Code Concatenation

Amnon Ta-Shma and Dean Doron

1 Code Concatenation

See Chapter 9.1 of [1].

1.1 Concatenating RS with Hadamard

Consider a RS code $\mathsf{RS} : \mathbb{F}_q^k \to \mathbb{F}_q^n$ for $n \le q$ for the outer code $\mathcal{C}_{out}$, and a Hadamard code $\mathsf{Had} : \{0,1\}^{\log q} \to \{0,1\}^q$ for the inner code $\mathcal{C}_{in}$. This gives $\mathsf{RS} \circ \mathsf{Had} : \{0,1\}^{k \log q} \to \{0,1\}^{nq}$ such that for every $x \in \{0,1\}^{k \log q} \cong \mathbb{F}_q^k$,

$$(\mathsf{RS} \circ \mathsf{Had})(x) \;=\; (\mathsf{Had}(\mathsf{RS}(x)_1), \ldots, \mathsf{Had}(\mathsf{RS}(x)_n)) \,.$$

By previous arguments, the code is linear, has relative rate $\frac{k \log q}{nq}$ and also:

Claim 1. *Let $\delta_1 = 1 - \frac{k}{n}$ be the relative distance of* RS *and $\delta_2 = \frac{1}{2}$ be the relative distance of* Had*. Then,* $\mathsf{RS} \circ \mathsf{Had}$ *is a code of relative distance $\delta_1 \delta_2 = \frac{1}{2} - \frac{k}{2n}$.*

1.2 Concatenating Hermitian with Hadamard

In an earlier lecture, we took $p = q^2$ and constructed an

$$\left[n = p\sqrt{p}, k, n - \sqrt{2k}(\sqrt{p}+1)\right]_p$$

code for $k \le \frac{p}{2}$. Concatenating it with the Hadamard code $\mathsf{Had} : \{0,1\}^{\log p} \to \{0,1\}^p$, we get an

$$\left[p^2\sqrt{p}, k \log p, \frac{p}{2}\left(p\sqrt{p} - \sqrt{2k}(\sqrt{p}+1)\right)\right]_2$$

code. Its relative distance is

$$\frac{\frac{p}{2}\left(p\sqrt{p} - \sqrt{2k}(\sqrt{p}+1)\right)}{p^2\sqrt{p}} \;\approx\; \frac{1}{2} - \frac{\sqrt{k}}{\sqrt{2}p},$$

which is better than $\mathsf{RS} \circ \mathsf{Had}$.

Let's compare the length of the concatenated codes N as a function of their dimension K and their *bias*, which is $\varepsilon = \frac{1}{2} - \frac{d}{n}$. For $\mathsf{RS} \circ \mathsf{Had}$, it is

$$N = O\left(\left(\frac{K}{\varepsilon \log q}\right)^2\right).$$

By taking the Hermitian code instead of RS, we get

$$N = O\left(\left(\frac{K}{\varepsilon^2 \log p}\right)^{5/4}\right).$$

A simple manipulation allows us to lose the $\log q$ and $\log p$ factors. Towards the end of the course we will re-visit the relation $N(K, \varepsilon)$ in depth.

2 Justensen code

We now show that by using different concatenation in each coordinate we can get an explicit binary code of constant relative rate and constant relative distance – an *asymptotically good* code.

See the separate handout, and also Chapter 9.3 of [1].

3 Decoding concatenated codes

For the naive decoding and the GMD algorithm, see Chapter 11 of [1].

References

[1] Venkatesan Guruswami, Atri Rudra, and Madhu Sudan. *Essential Coding Theory*. 2015. Available at `http://www.cse.buffalo.edu/faculty/atri/courses/coding-theory/book`.