Algebraic Codes and Invariance

Madhu Sudan
Microsoft Research

Disclaimer

- Very little Algebraic Geometry in this talk!

- Mainly:
  - Ex-Coding theorist's perspective on Algebraic and Algebraic-Geometric Codes
  - What additional properties it would be nice to have in algebraic-geometry codes.

Outline of the talk

- Part 1: Codes and Algebraic Codes
- Part 2: Combinatorics of Algebraic Codes

  $\Leftarrow$ Fundamental theorem(s) of algebra
- Part 3: Algorithmics of Algebraic Codes

  $\Leftarrow$ Product property
- Part 4: Locality of (some) Algebraic Codes

  $\Leftarrow$ Invariances
- Part 5: Conclusions

Part 1: Basic Definitions

Error-correcting codes

- Notation: $\mathbb{F}_q$- finite field of cardinality q
- Encoding function: messages $\mapsto$ codewords
  - $E: \mathbb{F}_q^k \to \mathbb{F}_q^n$; associated Code $C \triangleq \{E(m) | m \in \mathbb{F}_q^k\}$
  - Key parameters:
    - Rate $R(C) = k/n$;
    - Distance $\delta(C) = \min_{x \neq y \in C} \{\delta(x, y)\}$.
      - $\delta(x, y) = \frac{|\{i | x_i \neq y_i\}|}{n}$
- Pigeonhole Principle $\Rightarrow R(C) + \delta(C) \leq 1 + \frac{1}{n}$
- Algebraic codes: Get very close to this limit!

Algorithmic tasks

- Encoding: Compute $E(m)$ given m.
- Testing: Given $r \in \mathbb{F}_q^n$, decide if $\exists\, m$ s.t. $r = E(m)$?
- Decoding: Given $r \in \mathbb{F}_q^n$, compute m minimizing $\delta(E(m), r)$
- [All linear codes nicely encodable, but algebraic ones efficiently (list) decodable.]

Locality

- Perform tasks (testing/decoding) in $o(n)$ time.
  - Assume random access to r
  - Suffices to decode m_i, for given $i \in [k]$
- [Many algebraic codes locally decodable and testable!]

Algebraic Codes?

- Genera
  - Mess
  - Coor
  - Enco

Algebraic-Geometry Codes:

Domain = Rational points of irred. curve in $\mathbb{F}_q^m$

Messages = Functions of bounded "order"

- Examp
  - Reed-Solomon Codes
  - Reed-Muller Codes
  - Algebraic-Geometric Codes
  - Others (BCH codes, dual BCH codes ...)

Part 2: Combinatorics $\Leftarrow$ Fund. Thm

Essence of combinatorics

- Rate of code $\Leftarrow$ Dimension of vector space
- Distance of code $\Leftarrow$ Scarcity of roots
  - Univ poly of deg $\leq k$ has $\leq k$ roots.
  - Multiv poly of deg $\leq k$ has $\leq \frac{k}{q}$ fraction roots.
  - Functions of order $\leq k$ have fewer than $\leq k$ roots
    - [Bezout, Riemann-Roch, Ihara, Drinfeld-Vladuts]
    - [Tsfasman-Vladuts-Zink, Garcia-Stichtenoth]

Consequences

- $q \geq n \Rightarrow \exists$ codes C satisfying $R(C) + \delta(C) = 1 + \frac{1}{n}$
- For infinitely many q, there exist infinitely many n, and codes $C_{q,n}$ over $\mathbb{F}_q$ satisfying
$$R\left(C_{q,n}\right) + \delta\left(C_{q,n}\right) \geq 1 - \frac{1}{\sqrt{q} - 1}$$
- Many codes that are better than random codes
  - Reed-Solomon, Reed-Muller of order 1, AG, BCH, dual BCH ...

- Moral: Distance property $\Leftarrow$ Algebra!

Part 3: Algorithmics $\Leftarrow$ Product property

Remarkable algorithmics

- Combinatorial implications:
  - Code of distance δ
    - Corrects $\frac{\delta}{2}$ fraction errors uniquely.
    - Corrects $1 - \sqrt{1 - \delta}$ fraction errors with small lists.
- Algorithmically?
  - For all known algebraic codes, above can be matched!
  - Why?

