CSE522/Math581EB Coding Theory **Fall 2001**

Lecture 4: October 18

Lecturer: Chris Umans *Scribe: Matt Cary*

We are considering now $[n, k, d]_q$-codes, that is, linear codes that encode k bits into n bits over an alphabet of q characters such that the minimum distance of the code is d. Last time we built linear binary ($q = 2$) codes with minimum distance 1 (the identity map), 2 (parity check codes) and 3 (Hamming codes). The parity check codes introduced one extra bit—*i.e.* $n = k + 1$—and the Hamming codes introduce logarithmic extra bits. We argued that those codes were optimal in this sense, using the Hamming bound for $d = 3$.

Matters are more difficult for larger minimum distances. The Singleton bound claims that $d \leq n - k + 1$.[1] We showed that Reed-Solomon codes achieve the Singleton bound, but have the unfortunate property that $q \geq n$. In this lecture we try to improve on this, leading up to Reed-Muller codes, which have good minimum distance (although not optimal), and much smaller q. We begin by recapitulating Reed-Solomon codes.

4.1 Reed-Solomon Codes

Define RS_{nkq}, for $q \geq n$, as follows. Choose $c_0, \ldots, c_{n-1} \in \mathbb{F}_q$, all distinct.[2] A message $m = (m_0, \ldots, m_{k-1})$ with $m_i \in \mathbb{F}_q$ is viewed as the $k - 1$ degree polynomial

$$m(x) = \sum_{i=0}^{k-1} m_i x^i.$$

The encoding of m is the evaluation of $m(x)$ at all the c_i:

$$E(m) = (m(c_0), \ldots, m(c_{n-1})).$$

There are two claims.

First, RS_{nkq} is linear. This follows from the properties of adding polynomials.

The second and more interesting claim is that RS_{nkq} is a $[n, k, n - k + 1]_q$ code. That is, it matches the Singleton bound. This follows from the fact that a polynomial of degree $k - 1$ has at most $k - 1$ roots, and that if two polynomials agree on $\geq k - 1$ points, they must be the same polynomial.

Another way to see this is to remember that the minimum distance of a code, $\Delta(\mathcal{C})$, is equal to the minimum weight over non-zero codewords. The number of zeros in a codeword of RS_{nkq} is at most $k - 1$, so that the weight of a such a codeword is at least $n - k + 1$.

To make this more concrete, we show the generator matrix for RS_{nkq}. It will be a $k \times n$ VanDerMonde matrix:

$$\begin{bmatrix} 1 & 1 & & 1 \\ c_0 & c_1 & \cdots & c_{n-1} \\ c_0^2 & c_1^2 & & c_{n-1}^2 \\ \vdots & \vdots & \ddots & \vdots \\ c_0^{k-1} & c_1^{k-1} & \cdots & c_{n-1}^{k-1} \end{bmatrix}$$

[1] This holds for all codes, not just linear codes.

[2] The c_i are also parameters of the code, though we will leave them implicit. Usually it is best to think of $q = n$, so that the c_i are just all of $\mathbb{F}_q$.

4.2 An Improvement: Bivariate Codes

The drawback of Reed-Solomon codes is the condition that $q \geq n$. The problem is that we need each coordinate of a codeword to correspond to a distinct element of $\mathbb{F}_q$. If instead we use bivariate polynomials, then the codewords is formed by taking all points in a $q \times q$ square, so that q only needs to be $\sqrt{n}$.

Suppose we consider bivariate polynomials where the maximum degree in each variable is ℓ. Then there are $(\ell+1)^2$ coefficients:

$$m = \begin{bmatrix} m_{00} & \cdots & m_{0\ell} \\ \vdots & \ddots & \vdots \\ m_{\ell 0} & \cdots & m_{\ell\ell} \end{bmatrix}$$

Hence $k = (\ell+1)^2$. The polynomial associated with m is

$$m(x,y) = \sum_{i,j=0}^{\ell} m_{ij} x^i y^j,$$

and the encoding of m is

$$E(m) = (m(x,y) : x, y \in \mathbb{F}).$$

Thus now we only require that $q^2 = n$.

This is a linear code, by using the same properties of polynomials as for Reed-Solomon codes. Computing the minimum distance is a little more complicated. We claim that

$$d \geq \left(1 - \frac{2\ell}{q}\right) n.$$

Note that the claim is that at most a $(2\ell)/q$ fraction of points of $\mathbb{F}_q \times \mathbb{F}_q$ can be zeros of a bivariate polynomial with maximum degree ℓ in each variable. This fact follows from the Schwartz-Zippel Lemma.

