Topics in Quantum Information **U. Waterloo CO 781, Spring 2004**
Ashwin Nayak (Instructor) **Carlos A. Pérez-Delgado (Scribe)**
CSS Codes **June 8, 2004**

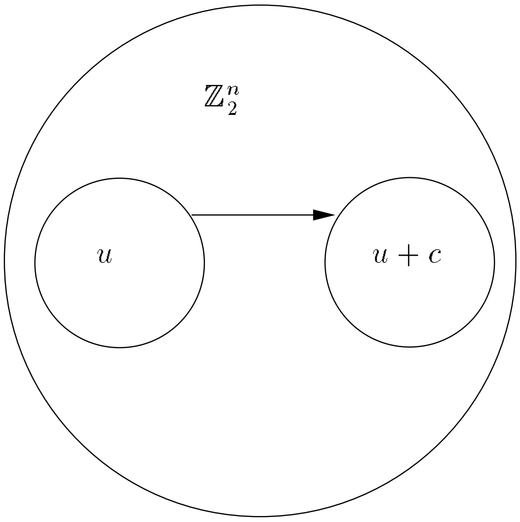
1 Calderbank-Shor-Steane (CSS) Codes

Recall from the last lecture that

Fact 1 *If C is an $[n,k,d]$ linear code in $\mathbb{Z}_2^n$ then $H^{\otimes n}|C\rangle = |C^\perp\rangle$, where $C^\perp$ is the dual $[n, n-k, d']$ code (with some minimum distance d').*

This extends to superpositions over cosets of C as well:

$$H^{\otimes n}|x + C\rangle = \frac{1}{2^{\frac{n-k}{2}}} \sum_{w \in C^\perp} (-1)^{x \cdot w} |w\rangle$$



Observation 1 Taking $x = e_i$ in the expression above, we see that the Hadamard tranform (the quantum Fourier transform over $\mathbb{Z}_2^n$) converts a bit error into a phase error, at the same location, and vice versa. This is captured by the relation $H\sigma_x = \sigma_z H$.

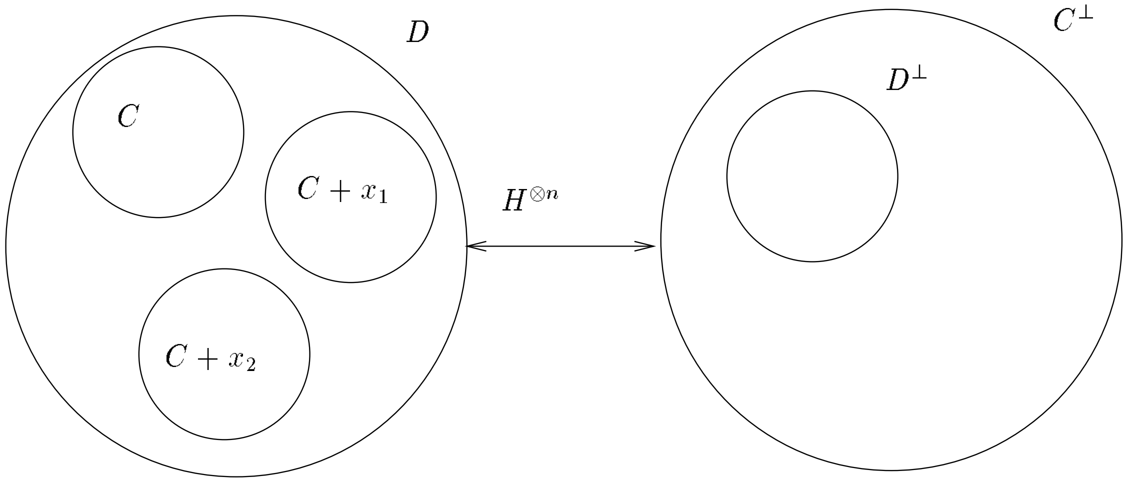
Observation 2 Correcting bit flips and phase flips (separately) suffices for quantum error-correction since every linear operator is generated by tensors of the Pauli operators. (The set of tensors $\bigotimes_{i=1}^n P_i$ of Pauli operators P_i form an orthonormal basis for the Hilbert space of $2^n \times 2^n$ complex matrices with respect to the trace inner-product $(A, B) = \mathrm{Tr}(B^\dagger A)$.)

This is a remarkable fact, since it gives us a way to handle a continuum of errors by reducing them to a finite set of unitary (and therefore correctable) error operators.

The classical theory of error correction tells us how we may handle bit errors. From these observations, we see that if both C and $C^\perp$ are error correcting codes that can correct t bit errors, then the state $|C\rangle$ is a quantum error correcting codeword that can correct an arbitrary error that operates on at most t locations. The CSS construction generalises this so as to to get a non-trivial information rate. The details follow.

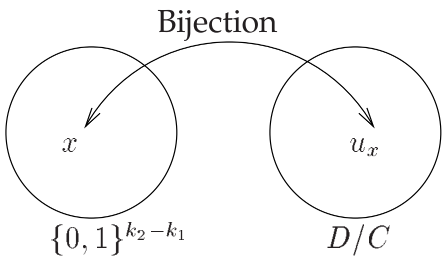
1.1 The construction

Let $\{0\} \subseteq C \subseteq D \subseteq \mathbb{Z}_2^n$ be an $[n, k_1, d_1]$ code and and $[n, k_2, d_2]$ code, respectively.



The code D can correct $t = \lfloor \frac{d_2 - 1}{2} \rfloor$ errors. We assume that $C^\perp$ can also correct at least t errors.

