6.S897 Algebra and Computation May 9, 2012

Lecture 24

Lecturer: Madhu Sudan *Scribe: Zachary Abel*

1 Administrivia

- Tomorrow is the last day of project presentations: 10AM–11:50AM, room 32-G631.
- Please fill out course evaluations online.
- Class dinner tomorrow; details TBD.

2 Construction of Locally Decodable Codes

In this lecture we will develop a construction of locally decodable codes developed in three papers by Yekhanin, Raghavendra, and Eframenko respectively (and chronologically). Yekhanin constructed a family of binary locally decodable codes with a 3-query decoding algorithm based on Mersenne primes. Raghavendra simplified Yekhanin's construction and extended the ideas beyond binary alphabets. The final construction presented here is due to Efremenko, building on the two previous works.

2.1 Setup

We wish to construct an ℓ-query locally decodable code $E : \mathbb{F}_q^k \to \mathbb{F}_q^n$. We will specify this with a $k \times n$ generator matrix G (with columns $v_1, \ldots, v_n$), so the encoding function is $E(x) = xG$. Recall from last lecture that the following two rough properties suffice for local decodability

- Linear Combinations: For each $1 \leq i \leq k$, there should exist ℓ columns of G, say $v_{j_1}, \ldots, v_{j_\ell}$, whose span contains the ith elementary vector, $e_i = (0, \ldots, 1, \ldots, 0)$. So indices $j_1, \ldots, j_\ell$ could be used to decode the ith symbol.
- Column Symmetry: We should have some symmetry in the column space of G, so that the single linear combination above may be permuted into many, uniformly distributed ℓ-tuples that may be used to decode symbol i.

To achieve this aim, the construction of Yekhanin, Raghavendra, and Efremenko works over a field $\mathbb{F}_q$ with a primitive mth root of unity g (in particular, $m \mid q-1$) and chooses an integer $m \in \mathbb{Z}^+$ and a subset $S \subseteq \mathbb{Z}_m - \{0\}$. A matrix $M \in \mathbb{Z}_m^{k \times n}$ is called *S-nice* if

- For $1 \leq i, j \leq k$ with $i \neq j$ (i.e., on the leftmost $k \times k$ submatrix), we have $M_{ii} = 0$ and $M_{ij} \in S$, and
- the columns of M are closed under addition: for any $1 \leq j, j' \leq n$ (even $j = j'$), $v_j + v_{j'}$ is a column of M.

If we choose an S-nice matrix M, then the generating matrix G for our code is the $k \times n$ matrix $G = [g^{M_{ij}}]$, denoted $G = g^M$. We will prove:

Theorem 1 *If M is S-nice, then $G = g^M$ generates an $(|S|+1)$-query locally decodable code.*

Since the rate of the code is k/n, we want n as small as possible as a function of k. The following propositions indicate performance bounds in particular cases.

Theorem 2 *1. If m is prime and $S = \{1\}$, then $n \geq p^{k-1}$, and this bound is exactly achievable.*

2. If m is prime and S is a multiplicative subgroup of $\mathbb{Z}_m^*$, then $n \geq p^{(k-1)^{1/|S|}}$, and this bound can be very nearly achieved.

3. If $m = O(1)$ is composite (say $m = 6$) and $S = \mathbb{Z}_m^*$, then constructions exist with $n \leq \exp(\exp(\sqrt{\log k}))$.

The bound in part 1 is straightforward to prove but gives poor performance as an error correcting code. The second claim is a bit more challenging, and the construction uses the tensor product of vectors. Part 3 gives much better performance, and is the feature of today's discussion. The remainder of this lecture is spent proving this last claim of Theorem 2.

2.2 Sparseness Implies Local Decoding

The notion of *sparseness* will provide better locality for the resulting codes:

Definition 3 *The set S is t-*sparse *if there is a polynomial $p \in \mathbb{F}_q[x]$ such that $p(1) = 1$, $p(g^s) = 0$ for all $s \in S$, and p is t-sparse, i.e., p has at most t nonzero coefficients.*

Theorem 4 *If S is t-sparse, the code G can be locally decoded with t queries.*

Observation 5 *Because any S is $(|S|+1)$-sparse, Theorem 1 is a direct corollary of this result.*

Proof Say S is t-sparse with polynomial $p(x) = \sum c_d x^d$ with at most only t nonzero coefficients. We may assume $p(0) = 0$ by replacing the constant term c_0 with $c_0 x^m$. Let $u_1, \ldots, u_n$ be the columns of M. For any two indices $1 \leq j, j' \leq n$, the sum $u_j + u_{j'}$ is another column of M, so let $j \oplus j'$ denote the index of this column: $u_j + u_{j'} = u_{j \oplus j'}$.

