1 CSS codes

In the previous lecture, we presented the Caldebank-Shor-Stein quantum error-correcting code. We began with two classical error-correcting codes C_1 and C_2, $C_1 \subset C_2$, with 2^{k_1} and 2^{k_2} n-bit codewords, respectively, such that $C_1^\perp$ and C_2 were each capable of correcting t errors. Then the cosets $\big|C_1 + x\big\rangle$ of C_1 in C_2 give a quantum code with $2^{k_2-k_1}$ codewords, which separately corrects t X and t Z errors. We used without proof the following claim:

Claim 1 $H\chi_z\big|C + x\big\rangle = (-1)^{x\cdot z}\chi_x\big|C^\perp + z\big\rangle$.

Proof: Recall $H\big|x\big\rangle = \frac{1}{\sqrt{2^n}}\sum_y (-1)^{x\cdot y}\big|y\big\rangle$. We write

$$H\chi_z\big|C + x\big\rangle \equiv H\frac{1}{\sqrt{|C|}}\sum_{y\in C}(-1)^{(y+x)\cdot z}\big|y + x\big\rangle \equiv \sum_w \alpha_w\big|w\big\rangle \quad .$$

Take $w \in C^\perp$, so $w \cdot y = 0$ for $y \in C$. Then

$$\alpha_{w+z} = \frac{1}{\sqrt{|C|}}\frac{1}{\sqrt{2^n}}\sum_{y\in C}(-1)^{(y+x)\cdot z}(-1)^{(y+x)\cdot(w+z)} = (-1)^{x\cdot z}\sqrt{\tfrac{|C|}{2^n}}(-1)^{x\cdot(w+z)} \quad .$$

Since $|C| \cdot |C^\perp| = 2^n$, $\sum_{w\in C^\perp}|\alpha_{w+z}|^2 = 1$, so all other coefficients are zero. ■

Thus to correct $\chi_{e_p}\big|C_1 + x + e_b\big\rangle$, we first correct in C_2 to $\chi_{e_p}\big|C_1 + x\big\rangle$. Then we apply H to obtain $\chi_x\big|C_1^\perp + e_p\big\rangle$. We can correct for the phase error e_p in C_1, then return to $\big|C_1 + x\big\rangle$ by another Hadamard transformation.

2 Classical versus quantum codes

Classical codes can detect $(1-\epsilon)n$ errors, correct $(1-\epsilon)n$ erasures, and correct $\frac{1-\epsilon}{2}$ errors, while still maintaining a constant rate δ. Since our quantum codes use two rounds of error correction, they can detect only $\frac{1-\epsilon}{2}n$ errors, correct $\frac{1-\epsilon}{2}n$ erasures, and correct $\frac{1-\epsilon}{4}n$ errors. These limits are in fact inherent: no QECC can correct $n/2$ erasures. Indeed, being able to recover from $n/2$ erasures would violate the no-cloning theorem. Moreover, one can show as an exercise that a QECC correcting t errors corrects $2t$ erasures, so our bounds are essentially tight.

However, quantum authentication somehow corrects $n/3$ errors – with very high probability.

3 Polynomial codes

A classical polynomial code encodes a message $a_1, \cdots, a_{d+1} \in \mathbf{F}_p$ as $f(1), \ldots, f(m)$, where f is the polynomial of degree at most d satisfying $f(j) = a_j$, $j = 1, \cdots, d+1$. Such f exists, and can be written explicitly

$$f(x) = \sum_k a_k \prod_{j \neq k} \frac{x-j}{k-j} \equiv \sum_k c_k(x) a_k \quad .$$

Since any two polynomials of degree at most d can agree at no more than d points, f is unique and the code is well-defined. The distance between codewords is at least d, so we can detect $m-d-1$ errors. The Berlekamp-Welch algorithm efficiently corrects $\lfloor \frac{m-d-1}{2} \rfloor$ errors.

4 Quantum polynomial codes

A *qupit* is a state $\sum_{a \in \mathbf{F}_p} \alpha_a \big|a\big\rangle$. An arbitrary qupit error is a $p \times p$ linear transformation in the vector space spanned by $B^x P^y$, where $B : \big|a\big\rangle \mapsto \big|a + 1 \bmod p\big\rangle$ is a bit error, and $P : \big|a\big\rangle \mapsto \omega^a \big|a\big\rangle$ is a phase error ($\omega = e^{2\pi i/p}$). We remark that $HB^xH = P^x$.

The quantum polynomial code, due to Aharonov and Ben-Or, encodes $a \in \mathrm{F}_p$ as

$$\big|C_a^d\big\rangle \equiv \frac{1}{\sqrt{p^d}} \sum_{\substack{f(0)=a \\ \deg(f) \leq d}} \big|f(1), \ldots, f(m)\big\rangle \quad .$$

As before, Berlekamp-Welch corrects $\lfloor \frac{m-d-1}{2} \rfloor$ bit errors. We need to show how to recover from phase errors.