The construction is as follows. We need only encode standard basis states. We'll encode $k_2 - k_1$ logical qubits in n physical qubits.



For $x \in \{0,1\}^{k_2-k_1}$, let $u_x \in D$ be a canonical representative of the coset $u_x + C$ in D.

The code maps $|x\rangle \mapsto |u_x + C\rangle$, and in general (by linearity):

$$\sum_x \alpha_x |x\rangle \mapsto \sum_x \alpha_x |u_x + C\rangle = |\phi\rangle$$

The error correcting procedure is as suggested by the earlier discussion. We correct bit and phase errors separately, as follows:

1. Identify bit errors by identifying which coset of D a basis state lies in.
2. Correct bit errors by applying the unitary (error) operator σ_x at the appropriate (error) location.
3. Apply $H^{\otimes n}$, repeat steps (1) and (2) for the code $C^\perp$. This corrects the phase errors. Then recover $|\phi\rangle$ by applying $H^{\otimes n}$ once more.

The correction procedure for σ_y errors is split into two steps, since $\sigma_y = i\sigma_x\sigma_z = -i\sigma_z\sigma_x$. The extra phase is irrelevant, being only a global phase.

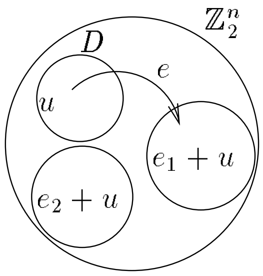
Note that the procedure effectively only measures the identity of the error operators, rather than any information about the encoded basis states. This ensures that the coherence of superpositions of basis states is preserved.

As long as the noise process is "local", i.e., only acts on at most t of the n physical qubits, the above construction protects arbitrary quantum states over k logical qubits.

Finally, we elaborate on a few steps in the CSS construction: how the errors are located, and then, whether codes C, D with the special properties described above indeed exist.

1.2 Correcting an error in a LECC

Let D be an $[n, k, d]$ linear code. An error e can be corrected as long as $h(e) \leq t = \left\lfloor \frac{d-1}{2} \right\rfloor$. Errors (only bit errors are possible classically) translate a codeword in D to a word in a coset of D in $\mathbb{Z}_2^n$. The cosets corresponding to different errors e_1 and e_2, (with $h(e_i) \leq t$) are distinct. To see why this is true, suppose the contrary. Then $e_1 + D = e_2 + D$ which implies $e_1 + e_2 \in D$, but $h(e_1 + e_2) \leq 2t < d$ where d is the minimum weight of D, clearly a contradiction.



Therefore, we need only identify which coset of D a corrupted word lies in.

Consider a basis $\{b_1, b_2, \ldots, b_{n-k}\}$ for $D^\perp$. The following matrix H is known as a parity check matrix for D:

$$H = \begin{pmatrix} \longleftarrow & b_1 & \longrightarrow \\ \longleftarrow & b_2 & \longrightarrow \\ & \vdots & \\ \longleftarrow & b_{n-k} & \longrightarrow \end{pmatrix}$$

Note that $Hw = 0$ iff $w \in D$. For any corrupted codeword $e + w$, $H(e + w) = He$, which uniquely identifies any error: if $h(e_1), h(e_2) \leq t$ then $He_1 = He_2$ implies that $e_1 = e_2$. This is because

$$He_1 = He_2 \implies H(e_1 + e_2) = 0 \implies e_1 + e_2 \in D \implies e_1 = e_2.$$

The vector He is called the error-syndrome of e. We can compute e given He efficiently for certain linear error correcting codes.

1.3 Reed-Muller Codes

The last piece is an explicit construction of a weakly self-dual code, that is, a linear code D such that $D^\perp \subseteq D$. Notice that this is exactly what we need for the CSS construction (we may choose $C = D^\perp$).

A Reed-Muller code is a generalization of Reed-Solomon codes. It is denoted by $\mathcal{R}(r, m)$, where r is the order of the code.

The code words are derived from multilinear polynomails $f : \mathbb{Z}_2^m \mapsto \mathbb{Z}_2$ of degree at most r in m variables.

The number of monomials of degree at most r is given by

$$k = \sum_{i=0}^{r} \binom{m}{i}.$$

Recall that a polynomial of degree at most r over $\mathbb{Z}_2$ may be seen as a subset of the set of all monomials of degree at most r. Hence the total number of polynomials of degree at most r is exactly 2^k.

A codeword is then the string of values of the polynomial at all points in $\mathbb{Z}_2^n$. Hence, $n = 2^m$.

Fact 2 *For Reed Muller codes:*

1. *The min-dist of $R(r, m)$ is $d = 2^{m-r}$.*
2. *$R(r, m)^{\perp} = R(m - r - 1, n)$.*

Note that $R(r, m) \subseteq R(r + 1, m)$. So if we choose $m \leq 2r + 1$, we get a weakly self-dual code.

If we choose r, m to be suitable fractions of n, e have that $n = 2^m$, $k = 2^{cm}$ and $d = 2^{\delta m}$, for constants c and δ. I.e., both the information rate and the error correction threshold are polynomial functions of the word length. Ideally, we would like to be able to simultaneously tolerate a constant error rate and carry a constant rate of information.

Codes in which we have $k = \Omega(n)$ and $d = \Omega(n)$ is called a *good code*. The Reed-Muller construction does *not* give us a good quantum code. It can be shown, via a counting argument, that good CSS codes exist.