CS 229r Essential Coding Theory, Lecture 8 Feb 16, 2017

Lecture 8

Instructor: Madhu Sudan *Scribes: Yi-Hsiu Chen*

1 Overview

Today, we introduce two families of codes, (1) *Dual BCH code* and (2) *Algebraic geometry codes*, which could be better than a random bound (Gilbert-Varshamov bound) in some proper settings of parameters. The codes rely on two mappings called *trace* and *norm*, which map an element form a large field to a small field. Also the Bézout Theorem is needed.

1.1 Parameters

As usual, we have the following parameters.

- k: message length.
- δ: relative distance $\delta = \frac{1}{2} - \epsilon$,
- n: code length

In this lecture we will mostly focus on the case that $k \to \infty$ and $\epsilon \to 0$. The question we are asking is, what is the smallest n we can get? (e.g., in the form of $\frac{k^\alpha}{\epsilon^\beta}$)

1.2 Review of known bounds

- The existential bound (random code) gives us $n = \frac{k}{\epsilon^2}$.
- Concatenation of Reed-Solomon code and Hadamard code: $[n, 2\epsilon n, (1-2\epsilon)n]_n \circ [n, \log_2 n, n/2]_2 \Rightarrow [n^2, 2\epsilon n \log n, n^2(1/2-\epsilon)]_2$ gives us $n = \frac{k^2}{\epsilon^2}$

2 Dual BCH Code

First, we introduce a mapping function, *trace*

2.1 Trace Function

Definition 1. *The trace function* $\mathrm{Tr} : \mathbb{F}_{q^\ell} \to \mathbb{F}_q$ *is defined by a polynomial* $\in \mathbb{F}_{q^\ell}[x]$ *as follows.*

$$\mathrm{Tr}(x) \stackrel{\text{def}}{=} x + x^q + x^{q^2} + \cdots + x^{q^{\ell-1}}$$

Some properties of Tr:

- $\mathrm{Tr}(rx + y) = r\,\mathrm{Tr}(x) + \mathrm{Tr}(y)$.
- The image of Tr is contained by $\mathbb{F}_q$. This can be shown by observing that

$$\forall\ \alpha \in \mathbb{F}_{q^\ell}\ , \quad \mathrm{Tr}(\alpha)^q = \left(\alpha + \cdots + \alpha^{q^{\ell-1}}\right)^q = \alpha^q + \alpha^{q^2} + \cdots \alpha^{q^\ell} = \mathrm{Tr}(\alpha) \pmod{x^{q^\ell} - x}$$

Exercise 2. $\mathrm{Tr} : F_{q^\ell} \to F_q$ *is a uniform mapping* ($q^{\ell-1}$ *to* 1*).*

2.2 Dual BCH Code with degree t

We start from a low degree of polynomial over a big field $\mathbb{F}_n$ where $n = 2^\ell$. As in Reed-Solomon code, we evaluate the function over the entire domain.

$$m(x) = \sum_{i=0}^{t-1} m_i x^i \text{ where } m_i \in \mathbb{F}_{2^\ell}$$

The coefficients can also be treated as $t \cdot \ell = (t \log n)$ elements over $\mathbb{F}_2$. We then apply the trace function $\mathrm{Tr} : \mathbb{F}_{2^\ell} \to \mathbb{F}_2$ on $m(x)$ to define the encoding function. That gives us a code $[n, t \log n, d]_2$ where d is to be decided.

To determine the distance d, we use the following theorem. (Proof is omitted)

Theorem 3. *If f is a degree r polynomial over $\mathbb{F}_n$ where $n = p^\ell$, then*

$$\left| (\#\textit{zeros of } \mathrm{Tr} \circ f) - \frac{n}{p} \right| \leq \frac{2(p-1)(r-1)}{p} \cdot \sqrt{n}.$$

Especially we consider the case that $p = 2$. That gives us the distance

$$d = n - \left(\frac{n}{2} + (r-1)\sqrt{n} \right) = n \left(\frac{1}{2} - \frac{r-1}{\sqrt{n}} \right).$$

Let $k = t \log n$, then it gives us $n \approx k^2/(\epsilon^2 \log^2(k/\epsilon))$, which is better than the constructive bound we had.

3 Algebraic Geometry Code

3.1 Motivation

Recall that in the Reed Muller code, we evaluate a multinomial function f over $\mathbb{F}_q^m$. Apparently, there are lots of redundancy. For instance, by seeing part of a line, the rest can be inferred. The "redundancy" is needed in an error-correcting code. However, we can try to remove some evaluation points to reduce the redundancy, which let us keep the same distance, but shorter code. Algebraic geometry provides us a way to choose points.

3.2 History

The concept of algebraic geometric code was first conceived by Goppa [Gop81]. Then Tsfasman, Vladut and Zink [TVZ82] provide the code fulfilling the following theorem.

