Introduction to Quantum Information Processing QIC 710 / CS 678 / PH 767 / CO 681 / AM 871

Lectures 15–16 (2013)

Richard Cleve DC 2117 / QNC 3129 cleve@cs.uwaterloo.ca

Classical error correcting codes

Binary symmetric channel

Each bit that goes through it has probability ϵ of being flipped

3-bit repetition code:

- •Encode each bit *b* as *bbb*
- •Decode each received message $b_1b_2b_3$ as majority(b_1, b_2, b_3)

This reduces the effective error probability per data bit to $3\epsilon^2$ at a cost of tripling the message length ("rate" is 1/3).

A theorem about "good" classical codes:

For all $\varepsilon < 1/2$, there exist encoding and decoding functions $E: \{0,1\}^n \rightarrow \{0,1\}^m$ and $D: \{0,1\}^m \rightarrow \{0,1\}^n$ such that m/n is **constant** and the probability of **any** errors $\rightarrow 0$ as $n \rightarrow \infty$

n/m is the *rate* of the code (= reciprocal of message expansion)

Shor's 9-qubit code

3-qubit code for one *X***-error**

The following 3-qubit quantum code protects against up to one error, if the error can only be a quantum bit-flip (an *X* operation)



Error can be any one of: $I \otimes I \otimes I$ $X \otimes I \otimes I$ $I \otimes X \otimes I$ $I \otimes I \otimes X$ Corresponding syndrome: $|00\rangle$ $|11\rangle$ $|10\rangle$ $|01\rangle$

The essential property is that, in each case, the data $\alpha |0\rangle + \beta |1\rangle$ is shielded from (i.e., unaffected by) the error

What about Z errors? This code leaves them intact ...

3-qubit code for one *Z***-error**

Using the fact that HZH = X, one can adapt the previous code to protect against *Z*-errors instead of *X*-errors



This code leaves *X*-errors intact

Is there a code that protects against errors that are arbitrary one-qubit unitaries?

Shor' 9-qubit quantum code



The "inner" part corrects any single-qubit *X*-error The "outer" part corrects any single-qubit *Z*-error Since Y = iXZ, single-qubit *Y*-errors are also corrected

Arbitrary one-qubit errors

Suppose that the error is some arbitrary one-qubit unitary operation ${\cal U}$

Since there exist scalars λ_1 , λ_2 , λ_3 and λ_4 , such that

 $U = \lambda_1 I + \lambda_2 X + \lambda_3 Y + \lambda_4 Z$

a straightforward calculation shows that, when a *U*-error occurs on the k^{th} qubit, the output of the decoding circuit is

 $(\alpha|0\rangle + \beta|1\rangle)(\lambda_1|s_{e_1}\rangle + \lambda_2|s_{e_2}\rangle + \lambda_3|s_{e_3}\rangle + \lambda_4|s_{e_4}\rangle)$

where s_{e_1} , s_{e_2} , s_{e_3} and s_{e_4} are the syndromes associated with the four errors (*I*, *X*, *Y* and *Z*) on the k^{th} qubit

Hence the code actually protects against *any* unitary one-qubit error (in fact the error can be any one-qubit quantum operation)

Introduction to Quantum Information Processing QIC 710 / CS 678 / PH 767 / CO 681 / AM 871

Lecture 16 (2013)

Richard Cleve DC 2117 / QNC 3129 cleve@cs.uwaterloo.ca



Introduction to CSS codes

CSS codes (named after Calderbank, Shor, and Steane) are quantum error correcting codes that are constructed from classical error-correcting codes with certain properties

A classical *linear* code is one whose codewords (a subset of $\{0,1\}^m$) constitute a vector space

In other words, they are closed under linear combinations (here the underlying field is {0,1} so the arithmetic is mod 2)

Examples of linear codes

For m = 7, consider these codes (which are linear):

- $C_2 = \{0000000, 1010101, 0110011, 1100110, 0001111, 101100, 0111100, 1101001\}$
- $C_1 = \{0000000, 1010101, 0110011, 1100110, 0001111, 1011010, 0111100, 1101001, 1111111, 0101010, 1001100, 0011001, 1110000, 0100101, 1000011, 0010110\}$
- Note that the minimum Hamming distance between any pair of codewords is: 4 for C_2 and 3 for C_1

The minimum distances imply each code can correct one error

Encoding

Since , $|C_2| = 8$, it can encode 3 bits

To encode a 3-bit string $b = b_1 b_2 b_3$ in C_2 , one multiplies b (on the right) by an appropriate 3×7 *generator matrix*

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Similarly, C_1 can encode 4 bits and an appropriate generator matrix for C_1 is

Orthogonal complement

For a linear code *C*, define its *orthogonal complement* as

$$C^{\perp} = \{w \in \{0,1\}^m : \text{ for all } v \in C, w \cdot v = 0\}$$

(where $w \cdot v = \sum_{j=1}^m w_j v_j \mod 2$, the "dot product")

Note that, in the previous example, $C_2^{\perp} = C_1$ and $C_1^{\perp} = C_2$

We will use some of these properties in the CSS construction

Parity check matrix

Linear codes with maximum distance d can correct up to $\lfloor \frac{d-1}{2} \rfloor$ bit-flip errors

