MP 472 Quantum Information and Computation

http://www.thphys.may.ie/staff/jvala/MP472.htm

Outline

Open quantum systems

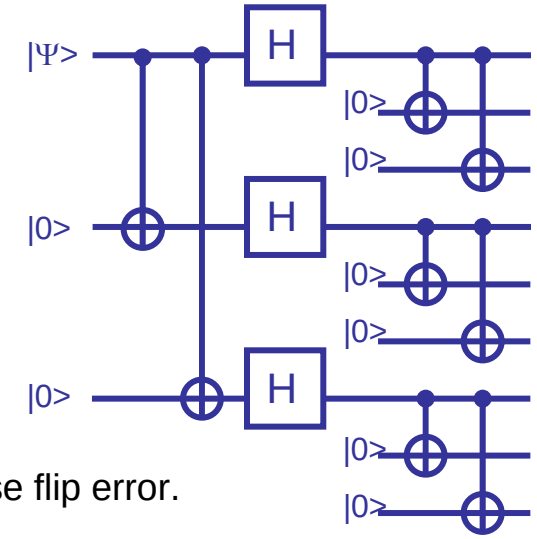
The density operator

Quantum noise (decoherence)

Quantum error correction
- Classical linear codes (cont.)
- Introduction to CSS codes

Fault-tolerant quantum computation

Shor code (review)



Encoding:

concatenated three-qubit quantum error correcting code

$|\psi\rangle = (c_0/2)^{3/2}[(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)]$

$+ (c_1/2)^{3/2}[(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)]$

Error

The code allows to correct any single qubit error, including the bit flip and phase flip error.

Error syndrome measurement

The full set of the bit flip syndromes is obtained by measuring the following six observables:

$$Z_1Z_2 \qquad Z_2Z_3 \qquad Z_4Z_5 \qquad Z_5Z_6 \qquad Z_7Z_8 \qquad Z_8Z_9$$

which detect whether the bit flip error occurred within each three-qubit block.
Since now the syndrom measurement has to identify on which three-qubit block the phase flip happened, the full set of the phase flip syndromes is obtained by measuring the following two observables:

$$X_1X_2X_3X_4X_5X_6 \qquad X_4X_5X_6X_7X_8X_9$$

Error recovery

If the bit flip error has been detected on k-th qubit, the state is fixed by applying X-operation on k-th qubit, X_k.

If the phase flip has been detected on j-th three-qubit block, then the state can be fixed by applying Z operation on each qubit of that block, i.e. by applying

$$Z_{3(j-1)+1}Z_{3(j-1)+2}Z_{(j-1)+3}$$

Classical linear codes (review)

A linear code C encoding k bits of information into a n bit code space is specified by n-by-k generator matrix G whose entries are elements of $\mathbb{Z}_2 = \{0,1\}$

message		encoded message
x	⟶	y = G(x) = Gx
		(all operations are mod2)

A code which uses n bits to encode k bits of information is an [n,k] code.

Error correction

Introducing **parity check matrix H:**
In this definition, an [n,k] code is defined to consist of all n-element vectors x over $\mathbb{Z}_2$ s.t.

$$H x = 0$$

Where H is an (n-k)-by-n matrix known as parity check matrix, with entries from zeros and ones, i.e. the code is defined by a kernel of H.

Error detection and recovery

Lets assume the encoding y = Gx.

Error e however corrupts y giving y' = y + e (bitwise addition).

Because Hy = 0 for all codewords, then Hy' = He

this is the error syndrome !!

Distance measures

The **Hamming distance** d(x,y) between x and y is defined to be the number of places at which x and y differ:
e.g. d((1,1,0,0),(0,1,0,1)) = 2.

Hamming weight of a word x:
wt(x) = d(x,0) (note d(x,y) = wt(x+y))

The **distance of a code C**
$d(C) = \min_{x,y \in C, x \neq y} d(x,y)$

But d(x,y) = wt(x+y) and since the code is linear, x+y is a codeword if x and y are codewords, so
$d(C) = \min_{x \in C, x \neq 0} wt(x)$

Setting d=d(C) then the code C can be described as [n,k,d] code.

Importance of distance:
If d > 2t+1, where t is an integer, the given code can correct up to t bits.

Hamming codes

A good illustrative class of linear ECC (error correcting codes).

Suppose an integer $r \geqq 2$, let H be the matrix whose columns are all 2^r-1 bit strings of length r which are not identically 0. This parity check matrix defines $[2^r\text{-}1, 2^r\text{-}r\text{-}1]$ linear code known as a Hamming code.

Example

[7,4] code

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

He_j gives a binary representation of j.

Gilbert-Varshamov bound

Let an [n,k] code, with large n, be an ECC protecting against errors on t bits for some k

$$k/n \geq 1 - H(t/n)$$

where $H(x) = -x\log(x) - (1-x)\log(1-x)$ is the binary Shannon entropy.

Calderbank-Shor-Steane (CSS) code

Dual construction of ECC

Let C be an [n,k] code with G and H, we can define another code, the dual of C, $C^{\perp}$, to be the code with the generator matrix H^T and the parity check matrix G^T.

Equivalently the dual of C consists of all codewords y s.t. y is orthogonal to all the codewords in C.

A code is said to be weakly self-dual if $C \subseteq C^{\perp}$, and
it is strictly self dual if $C = C^{\perp}$.

CSS Codes

Suppose C_1 and C_2 are $[n, k_1]$ and $[n, k_2]$ classical linear codes resp., such that $C_1 \subset C_2$ and both C_1 and $C_2^{\perp}$ can correct errors up to t bits. Then $CSS(C_1,C_2)$ is an $[n,k_1\text{-}k_2]$ code which can correct arbitrary error up to t qubits.

Furthermore, the error detection and recovery require only the application of Hadamard and CNOT gates, in each case a number of the gates is linear in the size of the code.