6.440 Essential Coding Theory Mar 4, 2013

Lecture 8

Lecturer: Madhu Sudan *Scribe: Josh Alman*

1 Guest Lecture

The next lecture, on Wednesday March 6th, will be a guest lecture by Professor Eli Ben-Sasson from the Technion. The topic will be *List-decoding limits to Reed-Solomon Codes*. It will mainly consider the problem of, given a Reed-Solomon code, finding points that have many codewords in a small ball around them. The lecture will be a pertinent digression from the class, but we won't build off of its results in future lectures.

2 Today: Algebraic Geometry Codes

1. Motivation: $\epsilon-$biased spaces
2. Algebraic Geometry Codes
   (a) History and General Principle
   (b) One Concrete Construction on Hermitian Curves (Using Bézout's theorem, and the trace and norm functions)
   (c) General Results ([TVZ] bound, Garcia-Stichtnoth curves)

Today we will learn about codes from Algebraic Geometry. Since we won't have time to delve very deep into the field, we will use some results from Algebraic Geometry without proof later in the lecture.

3 $\epsilon-$biased spaces

Today's goal will be to design an $\epsilon-$ biased space. These spaces, other than being useful in Error-Correcting Coding theory, are also useful in algorithm design and the design of Probabilistically-Checkable Proofs. We will motivate them more later.

Definition 1 *An* $\epsilon-$biased space *is a linear binary code* $C \subseteq \mathbb{F}_2^n$ *such that:*

1. *C has distance* $\left(\frac{1}{2} - \epsilon\right)$*, and,*
2. *The all 1s vector,* $1^n \in C$*.*

The goal, of course, is to make the dimension k as large as possible.

Note: In the literature, one might say '$k-\epsilon-$biased bits' to refer to a random column of the $k \times n$ generator matrix of an $\epsilon-$biased space.

3.1 Existential Results

Consider a random linear code of length n. By the Chernoff tail bound, two codewords disagree in at least $\left(\frac{1}{2}-\epsilon\right)n$ coordinates with probability $1-2^{-\epsilon^2 n}$. Hence, by the probabilistic method, there must exist codes with dimension as large as $\epsilon^2 n$ (from the exponent of 2). Alternatively, given k and ϵ, there exists an $\epsilon-$biased space with $n = O\left(\frac{k}{\epsilon^2}\right)$.

We can also apply the bounds from previous lectures to $\epsilon-$biased spaces. Indeed, by the Plotkin or Elias bounds, we get that $k = \Omega\left(\frac{n}{\epsilon}\right)$. There is also a better bound which we might not get to proving in class, called the Linear Programming bound.[1] It gives that $k = \Omega\left(\frac{n}{\epsilon^2 \log \frac{1}{\epsilon}}\right)$.

3.2 Constructive Results

We use the concatenation technique from last lecture to give two examples of $\epsilon-$biased spaces. Recall that if C_1 is a $[n_1, k_1, d_1]_q$ code, and C_2 is a $[n_2, k_2, d_2]_2$ code, with $2^{k_2} \geq q$, then $C_1 \circ C_2$ is a $[n_1 n_2, k_1 k_2, d_1 d_2]_2$ code.

3.2.1 Reed-Solomon and Hadamard codes

First, consider the concatenation of a Reed-Solomon code and a Hadamard code. As before, we can find a $[n, 2\epsilon n, (1-2\epsilon)n]_n$ Reed-Solomon code, and we can find a $[n, \log_2 n, n/2]_2$ Hadamard code. Their concatenation gives a code that is:

$$\left[n^2, 2\epsilon n \log n, \left(\frac{1}{2}-\epsilon\right)n^2\right]_2.$$

Rewriting in temrs of $N = n^2$, we have a code that is:

$$\left[N, \epsilon\sqrt{N}\log N, \left(\frac{1}{2}-\epsilon\right)N\right]_2.$$

Hence, we get that $K = \epsilon\sqrt{N}\log N$, and so $N \approx \frac{K^2}{\epsilon^2}$.