Lemma 4.1 (Schwartz-Zippel) *Given $Q(x_1, \ldots, x_n) : \mathbb{F}_q^n \to \mathbb{F}_q \not\equiv 0$ a polynomial of total degree d (that is, the sum of exponents of variables in any monomial of Q is at most d), then*

$$\Pr_{r_1,\ldots,r_n}[Q(r_1, \ldots, r_n) = 0] \leq \frac{d}{q}. \tag{4.1}$$

Note that as the bivariate polynomials used in our code have total degree $\leq 2\ell$, the minimum distance claim follows immediately.

Proof: We induct on the number of variables, n. For $n = 1$, we are dealing with univariate polynomials, so the Fundamental Theorem of Algebra says there are at most d roots.

For general n, there are two cases. If Q does not depend on x_1, that is $Q(x_1, \ldots, x_n) = Q'(x_2, \ldots, x_n)$, then by induction Q' has at most d roots. Otherwise, write

$$Q(x_1, \ldots, x_n) = \sum_{i=0}^{k} x_1^i Q_i(x_2, \ldots x_n),$$

where $k > 0$ is the maximum degree of x_1, and the Q_i are polynomials in $x_2, \ldots, x_n$. We have by induction that

$$\Pr_{r_2,\ldots,r_n}[Q_k(r_2, \ldots, r_n) = 0] \leq \frac{d-k}{q}. \tag{4.2}$$

Now supposed for fixed $r_2, \ldots, r_n$ that $Q_k(r_2, \ldots, r_n) \neq 0$, let

$$p(x_1) = \sum^{k} x_1^i Q_i(r_2, \ldots, r_n) = Q(x_1, r_2, \ldots, r_n),$$

and note by the Fundamental Theorem that

$$\Pr_{r_1}[p(r_1) = 0] \leq \frac{k}{q}.$$

In other words,

$$\Pr_{r_1,\ldots,r_n}[Q(r_1, \ldots, r_n) = 0 | Q_k(r_2, \ldots, r_n) \neq 0] \leq \frac{k}{q}.$$

We digress for a moment to discuss probability. Given two events E_1, E_2,

$$\begin{aligned} \Pr[E_1] &= \Pr[E_1|E_2]\Pr[E_2] + \Pr[E_1|\overline{E_2}]\Pr[\overline{E_2}] \\ &\leq \Pr[E_2] + \Pr[E_1|\overline{E_2}]. \end{aligned}$$

Taking (4.2) to be E_2 and (4.1) to be E_1 we prove the lemma. ■

4.3 Reed-Muller Codes

Extending the ideas of the previous section to multivariate polynomials, we arrive at Reed-Muller codes. Let $\mathrm{RM}_{t\ell q}$ be a multivariate polynomial code, where t is the number of variables, ℓ is the total degree, and q is the field size. The notation now becomes a little cumbersome: we define a message m to be

$$m = (m_{i_1,\ldots,i_t} | i_1 + \cdots + i_t \leq \ell),$$

and the polynomial associated with m is

$$m(x_1, \ldots, x_t) = \sum_{i_1+\cdots+i_t \leq \ell} m_{i_1+\cdots+i_t} x_1^{i_1} \cdots x_t^{i_t},$$

and as expected $E(m) = (m(x_1, \ldots, x_t) | x_1, \ldots, x_t \in \mathbb{F}_q)$. The notation may obscure the fact that a message is simply a list of the coefficients of a general t-variate polynomial.

The task now is to compute the code parameters. $n = q^t$, analogous to the bivariate case. To compute k, consider the following method of choosing degrees for the variables. Place $t + \ell$ dots in a line. Mark t of them. The degree of x_1 is the number of dots to the left of the first mark, the degree of x_2 is the number of dots between the first two marks, etc. Dots to the right of the t-th mark are unused; they correspond to a monomial with total degree $< \ell$. This shows that

$$k = \left(\begin{array}{c} t+\ell \\ t \end{array} \right).$$

From the Schwartz-Zippel Lemma, we have $d = (1 - \ell/q)n$, so that $\mathrm{RS}_{t\ell q}$ is

$$\left[q^t, \left(\begin{array}{c} t+\ell \\ t \end{array} \right), (1 - \frac{\ell}{q})n \right]_q.$$

This is not a particularly informative sentence. We will attempt to argue that these parameters are indeed about what we want.

Fix $k = \binom{t+l}{t}$. We want a polynomial rate, that is $n = k^2 = q^t$. We want $d = (1 - \mathrm{o}(1))n$, with q as small as possible. If we set $q = \log^2 k$, then

$$t = \frac{\log k}{\log \log k}$$

so that

$$q^t = 2^{2 \log \log k \cdot \frac{\log k}{\log \log k}} = k^2.$$

Approximating, $k = \binom{t+\ell}{t} \geq \left(\frac{\ell}{t}\right)^t$. Then

$$\ell \leq k^{1/t} t = \log k \cdot \frac{\log k}{\log \log k} = \frac{\log^2 k}{\log \log k} = \mathrm{o}(q).$$

Thus $1 - \ell/q = 1 - \mathrm{o}(1)$, as desired.