Algebraic Geometry Error-Correcting Codes
Math Club Talk 11/10/17

Matthew Weidner

November 12, 2017

Contents

1 Error-Correcting Codes

Motivation: want to send data over a noisy channel. E.g., satellite communications, CD. Each bit has some probability of being corrupted. Want to "encode" data beforehand by adding redundant information, so that we can decode original message at other end even if some errors occur.

Example 1.1. Repitition code.

We can define error-correcting codes in a general, mathematical way as follows.

Fix q, and let $\mathbb{F}_q$ be the finite field of order q.

(Recall: a field is a set F with binary operations $+, \times$ and constants $0, 1 \in F$, such that $(F, +, 0)$ and $(F \setminus \{0\}, \times, 1)$ are abelian groups, and $a(b + c) = ab + ac$, $1a = a$. E.g., $\mathbb{Q}$, integer modulo a prime. A unique finite field exists of any prime power order.)

Definition 1.2. A *linear block error-correcting code* over $\mathbb{F}_q$ of length N is a vector subspace $C \subset \mathbb{F}_q^N$. The *dimension* of C is $k(C) := \dim_{\mathbb{F}_q} C$. The *minimum distance* of C is $d(C) := \min_{x \in C, x \neq 0}$ # nonzero coordinates of x.

Note. Using C, we can encode k-symbol messages into N-symbol messages, such that we can detect $d - 1$ errors and correct $\frac{d-1}{2}$ errors. Indeed, if up to $d - 1$ coordinates are changed in an element of C, it will not end up at a different element of C, so we will know that an error occurred; and if up to $\frac{d-1}{2}$ coordinates are changed, then the original element of C will still be the element of C which is closest to the altered element.

Obviously want $d(C), k(C)$ to be large and N to be small. Intuitively, we cannot detect more errors than the number of "redundant" symbols. This is formalized as follows:

Theorem 1.3 (Singleton Bound)**.** *Let C be as above. Then $k(C) + (d(C) - 1) \leq N$.*

Proof. Let $E := \{\vec{a} \in \mathbb{F}_q^N \mid \forall i \geq d, a_i = 0\}$. Note $E \cap C = 0$. Then

$$k + (d-1) = \dim C + \dim E = \dim(C+E) + \dim(C \cap E) = \dim(C+E) \leq n.$$

□

It turns out that there are codes meeting this bound when $N = q$, for all k:

Definition 1.4. Let $1 \leq k \leq q$. For $\vec{a} \in \mathbb{F}_q^k$, define the polynomial $f_{\vec{a}}(x) = a_1 + a_2 x + \cdots + a_k x^{k-1}$. Letting $\mathbb{F}_q = \{b_1, \ldots, b_q\}$, define

$$\begin{aligned} \text{ev} : \mathbb{F}_q^k &\to \mathbb{F}_q^q \\ \vec{a} &\mapsto (f_{\vec{a}}(b_1), \ldots, f_{\vec{a}}(b_n)). \end{aligned}$$

We call $C_{k,q} := \text{Im}(\text{ev})$ the *Reed-Solomon code* of dimension k over $\mathbb{F}_q$.

Theorem 1.5. *(1)* $k(C_{k,q}) = k$

(2) $d(C_{k,q}) = q - k + 1$

Proof. It suffices to show that for all $0 \neq \vec{a} \in \mathbb{F}_q^k$, $\text{ev}(\vec{a})$ has at least $q - k + 1$ nonzero entries. Suppose this fails for $\vec{a}$. Then $f_{\vec{a}}$ has at least k zeroes, but it is a polynomial of degree at most $k - 1$, so $\vec{a} = 0$, a contradiction. □

Reed-Solomon codes are used in real life, e.g., CDs, QR codes, satellite communications. For example, they allow CDs to tolerate scratches. To do so, CDs use "interleaved" Reed-Solomon codes, which spread out each block so that only a few bits of each block appear in any one possible scratch. Without this, a scratch could erase an entire block, since the length q can't be too large (else encoding and decoding are time-consuming).

But what if we don't know that errors will occur in nice patterns, like a scratch? Codes with long block length are better at tolerating errors which might occur in any pattern, since each block can absorb a certain fraction of errors no matter where they occur. With long blocks, it's less likely that an entire block will be corrupted. So we want codes which, like Reed-Solomon codes, meet the Singleton Bound, but have arbitrarily long length.

It turns that we cannot do this. But we can get close, for arbitrarily long length, using algebraic geometry codes.

2 Function Fields over Finite Fields

Fix a finite field $\mathbb{F}_q$.

