On varieties and codes defined by quadratic equations

Ruud Pellikaan
g.r.pellikaan@tue.nl

Computer Algebra in Coding Theory and Cryptography (CACTC)
24th Conference on Applications of Computer Algebra (ACA)

Santiago de Compostela, 18 - 22 June 2018

Faculteit Wiskunde & Informatica

TU/e Technische Universiteit Eindhoven University of Technology

Introduction and content

- Error-correcting codes
- Generalized Reed-Solomon codes and Normal rational curves
- Codes on curves
- Product of functions versus star product
- Algebraic geometry codes defined by quadratic equations
- Reed-Muller defined by quadratic equations
- Questions

Error-correcting codes

Error-correcting codes

$\mathbb{F}_q$ the finite field with $q = p^e$ elements with p a prime
C linear block code: $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$

parameters $[n, k, d]$:
n = length
k = dimension of C
d = minimum distance of C

$$d = \min |\{ d(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y} \}|$$

t = error-correcting capacity of C

$$t = \lfloor \tfrac{d-1}{2} \rfloor$$

Inner product and dual code

The standard inner product is defined by

$$\mathbf{a} \cdot \mathbf{b} = a_1 b_1 + \cdots + a_n b_n$$

For two subsets A and B of $\mathbb{F}_q^n$
$A \perp B$ if and only if $\mathbf{a} \cdot \mathbf{b} = 0$ for all $\mathbf{a} \in A$ and $\mathbf{b} \in B$

Let $C \subseteq \mathbb{F}_q^n$ be an $\mathbb{F}_q$-linear $[n, k]$ code
The dual code of C is defined by

$$C^\perp = \{ \mathbf{b} \mid \mathbf{b} \cdot \mathbf{c} = 0 \text{ for all } \mathbf{c} \in C \}$$

Then $C^\perp$ has parameters $[n, n - k]$

Star product

Let $\mathbf{a}$ and $\mathbf{b}$ in $\mathbb{F}_q^n$
The star product is defined by coordinatewise multiplication:

$$\mathbf{a} * \mathbf{b} = (a_1 b_1, \ldots, a_n b_n)$$

For two subsets A and B of $\mathbb{F}_q^n$

$$A * B = \langle \{ \mathbf{a} * \mathbf{b} \mid \mathbf{a} \in A \text{ and } \mathbf{b} \in B \} \rangle$$

Generalized Reed-Solomon codes
and
Normal rational curves

Generalized Reed-Solomon codes

$\mathbf{a} = (a_1, \ldots, a_n)$ an n-tuple of mutually distinct elements of $\mathbb{F}_q$
$\mathbf{b} = (b_1, \ldots, b_n)$ an n-tuple of nonzero elements of $\mathbb{F}_q$

$$GRS_k(\mathbf{a}, \mathbf{b}) = \{ (f(a_1)b_1, \ldots, f(a_n)b_n) \mid f(X) \in \mathbb{F}_q[X], \deg(f(X) < k \}$$

parameters: $[n, k, n-k+1]$ if $k \leq n$

generator matrix:

$$G_k(\mathbf{a}, \mathbf{b}) = \begin{pmatrix} b_1 & \cdots & b_j & \cdots & b_n \\ a_1 b_1 & \cdots & a_j b_j & \cdots & a_n b_n \\ \vdots & \cdots & \vdots & \cdots & \vdots \\ a_1^{k-1} b_1 & \cdots & a_j^{k-1} b_j & \cdots & a_n^{k-1} b_n \end{pmatrix}$$

Normal rational curves and GRS codes

The projective system of the the code $GRS_k(\mathbf{a}, \mathbf{b})$ with generator matrix $G_k(\mathbf{a}, \mathbf{b})$ is

$$\mathcal{P}_k(\mathbf{a}) = ((1 : a_j : \cdots : a_j^i : \cdots : a_j^{k-1}) \mid j = 1, \ldots, n)$$

