CS 4424
Reed-Solomon codes

Overview

Error-correcting codes allow

- to detect
- and correct

errors in digital messages.

Our messages will be made of symbols from a finite alphabet.

Example

- our alphabet is $\{\mathtt{0}, \mathtt{1}, \mathtt{2}, \mathtt{3}, \mathtt{4}, \mathtt{5}, \mathtt{6}, \mathtt{7}, \mathtt{8}, \mathtt{9}, \mathtt{A}, \mathtt{B}, \mathtt{C}, \mathtt{D}, \mathtt{E}\}$
- the message we send is $m = \mathtt{12AB66CE71DB20F}$
- we receive $r = \mathtt{12AC66CE71DB21F}$

Algebra

Usually, it helps to see the problem in an algebraic context.

This lecture: Reed-Solomon codes:

- defined in terms of polynomials over finite fields
- used in digital radio, CDs, ...

Roughly speaking:

- encoding: polynomial multiplication
- error detection: polynomial division
- error correction: rational reconstruction

Rings

Reminder: a ring is

- a set, with an operation called $+$ and another operation called $\times$
- with some obvious properties
  - $a + b = b + a$, $a + (b + c) = (a + b) + c$
  - $ab = ba$, $a(bc) = (ab)c$
  - $a(b + c) = ab + ac$
  - subtraction works too

These rules were used in most algorithms we've seen, under the hood.

Fields

We have secretely been using fields for a while.

A field is a ring, where in addition:

- any element $x \neq 0$ can be inverted.

Every time we used Euclid's GCD algorithm, we (implicitly) had to do divisions, so we were working in a field.

Examples

Fields

- $\mathbb{Q}$
- $\mathbb{R}$
- $\mathbb{C}$
- $\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2 = \{0, 1\}$, with operations modulo 2.

Not fields

- $\mathbb{Z}$
- $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$, with operations modulo 4.

Building new fields

If k is a field, we can build more fields as follows.

Reminder. If P is any polynomial in $k[X]$, of degree d, then

$$k[X]/P = \{ \text{ all polynomials of degree less than } d \},$$

with addition and multiplication done modulo P. This is a ring.

Prop. If P is an irreducible polynomial in $k[X]$, then $k[X]/P$ is a field.

- To prove: if Q is a polynomial $\neq 0$, of degree less than d, then there exists a polynomial U of degree less than d such that QU rem $P = 1$.
- Claim: $\gcd(P, Q) = 1$ (because P is irreducible, and $\deg(Q) < \deg(P)$)
- So there exist U, V with $UQ + VP = 1$.

Examples

Complex numbers

$$\mathbb{C} = \mathbb{R}[X]/(X^2 + 1)$$

a complex number can be seen as a polynomial $a + bX$, with operations done modulo $X^2 + 1$.

Binary fields

- take an irreducible polynomial P of degree d in $\mathbb{F}_2[X]$
- then

  $$\mathbb{F}_{2^d} = \mathbb{F}_2[X]/P$$

  is a field, with 2^d elements.
- Claim: for any d, there exists an irreducible polynomial of degree d.

$\mathbb{F}_4$

Claim. The polynomial

$$P = X^2 + X + 1 \in \mathbb{F}_2[X]$$

is irreducible.

Proof.

- the polynomials of degree 1 are X and $X+1$, and they do not divide P.

Corollary: $\mathbb{F}_2[X]/P$ is a field.

- the elements are $0, 1, X, X+1$, and the multiplication table is

$\times$	0	1	X	$X+1$
0	0	0	0	0
1	0	1	X	$X+1$
X	0	X	$X+1$	1
$X+1$	0	$X+1$	1	X

not $\mathbb{F}_4$

Claim. The polynomial

$$Q = X^2 + 1 \in \mathbb{F}_2[X]$$

is not irreducible.

Proof.

- $X^2 + 1 = (X + 1)^2$

Remark: $\mathbb{F}_2[X]/Q$ is a not field.

- the elements are $0, 1, X, X + 1$, and the multiplication table is

$\times$	0	1	X	$X+1$
0	0	0	0	0
1	0	1	X	$X+1$
X	0	X	1	$X+1$
$X+1$	0	$X+1$	$X+1$	0

How to compute in $\mathbb{F}_{2^d}$

Prop.

