Error Correcting Codes: Combinatorics, Algorithms and Applications **(Fall 2007)**

Lecture 26: ℓ-Wise Independent Sources

Wednesday, March 25, 2009

Lecturer: Atri Rudra *Scribe: Annonymous*

1 ℓ-Wise Independent Sources

In the first part of today's lecture, we will prove the following general result: any linear code $\mathbf{S} \subseteq \mathbb{F}_2^m$ with dual distance at least $\ell + 1$, is an ℓ-wise independent source. As a corollary, we see that the dual of the $BCH_{2,\log n,\ell+1}$ code is an ℓ-wise independent source of size $O\left(n^{\lfloor \frac{\ell}{2} \rfloor}\right)$. Next, we return to the question of an explicit asymptotically good code. The best construction we have seen so far is the trivial conversion of a Reed-Solomon (RS) code over $\mathbb{F}_{2^m}$ into a binary code using a linearity-preserving bijective map $f : \mathbb{F}_{2^m} \to \mathbb{F}_2^m$. We finally observed that we need to replace f by a code with large distance. Next lecture, we will see a general code composition technique called code concatenation that does exactly this. We recall the definition of an ℓ-wise independent source: A subset $\mathbf{S} \subseteq \{0,1\}^n$ is an ℓ-wise independent source if $(x_1, \ldots, x_n)$ if for a uniformly chosen random $(x_1, \ldots, x_n) \in \mathbf{S}$, $(x_1, \ldots, x_n)$ are ℓ-wise independent random variables. We saw last Friday, that given an efficient ℓ-wise independent source, $\mathbf{S}$ implies an $O(T(n) \cdot |\mathbf{S}|)$ time $(1 - 2^{-\ell})$ approximate algorithm for MAXEℓSAT, where $T(n) = O(n^2)$.

Lemma 1.1. *Let $\mathbf{S} \subseteq \mathbb{F}_2^n$ be a linear code such that $\mathbf{S}^\perp$ has distance $\geq \ell + 1$. Then, $\mathbf{S}$ is an ℓ-wise independent source.*

The above leads to the following result:

Corollary 1.2. *Let $\mathbf{S}^\perp$ be $BCH_{2,\log n,\ell+1}$. Then, $\mathbf{S}$ is an ℓ-wise independent source of size $o(n^{\lfloor \ell/2 \rfloor})$*

Proof. Recall $BCH_{2,m,d}$ is an

$$\left[n = 2^m, n - 1 - \left\lceil \frac{d-2}{2} \right\rceil m, d\right]_2 \text{ code.}$$

This implies that

$$\dim(\mathbf{S}) = \left\lceil \frac{\ell + 1 - 2}{2} \right\rceil \log n + 1 = \left\lceil \frac{\ell - 1}{2} \right\rceil \log n + 1 = \left\lfloor \frac{\ell}{2} \right\rfloor \log n + 1,$$

where we used the fact that for integer $\ell \geq 1$, $\left\lceil \frac{\ell+1-2}{2} \right\rceil = \left\lfloor \frac{\ell}{2} \right\rfloor$. Thus, we have

$$|\mathbf{S}| = 2^{\dim(\mathbf{S})} = O(n^{\lfloor \ell/2 \rfloor}),$$

as desired. As generator matrices of dual BCH codes are strongly explicit they are linear codes. We obtain for such ℓ-wise independent sources $T(n) = O\left(n^2\right)$. □

Next, we move to the proof of **Lemma 1.1**. To do this, we recall a property of linear codes that we proved earlier in the course:

Lemma 1.3. *If $\mathbf{C}^{\perp}$ has distance d, then any $d-1$ columns in a generator matrix for $\mathbf{C}$ are linearly independent.*

Proof. **Lemma 1.1:** First, recall that one way to think of a field element, is by defining a map $\beta \mapsto \alpha \cdot \beta$. If β is represented by its linear representation, α is a linear map from $\mathbb{F}_2^{\ell}$ to $\mathbb{F}_2^{\ell}$. If the linear representation L is fixed, then corresponding to α, we can define a map $M_{\alpha} : \mathbb{F}_2^{\ell} \to \mathbb{F}_2^{\ell}$, with $M_{\alpha}\left(L\left(\beta\right)\right) = L\left(\alpha \cdot \beta\right)$. Note that this map satisfies $M_{\alpha}\left(L\left(\beta\right) + L\left(\gamma\right)\right) = M_{\alpha}\left(L\left(\beta\right)\right) + M_{\alpha}\left(L\left(\gamma\right)\right)$. Since this is a linear map, this means that $\exists \mathbf{M}_{\alpha} \in \mathbb{F}_p^{k \times k}$ such that $M_{\alpha}(\mathbf{x}) = \mathbf{x}\mathbf{M}_{\alpha}$. In this case, $\mathbf{M}_{\alpha_1 \cdot \alpha_2} = \mathbf{M}_{\alpha_1} \cdot \mathbf{M}_{\alpha_2}$ and $\mathbf{M}_{\alpha_1 + \alpha_2} = \mathbf{M}_{\alpha_1} + \mathbf{M}_{\alpha_2}$. So addition and multiplication in the field are just addition and multiplication of matrices. Let $\mathbf{x} \in \mathbb{F}_2^{k}$ be a $1 \times k$ vector such that

$$\mathbf{x} = [\mathbf{x}_1 | \mathbf{x}_2],$$

when $\mathbf{x}_1 \in \mathbb{F}_2^{\ell}$ and $\mathbf{x}_2 \in \mathbb{F}_2^{k-\ell}$. This means that $\mathbf{x}_1$ is a $1 \times \ell$ vector, and $\mathbf{x}_2$ is $1 \times (k - \ell)$ vector. Making $\mathbf{x}$ a $1 \times k$ vector. Let $\mathbf{y} \in \mathbb{F}_2^{n}$ be an $(\ell + l_0 + l_1) \times 1$ vector such that

$$\mathbf{y} = \begin{bmatrix} \mathbf{y}_0 \\ \mathbf{y}_{\ell} \\ \mathbf{y}_1 \end{bmatrix}.$$

