Quantum Coding Theory **(UC Berkeley CS294, Spring 2024)**

Lecture 10: Polynomial Codes, Bounds on Codes

February 23, 2024

Lecturer: John Wright *Scribe: Rohit Agarwal*

1 Polynomial Codes

Recall that last time, we were constructing a large alphabet qudit CSS code based on the Reed-Solomon (classical) code.

Definition 1.1. The **Reed-Solomon Code** over $\mathbb{Z}_p = \{0, \dots, p-1\}$ is

$$\mathrm{RS}_d := \{\mathrm{val}(f) : f(x) = f_0 + f_1 x + \cdots + f_d x^d\}$$

where the evaluation vector $\mathrm{val}(f)$ is defined over nearly the entire space,

$$\mathrm{val}(f) := (f(1), f(2), \dots, f(p-1)).$$

Defining $n = p - 1$, this yielded that RS_d is a $[n, d+1, n-d]_p$ code. This is a linear code, and there is a "nice" basis for it as $\mathrm{val}(1), \mathrm{val}(x), \dots, \mathrm{val}(x^d)$, since the set of degree at most d polynomials is spanned by these monomials.

1.1 The Dual of Reed-Solomon

It turns out the dual to the RS code is also easy.

Definition 1.2. A **primitive root** mod p is $r \in \mathbb{Z}_p$ such that $\{r^0, r^1, \dots, r^{p-2}\} = \mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$.

Example 1.3. *For example, we can observe that* 2 *is primitive mod* 5*, as*

$$r^0 \equiv 1, r^1 \equiv 2, r^2 \equiv 4, r^3 \equiv 3, r^4 \equiv 1$$

So instead we will henceforth reorder $\mathrm{val}(f) = (f(r^0), f(r^1), \dots, f(r^{p-2}))$.

Fact 1.4. *The parity checks for* RS_d *are* $\mathrm{val}(x^c)$ *for* $1 \le c \le (p-2) - d$*. Therefore,*

$$\mathrm{RS}_d^\perp = \mathrm{Span}\{\mathrm{val}(x^c) : 1 \le c \le (p-2) - d\} = \{\mathrm{val}(g) = g_1 x^1 + g_2 x^2 + \cdots + g_{(p-2)-d} x^{(p-2)-d}\}$$

Proof. We only need to check that basis elements satisfy this parity checks. Since we have the right amount of independent parity checks, we are done. Consider for $0 \le i \le d$,

$$\begin{aligned}\mathrm{val}(x^i) \cdot \mathrm{val}(x^c) &= (r^0)^i (r^0)^c + (r^1)^i (r^1)^c + \cdots + \\ &= (r^0)^{i+c} + (r^1)^{i+c} + \cdots + (r^{p-2})^{i+c}\end{aligned}$$

Calling $x = r^{i+c}$, we can rewrite this as

$$\mathrm{val}(x^i) \cdot \mathrm{val}(x^c) = \sum_{j=0}^{p-2} x^j = \frac{x^{p-1} - 1}{x - 1}$$

But, we know that $i + c \neq 0$ by the bounds we have placed, so $x \neq 1$ and also $x \neq 0$ because it is a power of r. So by Fermat's little theorem, $x^{p-1} \equiv 1$ and the denominator doesn't vanish, so the dot product is 0. □

Corollary 1.5. $\mathrm{RS}_{d_1}^{\perp} \subseteq \mathrm{RS}_{d_2}$ *if* $(p-2) - d_1 \leq d_2$*, e.g. when* $p \leq d_1 + d_2 + 2$*.*

With this condition in hand, we can define the polynomial code.

Definition 1.6. The **Polynomial code** is the qudit CSS code with $C_X = \mathrm{RS}_{d_X}, C_Z = \mathrm{RS}_{d_Z}$, where $d_X + d_Z + 2 \geq p$. This is a $[\![n, n - (n - d_X - 1) - (n - d_Z - 1), \min\{n - d_X, n - d_Z\}]\!]_p$ code.

It is typical to take $d = d_X = d_Z$. Then this becomes a $[\![n, 2d + 2 - n, n - d]\!]_p$ code. We will see next lecture that the Quantum Singleton bound shows that this is exactly the maximum distance of the code. Reparametrizing, we can write k as the size of the logical qudit space, writing this as a $[\![n, k, \frac{n-k}{2} + 1]\!]_p$ code. Parametrizing like this, the classical Reed-Solomon code is $[n, k, n - k + 1]_p$, so the distance is about half that of the classical version.

