parity-check codes using irregular graphs and belief propagation. *IEEE Trans. on Info. Theory* **47** (2): 585–598.

Lucas, R., Fossorier, M., Kou, Y., and Lin, S. (2000) Iterative decoding of one-step majority logic decodable codes based on belief propagation. *IEEE Trans. on Communications* **48**: 931–937.

MacKay, D. J. C. (1999) Good error correcting codes based on very sparse matrices. *IEEE Trans. on Info. Theory* **45** (2): 399–431.

MacKay, D. J. C. (2003) *Information Theory, Inference, and Learning Algorithms*. Cambridge University Press. Available from `http://www.inference.phy.cam.ac.uk/mackay/itila/`.

MacKay, D. J. C. and Davey, M. C. (2000) Evaluation of Gallager codes for short block length and high rate applications. In *Codes, Systems and Graphical Models*, ed. by B. Marcus and J. Rosenthal, volume 123 of *IMA Volumes in Mathematics and its Applications*, pp. 113–130. Springer.

MacKay, D. J. C. and Neal, R. M. (1996) Near Shannon limit performance of low density parity check codes. *Electronics Letters* **32** (18): 1645–1646. Reprinted *Electronics Letters*, **33**(6):457–458, March 1997.

MacKay, D. J. C. and Postol, M. J. (2003) Weaknesses of Margulis and Ramanujan–Margulis low-density parity-check codes. In *Proceedings of MFCSIT2002, Galway*, volume 74 of *Electronic Notes in Theoretical Computer Science*. Elsevier.

Matsumoto, R. (2002) Improvement of Ashikhmin–Litsyn–Tsfasman bound for quantum codes. *IEEE Trans. on Info. Theory* **48** (7): 2122–2124.

Postol, M. S., (2001) A proposed quantum low density parity check code. `quant-ph/0108131`.

Preskill, J., (2001) Lecture notes for Physics 219: Quantum computation. Available from `http://www.theory.caltech.edu/people/preskill/ph219`.

Richardson, T., Shokrollahi, M. A., and Urbanke, R. (2001) Design of capacity-approaching irregular low-density parity check codes. *IEEE Trans. on Info. Theory* **47** (2): 619–637.

Richardson, T. and Urbanke, R. (2001a) The capacity of low-density parity check codes under message-passing decoding. *IEEE Trans. on Info. Theory* **47** (2): 599–618.

Richardson, T. and Urbanke, R. (2001b) Efficient encoding of low-density parity-check codes. *IEEE Trans. on Info. Theory* **47** (2): 638–656.

Schlingemann, D. and Werner, R. F. (2002) Stabilizer codes can be realized as graph codes. *Quant. Inf. Comp.* **2**: 307–323.

Shor, P. W. (1995) Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A* **52** (R): 2493–6.

Steane, A. (1996) Multiple particle interference and quantum error correction. *Proc. Roy. Soc. Lond. A* **452**: 2551–2577.

Steane, A. (1999) Enlargement of Calderbank Shor Steane quantum codes. *IEEE Trans. on Info. Theory* **45**: 2492–2495. `quant-ph/9802061`.

Steane, A. (2001) Quantum computing and error correction. In *Decoherence and its implications in quantum computation and information transfer*, ed. by P. Turchi and A. Gonis, volume 182 of *NATO Science Series: Computer & Systems Sciences*, pp. 284–298. IOS Press. `quant-ph/0304016`.

Yedidia, J. S., Freeman, W. T., and Weiss, Y. (2000) Generalized belief propagation. Technical report, Mitsubishi Electric Res. Labs. TR-2000-26.

Yedidia, J. S., Freeman, W. T., and Weiss, Y. (2002) Constructing free energy approximations and generalized belief propagation algorithms. Technical report, Mitsubishi Electric Res. Labs. TR-2002-35.