3.2.2 Reed-Solomon and Random codes

We now consider the concatenation of a Reed-Solomon code and a Random code. We can find a $[n, 2\epsilon n, (1-2\epsilon)n]_n$ Reed-Solomon code, and we can find a $[\ell, \log_2 n, (1-\epsilon)/2]_2$ Random code when $\ell = O(\log n/\epsilon^2)$. Their concatenation gives a code that is:

$$\left[n\ell, \frac{1}{2}\epsilon n \log n, \left(\frac{1}{2}-\epsilon\right)n\ell\right]_2.$$

Rewriting in temrs of $N = n\ell$, we have a code that is:

[1] It is also named the MRRW bound after the authors, or the JPL bound after their workplace.

$$\left[N, \Omega(\epsilon^3 N), \left(\frac{1}{2} - \epsilon\right) N\right]_2.$$

Hence, we get that $K = \epsilon^3 N$, and so $N = \frac{K}{\epsilon^3}$.

3.2.3 Summary

The best known $\epsilon-$biased space has:

$$n = \frac{k}{\epsilon^2}.$$

However, in general, the best explicit codes we know are the two we just derived, with:

$$n = \frac{k^2}{\epsilon^2}, \quad \textbf{or} \quad n = \frac{k}{\epsilon^3}.$$

We will now examine a code by Ben-Aroya and Ta-Shma, which concatenates an Algebraic Geometry code with a Hadamard code. It will achieve:

$$n = \frac{k^{\frac{5}{4}}}{\epsilon^{\frac{5}{2}}}.$$

In many applications, we think of $\epsilon = \frac{1}{k}$, so that our codes from before achieved $n = k^4$, while this new code will achieve the improved result of $n = k^{\frac{15}{4}}$.

4 Algebraic Geometry Codes

4.1 Main Idea

We typically think of codes as functions $f : \mathbb{F}_q^m \to \mathbb{F}_q$. In Algebraic Geometry codes, we instead pick a subset $S \subseteq \mathbb{F}_q^m$ which has nice geometric properties, and instead consider functions $f : S \to \mathbb{F}_q$.

For instance, a common choice for S is to select $m-1$ polynomials $p_1, \cdots, p_{m-1}$, and then set

$$S = \{\bar{x} \in \mathbb{F}_q^m \mid p_1(\bar{x}) = p_2(\bar{x}) = \cdots = p_{m-1}(\bar{x}) = 0\}.$$

Both the message space and the coordinates of an Algebraic Geometry code need to be carefully picked to satisfy algebraic geometric properties.

4.2 History

The idea of Algebraic Geometry codes was first conceived by V. D. Gioppa in the late '70s. The first breakthrough construction was made by Tsfasman, Vladuts, and Zink in 1982. When q is a square and prime power, then they designed a code that is:

$$\left[n, k, n-k-\frac{n}{\sqrt{q}-1}\right]_q.$$

In particular, this achieves $R+\delta \geq 1-\frac{1}{\sqrt{q}-1}$. This is better than the random code construction, since here q grows polynomially in the gap $\frac{1}{1-(R+\delta)}$ instead of exponentially in it. Moreover, when q is big enough ($q \geq 49$), this beats the Gilbert-Varshamov bound.

We will now develop some Algebraic Geometry theory. We will then use it to describe their code, which is based on the Hermitian curve.

4.3 Algebraic Geometry Ingredients

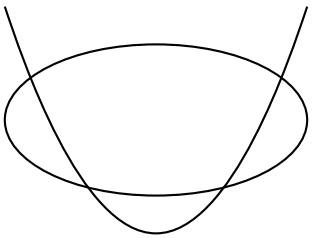
To analyze Tsfasman, Vladuts, and Zink's code, we will need to use Bézout's theorem, and the Trace and Norm functions from Algebraic Geometry.

4.3.1 Bézout's theorem

We will need one direction of Bézout's theorem. Although it can be proved by elementary methods, we state it without proof:

Theorem 2 *If $\mathbb{F}$ is a field, and $f, g \in \mathbb{F}[X, Y]$ are polynomials with no common factors, then*

$$|\{(\alpha, \beta) \in \mathbb{F} \times \mathbb{F} \mid f(\alpha, \beta) = g(\alpha, \beta) = 0\}| \leq \deg(f) \cdot \deg(g).$$



Example: Since an ellipse and a parabola both have degree 2, they can have at most 4 intersection points.

4.3.2 Trace and Norm functions

Definition 3 *The* trace*, Tr, and* norm*, N, are functions $Tr, N : \mathbb{F}_{q^t} \to \mathbb{F}_{q^t}$ given by:*

$$Tr(x) = x + x^q + x^{q^2} + \cdots + x^{q^{t-1}},$$
$$N(y) = y^{1+q+q^2+\cdots+q^{t-1}}.$$

When $t = 1$ and q is a prime, these functions are not interesting, as they are both equal to the identity. However, they are more interesting when $t > 1$, and we will use their properties when $t = 2$ for our Hermitian codes.