Note that $\mathbf{y}_0$ is $l_0 \times 1$ and $\mathbf{y}_1$ is $l_1 \times 1$. Let $\mathbf{G} = [\mathbf{G}_0 | \mathbf{G}_{\ell} | \mathbf{G}_1]$ be any generator matrix for $\mathbf{S}$. With $\mathbf{G}_0$ a $k \times l_0$ matrix and $\mathbf{G}_1$ a $k \times l_1$ matrix, $\mathbf{G}$ is a $k \times (\ell + l_0 + l_1)$ matrix with $\text{rank}(\mathbf{G}_{\ell}) = \ell$. $\mathbf{x} \cdot \mathbf{G} = \mathbf{y}^T$, from **Lemma 1.3**. Next note that any $k \times \ell$ matrix $\mathbf{M}$ of rank ℓ, with $k \geq \ell$, $\mathbf{x} \cdot \mathbf{G} = \mathbf{y}^T$ takes every value in $\mathbb{F}_2^{\ell}$ the same number of times $\forall \mathbf{x} \in \mathbb{F}_2^{k}$. Let

$$\mathbf{M} = \begin{bmatrix} \mathbf{M}_1 \\ \mathbf{M}_2 \end{bmatrix},$$

be a $k \times \ell$ matrix such that $\mathbf{M}_1$ is $\ell \times \ell$ and $\mathbf{M}_2$ is $(k - \ell) \times \ell$. Then form $\mathbf{x} \cdot \mathbf{M} = \mathbf{y}^T \in \mathbb{F}_2^{\ell}$, with $2^{k-\ell}$ choices. $\mathbf{x}_1\mathbf{M}_1 + \mathbf{x}_2\mathbf{M}_2 = \mathbf{y}^T$, or $\mathbf{x}_1\mathbf{M}_1 = \mathbf{y} - \mathbf{x}_2\mathbf{M}_2$, and there is exactly one solution to $\mathbf{x}_1\mathbf{M}_1 = b$ since $\mathbf{M}_1$ has full rank. □

2 The R Versus δ Question

Let us go back to the R versus δ question. We will now recollect all the explicit families of binary codes that we have seen so far and record the rate and relative distance they achieve. Can we find any explicit asymptotically good linear codes, with polynomial or log-space construction? Consider Hadamard codes:

$$R = \frac{\log n}{n}, \ \delta = \frac{1}{2}.$$

For dual $BCH_{2,\log n,2t+1}$ codes, we have:

$$R \sim \frac{t \log n}{n}\,,\ \delta = \frac{1}{2} - n^{-(t-1)}$$

This follows from the Weil-Carlitz-Uchiyama bound, which we state next.

Theorem 2.1. Weil-Carlitz-Uchiyama bound: *Any non-zero codewords in the dual of the $BCH_{2,m,2t+1}$ has Hamming weight w such that*

$$2^{m-1} - (t-1)2^{m/2} \leq w \leq 2^{m-1} + (t-1)2^{m/2},$$

provided $2t - 2 < 2^{m/2}$. All non-zero Hamming weight:

$$\in (\frac{1}{2} - n^{-(t-1)}, \frac{1}{2} + n^{-(t-1)}).$$

However, none of the codes above are asymptotically good. On the other hand, consider the Hamming code, for which we obtain

$$R = 1 - \frac{\log n}{n}\,,\ \delta = \frac{3}{n}.$$

Also, for BCH codes, we obtain the following for any constant $t \geq 1$:

$$R = 1 - \frac{t \log n}{n}\,,\ \delta = \frac{2t+1}{n}.$$

For a family of codes called Reed-Muller (RM) codes, which we have not studied so far, we can get:

$$R = \frac{1}{2}\,,\ \delta = \frac{1}{\sqrt{n}}.$$

Recall that RS codes are evaluations of univariate polynomials of bounded degree. RM codes are generalizations of RS codes in that they are evaluations of multivariate polynomials over the underlying $\mathbb{F}_q$. The Hadamard code is a special case where the degree of the polynomial is equal to 1. RS codes are asymptotically good codes but we have $q = n = 2^m$. Unlike RS codes, RM codes can be defined over any $\mathbb{F}_q$ including $q = 2$. Consider the case with $q = 2^n$, and we have an RS code of rate R_{RS} and relative distance δ_{RS}: (R_{RS}, δ_{RS}). A trivial conversion to a binary $BCH_{2,\log n,\ell+1}$ code gives

$$R = R_{RS}\,,\ \delta = \left\lceil \frac{\delta_{RS}}{\log n} \right\rceil.$$

With C_1 and $C_2 \in$ RS:

$$C_1 = (c_{0,1}, \ldots, \alpha, \ldots, c_{m,1})$$
$$C_2 = (c_{0,2}, \ldots, \beta, \ldots, c_{m,2})$$

Recall that a RS code over $\mathbb{F}_{2^m}$ can be converted into a binary code using a linearity-preserving bijective map $f : \mathbb{F}_{2^m} \to \mathbb{F}_2^m$. The problem is that if $\alpha \neq \beta$, all we can guarantee is that $\Delta(f(\alpha), f(\beta)) \geq 1$. To solve this problem, pick f to be a code with a large distance.