

Classical and Quantum Error Correcting Codes

Ana Sălăgean
Department of Computer Science
Loughborough University

November 2002

Classical error-correcting codes

Codeword: word over $\{0, 1\}$ or some other (finite) alphabet V

Code: a set C of codewords

Block code: all codewords have the same length n , i.e. $C \subseteq V^n$

Error: some symbols are changed, but we do not know which ones. We assume that only “a few” symbols are erroneous in each codeword and that all symbols have the same probability of having been changed (binary symmetric channel).

Error detection

Example: parity check bit

- detects one error
- cannot correct errors
- cannot detect 2 errors

Error correction

Main idea : the codewords have to be “sufficiently different” from each other so that we can still tell them apart even when “a few” errors occurred.

Example Repetition code

Triple each symbol: $0 \rightarrow 000, 1 \rightarrow 111$.

$$C = \{000, 111\}$$

$10 \rightarrow 111000 \rightsquigarrow 101001 \rightarrow 111000 \rightarrow 10$

can correct one erroneous symbol per codeword.

Hamming distance between two words: the number of positions in which they disagree.

Hamming distance of a code C : the minimum distance between two codewords in the code; denoted $d(C)$.

Hamming weight of a word w : the number of non-zero entries; denoted $\text{wt}(w)$.

Theorem A code with distance d is $(d - 1)$ -error detecting and $\lfloor (d - 1)/2 \rfloor$ -error correcting.

Linear Codes

It is useful to have codes with algebraic structure.

V is a finite field

$\{0, 1\} = \mathbb{Z}_2$ is a finite field with $+$ and \cdot modulo 2.

C is a $[n, k, d]$ linear code: C is a linear subspace of V^n

$k = \dim(C)$

$d = d(C)$

Theorem For C linear code,

$$d(C) = \min_{c \in C} \text{wt}(c)$$

C is described by a basis.

G generator matrix: $k \times n$ matrix having as rows a basis for C .

$$C = \{c \in V^n \mid c = mG, m \in V^k\}$$

H parity check matrix: $(n - k) \times n$ matrix such that

$$C = \{c \in V^n \mid cH^t = 0\}.$$

C^\perp the dual code of C (orthogonal complement):

$$C^\perp := \{a \in V^n \mid a \cdot c = 0 \text{ for all } c \in C\}$$

($a \cdot c$ inner product/scalar product)

Theorem C^\perp has generator matrix H and parity check matrix G .

Example The repetition code of length 3:

$$G = (1 \ 1 \ 1)$$

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

Example The $[7, 4, 3]$ Hamming Code:

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

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

Encoding and decoding with linear codes

Encoding: message $m \in V^k$ encoded as $c = mG$

Error: $e \in V^n$; received word: $r = c + e$.

Number of erroneous symbols = Hamming weight of e

Error detection: $rH^t = 0$?

Syndrome:

$$s := rH^t = cH^t + eH^t = eH^t$$

The syndrome depends only on the error, not on the codeword transmitted.

Theorem All errors of weight up to $\lfloor (d-1)/2 \rfloor$ have distinct syndromes.

For 1 error in the i -th bit, the syndrome is the i -th column of H .

Notions of Quantum Computing

$|0\rangle, |1\rangle$ two states

A *qubit* is in a *superposition* of the two states:

$$|q\rangle = a|0\rangle + b|1\rangle \quad a, b \in \mathbb{C}, |a|^2 + |b|^2 = 1$$

2 dimensional vector space over \mathbb{C}

n qubits are in an *entangled* state: an element of the tensor product of n 2-dimensional spaces.

Example: 2 qubits

$$a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$$

n qubits form a 2^n dimensional vector space over \mathbb{C} .

Quantum gates

Hadamard (Welsh-Hadamard) transform: 1 qubit gate

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

CNOT (controlled not): 2 qubit gate

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

Quantum error correcting codes

Repetition code: not possible

Theorem (no cloning) There is no quantum operation that takes a state $|\psi\rangle$ to $|\psi\rangle \otimes |\psi\rangle$ for all states $|\psi\rangle$.