Product property

- For ir
  coo
- For

Reed-Solomon Codes:

$C =$ deg k poly

$E =$ deg $\frac{n-k}{2}$ poly

$E * C =$ deg $\frac{n+k}{2}$ poly

- Obvious, but remarkable, feature:
  - For every known algebraic code C of distance δ

    $\exists$ code E of co-dimension $\approx \frac{\delta}{2} n$ s.t.

    $E * C$ is a code of distance $\frac{\delta}{2}$.
- Terminology: $(E, E * C) \triangleq$ error-locating pair for C

Unique decoding by error-locating pairs

- Given $r \in \mathbb{F}_q^n$: Find $x \in C$ s.t. $\delta(x, r) \leq \frac{\delta}{2}$
- Algorithm
  - Step 1: Find $e \in E, f \in E * C$ s.t. $e * r = f$

[Pellikaan], [Koetter], [Duursma] – 90s

  - St
    - [Linear system again!]
- Analysis:
  - Solution to Step 1 exists?
    - Yes – provided $\dim(E) > \#$errors
  - Solution to Step 2 $\hat{x} = x$?
    - Yes – Provided $\delta(E)$ large enough.

List decoding abstraction

- Increasing basis sequence $b_1, b_2, \ldots$
- $C_i \triangleq \mathrm{span}\{b_1, \ldots, b_i\}$
- $\delta(C_i) \approx n - i + o(n)$
- $b_i * b_j \in C_{i+j} \quad (\Leftrightarrow C_i * C_j \subseteq C_{i+j})$

Reed-Solomon Codes:

$b_i = x^i$ (or its evaluations etc.)

- ing a rrors exist for codes with increasing basis sequences.

- (Increasing basis ⇒ Error-locating pairs)

Part 4: Locality $\Leftarrow$ Invariances

Locality in Codes

- General motivation:
  - Does correcting linear fraction of errors require scanning the whole code? Does testing?
    - Deterministically: Yes!
    - Probabilistically? Not necessarily!!
  - If possible, potentially a very useful concept
    - Definitely in other mathematical settings
      - PCPs, Small-set expanders, Hardness amplification, Private information retrieval ...
    - Maybe even in practice
- Aside: Related to LRCs from Judy Walker's talk.
  - Focus here on more errors.

Locality of some algebraic codes

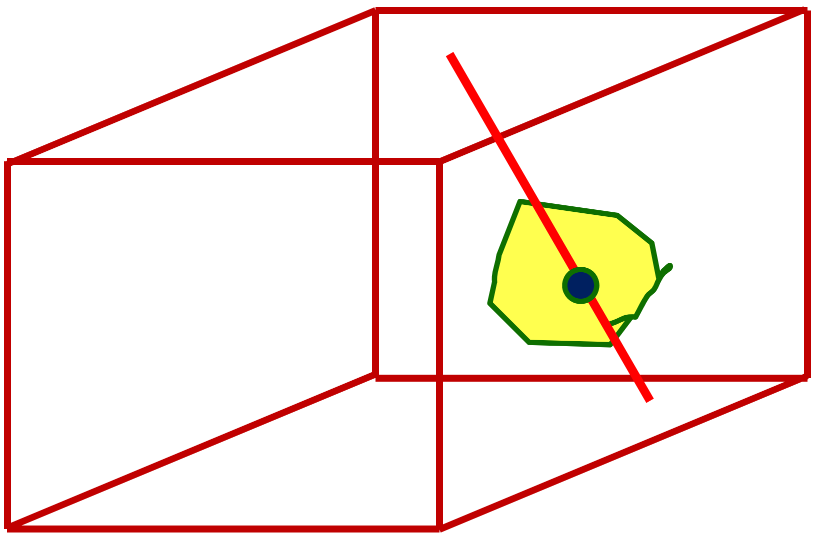
- Locality is a rare phenomenon.
  - Reed-Solomon codes are not.
  - Random codes are not.
  - AG codes are (usually) not.
- Basic examples are algebraic ...
- ... and a few composition operators preserve it.

- Canonical example: Reed-Muller Codes = low-degree polynomials.