For notational simplicity let $\bar{f} \equiv (f(1), \ldots, f(m))$. Let $c_j \equiv \prod_{i \neq j} \frac{-i}{j-i}$, $j = 1, \ldots, m$, be the interpolation coefficients at zero. For $x, y \in \mathbf{F}_p^m$, define $x \cdot_c y \equiv c_1 x_1 y_1 + \cdots c_m x_m y_m$. Consider $e_p \in \mathrm{F}_p^m$ with at most $\lfloor \frac{d}{2} \rfloor$ nonzero components, and let the corrupted codeword be

$$\chi_{e_p} \big|C_a^d\big\rangle \equiv \frac{1}{\sqrt{p^d}} \sum_{\substack{f(0)=a \\ \deg(f) \leq d}} \omega^{e_p \cdot_c \bar{f}} \big|\bar{f}\big\rangle \quad .$$

Define $H_p(\omega^c)$ to be the Fourier transform mod p using ω^c as the primitive p-th root of unity, i.e., for $x \in \mathbf{F}_p$, $H_p(\omega^c)\big|x\big\rangle = \frac{1}{\sqrt{p}} \sum_{y \in \mathbf{F}_p} \omega^{cxy} \big|y\big\rangle$. Let $H \equiv H_p(c_1) \otimes \cdots \otimes H_p(c_m)$. Then

$$H\chi_{e_p}\big|C_a^d\big\rangle = \frac{1}{\sqrt{p^d}} \sum_{\substack{f(0)=a \\ \deg(f)\leq d}} \omega^{e_p \cdot_c \bar{f}} H\big|\bar{f}\big\rangle \equiv \sum_y \alpha_y \big|y\big\rangle \quad .$$

The coefficient of $\big|y - e_p\big\rangle$ is

$$\alpha_{y-e_p} = \frac{1}{\sqrt{p^d}\sqrt{p^m}} \sum_{\substack{f(0)=a \\ \deg(f)\leq d}} \omega^{e_p \cdot_c \bar{f}} \omega^{(y-e_p)\cdot_c \bar{f}} = \frac{1}{\sqrt{p^{m+d}}} \sum_{\substack{f(0)=a \\ \deg(f)\leq d}} \omega^{y \cdot_c \bar{f}} \quad .$$

Take g any polynomial of degree at most $m-d-1$ with $g(0) = b$. Then $\bar{g} \cdot_c \bar{f} = c_1 g(1) f(1) + \cdots + c_m g(m) f(m) = (gf)(0) = g(0)f(0) = ba$, where the second equality is by interpolation (on a polynomial of degree at most $m-1$). Thus $\alpha_{\bar{g}-e_p} = \omega^{ab}/\sqrt{p^{m-d}}$. Now since there are p^{m-d-1} such g for each b, and p possible choices for b, we have accounted for all the nonzero coefficients α_y:

$$H\chi_{e_p}\big|C_a^d\big\rangle = \frac{1}{\sqrt{p^{m-d}}} \sum_{\deg(g)\leq m-d-1} \omega^{ag(0)} \big|\bar{g} - e_p\big\rangle \quad .$$

We have now converted the phase error to a bit error, which we can correct using Berlekamp-Welch (since e_p has weight at most $\lfloor \frac{d}{2} \rfloor = \lfloor \frac{m-(m-d-1)-1}{2} \rfloor$). The state is then

$$\frac{1}{\sqrt{p^{m-d}}} \sum_{\deg(g)\leq m-d-1} \omega^{ag(0)} \big|\bar{g}\big\rangle \quad .$$

Apply the Fourier tranform $H_p(-c_1) \otimes \cdots \otimes H_p(-c_m)$. If f is a polynomial of degree at most d with $f(0) = a$, then the coefficient of $\big|\bar{f}\big\rangle$ is

$$\frac{1}{\sqrt{p^{m-d}}} \sum_{\deg(g)\leq m-d-1} \omega^{ag(0)} \frac{1}{\sqrt{p^m}} \omega^{-\bar{g}\cdot_c \bar{f}} = \frac{1}{\sqrt{p^d}} \quad ,$$

where the exponents of ω cancel by interpolation. Therefore the correct codeword $\big|C_a^d\big\rangle$ is restored.

5 Overview of fault-tolerant computation

Consider the generalized CNOT gate: $\big|a\big\rangle \otimes \big|b\big\rangle \mapsto \big|a\big\rangle \otimes \big|a + b \bmod p\big\rangle$. On quantum polynomial encodings, the CNOT operation is tranversal. That is, if the input encodings are $\big|C_a\big\rangle = \sum_f \big|f(1), \ldots, f(m)\big\rangle$ and $\big|C_b\big\rangle = \sum_g \big|g(1), \ldots, g(m)\big\rangle$, then $\big|C_{a+b}\big\rangle =$

$\sum_h \left|h(1), \ldots, h(m)\right\rangle = \sum_{f,g} \left|(f+g)(1), \ldots, (f+g)(m)\right\rangle$. (Note that if h is a polynomial with $h(0) = a+b$, $\deg(h) \leq d$, then there are exactly p^m different f and g – $f(0) = a, g(0) = b$, $\deg(f), \deg(g) \leq d$ – with $h = f + g$.) We can also add a constant to a qupit transversally. Therefore these gates can be accomplished without decoding and without spreading any possible errors across pit positions.

To get a universal set of fault-tolerant gates, we need to show how to implement the generalized Toffoli gate: $\left|a\right\rangle \left|b\right\rangle \left|c\right\rangle \mapsto \left|a\right\rangle \left|b\right\rangle \left|c + ab \bmod p\right\rangle$. We'd like to write $\left|C_{ab+c}\right\rangle = \sum_{f,g,h} \left|f(1)g(1) + h(1), \ldots\right\rangle$, but multiplying polynomials increases the degree. A degree-reduction technique is needed, taking $\left|C_a^{2d}\right\rangle$ to $\left|C_a^d\right\rangle$ with decoding and exposing a.