Consider the embedding $\mathbb{P}^1 \to \mathbb{P}^r$ by the degree r map given by

$$(y_0 : y_1) \mapsto (y_0^r : y_0^{r-1}y_1 : \cdots : y_0^{r-i}y_1^i : \cdots : y_0y_1^{r-1} : y_1^r)$$

The image of this map in $\mathbb{P}^r$ is the NRC (normal rational curve) $\mathcal{X}_r$

Every hyperplane intersects $\mathcal{X}_r$ in at most $r = k - 1$ points and

$$\mathcal{P}_{r+1}(\mathbf{a}) \subseteq \mathcal{X}_r(\mathbb{F}_q)$$

Vanishing ideal of rational normal curve

The vanishing ideal $I(\mathcal{X}_r)$ of $\mathcal{X}_r$ is generated by the quadratic polynomials:

$$X_i X_{r-i} - X_j X_{r-j}, \quad \text{for } 0 \leq i < j \leq r$$

that is the determinantal ideal of the 2×2 minors of the $2 \times r$ matrix

$$\begin{pmatrix} X_0 & X_1 & \cdots & X_i & \cdots & X_{r-1} \\ X_1 & X_2 & \cdots & X_{i+1} & \cdots & X_r \end{pmatrix}$$

since the rows of the matrix

$$\begin{pmatrix} 1 & y & \cdots & y^i & \cdots & y^{r-1} \\ y & y^2 & \cdots & y^{i+1} & \cdots & y^r \end{pmatrix}$$

are dependent for all y

Codes on curves

Codes on curves - 1

Let $\mathcal{X}$ be an algebraic curve defined over $\mathbb{F}_q$ of genus g
Let $\mathcal{P} = (P_1, \ldots, P_n)$ an n-tuple of mutual distinct points of $\mathcal{X}(\mathbb{F}_q)$

(If the support of E is disjoint from $\mathcal{P}$), then the evaluation map

$$\mathrm{ev}_{\mathcal{P}} : L(E) \to \mathbb{F}_q^n$$

where $\mathrm{ev}_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n))$, is well defined.

The algebraic geometry code $C_L(\mathcal{X}, \mathcal{P}, E)$
is the image of $L(E)$ under the evaluation map $\mathrm{ev}_{\mathcal{P}}$
If $m < n$, then $C_L(\mathcal{X}, \mathcal{P}, E)$ is an $[n, k, d]$ code with

$$k \geq m + 1 - g \quad \text{and} \quad d \geq n - m$$

$n - m$ is called the designed minimum distance of $C_L(\mathcal{X}, \mathcal{P}, E)$

Codes on curves - 2

Embedding of $\mathcal{X}$ in linear system of E of degree m
Let $f_1, f_2, \ldots, f_k$ be a basis of $L(E)$

$$\varphi_E : \mathcal{X} \longrightarrow \mathbb{P}^{k-1}$$

$$P \mapsto (f_1(P) : f_2(P) : \ldots : f_k(P))$$

$\mathcal{Y} = \varphi_E(\mathcal{X})$ is a curve of degree m in $\mathbb{P}^{k-1}$
$\mathcal{Q} = (\varphi_E(P_1), \ldots, \varphi_E(P_n))$ projective system

$$G_{\mathcal{Q}} = \begin{pmatrix} f_1(P_1) & \cdots & f_1(P_j) & \cdots & f_1(P_n) \\ f_2(P_1) & \cdots & f_2(P_j) & \cdots & f_2(P_n) \\ \vdots & \cdots & \vdots & \cdots & \vdots \\ f_k(P_1) & \cdots & f_k(P_j) & \cdots & f_k(P_n) \end{pmatrix}$$ generator matrix

minimum distance $\geq n - m$

Product of functions
versus
star product

Product of functions versus star product - 1

Let F and G be divisors
Then there is a well defined linear map

$$L(F) \otimes L(G) \longrightarrow L(F+G)$$

given on generators by

$$f \otimes g \mapsto fg$$

and

$$\mathrm{ev}_{\mathcal{P}}(fg) = \mathrm{ev}_{\mathcal{P}}(f) * \mathrm{ev}_{\mathcal{P}}(g)$$

hence

$$C_L(\mathcal{X}, \mathcal{P}, F) * C_L(\mathcal{X}, \mathcal{P}, G) \subseteq C_L(\mathcal{X}, \mathcal{P}, F+G)$$