Note that $p(g^{M_{ij}}) = \sum_d c_d g^{dM_{ij}}$ for $1 \leq i, j \leq k$, and by choice of p, this value is 1 if $i = j$ and 0 if $i \neq j$. Fix some j with $1 \leq j \leq k$. For each $d > 0$, write $j \oplus j \oplus \cdots \oplus j = j_d$ (there are d terms in the sum), so $d \cdot u_j = u_j + u_j + \cdots + u_j = u_{j_d}$. It follows that $\sum_d c_d v_{j_d} = e_j$, the jth elementary vector: indeed, the ith entry of this vector is

$$\sum_d c_d (v_{j_d})_i = \sum_d c_d g^{d \cdot M_{ij}} = p(g^{M_{ij}}),$$

which is 1 or 0 depending on $j = i$ or $j \neq i$, as needed. This gives us the *Linear Combination* property described above.

The *Symmetry* property is given by the following transformation: if $1 \leq r \leq n$ is chosen randomly, then we may "replace" the columns u_{j_d} by $u_{j_d} + u_r = u_{j_d \oplus r}$. Specifically, a similar computation shows that

$$\sum_d c_d \cdot v_{j_d \oplus r} = g^{M_{ir}} \cdot e_j.$$

So the local decoding algorithm to recover the jth symbol of message w is as follows: pick r randomly as above, query the values at indices $j_d \oplus r$ in the encoded message, and return $g^{-M_{ir}} \sum_d c_d w_{j_d \oplus r}$. Note that for each fixed d the quantity $j_d \oplus r$ is a uniformly random index (but the distributions for different ds are not independent), so a union bound shows that this successfully corrects an ϵ fraction of errors with probability $1 - d\epsilon$. ■

While our eventual construction will not rely on sparseness beyond $|S| + 1$, Yekhanin's original paper used this stronger idea to construct 3-query, binary locally decodable codes from Mersenne primes:

Lemma 6 (Yekhanin) *If $q = m + 1 = 2^t$ is a Mersenne prime, then $S = \{1, 2, 2^2, \ldots, 2^{t-1}\}$ is 3-sparse.*

Proof Because g is a primitive mth root of unity where $m = \left|\mathbb{F}_q^*\right|$, all elements in $\mathbb{F}_q^*$ are powers of g. In particular, $1 + g = g^i$ for some i, so define $p(x) = 1 + x + x^i$. We have $p(1) = 1 + 1 + 1 = 1$, and for each $0 \le t \le t - 1$, we have $1 + g^{2^t} = (1 + g)^{2^t} = (g^i)^{2^t}$, i.e., $p(g^{2^t}) = 0$. ■

2.3 OR Polynomials and the Final Construction

Efremenko's construction makes clever use of polynomials that compute a mod-m version of the OR of inputs on the $\{0, 1\}$ cube:

Definition 7 *A polynomial $f(x_1, \ldots, x_\ell) \in \mathbb{Z}_m[x_1, \ldots, x_\ell]$ is an* OR polynomial *if $f(0, \ldots, 0) = 0 \bmod m$ and $f(b_1, \ldots, b_\ell) \neq 0 \bmod m$ for all $(b_1, \ldots, b_\ell) \in \{0, 1\}^\ell - \{(0, \ldots, 0)\}$.*

These polynomials were studied by Rasborov and Smolensky, who showed that if m is prime, then any such polynomial has total degree $\Omega(\ell)$. It was conjectured that this bound would hold for composite m as well, but this is not the case:

Theorem 8 (Beigel, Barrington, Rudich) *If m is composite, there exists an ℓ-variable OR polynomial modulo m of degree $O(\ell^{1/r})$, where r is the number of prime factors of m.*

For example, there are OR polynomials for $m = 6$ of degree $O(\sqrt{\ell})$. Assuming this fact for now, we can complete Efremenko's construction of 6-query locally decodable codes with length $n \le \exp(\exp(\sqrt{\log k}))$.

Proof [Proof of Theorem 2 part 3] We take $m = 6$ and $S = \mathbb{Z}_m^*$, so the construction works for any $\mathbb{F}_q$ with a primitive 6th root of unity. Let $k = 2^\ell$ and identify $\{1, \ldots, k\}$ with $\{0, 1\}^\ell$, so the k rows of our matrix M are indexed by points of $\{0, 1\}^\ell \in \mathbb{Z}_m^\ell$. Let $f(x_1, \ldots, x_\ell) \in \mathbb{Z}_m[x_1, \ldots, x_\ell]$ be an OR polynomial of degree $d = O(\sqrt{k})$, and let the columns of M correspond to all polynomials in $\mathbb{Z}_m[x_1, \ldots, x_\ell]$ of total degree at most d. The number of such polynomials is $n \approx 6^{\ell^d} \approx 6^{2^{\sqrt{\ell}\log\ell}} \approx \exp(\exp(\sqrt{\log k}))$. The matrix M is defined as follows: For $u \in \{0, 1\}^\ell$ and $h \in \mathbb{Z}_m[x_1, \ldots, x_\ell]$ of degree $\le d$, define $M_{u,h} = h(u)$.