2 Bounds on Codes

We will search for what the optimal rate-distance trade-off(s) are for quantum codes. It turns out that most bounds for quantum codes come from classical codes.

2.1 Classical Bounds

For the theorems in this secetion, let $C \subseteq \{0,1\}^n$ be an $[n, k, d]$ code. Sometimes we will write $\Delta = \frac{n}{d}$. Then, by the definition of unique decodability, for any two distinct codewords $c_1, c_2 \in C$, the Hamming balls of radius $\frac{d-1}{2}$ must be disjoint. If they intersected, then there would be a word of distance $\frac{d-1}{2}$ away from both; but then there would be no way to decode such a received word. The volume of these Hamming balls are

$$\mathrm{vol}\left(n, \frac{d-1}{2}\right) = \sum_{i=0}^{\frac{d-1}{2}} \binom{n}{i}$$

Since there are 2^k elements in the code, the total volume of these disjoint balls cannot exceed the size of the entire space.

Theorem 2.1 (Hamming Bound)**.** *Any* $[n, k, d]$ *code satisfies*

$$2^k \mathrm{vol}\left(n, \frac{d-1}{2}\right) \leq 2^n$$

If there is equality, the set of these Hamming balls cover the entire space.

Definition 2.2. If a code satisfies the Hamming bound with equality, it is a **perfect code**.

Here are some examples of perfect codes.

1. The $[7, 4, 3]$ Hamming code.
2. The trivial code.
3. The repetition code.
4. The code with a single codeword.
5. The $[23, 12, 7]$ Golay code.

Let's now try to find a lower bound on a code we could possibly construct. Consider greedily constructing a distance d code C. We loop while there exists $x \in \{0, 1\}^n$ of distance at least d from C, and add x to C. At termination, the balls of radius $d - 1$ must completely cover the space; if they didn't, there would exist a word that is distance at least d from C, which would contradict termination. Thus, the balls of $\text{vol}(n, d - 1)$ must cover the space.

Theorem 2.3 (Gilbert-Varshamov (GV) Bound)**.** *There exists a* $[n, k, d]$ *code* C *such that*

$$|C| \cdot \text{vol}(n, d - 1) \geq 2^n.$$

It turns out linear codes can attain this bound as well (by e.g. greedily choosing the columns of the generator matrix).

2.2 Asymptotic Classical Bounds

We can write these formulae a bit nicer if our codes are "good" e.g. $d = \Theta(n)$.

Definition 2.4. The **binary entropy** function is

$$h(x) = -x \log_2(x) - (1 - x) \log_2(1 - x).$$

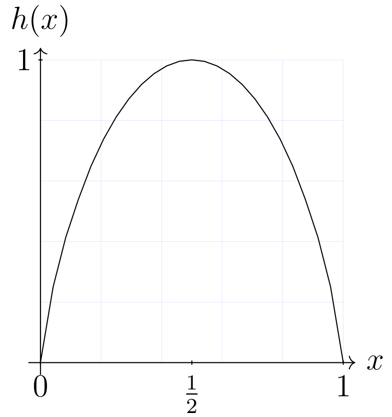

Figure 1: A plot of the binary entropy function.

Fact 2.5. *Assume $\delta := \ell/n \leq 1/2$. Then,*

$$\frac{1}{n+1} 2^{nh(\delta)} \leq \mathrm{vol}(n,\ell) \leq 2^{nh(\delta)}$$

So this means that $n(h(\delta) - o(1)) \leq \log_2 \mathrm{vol}(n,\ell) \leq nh(\delta)$. Taking log of both sides of 2.1 and 2.3, we get the following estimates:

Theorem 2.6 (Asymptotic Hamming Bound)**.** *For a $[n, k, \Delta n]$ code, we have*

$$k \leq n(1 - h(\Delta/2)).$$

Theorem 2.7 (Asymptotic Gilbert-Varshamov Bound)**.** *There exists a $[n, k, \Delta n]$ code with*

$$k \geq n(1 - h(\Delta)).$$

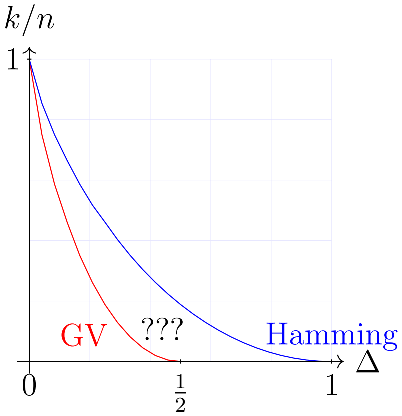

Figure 2: A plot comparing the two classical bounds.

