Today

- Decoding Reed-Solomon Codes: The Welch-Berlekamp algorithm.
- Abstracting the decoding algorithm.
- Decoding Algebraic-Geometry Codes.

Problem Statement

Given Distinct points $\langle(\alpha_i, r_i) \in \mathbb{F} \times \mathbb{F}\rangle_{i=1}^n$, and parameter k

Task Compute (coefficients of) polynomial p of degree at most k such that $p(\alpha_i) = r_i$ for at least $(n+k)/2$ values of $i \in [n]$.

Key concept: Error-locator Polynomial

- Given $\langle(\alpha_i, r_i)\rangle_i$ s.t. $\exists p$ of deg. k agreeing with seq. on $(n+k)/2$ points, a polynomial $E(x)$ is an error-locating polynomial if:
  - $p(\alpha_i) \neq r_i$ implies $E(\alpha_i = 0)$.
  - E is not zero "too often" (at least $k+1$ non-zeroes).
- Simple Fact: Given an error-locator polynomial E, can compute p efficiently.
- Simple fact: Such an E of degree e (# errors) exists $E(x) = \prod_{i | r_i \neq p(\alpha_i)} (x - \alpha_i)$.
- Question: How to find E?
- Grammatical aside: "Key" is an adjective, not a noun.

Key equation & Algorithm

- Grammatical aside: "Key" is an adjective, not a noun.
- Fix E of degree e and p and let $N(x) = p(x).E(x)$.
- Then (the key equation)

$$\forall i, \quad N(\alpha_i)(= p(\alpha_i)E(\alpha_i)) = r_i E(\alpha_i).$$

- Algorithm:

1. Find (N, E) with $(N, E) \neq (0, 0)$ and $\deg(N) \leq k + e$ and $\deg(E) \leq e$ satisfying key equation.

2. Output N/E if it is a polynomial satisfying the right conditions, else say none exists.

- Over time, key equation became Key equation.

Analysis

- Why can we find such a pair (N, E)?
  - Substitute unknowns for coefficients.
  - Solve linear system!
- Why does a solution exist? We just argued it!
- Why is it unique?
  - It is NOT!
  - But any solution will do.

Analysis (contd.)

- Claim: If (N, E) and (M, F) are both solutions to Step 1, then $N/E \equiv M/F$.
- Proof:
  - $\forall i, \quad r_i N(\alpha_i) F(\alpha_i) = r_i M(\alpha_i) E(\alpha_i)$.
  - If $r_i \neq 0$ then can cancel from both sides above to get $N(\alpha_i) F(\alpha_i) = M(\alpha_i) E(\alpha_i)$.
  - If $r_i = 0$ then $N(\alpha_i) F(\alpha_i) = M(\alpha_i) E(\alpha_i) = 0$.
  - So for n values, we have $N \cdot F = M \cdot E$.
  - If $n > k + 2e$ then $N/E \equiv M/F$.

Summary

- Gives polytime algorithm for decoding up to error-correction capacity of code.
- Highly non-trivial result - no reason to exist!
- Algebra often has non-trivial solutions to seemingly hard problems. Have to be very careful when basing cryptography on it.

Abstract decoding algorithm

- How much of the prev. algorithm is linear algebra? And how much polynomial arithmetic?
- Investigated by [Pellikaan,Kotter,Duursma 88].
- Surprisingly little polynomial arithmetic.

Abstract decoding (contd.)

Fix a code $\mathcal{C} = [n, k, d]$.

Defn: $(\mathcal{Y}, \mathcal{Z})$ are e-error-correcting pair for $\mathcal{C}$ if the following hold:

- $\mathcal{Y}$ are linear codes.
- $\mathcal{Y} = [n, e+1, n-d+1]$ code.
- $\mathcal{Z} = [n, ?, e+1]$ code.
- $\mathcal{Y} * \mathcal{C} \subset \mathcal{Z}$, where

$A * B = \{a * b | a \in A, b \in B\}$
and $a * b$ denotes coordinatewise product.

Thm: If $\mathcal{C}$ has a e-error-correcting pair then it has an e-error-correcting algorithm.

Algorithm

Given: $r = \langle r_1, \ldots, r_n \rangle \in \mathbb{F}_q^n$.

- Find $(y \in \mathcal{Y}, z \in \mathcal{Z})$ s.t.
  - $y \neq 0$.
  - $y * r = z$.
- Set $c_i = r_i$ if $y_i \neq 0$ and erasure otherwise.
- Erasure decode for c.

Proof steps

1. Such a pair (y, z) exists:
   - Set y_i to zero whenever $c_i \neq r_i$.
   - Find non-zero $y \in \mathcal{Y}$ subject to above. (Exists by dim. of $\mathcal{Y}$.)
   - Set $z = c * y$.
2. Pair can be found (linear system).
3. For any (y, z) found by alg. and any c s.t. $\Delta(c, r) \leq e$, we have $y * c = z$. (Follows from distance of $\mathcal{Z}$.)
4. Any pair y, z has at most one c s.t. $y * c = z$. (Follows from distance of $\mathcal{Y}$.)

Recall: AG codes

- Code determined by subset of n points in $\mathbb{F}_q^m$.
- Codewords/Messages: Multivariate polynomials.
  - But weight determined by "order" not degree!
- Order axioms
  - $\text{ord}(f+g) \le \max\{\text{ord}(f), \text{ord}(g)\}$.
  - $\text{ord}(f \cdot g) = \text{ord}(f) \cdot \text{ord}(g)$.
  - Exist functions of every order except $g \le n/(\sqrt{q}-1)$.

Application: AG codes

- Recall order axioms for algebraic-geometry codes. (Product rule, and # zeroes.)
- $\mathcal{C} =$ functions of order $< k$..
- $\mathcal{Y} =$ functions of order $< (n-k+g)/2$.
- $\mathcal{Z} =$ functions of order $< (n+k+g)/2$.
- Gives $(n-k-g)/2$-error-correcting pair.
- Thus every AG code $\mathcal{C}$ has a decoding alg. going up to $(d(\mathcal{C})-g)/2$ errors.