Main Example: Reed-Muller Codes

- Message = multivariate polynomial; Encoding = evaluations everywhere.
  - $\mathrm{RM}[m, r, q] = \{\langle f(\alpha)\rangle_{\alpha \in \mathbb{F}_q^m} \mid f \in \mathbb{F}_\mathrm{q}[x_1, \dots, x_m], \deg(f) \leq r\}$

- Locality? (when $r < q$)
  - Restrictions of low-degree polynomials to lines yield low-degree (univ.) polys.
  - Random lines sample $\mathbb{F}_q^m$ uniformly (pairwise ind'ly)
  - Locality ~ q



Locality $\Leftarrow$?

- Necessary condition: Small (local) constraints.
  - Examples
    - $\deg(f) \leq 1 \Leftrightarrow f(x) + f(x+2y) = 2f(x+y)$
    - $f|_{line}$ has low-degree (so values on line are not arbitrary)

- Local Constraints $\Rightarrow$ local decoding/testing?
  - No!

- Transitivity + locality?

Symmetry in codes

- $Aut(C) \triangleq \{\pi \in S_n \mid \forall\, x \in C, x^{\pi} \in C\}$

- Well-studied concept.
  - "Cyclic codes"

- Basic algebraic codes (Reed-Solomon, Reed-Muller, BCH) symmetric under affine group
  - Domain is vector space $\mathbb{F}_Q^t$ (where $Q^t = n$)
  - Code invariant under non-singular affine transforms from $\mathbb{F}_Q^t \to \mathbb{F}_Q^t$

Symmetry and Locality

- Code has ℓ-local constraint + 2-transitive ⇒ Code is ℓ-locally decodable from $O\left(\frac{1}{\ell}\right)$-fraction errors.
  - 2-transitive? –
    - $\forall i \neq j, k \neq l \;\; \exists \pi \in \mathrm{Aut}(C)$ s.t. $\pi(i) = k, \pi(j) = l$
  - Why?
    - Suppose constraint $f(a) = f(b) + f(c) + f(d)$
    - Wish to determine $f(x)$
    - Find random $\pi \in \mathrm{Aut}(C)$ s.t. $\pi(a) = x$;

      $f(x) = f\big(\pi(b)\big) + f\big(\pi(c)\big) + f(\pi(d))$;

      $\pi(b), \pi(c), \pi\,(d)$ random, ind. of x

Symmetry + Locality - II

- Local constraint + affine-invariance ⇒ Local testing … specifically
- Theorem [Kaufman-S.'08]:
  - C ℓ-local constraint & is $\mathbb{F}_Q^t$-affine-invariant ⇒ C is $\ell'(\ell, Q)$-locally testable.

- Theorem [Ben-Sasson,Kaplan,Kopparty,Meir]
  - C has product property & 1-transitive ⇒ $\exists C'$ 1-transitive and locally testable and product property
- Theorem [B-S,K,K,M,Stichtenoth]
  - Such C exists. (C = AG code)

Aside: Recent Progress in Locality - 1

- [Yekhanin,Efremenko '06]: 3-Locally decodable codes of subexponential length.
- [Kopparty-Meir-RonZewi-Saraf '15]:
  - $n^{o(1)}$-locally decodable codes w. $R + \delta \to 1$
  - $\log n^{\log n}$-locally testable codes w. $R + \delta \to 1$
  - Codes not symmetric, but based on symmetric codes.

Aside – 2: Symmetric Ingredients …

- Lifted Codes [Guo-Kopparty-S.'13]
  - $C_{m,d,q} = \{ f : \mathbb{F}_q^m \to \mathbb{F}_q \mid \deg(f|_{line}) \leq d \ \forall\ line \}$
- Multiplicity Codes [Kopparty-Saraf-Yekhanin'10]
  - Message = biv. polynomial
  - Encode f via evaluations of (f, f_x, f_y)

Part 5: Conclusions

Remarkable properties of Algebraic Codes

- Strikingly strong combinatorially:
  - Often only proof that extreme choices of parameters are feasible.

- Algorithmically tractable!
  - The product property!

- Surprisingly versatile
  - Broad search space (domain, space of functions)

Quest for future

- Construct algebraic geometric codes with rich symmetries.
  - In general points on curve have few(er) symmetries.
  - Can we construct curve carefully?
    - Symmetry inherently?
    - Symmetry by design?

  - Still work to be done for specific applications.

Thank You!