An open question in coding theory is achieving an explicit, efficiently decodable binary code that lies between these two bounds (we have such codes for larger alphabets). Another open question is what the optimal trade-off between a code's dimension ("rate") and distance are.

2.3 Quantum Bounds

Let C be a nondegenerate $[\![n,k,d]\!]$ quantum ECC and let $\{|\overline{x}\rangle\}_{x\in\{0,1\}^k}$ be an orthonormal basis of C. This can correct any Pauli error P of weight at most $\frac{d-1}{2}$. Then consider the collection $\{P\,|\overline{x}\rangle : |\overline{x}\rangle_{x\in\{0,1\}^k}, P \text{ correctable}\}$. For all correctable Paulis, since there is no degeneracy, no Pauli can be a linear combination of other Paulis. Combined with the Knill-Laflamme conditions, we can conclude all of these vectors must be linearly independent. Since the whole Hilbert space of states has dimension 2^n, this set has size as most 2^n. There are 2^k choices for $|\overline{x}\rangle$, and $\mathrm{Qvol}\big(n, \frac{d-1}{2}\big) := \sum_{i=0}^{\frac{d-1}{2}} \binom{n}{i} 3^i$ choices for P (there are 3 types of error Paulis, and we have to choose i places to put them).

Theorem 2.8 (Quantum Hamming Bound)**.**

$$2^k \cdot \mathrm{Qvol}\left(n, \frac{d-1}{2}\right) \leq 2^n$$

If $d = 3$, this bound looks like $2^k(1+3n) \leq 2^n$. Note that is tight for the $[\![5,1,3]\!]$ code. Thus we also term this code a **perfect code**.
There is also a quantum Gilbert-Varshamov Bound, greedily picking stabilizers.

Theorem 2.9 (Quantum Gilbert-Varshamov Bound)**.** *There exists $[\![n,k,d]\!]$ stabilizer code where*

$$2^k \cdot \mathrm{Qvol}(n, d-1) \geq 2^n$$

There are also similar estimates on the quantum volume that gets asymptotic versions.

Fact 2.10. *Assume $\ell \leq n/2$.*

$$\frac{1}{n+1} 3^\ell 2^{nh(\delta)} \leq \mathrm{Qvol}(n,\ell) \leq 3^\ell 2^{nh(\delta)}$$

Therefore, $\log_2 \mathrm{Qvol}(n,\ell) \approx nh(\delta) + n\delta \log_2(3)$.

Theorem 2.11 (Asymptotic Quantum Hamming Bound)**.** *For a $[\![n,k,\Delta n]\!]$ code, we have*

$$k \leq n\left(1 - h(\Delta/2) - \frac{\Delta}{2}\log_2(3)\right).$$

Theorem 2.12 (Asymptotic Gilbert-Varshamov Bound)**.** *There exists a $[\![n,k,\Delta n]\!]$ code with*

$$k \geq n(1 - h(\Delta) - \Delta \log_2(3)).$$

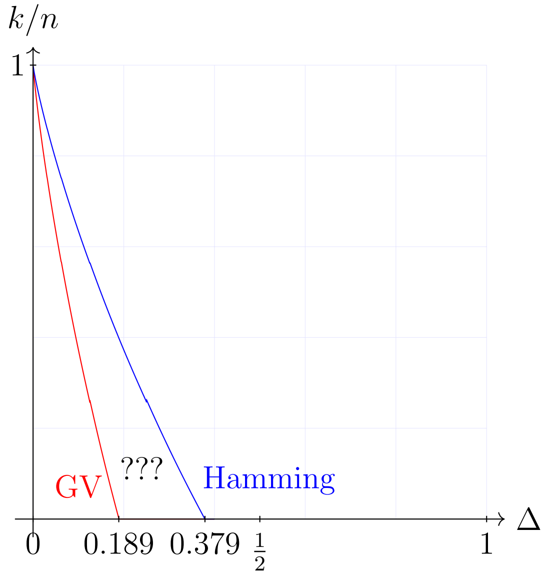

Figure 3: A plot comparing the two quantum bounds.