The columns of M are closed under addition because low-degree polynomials are closed under addition. It remains to find the $k \times k$ submatrix satisfying the first condition of S-niceness. For $u = (u_1, \ldots, u_\ell) \in \{0, 1\}^\ell$, define $h_u(x_1, \ldots, x_\ell) = f(t(u_1, x_1), \ldots, t(u_\ell, x_\ell))$, where $t(u_i, x_i)$ denotes x_i if $u_i = 0$ or $1 - x_i$ if $u_i = 1$. For $u' \in \{0, 1\}^\ell$, notice that $(t(u_1, u'_1), \ldots, t(u_\ell, u'_\ell))$ is a $\{0, 1\}$ vector which is $(0, \ldots, 0)$ if and only if $u = u'$, so it follows that $h_u(u') = 0$ if $u = u'$ and otherwise $h_u(u') \neq 0 \bmod m$, i.e., $h_u(u') \in S$. Taking the columns corresponding to functions h_u as the first columns of M therefore shows that M is S-nice, as required. ■

It remains to construct an OR function for $m = 6$ of degree $\sqrt{\ell}$. We roughly follow Beigel, Barrington, and Rudich's original proof:

Proof [Proof of Theorem 8 for $m = 6$] Choose integers a and b so that $\sqrt{\ell} < 2^a, 3^b \le O(\sqrt{\ell})$.

Let $h(x) = 1 - \binom{x-1}{2^a}$, so that $h(x) \in \mathbb{Q}[x]$ satisfies $h(0) = 0$ and $h(1) = \cdots = h(2^a) = 1$ and, furthermore, h is *integer-valued*: $h(m) \in \mathbb{Z}$ for any $m \in \mathbb{Z}$. It may be checked that $h(x) \bmod 2$ is periodic with period 2^a; in other words, for $m \in \mathbb{Z}$, $h(m)$ is even if and only if $2^a \mid m$.

By general facts about integer-valued polynomials (or by explicit computation), we may alternatively write $h(x) = \sum_{i=0}^{2^a} c_i \binom{x}{i}$ with $c_i \in \mathbb{Z}$. Now define $f_2(x_1, \ldots, x_\ell) = \sum_{i=0}^{2^a} c_i p_i(x_1, \ldots, x_\ell)$, where $p_i(x_1, \ldots, x_\ell)$ is the symmetric polynomial obtained by adding the $\binom{\ell}{i}$ monomials of the form $x_{j_1} x_{j_2} \cdots x_{j_i}$ with $j_1 < j_2 < \cdots < j_i$. If vector $(b_1, \ldots, b_\ell) \in \{0, 1\}^\ell$ has exactly t ones and $\ell - t$

zeros, then $p_i(b_1, \ldots, b_\ell) = \binom{t}{i}$, so it follows that $f_2(b_1, \ldots, b_\ell) = h(t)$, which is even when $2^a \mid t$ and odd otherwise. Furthermore, by construction, f_2 has integer coefficients.

Similarly, we may construct a polynomial $f_3 \in \mathbb{Z}[x_1, \ldots, x_\ell]$ so that, for $(b_1, \ldots, b_\ell) \in \{0,1\}^\ell$ with t ones, the value of $f_3(b_1, \ldots, b_\ell)$ is divisible by 3 if and only if $3^b \mid t$.

Finally, define $f \in \mathbb{Z}_6[x_1, \ldots, x_\ell]$ via the Chinese Remainder Theorem by the conditions $f \equiv f_2 \bmod 2$ and $f \equiv f_3 \bmod 3$. It follows that for any $(b_1, \ldots, b_\ell) \in \{0,1\}^\ell$ with t ones, $f(b_1, \ldots, b_\ell) = 0 \in \mathbb{Z}_6$ if and only if $2^a 3^b \mid t$, and since $0 \le t \le \ell < 2^a 3^b$, this happens if and only if $t = 0$. Since $\deg(f) = \max(\deg(f_2), \deg(f_3)) = \max(2^a, 3^b) = O(\sqrt{\ell})$, this is the desired OR function. ■