Algebraic Codes and Invariance

Madhu Sudan
Harvard
Disclaimer

- Very little new work 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
  - Fundamental theorem(s) of algebra
- Part 3: Algorithmics of Algebraic Codes
  - Product property
- Part 4: Locality of (some) Algebraic Codes
  - 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
  - $E: \mathbb{F}_q^k \rightarrow \mathbb{F}_q^n$; associated Code $C \triangleq \{E(m) | m \in \mathbb{F}_q^k\}$

- Key parameters:
  - Rate $R(C) = \frac{k}{n}$
  - 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!

April 30, 2016

AAD3: Algebraic Codes and Invariance
Algorithmic tasks

- **Encoding**: Compute $E(m)$ given $m$.
- **Testing**: Given $r \in \mathbb{F}_q^n$, decide if $\exists m \text{ s.t. } r = E(m)$?
- **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?

- **General paradigm:**
  - Message space = (Vector) space of functions
  - Coordinates = Subset of domain of functions
  - Encoding = evaluations of message on domain

- **Examples:**
  - Reed-Solomon Codes
  - Reed-Muller Codes
  - Algebraic-Geometric Codes
  - Others (BCH codes, dual BCH codes ...)

**Algebraic-Geometry Codes:**
- Domain = Rational points of irreducible curve in $\mathbb{F}_q^m$
- Messages = Functions of bounded "order"
Part 2: Combinatorics ⇐ Fund. Thm
Essence of combinatorics

- Rate of code $\equiv$ Dimension of vector space
- Distance of code $\equiv$ 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]
    - [Goppa, 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

$$R(C_{q,n}) + \delta(C_{q,n}) \geq 1 - \frac{1}{\sqrt{q} - 1}$$

- Many codes that are better than random codes
  - Reed-Solomon, Reed-Muller of order 1, AG, BCH, dual BCH ...

- Moral: Distance property $\iff$ Algebra!
Part 3: Algorithmics $\iff$ Product property
Remarkable algorithmics

- Combinatorial implications:
  - Code of distance $\delta$
    - 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?
For vectors $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$, let $\mathbf{u} \ast \mathbf{v} \in \mathbb{F}_q^n$ denote their coordinate-wise product.

For linear codes $A, B \leq \mathbb{F}_q^n$, let $A \ast B = \text{span} \{a \ast b : a \in A, b \in B\}$.

Obvious, but remarkable, feature:

For every known algebraic code $C$ of distance $\delta$

\[ \exists \text{ code } E \text{ of dimension } \approx \frac{\delta}{2} n \text{ s.t. } \]

\[ E \ast C \text{ is a code of distance } \frac{\delta}{2}. \]

Terminology: $(E, E \ast C) \triangleq \text{error-locating pair for } C$
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 \( e \in E, f \in E \cdot C \) s.t. \( e \cdot r = f \)
- **Step 2**: Find \( \hat{x} \in C \) s.t. \( e \cdot \hat{x} = f \)

Analysis:

- Solution to Step 1 exists?
  - Yes – provided \( \text{dim}(E) > \text{#errors} \)
- Solution to Step 2 \( \hat{x} = x \)?
  - Yes – Provided \( \delta(E \cdot C) \) large enough.

[Pellikaan], [Koetter], [Duursma] – 90s
List decoding abstraction

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

Reed-Solomon Codes:
\( b_i \equiv x^i \) (or its evaluations etc.)

(List-decoding algorithms correcting \( 1 - \delta \) fraction errors exist for codes with increasing basis sequences.)

(Increasing basis \( \Rightarrow \) Error-locating pairs)
Part 4: Locality ⇐ 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
Locality of some algebraic codes

- Locality is a rare phenomenon.
  - Reed-Solomon codes are not local.
  - Random codes are not local.
  - AG codes are (usually) not local.
- 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.
  
  \[ \text{RM}[m, r, q] = \{ \langle f(\alpha) \rangle_{\alpha \in \mathbb{F}_q^m} \mid f \in \mathbb{F}_q[x_1, \ldots, x_m], \deg(f) \leq r \} \]

- **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 \( \sim q \)
Locality ⇐ ?

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

- Local Constraints ⇒ 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 \( \mathbb{F}_Q^t \rightarrow \mathbb{F}_Q^t \)
Symmetry and Locality

- Code has $\ell$-local constraint + 2-transitive $\Rightarrow$ Code is $\ell$-locally decodable from $O\left(\frac{1}{\ell}\right)$-fraction errors.

- 2-transitive? –
  - $\forall i \neq j, k \neq l \exists \pi \in \text{Aut}(C)$ 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 $\pi \in \text{Aut}(C)$ s.t. $\pi(a) = x$;
    
    $$f(x) = f(\pi(b)) + f(\pi(c)) + f(\pi(d));$$

    $\pi(b), \pi(c), \pi(d)$ random, ind. of $x$
Symmetry + Locality - II

- Local constraint + affine-invariance $\Rightarrow$ Local testing ... specifically

- Theorem [Kaufman-S.’08]:
  - $C$ $\ell$-local constraint & is $F_Q^t$-affine-invariant $\Rightarrow C$ is $\ell'(\ell, Q)$-locally testable.

- Theorem [Ben-Sasson,Kaplan,Kopparty,Meir]
  - $C$ has product property & 1-transitive $\Rightarrow \exists C'$ 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]**
  \[ C_{m,d,q} = \{ f : \mathbb{F}_q^m \to \mathbb{F}_q | \deg(f|_{\text{line}}) \leq d \ \forall \text{ line} \} \]

- **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!