The 9-qubit code (Shor)

One qubit is encoded into 9 qubits:

$$\begin{aligned} |0\rangle &\rightarrow |\bar{0}\rangle := (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \\ |1\rangle &\rightarrow |\bar{1}\rangle := (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \end{aligned}$$

Correction of bit flips:

$|010\rangle$ corrected to $|000\rangle$ by majority

Correction of phase flips:

$(|.\rangle - |.\rangle) \otimes (|.\rangle + |.\rangle) \otimes (|.\rangle + |.\rangle)$ corrected to
 $(|.\rangle + |.\rangle) \otimes (|.\rangle + |.\rangle) \otimes (|.\rangle + |.\rangle)$ by majority.

How to measure for error correction

How do we measure e.g. $|010\rangle$ to correct it to $|000\rangle$, without disturbing the state?

We use ancilla qubits, initialised to $|0\rangle$, which compute syndromes. Measuring them does not disturb the codeword. Their state tells which correction should be applied to the codeword.

Errors in quantum codes

The Pauli matrices:

$$\begin{aligned} I &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ Identity} \\ X &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ Bit flip} \\ Z &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ Phase flip} \\ Y &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \text{ Bit and phase flip} \end{aligned}$$

The Pauli group:

$$\mathcal{P}_n = \{\pm u_1 \otimes \cdots \otimes u_n, \pm i u_1 \otimes \cdots \otimes u_n \mid u_i \in \{I, X, Y, Z\}\}$$

Error in an n -qubit codeword: element of the Pauli group.

Hamming weight of an error: number of elements different from I in the tensor product.

More general errors:

- other errors on individual qubits, e.g. other phase shifts
- errors on n qubits that cannot be written as tensor products of n individual qubit errors.

Theorem Any quantum error correcting code that can correct errors of weight up to t in \mathcal{P}_n , can correct arbitrary errors in t qubits.

Systematic construction of error-correcting codes based on classical linear codes

Theorem (Calderbank, Shor, Steane)

C_1 a $[n, k_1, d_1]$ linear code

C_2 a $[n, k_2, d_2]$ linear code so that $C_2^\perp \subseteq C_1$

$k = \dim(C_1) - \dim(C_2^\perp) = k_1 - (n - k_2)$

$\mathcal{W} = \{w_1, \dots, w_{2^k}\}$ set of coset representatives of C_1/C_2^\perp .

Define

$$|\bar{i}\rangle = \frac{1}{\sqrt{|C_2^\perp|}} \sum_{c \in C_2^\perp} |c + w_i\rangle$$

Then $\{|\bar{i}\rangle | i = 1, \dots, 2^k\}$ are orthogonal states and span a quantum error correcting code \mathcal{C} of length n and dimension 2^k . \mathcal{C} can correct up to $(d_1 - 1)/2$ bit flip errors and up to $(d_2 - 1)/2$ phase flip errors.

Codes obtained by this construction are called *additive* codes.

Quantum code based on Hamming code

$C_1 = C_2 =$ the $[7,4,3]$ Hamming code.

$$G = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} g_4 \\ g_3 \\ g_2 \\ g_1 \end{pmatrix}$$
$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} g_1 \\ g_2 \\ g_3 \end{pmatrix}$$

$$k = 0$$

$$\mathcal{W} = \{0, g_4\}$$

$$|\bar{0}\rangle = \frac{1}{\sqrt{8}} \sum_{i_1, i_2, i_3 \in \{0,1\}} |0g_4 + i_3g_3 + i_2g_2 + i_1g_1\rangle$$

$$|\bar{1}\rangle = \frac{1}{\sqrt{8}} \sum_{i_1, i_2, i_3 \in \{0,1\}} |1g_4 + i_3g_3 + i_2g_2 + i_1g_1\rangle$$

Correction of phase flip errors: transform them into bit flip errors

$$HX = ZH \text{ and } HZ = XH$$

Other quantum error correcting codes:

- 1 qubit can be encoded by a 5 qubit code.
- constructions of quantum ecc based on classical ecc over $GF(4)$
- bounds on the parameters of quantum codes have been obtained
- quantum analogue of Shannon's theory giving the capacity of a channel still not fully solved.

Tutorial papers used in this presentation

M. Grassl, T. Beth, Relations between classical and quantum error-correcting codes, Workshop on Physics and Computer Science, Heidelberg 1999.

D. Gottesman, An introduction to quantum error correction, in *Quantum Computation*, S. Lomonaco (Ed) Proceedings of Symposia in Applied Mathematics, AMS, 2002.