- one addition in $\mathbb{F}_{2^d}$ takes d operations in $\mathbb{F}_2$
- one multiplication in $\mathbb{F}_{2^d}$ takes $O(\mathsf{M}(d))$ operations in $\mathbb{F}_2$

  Fast Euclidean division
- one inversion in $\mathbb{F}_{2^d}$ takes $O(\mathsf{M}(d)\log(d))$ operations in $\mathbb{F}_2$

  Fast XGCD

Remark

- for small fields (say 2^{16} elements), one usually uses table look-up instead.

Back to error-correction

Overview of $\mathrm{RS}(n, k)$

- alphabet: a binary field $\mathbb{F} = \mathbb{F}_{2^d}$
- message to encode: a polynomial P of degree less than k

  k symbols before encoding
- encoded message: $S = PG$, for a fixed G of degree $n - k$

  n symbols after encoding

Remark

- we add $n - k$ symbols
- usually, we write $t = (n - k)/2$
- CD use $\mathrm{RS}(32, 28)$

Choosing G

We will take

$$G = (X - a)(X - a^2) \cdots (X - a^{n-k}),$$

where a is chosen such that all powers are pairwise different.

Remark

- do not take $a = 0$ or $a = 1$!
- actually, we want more: we want that

  $$a,\ a^2,\ \ldots, a^n$$

  are pairwise distinct
- it is not obvious (but true) that if $n < 2^d$, we can always find such an a.

Transmission errors

We may not receive S, but another polynomial R of degree $< n$:

$$R = S + E = PG + E,$$

with

- R = received polynomial (known)
- $S = PG$ = message (unknown)
- E = error (unknown)

Prop.

- if there are at most t errors, we can reconstruct S from R.

Remark.

- because $G(a^i) = 0$, we know that $R(a^i) = E(a^i)$, so we can know the values $E(a^i)$.

The error locator polynomial

We write

$$\begin{aligned} S &= s_0 + \cdots + s_{n-1}X^{n-1} \\ E &= e_0 + \cdots + e_{n-1}X^{n-1} \\ R &= r_0 + \cdots + r_{n-1}X^{n-1} \\ &= (s_0 + e_0) + \cdots + (s_{n-1} + e_{n-1})X^{n-1}, \end{aligned}$$

then

$$M = \{i \text{ such that } e_i \neq 0\}$$

and

$$u = \prod_{i \in M} (1 - a^i X).$$

This is the error locator polynomial. By assumption, $|M| \leq (n-k)/2$, so $\deg(u) \leq (n-k)/2$.

Remark: we do not know E, M or u.

A useful fraction

Prop. The generating series

$$\sum_{k\geq 0} E(a^k)X^k$$

can be written v/u, with

$$v = \sum_{i\in M} e_i \prod_{i'\neq i}(1 - a^{i'}X).$$

Proof.

$$\begin{aligned}
\sum_{k\geq 0} E(a^k)X^k &= \sum_{k\geq 0}\sum_{i\in M} e_i (a^k)^i X^k \\
&= \sum_{i\in M} e_i \sum_{k\geq 0} (a^k)^i X^k \\
&= \sum_{i\in M} e_i \frac{1}{1-a^i X} \\
&= \frac{\sum_{i\in M} e_i \prod_{i'\neq i}(1-a^{i'}X)}{u}
\end{aligned}$$

Algorithm

1. We compute
$$E(1) = R(1), \ldots, E(a^{n-k}) = R(a^{n-k}).$$

2. Because
$$\deg(v) < (n-k)/2, \quad \deg(u) \leq (n-k)/2,$$
so it is enough to know $n-k$ terms of v/u to reconstruct u and v by rational function reconstruction.

3. $u(a^{-i}) = 0$ iff $i \in M$, so by evaluating u at $a^0, a^{-1}, \ldots, a^{-n+1}$, we can find M.

4. for i in M, we have
$$\frac{v(a^{-i})}{u'(a^{-i})} = -\frac{e_i}{a^i}.$$