Product of functions versus star product - 2

If furthermore $\deg(F), \deg(G) \geq 2g+1$
Then the map

$$L(F) \otimes L(G) \longrightarrow L(F+G)$$

is surjective
Hence

$$C_L(\mathcal{X}, \mathcal{P}, F) * C_L(\mathcal{X}, \mathcal{P}, G) = C_L(\mathcal{X}, \mathcal{P}, F+G)$$

Algebraic geometry codes
defined by
quadratic equations

Curves defined by quadrics

Normal rational normal curve is defined by quadratic equations.

The canonical model of a non-hyperelliptic projective curve
of genus at least three is the intersection of quadrics and cubics,
and of quadrics only except in case of
a trigonal curve and a plane quintic
Enriques 1919, Petri 1923 and Babbage 1939

This result for the canonical divisor was generalized for
arbitrary divisors E under certain constraints on the degree
Mumford 1970, Saint-Donat 1972 and Arbarello 1978

AG codes defined by quadratic equations - 1

Let $\mathcal{X}$ be an absolutely irreducible and nonsingular curve of genus g over the perfect field $\mathbb{F}$

Let E be a divisor on $\mathcal{X}$ of degree m

If $m \geq 2g + 1$
then φ_E gives an embedding of $\mathcal{X}$ onto $\mathcal{Y} = \varphi_E(\mathcal{X})$
which is a normal curve in the linear system $|E| = \mathbb{P}^{m-g}$

If $m \geq 2g + 2$, then $\mathcal{Y}$ is an intersection of quadrics
More precisely:
$I(\mathcal{Y})$ is generated by $I_2(\mathcal{Y})$
the set of homogeneous elements of degree two in $I(\mathcal{Y})$

AG codes defined by quadratic equations - 2

Let $\mathcal{Y}$ be a curve embedded in projective r-space of degree m
Let $I(\mathcal{Y})$ be the vanishing ideal of $\mathcal{Y}$
Let $\mathcal{Q}$ be a subset of $\mathcal{Y}$ of n points
Then

$$I(\mathcal{Y}) \subseteq I(\mathcal{Q})$$

Hence

$$I_2(\mathcal{Y}) \subseteq I_2(\mathcal{Q})$$

Suppose $I(\mathcal{Y})$ is generated by $I_2(\mathcal{Y})$

$$\text{If } n > 2m, \text{ then } I_2(\mathcal{Y}) = I_2(\mathcal{Q})$$

By Bézout's Theorem

AG codes defined by quadratic equations - 3

$\mathbf{g}_1, \ldots, \mathbf{g}_k$ a basis of C

$S^2(C)$ is the second symmetric power of C
$S^2(C)$ has basis $\{X_i X_j \mid 1 \leq i \leq j \leq n\}$ and dimension $\binom{k+1}{2}$
with $X_i = \mathbf{g}_i$

$C^{(2)} = C * C$ the square of C

Consider the linear map

$$\begin{array}{rccc} \sigma: & S^2(C) & \longrightarrow & C^{(2)} \\ & X_i X_j & \longmapsto & \mathbf{g}_i * \mathbf{g}_j \end{array}$$

$K_2(C)$ is the kernel of this map

AG codes defined by quadratic equations - 4

Then

$$0 \longrightarrow K_2(C) \longrightarrow S^2(C) \longrightarrow C^{(2)} \longrightarrow 0$$

is an exact sequence and

$$I_2(\mathcal{Q}) = K_2(C) := \{ \sum_{1 \le i \le j \le k} a_{ij} X_i X_j \mid \sum_{1 \le i \le j \le k} a_{ij} g_i * g_j = 0 \}$$