First, note that the trace function is linear, while the norm function is multiplicative. To see that Tr is linear, recall that when working over $\mathbb{F}_{q^t}$, we have that $(a+b)^q = a^q + b^q$.

Next, the images of both the trace and norm functions are in $\mathbb{F}_q$, in the following sense: We usually think of $\mathbb{F}_q^t$ as a vector space over $\mathbb{F}_q$. However, we can also view $\mathbb{F}_q \subseteq \mathbb{F}_{q^t}$, as:

$$\mathbb{F}_q = \{\alpha \in \mathbb{F}_{q^t} \mid \alpha^q = \alpha\}.$$

Since $\alpha^q = \alpha$ is a degree q polynomial, it has at most q roots. In fact, it is not hard to see that it has q roots that are closed under multiplication and addition, justifying the above. Now, since any $x \in \mathbb{F}_{q^t}$ satisfies $x^{q^t} = x$, we have that for any $x \in \mathbb{F}_{q^t}$:

$$(Tr(x))^q = (x + x^q + x^{q^2} + \cdots + x^{q^{t-1}})^q = x^q + x^{q^2} + x^{q^3} + \cdots + x^{q^t} = Tr(x),$$

and so the image of Tr is indeed in $\mathbb{F}_q$. A similar argument works for N.

Finally, Tr is a perfect q^{t-1} to 1 map, while N is a perfect $1+q+q^2+\cdots+q^{t-1}$ to 1 map. First, consider Tr. It is a polynomial of degree q^{t-1}, and so it maps at most q^{t-1} points to each element of $\mathbb{F}_q$. But, there are q^t total points in the domain, and only q in the range, so it must be a perect map. Again, a similar argument works for N.

To summarize, the functions satisfy the following properties:

Trace	**Norm**
Linear $(Tr(x+y) = Tr(x) + Tr(y))$	Multiplicative
Image $\subseteq \mathbb{F}_q$	Image $\subseteq \mathbb{F}_q$
perfect $q^{t-1} \to 1$ map	perfect $1 + q + q^2 + \cdots + q^{t-1} \to 1$ map

4.4 Hermitian Codes

The Hermitian code is a code on the Hermitian curve $S \subseteq \mathbb{F}_{q^2}^2$ given by:

$$S = \{(x,y) \in \mathbb{F}_{q^2}^2 \mid x^q + x = y^{q+1}\} = \{(x,y) \in \mathbb{F}_{q^2}^2 \mid Tr(x) = N(y)\}.$$

It is parameterized by some $r \leq q$, and its message space is given by $\{f \in \mathbb{F}_{q^2}[X,Y] \mid \deg(f) \leq r\}$. Its encoding is by evaluations of the polynomials.

4.4.1 Parameters of Hermitian Codes

Let us analyze the parameters of Hermitian codes. We first find the size of S:

Lemma 4 $|S| = q^3$.

Proof For each of the q^2 choices of $\beta \in \mathbb{F}^{q^2}$, let $\gamma = N(\beta) \in \mathbb{F}_q$. Then, there are q choices of $\alpha \in \mathbb{F}^{q^2}$ such that $Tr(\alpha) = \gamma$, since Tr is a perfect map. This gives a total of $q^2 \times q = q^3$ choices for $(\alpha, \beta) \in S$. ■

We next look at the distance of the code. Let $R(x, y) = Tr(x) - N(y)$, so that $S = \{(x, y) \mid R(x, y) = 0\}$. Then, R has a property that will be convenient in conjunction with Bézout's theorem, that we state without proof:

Lemma 5 *R is irreducible.*

Using this, we get that:

Lemma 6 *The distance, d, of the Hermitian code, satisfies $d \geq q^3 - r(q+1)$.*

Proof Fix any $f \in \mathbb{F}_{q^2}[X, Y]$ of degree r. Since R has degree $q+1 > r$, and R is irreducible, R and f cannot share any factors. Hence, by Bézout's theorem, we get that:

$$|\{(\alpha, \beta) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \mid f(\alpha, \beta) = R(\alpha, \beta) = 0\}| \leq r(q+1).$$