Every *n*-dimensional linear code has a *parity-check matrix* M (*m* by m-n) such that:

- For every codeword v, vM = 0
- For any *error-vector* $e \in \{0,1\}^m$ with weight $\leq \lfloor \frac{d-1}{2} \rfloor$, e can be uniquely determined by multiplying the disturbed codeword (which is v+e) by M

Error syndrome: $(v+e) M = s_e$ and *e* is a function of s_e only

Exercise: determine the parity check matrix for C_1 and for C_2

CSS construction

Let $C_2 \subset C_1 \subset \{0,1\}^m$ be two classical linear codes such that:

• The minimum distance of C_1 is d

• $C_2^{\perp} \subseteq C_1$

Let
$$r = \dim(C_1) - \dim(C_2) = \log(|C_1|/|C_2|)$$

Then the resulting CSS code maps each *r*-qubit basis state $|b_1...b_r\rangle$ to some "coset state" of the form

$$\frac{1}{\sqrt{|C_2|}} \sum_{v \in C_2} |v + w\rangle$$

where $w = w_1 \dots w_m$ is a linear function of $b_1 \dots b_r$ chosen so that each value of *w* occurs in a unique coset in the quotient space C_1/C_2 The quantum code can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors

Example of CSS construction

For m = 7, for the C_1 and C_2 in the previous example we obtain these basis codewords:

- $\begin{aligned} |0_L\rangle &= |0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\ &+ |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle \end{aligned}$
- $\begin{aligned} |1_L\rangle &= |1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \\ &+ |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle \end{aligned}$

There is a quantum circuit that transforms between $(\alpha|0\rangle + \beta|1\rangle)|0^{m-1}\rangle$ and $\alpha|0_L\rangle + \beta|1_L\rangle$

CSS error correction I

Using the error-correcting properties of C_1 , one can construct a quantum circuit that computes the syndrome *s* for any combination of up to *d X*-errors in the following sense



Once the syndrome s_e , has been computed, the *X*-errors can be determined and undone

What about *Z*-errors?

The above procedure for correcting *X*-errors has no effect on any *Z*-errors that occur

CSS error correction II

Note that any *Z*-error is an *X*-error in the Hadamard basis

Changing to Hadamard basis is like changing from C_2 to C_1 since

$$H^{\otimes m}\left(\sum_{v\in C_2} |v\rangle\right) = \sum_{u\in C_2^{\perp}} |u\rangle \quad \text{and} \quad H^{\otimes m}\left(\sum_{v\in C_2} |v+w\rangle\right) = \sum_{u\in C_2^{\perp}} (-1)^{w\cdot u} |u\rangle$$

Applying $H^{\otimes n}$ to a superposition of basis codewords yields $H^{\otimes m}\left(\sum_{b\in\{0,1\}^r}\alpha_b\sum_{v\in C_2}|v+b\cdot G\rangle\right) = \sum_{b\in\{0,1\}^r}\alpha_b\sum_{u\in C_2^{\perp}}(-1)^{b\cdot G\cdot u}|u\rangle = \sum_{u\in C_2^{\perp}}\sum_{b\in\{0,1\}^r}\alpha_b(-1)^{b\cdot G\cdot u}|u\rangle$

Note that, since $C_2^{\perp} \subseteq C_1$, this is a superposition of elements of C_1 , so we can use the error-correcting properties of C_1 to correct

Then, applying Hadamards again, restores the codeword with up to d Z-errors corrected

CSS error correction III

The two procedures together correct up to d errors that can each be either an *X*-error or a *Z*-error — and, since Y = iXZ, they can also be *Y*-errors

From this, a standard linearity argument can be applied to show that the code corrects up to d arbitrary errors (that is, the error can be any quantum operation performed on up to d qubits)

Since there exist pretty good classical codes that satisfy the properties needed for the CSS construction, this approach can be used to construct pretty good quantum codes

For any noise rate below some constant, the codes have:

- finite rate (message expansion by a constant factor: r = n/m)
- error probability approaching zero as $n \rightarrow \infty$

Brief remarks about fault-tolerant computing

A simple error model



At each qubit there is an \times error per unit of time, that denotes the following noise: $\int I$ with probability 1- ϵ

 $\begin{bmatrix}
I \\
X \\
Y \\
Z
\end{bmatrix}$

with probability 1- ϵ with probability $\epsilon/3$ with probability $\epsilon/3$ with probability $\epsilon/3$

Threshold theorem

If ϵ is very small then this is okay—a computation of size* less than $1/(10\epsilon)$ will still succeed most of the time

But, for every constant value of ε , the size of the maximum computation possible is constant

Threshold theorem: There is a *fixed* constant $\varepsilon_0 > 0$ such that *any* computation of size *T* can be translated into one of size $O(T \log^c(T))$ that is robust against the error model with parameter ε_0

(The proof is omitted here)

* where size = (# qubits)x(# time steps)

Comments about the threshold theorem

Idea is to use a quantum error-correcting code at the start and then perform all the gates **on the encoded data**

At regular intervals, an error-correction procedure is performed, very carefully, since these operations are also subject to errors!

The 7-qubit CSS code has some nice properties that enable some (not all) gates to be directly performed on the encoded data: H and CNOT gates act "transversally" in the sense that:



Also, codes applied recursively become stronger