Proposition

Let $\mathcal{Q}$ be an n-tuple of points in $\mathbb{P}^r$ over $\mathbb{F}$ not in a hyperplane
Then the complexity of the computation of $I_2(\mathcal{Q})$ is at most $\mathcal{O}(n^4)$

AG codes defined by quadratic equations - 5

C is called very strong algebraic-geometric (VSAG)

if $C = C_L(\mathcal{X}, \mathcal{P}, E)$ and the curve $\mathcal{X}$ has genus g
$\mathcal{P}$ consists of n points and E has degree m such that

$$2g + 2 \leq m < \tfrac{1}{2}n \quad \text{or} \quad \tfrac{1}{2}n + 2g - 2 < m \leq n - 4$$

The dual of a VSAG code is again VSAG

AG codes defined by quadratic equations - 6

Main Theorem

Let C be a VSAG code

Then a VSAG representation of C can be obtained efficiently from its generator matrix

Moreover all VSAG representations of C are strict isomorphic

Proof:
Irene Márquez, Edgar Martínez, Diego Ruano and RP

Reed-Muller codes
defined by
quadratic equations

Veronese variety - 1

Let $(x_0 : x_1 : \ldots : x_m)$ be the coordinates of $\mathbb{P}^m$
Let $\mathbb{N}_0$ be the set of nonnegative integers and define for $\alpha \in \mathbb{N}_0^{m+1}$

$$\deg(\alpha) = \alpha_0 + \alpha_1 + \cdots + \alpha_m$$

Let $(x_\alpha | \alpha \in \mathbb{N}_0^{m+1}, \deg(\alpha) = r)$ be the coordinates of $\mathbb{P}^{\binom{m+r}{r}-1}$
Define

$$x^\alpha = x_0^{\alpha_0} x_1^{\alpha_1} \cdots x_m^{\alpha_m}$$

Consider the map from

$$\mathbb{P}^m \longrightarrow \mathbb{P}^{\binom{m+r}{r}-1}$$

given by $(x_0 : x_1 : \ldots : x_m) \mapsto (x^\alpha)$
that is the product x^α has coordinate x_α
The image of this map is called the Veronese variety $\mathcal{V}(r, m)$

Veronese variety - 2

Consider the sets defined by

$$A(r,m) = \{\, \alpha \in \mathbb{N}_0^{m+1} \mid \deg(\alpha) = r \,\}$$

$$B(r,m) = \{\, (\alpha,\beta) \in A(r,m)^2 \mid \alpha \leq \beta \,\} \text{ and}$$

$$C(r,m) = \{\, ((\alpha,\beta),(\gamma,\delta)) \in B(r,m)^2 \mid \alpha+\beta = \gamma+\delta,\ (\alpha,\beta) < (\gamma,\delta) \,\}$$

where $\leq$ is the lexicographic order
Then $\mathcal{V}(r,m)$ is a projective variety
with homogeneous vanishing ideal $I(r,m)$ that is generated
by the quadratic polynomials

$$X_\alpha X_\beta - X_\gamma X_\delta, \quad ((\alpha,\beta),(\gamma,\delta)) \in C(r,m).$$

The affine $\mathbb{F}_q$-rational part of the Veronese variety corresponds to a Reed-Muller code as we will see in the following

Reed-Muller codes - 1

Let $n = q^m$ and $\mathbf{a} = (a_1, \ldots, a_n)$ an enumeration of the elements of $\mathbb{F}_q^m$

Then

$$RM_q(r, m) = \{ (f(a_1), \ldots, f(a_n)) \mid f(X) \in \mathbb{F}_q[X_1, \ldots, X_m], \deg(f(X) \leq r \}$$

is the Reed-Muller code of order r in m variables over $\mathbb{F}_q$

Reed-Muller codes - 2

PROPOSITION

Let $\mathcal{C} = RM_q(r, m)$ and $2r < q$
Then

$$I_2(\mathcal{C}) = I_2(r, m)$$

the $\mathbb{F}_q$-linear subspace of $I(r, m)$ of elements of degree 2

QUESTIONS?

muchas gracias