Quantum Error Correction

Peter J. Cameron

School of Mathematical Sciences
Queen Mary and Westfield College
London E1 4NS, U.K.
p.j.cameron@qmw.ac.uk

MathFIT London, 5 April 2000

Why quantum computing?

In 1990 Peter Shor proved the following theorem.

Theorem 1 *There exists a randomized algorithm for integer factorization which runs in polynomial time on a quantum computer.*

On a classical computer, primality testing is 'easy' but factorization is 'hard'. This is the basis of the RSA cryptosystem.

Roughly speaking, a quantum computer is highly parallel; we can run exponentially many computations at the same time, and only those which terminate with a positive result will produce output.

Classical v quantum

In a classical computer, each bit of information is stored by a transistor containing trillions of electrons.

On a quantum computer, a single electron or nucleus in a magnetic field carries a bit of information. Interaction with the environment is much more serious.

Decoherence puts a limit on the space and time resources available to a quantum computer.

In order to get round this limit, the computer must be *fault tolerant*, that is, it must have error correction built in; and the error correction circuits should not introduce more errors than they correct!

Classical error correction

Let $F = \mathrm{GF}(2) = \{0,1\}$. An element of F is a *bit* of information. A *word* of length n (an element of $V = F^n$) contains n bits of information.

A code is a subset C of V such that any two elements of C are far apart. We only use codewords to carry information; if few errors occur, the correct codeword is likely to be the nearest.

For $v, w \in V$, the *Hamming distance* $d(v,w)$ is the number of coordinates i such that $v_i \neq w_i$.

If the minimum Hamming distance between distinct elements of C is d, then C can correct up to $\lfloor (d-1)/2 \rfloor$ errors. So an error pattern is correctable if it has weight at most $\lfloor (d-1)/2 \rfloor$.

The *weight* of v is $\mathrm{wt}(v) = d(v,0)$. If C is linear, then its minimum distance is equal to its minimum weight.

States and observables

The state of a quantum system is a unit vector in a complex Hilbert space. An observable is a self-adjoint operator on the state space, whose eigenvalues are the possible values of the observable.

The interpretation of the coefficients a_i of a state vector with respect to an orthonormal basis of eigenvectors of an observable is that $|a_i|^2$ is the probability of obtaining the corresponding eigenvalue as the value of a measurement.

Bits and qubits

The quantum analogue of a bit of information is called a *qubit*. It is the state of a system in a 2-dimensional Hilbert space $\mathbb{C}^2$ spanned by e_0 and e_1, where e_0 and e_1 are eigenvectors corresponding to the eigenvalues 0 and 1 of the qubit.

Thus, the qubit is represented by the self-adjoint matrix

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

relative to this basis. So in the state $\alpha e_0 + \beta e_1$, the probabilities of measuring 0 and 1 are $|\alpha|^2$ and $|\beta|^2$ respectively.

An n-tuple of qubits is an element of the tensor product

$$\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 = \mathbb{C}^{2^n}.$$

a basis for this space consists of all vectors

$$e_v = e_{v_1} \otimes \cdots \otimes e_{v_n},$$

for $v = (v_1, \ldots, v_n) \in V$.

Quantum errors

An error, like any physical process, is a unitary transformation of the state space. The space of errors to a single qubit is 4-dimensional, and is spanned by the four unitary matrices

I	(no error)	$e_0 \mapsto e_0$, $e_1 \mapsto e_1$
X	(bit error)	$e_0 \mapsto e_1$, $e_1 \mapsto e_0$
Z	(phase error)	$e_0 \mapsto e_0$, $e_1 \mapsto -e_1$
$Y = iXZ$	(combination)	

Note that I, X, Y, Z are the *Pauli spin matrices*.

We can write $Xe_v = e_{v+1}$, $Ze_v = (-1)^v e_v$.

Quantum errors

Now the errors to n qubits act coordinatewise, and are generated by $X(a)$ and $Z(b)$ for $a, b \in V$, where

$$X(a) : e_v \mapsto e_{v+a}, \quad Z(b) : e_v \mapsto (-1)^{v.b} e_v.$$

These generate the *error group*, an extraspecial 2-group E of order 2^{2n+1} with centre $Z(E) = \pm I$.

$\overline{E} = E/Z(E) \cong \mathrm{GF}(2)^{2n}$; we represent the coset $\{\pm X(a)Z(b)\}$ by $(a|b)$.

On $\overline{E}$, we have a *quadratic form* q given by

$$((X(a)Z(b))^2 = (-1)^{q(a|b)} I$$

and associated *symplectic form* $*$ given by

$$[X(a)Z(b), X(a')Z(b')] = (-1)^{(a|b)*(a'|b')} I.$$

Quantum codes

Let S be an abelian subgroup of E such that $\overline{S}$ is totally singular (w.r.t. q). Then under the action of S, the state space $\mathbb{C}^{2^n}$ is the sum of $|S|$ orthogonal eigenspaces. Let Q be an eigenspace. Then

- the error group permutes the eigenspaces regularly;
- the stabilizer of Q is $S^\perp$;
- S acts trivially on Q.

Thus, errors in $S^\perp$ are undetectable, while errors in S have no effect. So if $\mathcal{E}$ is a subset of E with the property

$$e, f \in \mathcal{E} \Rightarrow f^{-1}e \notin S^\perp \setminus S,$$

then errors in $\mathcal{E}$ can be corrected. (If two such errors have undetectably different effect, then they have the same effect!)

Quantum error correction

The subspace Q is our quantum code. If $|S| = 2^r$, then $\dim(Q) = 2^{n-r}$; we can think of Q as consisting of $n-r$ qubits "smeared out" over the space of n qubits.

Define the *quantum weight* of $(a|b) \in \overline{E}$ to be the number of coordinates i such that either a_i or b_i (or both) is non-zero, that is, some error has occurred in the ith qubit.

By taking $\mathcal{E}$ to consist of all errors with quantum weight at most $\lfloor (d-1)/2 \rfloor$, Calderbank, Rains, Shor and Sloane proved the following analogue of classical error correction:

Theorem 2 *Suppose that the minimum quantum weight of* $\overline{S}^\perp \setminus \overline{S}$ *is* d*. Then* Q *corrects* $\lfloor (d-1)/2 \rfloor$ *qubit errors.*

$\mathrm{GF}(4)$ to quantum

The field $\mathrm{GF}(4)$ can be written as

$$\{a\omega + b\overline{\omega} : a, b \in \mathrm{GF}(2)\}.$$

So we have a bijection θ between $\overline{E}$ and $\mathrm{GF}(4)^n$, given by $(a|b) \mapsto a\omega + b\overline{\omega}$.

Moreover, if a subspace of $\mathrm{GF}(4)^n$ is totally isotropic with respect to the Hermitian inner product on $\mathrm{GF}(4)^n$, then its image in $\overline{E}$ is totally singular.

Also, the quantum weight of $(a|b)$ is equal to the Hamming weight of $a\omega + b\overline{\omega}$.

So good $\mathrm{GF}(4)$-codes can be used to construct good quantum codes.