Hence, $d \geq n - r(q+1) = q^3 - r(q+1)$ as desired. ■

Finally, by counting polynomials, we see that $k = \binom{r}{2} \geq \frac{r^2}{2}$. Hence, the code we get is of:

$$\left[q^3, \frac{r^2}{2}, q^3 - r(q+1)\right]_{q^2}.$$

4.5 Concatenating Hermitian and Hadamard codes

The Hermitian code does not meet the desired bound just yet. First, we need to concatenate with the Hadamard code $\left[q^2, \log_2 q^2, \frac{1}{2}q^2\right]_2$. Although we could be more careful and use a dimension of less than $\log_2 q^2$, it would give us a negligible improvement so we do not bother. Then, the resulting code is of:

$$\left[q^5, r^2, \frac{q^5}{2}\left(1 - \frac{r}{q^2}\right)\right]_2.$$

If we set $k = r^2$ and $\epsilon = \frac{r}{q^2}$, then we get that $r = \sqrt{k}$, so $q = \frac{k^{1/4}}{\epsilon^{1/2}}$, and thus $n = q^5 = \frac{k^{5/4}}{\epsilon^{5/2}}$, which is the desired bound.[2]

[2]Note that for our parameter settings we needed that $\epsilon \leq \frac{1}{\sqrt{k}}$. If ϵ were very small, like a constant, then using the construction from before with $n = \frac{k}{\epsilon^3}$ would give a better result.

4.6 Garcia-Stichtenoth Codes

Like with the Hermitian Code, Algebraic Geometry codes in general are constructed in three steps:

1. Pick a curve.
2. Choose functions to evaluate on the curve.
3. Prove a distance bound, usually involving some complicated Algebraic Geometry.

We briefly give a glimpse into another such code, the Garcia-Stichtenoth Code, published in 1999.

First, fix and m and any prime power q. Then, for each $i \in \{1, 2, \cdots, m-1\}$, define the polynomial $p_i : \mathbb{F}_{q^2}^m \to \mathbb{F}_{q^2}$ by $p_i(\bar{x}) = N(x_i) - Tr(x_i) \cdot Tr(x_{i+1})$. Then, we will work over the curve $S \subseteq \mathbb{F}_{q^2}^m$, with:

$$S = \{\bar{x} \in \mathbb{F}_{q^2}^m \mid p_1(\bar{x}) = \cdots = p_{m-1}(\bar{x}) = 0\}.$$

It is an easy exercise to show that:

Lemma 7 $|S| \geq q^{m+1}$.

Setting $n = q^{m+1}$, our codes will be determined by a basis of functions $b_1, b_2, \cdots, b_n : S \to \mathbb{F}_{q^2}$.n particular, for $i \in \{1, \cdots, n\}$, we will have that:

$$C_i = \mathbf{span}(b_1, \cdots, b_i).$$

We state some results, without proof, about these codes:

First, while we clearly have that $C_i \supseteq C_{i-1}$ for each i, we in fact get that

$$|\{i \mid C_i = C_{i-1}\}| \leq \frac{n}{q-1}.$$

$\frac{n}{q-1}$ is called the genus of the curve. The Garcia-Stichtenoth codes act very similarly to Reed-Solomon codes except in these gaps.

Second, we have for all i that $\Delta(C_i) \geq n - i$.

Finally, if for $x, y \in \mathbb{F}_{q^2}^n$, we write:

$$x \star y = (x_1 y_1, x_2 y_2, \cdots, x_n y_n),$$

then we have that for all $x \in C_i$ and $y \in C_j$, then $x \star y \in C_{i+j}$. The code words act similarly to polynomials.

Combining these results, we get codes over $\mathbb{F}_{q^2}$ that have $R + \delta \geq 1 - \frac{1}{q-1}$. This is the same bound as before since we are working over $\mathbb{F}_{q^2}$ so that q is the square root of the field size.

5 Conclusion

To briefly return to $\epsilon-$biased spaces, we can show as an exercise that the concatenation of an Algebric Geometry code and a Hadamard code can give an $\epsilon-$biased space.

This concludes our introduction of algebraic codes. Starting next week, we will begin with the decoding of algebraic codes.

References

[1] Tsfasman, M. A.; Vladut S. G. and Zink Th. Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. *Mathematische Nachrichten* 109: 21-28, 1982.

[2] Garcia, A. and Stichtenoth, H. Algebraic function fields over finite fields with many rational places. *IEEE Transactions on Information Theory* 41: 1548-1563, 1995.