1 Code Concatenation

See Chapter 9.1 of [1].

1.1 Concatenating RS with Hadamard

Consider a RS code \( \text{RS} : \mathbb{F}_q^k \rightarrow \mathbb{F}_q^n \) for \( n \leq q \) for the outer code \( C_{out} \), and a Hadamard code \( \text{Had} : \{0,1\}^{\log q} \rightarrow \{0,1\}^{q} \) for the inner code \( C_{in} \). This gives \( \text{RS} \circ \text{Had} : \{0,1\}^{k \log q} \rightarrow \{0,1\}^{nq} \) such that for every \( x \in \{0,1\}^{k \log q} \)

\[
(\text{RS} \circ \text{Had})(x) = (\text{Had}(\text{RS}(x)_1), \ldots, \text{Had}(\text{RS}(x)_n)).
\]

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 \( \text{RS} \) and \( \delta_2 = \frac{1}{2} \) be the relative distance of \( \text{Had} \). Then, \( \text{RS} \circ \text{Had} \) 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 \( k \leq \frac{p}{2} \). Concatenating it with the Hadamard code \( \text{Had} : \{0,1\}^{\log p} \rightarrow \{0,1\}^{p} \), 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

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

which is better than \( \text{RS} \circ \text{Had} \).

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 \( \text{RS} \circ \text{Had} \), it is

\[
N = O \left( \left( \frac{K}{\varepsilon \log q} \right)^2 \right).
\]
By taking the Hermitian code instead of RS, we get

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

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 \( N(K, \epsilon) \) 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 \textit{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