BCH Codes

BCH codes are binary codes obtained from RS codes, not by code concatenation, but by restricting to "subfield subcodes". Here, the "subfield" of $\mathbb{F}$ is precisely $\mathbb{F}_2$ and a BCH code is obtained as that largest binary subcode of an RS code. More precisely, recall from the parity-check characterization of RS codes that when $S = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$, for some primitive element $\alpha \in \mathbb{F}^*$,

$$RS[n,k] = \{(c_0, \ldots, c_{n-1}) \in \mathbb{F}^n : c(X) = c_0 + c_1 X + \ldots + c_{n-1} X^{n-1} \text{ obeys}$$
$$c(\alpha) = c(\alpha^2) = \cdots = c(\alpha^{n-k}) = 0\}.$$

HW: Show this. [One uses the fact that $\sum_{\alpha \in \mathbb{F}^*} \alpha^i = 0$, for $1 \le i < q-1 = n$, yielding $\sum_{\alpha \in \mathbb{F}^*} \alpha^i \alpha^j = 0$, for $0 \le i < k$ and $1 \le j \le n-k$]

The binary BCH code $BCH[n,d]$ is:

Def 2: For $n = 2^m - 1$ and a primitive element $\alpha \in \mathbb{F}^*$,

$$BCH[n,d] = \{(c_0, \ldots, c_{n-1}) \in \mathbb{F}_2^n : c(X) = c_0 + c_1 X + \ldots + c_{n-1} X^{n-1} \text{ obeys}$$
$$c(\alpha) = c(\alpha^2) = \cdots = c(\alpha^{d-1}) = 0\}.$$

↓ note this!

Remark: Contrast the definition above with that of $RS[n, n-d+1]$!

$BCH[n,d]$ is a linear code with blocklength n and distance at least d. What is its dimension?

Lemma 4: We have that $\dim(BCH[n,d]) \geq n - \lceil \frac{d-1}{2} \rceil \cdot \log(n+1)$.

Proof: The $d-1$ constraints on $\underline{c} = (c_0, \cdots, c_{n-1})$ give rise to $(d-1)\log(n+1)$ constraints over $\mathbb{F}_2$ (not necessarily linearly independent). Hence, we must have $\dim(BCH[n,d]) \geq n - (d-1)\log(n+1)$. However, we can identify some linear dependencies among the constraints and tighten this bound.

In particular, note that for $\gamma \in \mathbb{F}$, if $c(\gamma) = 0$, then $c(\gamma^2) = 0$. To see this, observe that

$$c(\gamma) = 0 \iff (c(\gamma))^2 = 0$$

$$\Updownarrow$$

$$(c_0 + c_1\gamma + \cdots + c_{n-1}\gamma^{n-1})^2 = 0 \iff c_0^2 + c_1^2\gamma^2 + \cdots + c_{n-1}^2\gamma^2 = 0 \quad [\text{Why?}]_2$$

$$\Updownarrow$$

$$c(\gamma^2) = 0. \quad [\text{Why?}]$$

Hence, the number of constraints comes down by a factor of 2. ▨

Remark: As a consequence, note that

$$|BCH[n,d]| \geq \frac{2^n}{(n+1)^{\lceil \frac{d-1}{2} \rceil}};$$

for d = constant, we have that $\lim_{n \to \infty} R(BCH[n,d]) = 1$.

Further, from the Hamming bound, we have that (for d being even)

$$|BCH[n,d]| \leq \frac{2^n}{Vol\left(n, \frac{d-1}{2}\right)} = \frac{2^n}{\Theta\left(n^{\lceil \frac{d-1}{2} \rceil}\right)}.$$

Hence, BCH codes asymptotically match the Hamming bound (but only at rates ≈ 1).

Lecture: Decoding RS codes and An Introduction to RM Codes

In this lecture, we shall work towards a low-complexity algorithm for decoding RS codes. While any linear code can be decoded via standard array decoding (which is also MAP over the BSC), as seen earlier, such a decoding procedure has time (and space) complexity that is exponential in the blocklength n. Our objective is to come up with decoders that "work" in time $\approx$ poly(n).

Interpolating RS codes from erasures

Recall that the message vector $\underline{m} \in \mathbb{F}^K$ of an RS code is mapped to the polynomial

$$f(x) = m_0 + m_1 x + \cdots + m_{K-1} x^{K-1}$$

and then evaluated at points $\{\alpha_1, \cdots, \alpha_n\}$.

Now, suppose that upto $t \leq n-K = d-1$ erasures occur in a codeword $\underline{c} \in RS[n,K]$. Erasure decoding of RS codes is hence equivalent to interpolating a polynomial $(f(x))$ from its evaluations (at the unerased locations).

FACT: Any polynomial of degree $K-1$ is uniquely determined by its value at $n \geq K$ points.

HW: Prove the above fact using the fundamental theorem of algebra.