Definition 2.1. The *rational function field over* $\mathbb{F}_q$ is the set

$$\mathbb{F}_q(x) := \left\{ \frac{p(x)}{q(x)} \mid p(x), q(x) \text{ are polynomials with coefficients in } \mathbb{F}_q;\ q(x) \neq 0 \right\} / \sim,$$

where $\frac{p(x)}{q(x)} \sim \frac{r(x)}{s(x)}$ if $p(x)s(x) = q(x)r(x)$, with addition and multiplication defined using the usual rules for fractions. Here $p(x)/q(x)$ is a "formal fraction", i.e., it is really just an ordered pair $(p(x), q(x))$, but we think of it as a fraction. It is easy to see that $\mathbb{F}_q(x)$ is a field, with 0 and 1 given by $0/1$ and $1/1$, respectively.

Definition 2.2. A *function field over* $\mathbb{F}_q$ is a finite extension F of $\mathbb{F}_q(x)$. (Intuitively, this is a field containing $\mathbb{F}_q(x)$ where there are finitely many new variables, each of which solves a polynomial over $\mathbb{F}_q(x)$.)

Example 2.3. $F = \mathbb{F}_q(x, y)$ where $y = x^2$. F consists of quotients of polynomials $p(x, y)/q(x, y)$ where $y = x^2$ is built into the relation $\sim$ used to identify fractions.

Technical point: we assume that F contains no finite fields larger than $\mathbb{F}_q$, i.e., $\mathbb{F}_q$ is algebraically closed in F.

Valuations

To motivate valuations, let's look at some nice functions on the rational function field.

Set $v_\infty(p(x)/q(x)) = \deg q(x) - \deg p(x)$.

For $t(x)$ irreducible, can uniquely write $p(x)/q(x) = t^n(x)(r(x)/s(x))$ with $t(x) \nmid r(x), s(x)$. Set $v_{t(x)}(p(x)/q(x)) = n$.

These functions are examples of *valuations*, functions $v : F \to \mathbb{Z} \cup \infty$ (F a function field) which satisfy:

- $v(xy) = v(x) + v(y)$
- $v(x + y) \geq \min\{v(x), v(y)\}$
- $v(a) = 0$ for $0 \neq a \in \mathbb{F}_q$
- $v(x) = \infty$ iff $x = 0$
- There exists $x \in F$ such that $v(x) = 1$.

In fact, we have listed all valuations of $\mathbb{F}_q(x)$.

I bring these valuations up because we can tie them into Reed-Solomon codes, as follows.

Example 2.4. Fix $k \geq 0$, and let $f \in \mathbb{F}_q(x)$ be such that for all irreducible polynomials $t(x)$, $v_{t(x)}(f) \geq 0$, and $v_\infty(x) > -k$. For each $t(x)$, $v_{t(x)}(f) \geq 0$ implies $t(x) \nmid q(x)$, hence $q(x)$ is constant. Then WLOG $f = p(x)$. Since $v_\infty(f) > -k$, $\deg(p(x)) < k$. Thus the space of functions with this property is precisely the space of polynomials with degree less than k — the message space of the Reed-Solomon code $C_{k,q}$.

What this suggests is that, by using more general function fields and valuations, perhaps we can define similar error-correcting codes.

Fix a function field $F/\mathbb{F}_q$. We defined valuations of F above. We now want to define a way to "evaluate" some functions at valuations, analogous to how we evaluate polynomials in the definition of a Reed-Solomon code.

Definition 2.5. Let v be a valuation. The *place* corresponding to v is the set $P := \{f \in F \mid v(f) > 0\}$. Each place corresponds to a unique v. We usually denote a valuation by v_P, where P is the corresponding place.

The *valuation ring* of P is $R_P := \{f \in F \mid v_P(f) \geq 0\}$.

Fact. R_P is a ring, and P is its unique maximal ideal.

Hence R_P/P is a field. For $f \in R_P$, we let $f(P)$ denote the image of f in R_P/P.

We have $\mathbb{F}_q \hookrightarrow R_P/P$ because $v_P(a) = 0$ for all $a \in \mathbb{F}_q \setminus \{0\}$, so we can think of R_P/P as an extension of $\mathbb{F}_q$. If $R_P/P = \mathbb{F}_q$, we call P a *rational place*. Then $f(P) \in \mathbb{F}_q$ for all $f \in R_P$.

Example 2.6. In $\mathbb{F}_q(x)$, let $a \in \mathbb{F}_q$, and let P be the place corresponding to v_{x-a}. Then P is $\mathbb{F}_q$-rational, and for any polynomial $p(x)$, $(p(x)/1)(P) = p(a)$.

Divisors

We saw before that it can be interesting to ask what functions have certain valuations. To phrase the question more generally, we introduce divisors:

Definition 2.7. A *divisor* D of F is a formal finite sum of places of F, with coefficients in $\mathbb{Z}$. We let $v_P(D)$ denote the coefficient of P in D, with $v_P(D) = 0$ if P is not present in D.

Example 2.8. In $\mathbb{F}_q(x)$, letting P_∞ and $P_{t(x)}$ be the places corresponding to the valuations v_∞ and $v_{t(x)}$, we have a divisor $(P_\infty) + 3(P_{x-1}) - 2(P_{x^2-1})$.