Theorem 4. *For all even prime power q, for all $n, k \in \mathbb{N}$, there exists a code over $\mathbb{F}_q$ with length n, dimension k, and distance $n - k - \frac{n}{\sqrt{q}-1}$.*

Then the code is simplified recently by Garcia and Stichtenoth [GS96], which we will mention the construction without showing the distance in Section 3.5. Note that it could be better than a random code when $q \geq 49$.

3.3 Norm function

Definition 5. *Norm function $N : \mathbb{F}_{q^\ell} \to \mathbb{F}_q$ is defined as*

$$N(x) = x^{1+q+q^2+\cdots+q^{\ell-1}}.$$

Exercise 6. *Show the following properties of a norm function $N : \mathbb{F}_{q^\ell} \to \mathbb{F}_q$.*

- $N(xy) = N(x)N(y)$.
- $\forall\ \alpha \in \mathbb{F}_{q^\ell}$, $N(\alpha)^\ell = N(\alpha) \pmod{(x^{q^\ell} - x)}$, *which means the image of* N *is contained by* $\mathbb{F}_q$.
- N *is a* $(1+q+\cdots+q^{\ell-1})$ *to* 1 *mapping. That is, for all* $\beta \in \mathbb{F}_{q^\ell}$ $\#\{\alpha : N(\alpha) = \beta\} = 1+q+\cdots+q^{\ell-1}$.

3.4 Code over the Hermitian Curve

Let a polynomial $R(x, y) = N(x) - \mathrm{Tr}(y)$, then the Hermitian Curve H over $\mathbb{F}_{q^2}$ is defined as

$$H = \{(\alpha, \beta) \in \mathbb{F}_{q^2}^2 \mid R(\alpha, \beta) = 0\}.$$

The size of H is exactly q^3, which can be seen by considering each fixed β.

Now we can define a code on the curve C_r where $r \leq q$ to be evaluations of polynomial with degree $\leq r$ over H. The number of coefficients is at least $r^2/2$, so $k \geq r^2/2$, and the code length is $n = |H| = q^3$. To calculate the distance, we need the Bézout's Theorem (in a plane).

Theorem 7. *If* $f, g \in \mathbb{F}[x, y]$ *are of degree* D_1 *and* D_2 *respectively, then either* f *and* g *have a common factor, or they have at most* $D_1 D_2$ *common zeros.*

The degree of R is $q+1$ and the degree of f is r. Since R is irreducible and $r < q+1$, f and R can have at most $r(q+1)$ common factors. Therefore, the distance d is at least $n - r(q+1)$. Summarily, we get the code $\left[q^3, r^2/2, q^3 - r(q+1)\right]_{q^2}$, or $\left[q^3, q^2/2, q^3 - q(q+1)\right]_{q^2}$ if we let $r = q$.

Note that the size of the alphabet q^2 is smaller than the code length. Does that mean it gives us a code better than Reed-Solomon code? To compare it clearer, we concatenate them to Hadamard code $\left[q^2, \log(q^2), \frac{1}{2}q^2\right]_2$. That gives us $\left[q^5, r^2/2, q^5(\frac{1}{2} - \frac{r}{2q^2}(1 + \frac{1}{q}))\right]_2$. Set $\epsilon = \frac{r}{q^2}$, $k = r^2/2$, it yields $n \approx \frac{k^{5/4}}{\epsilon^{5/2}}$. Consider the case that $\epsilon = 1/k$, then $n \approx k^{15/4}$ which is better than the known constructive bound! ($n = k^4$, e.g., Concatenating Reed-Solomon and Hadamard).

3.5 Garcia-Stichtenoth Codes

We define the set S as follows,

$$S \stackrel{\text{def}}{=} \{(\alpha_1 ... \alpha_n) | P_1(\overline{\alpha}) = 0, \ldots, P_m(\overline{\alpha}) = 0\}$$

where $P_i(\alpha) = \mathrm{Tr}(\alpha_{i+1}) = N(\alpha_i)/\mathrm{Tr}(\alpha_i)$ and $\mathrm{Tr}, N : \mathbb{F}_{q^2} -> \mathbb{F}_q$

There are $q^2 - q$ choices of α_1, q choices of α_2 ... q choices of α_m, so $q^{m+1}(1 - 1/q)$ points in total. Then the code is constructed by evaluations of a polynomial on S.

References

[Gop81] Valerii Denisovich Goppa. Codes on algebraic curves. In *Soviet Math. Dokl.*, volume 24, pages 170–172, 1981.

[GS96] Arnaldo Garcia and Henning Stichtenoth. On the asymptotic behaviour of some towers of function fields over finite fields. *Journal of number theory*, 61(2):248–273, 1996.

[TVZ82] Michael A Tsfasman, SG Vlădutx, and Th Zink. Modular curves, shimura curves, and goppa codes, better than varshamov-gilbert bound. *Mathematische Nachrichten*, 109(1):21–28, 1982.