Definition 2.9. The *Riemann-Roch space of* D is

$$\mathcal{L}(D) := \{f \in F \mid \text{for all places } P \text{ of } F,\ v_P(f) \geq -v_P(D)\}.$$

This is an $\mathbb{F}_q$-vector space. We set $l(D) := \dim_{\mathbb{F}_q} \mathcal{L}(D)$ (possibly ∞, a priori).

Example 2.10. In $\mathbb{F}_q(x)$, $\mathcal{L}((k-1)P_\infty) = $ (polynomials of degree $< k$) by Example 2.4.

It is a remarkable and deep fact that we get very good bounds on $l(D)$ in general.

Theorem 2.11 (Riemann-Roch)**.** *Let D be a divisor. Define*

$$\deg(D) = \sum_{P:place} v_P(D) \cdot [R_P/P : \mathbb{F}_q]$$

(the extension degree $[R_P/P : \mathbb{F}_q]$ turns out to always be finite). There is a constant $g(F)$, called the genus of F, independent of D, such that

$$\deg(D) + 1 - g \leq l(D) \leq \deg(D) + 1.$$

3 Algebraic Geometry Codes

Defining algebraic geometry codes is now fairly simple.

Let F be a function field over $\mathbb{F}_q$. Let D be a divisor of F. Let $P_1, \ldots, P_N$ be rational places of F such that $v_{P_i}(D) = 0$ for all i. Define

$$\begin{aligned} \text{ev} : \mathcal{L}(D) &\to \mathbb{F}_q^N \\ f &\mapsto (f(P_1), \ldots, f(P_N)). \end{aligned}$$

This makes sense because the P_i are rational, and because $f \in \mathcal{L}(D)$ implies $v_{P_i}(f) \geq 0$. Then

$$C_{D,\vec{P}} := \text{Im}(\text{ev})$$

is the *algebraic geometry code* associated to D and the P_i.

As always, we want to know how good of a code this is.

Theorem 3.1. *Assume* $\deg(D) < N$. *Then:*

1. $k(C_{D,\vec{P}}) = l(D) \geq \deg(D) - g + 1$
2. $d(C_{D,\vec{P}}) \geq N - \deg(D)$.

Proof. As for Reed-Solomon codes, it suffices to prove that for $0 \neq f \in \mathcal{L}(D)$, $\mathrm{ev}(f)$ has at least $N - \deg(D)$ nonzero entries, so in particular ev is injective. Say else. Then $f(P_{i_1}) = 0, \ldots, f(P_{i_{\deg(D)+1}}) = 0$ for some $i_1, \ldots, i_{\deg(D)+1}$. Then

$$f \in \mathcal{L}(D' := D - P_{i_1} - \cdots - P_{i_{\deg(D)+1}}).$$

But $\deg(D') = -1$, so by the Riemann-Roch theorem, $\mathcal{L}(D') = 0$, hence $f = 0$, a contradiction. □

Note $k + d \geq N - g(F) + 1$. Dividing by N, we get

$$R + \delta \geq 1 - \frac{g(F)}{N},$$

where $R := k/N$ is the *rate* and $\delta := d/N$ is the *relative distance* of the code. (These are just length-scaled versions of k and d, which are useful when we want to compare codes of different lengths.) Since $N \approx N(F) :=$ # of rational places of F (e.g., if we take $D = r(Q)$ for some rational place Q and take the P_i's to be all other rational places of F), we see that to get arbitrarily long "good" codes, we want a series of function fields $F_1, F_2, \ldots$ such that:

- $N(F_n) \to \infty$
- $\lim_{n\to\infty} \frac{g(F_n)}{N(F_n)}$ is a small constant < 1.

Theorem 3.2 (Drinfeld-Vladut bound (1983))**.** *In the above situation,* $\lim_{n\to\infty} \frac{g(F_n)}{N(F_n)} \geq \frac{1}{\sqrt{q}-1}$.

Theorem 3.3 (Tsfasman-Vladut-Zink (1982))**.** *This limit can be obtained when* q *is a square.*

Hence when q is a square, we can define codes of arbitrary length over $\mathbb{F}_q$ with

$$R + \delta \geq 1 - \frac{1}{\sqrt{q} - 1},$$

not far from the Singleton bound $R + \delta \leq 1 + 1/N$. No other family of codes is this good, at least for certain choices of R and q. In particular, this bound beats the Gilbert-Varshamov bound, which describes the behavior of arbitrarily long random codes, in which $C \subset \mathbb{F}_q^N$ is chosen at random; until the Tsfasman-Vladut-Zink theorem, coding theorists considered this impossible.

It is known how to encode and decode algebraic geometry codes having these optimal parameters, for arbitrarily large length N, in time about $O(N^3)$. This is promising, but not really useful — for big N, where algebraic geometry codes actually matter, this is impractically long. I think it is a very interesting problem to try to reduce this runtime to something more like linear time, which we can do for Reed-Solomon codes.

Further Reading

H. Stichtenoth, "Algebraic Function Fields and Codes".