Affine variety codes are better than their reputation

Olav Geil
Aalborg University
(joint with Stefano Martin)

Special Semester on
Applications of Algebra and Number Theory
Algebraic Curves over Finite Fields
RICAM
November 2013

Affine variety codes

$$I \subseteq \mathbb{F}_q[X_1, \ldots, X_m] \qquad I_q = I + \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle.$$

$$\{P_1, \ldots, P_n\} = \mathbb{V}_{\mathbb{F}_q}(I_q),$$

$\{N_1 + I_q, \ldots, N_n + I_q\}$ a basis for $\mathbb{F}_q[X_1, \ldots, X_m]/I_q$.

We get a basis for $\mathbb{F}_q^n$:
$\{\vec{b}_1 = \big(N_1(P_1), \ldots, N_1(P_n)\big), \ldots, \vec{b}_n = \big(N_n(P_1), \ldots, N_n(P_n)\big)\}$

Definition

Consider $L \subseteq \{1, \ldots, n\}$. $C(I, L) = \mathrm{Span}_{\mathbb{F}_q}\{\vec{b}_i \mid i \in L\}$
$C^\perp(I, L) = \big(C(I, L)\big)^\perp$.

Theorem

C is a linear code $\Leftrightarrow$ C is an affine variety code.

Affine variety codes

$$I \subseteq \mathbb{F}_q[X_1, \ldots, X_m] \quad I_q = I + \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle.$$

$$\{P_1, \ldots, P_n\} = \mathbb{V}_{\mathbb{F}_q}(I_q),$$

$\{N_1 + I_q, \ldots, N_n + I_q\}$ a basis for $\mathbb{F}_q[X_1, \ldots, X_m]/I_q$.

We get a basis for $\mathbb{F}_q^n$:
$\{\vec{b}_1 = (N_1(P_1), \ldots, N_1(P_n)), \ldots, \vec{b}_n = (N_n(P_1), \ldots, N_n(P_n))\}$

Definition

Consider $L \subseteq \{1, \ldots, n\}$. $C(I, L) = \mathrm{Span}_{\mathbb{F}_q}\{\vec{b}_i \mid i \in L\}$
$C^{\perp}(I, L) = (C(I, L))^{\perp}$.

Theorem

C is a linear code $\Leftrightarrow$ C is an affine variety code.

One-point AG codes

Theorem

If Q is a rational place then $\cup_{s=0}^{\infty}\mathcal{L}(sQ) \simeq \mathbb{F}_q[X_1,\ldots,X_m]/I$ where I satisfies the order domain conditions.

Theorem

A map $h : \mathbb{F}_q[X_1,\ldots,X_m]/I \to \mathbb{F}_q^n$ such that

- *h is $\mathbb{F}_q$-linear,*
- *$h(f) = (c_1,\ldots,c_n)$ and $h(g) = (d_1,\ldots,d_n)$*
  $$\Rightarrow h(fg) = (c_1d_1,\ldots,c_nd_n)$$

is of the form $h(f = F + I) = (F(P_1),\ldots,F(P_n))$, where $P_1,\ldots,P_n$ are affine points.

Our work

- Most known affine variety codes are one-point AG codes in disguise.
- We introduce a much broader class of affine variety codes.
- We
  - generalise the Feng-Rao-bound/order-bound for dual codes (also simply known as the Feng-Rao-bound/order-bound). Our method builds on work by Salazar et al.
  - generalise the Feng-Rao-bound/order-bound for primary codes (sometimes called the Andersen–G bound),

  We treat affine variety codes and general linear codes. We treat minimum distance and generalised Hamming weights.

Our work

- Most known affine variety codes are one-point AG codes in disguise.
- We introduce a much broader class of affine variety codes.
- We
  - generalise the Feng-Rao-bound/order-bound for dual codes (also simply known as the Feng-Rao-bound/order-bound). Our method builds on work by Salazar et al.
  - generalise the Feng-Rao-bound/order-bound for primary codes (sometimes called the Andersen–G bound),

  We treat affine variety codes and general linear codes. We treat minimum distance and generalised Hamming weights.

Our work

- Most known affine variety codes are one-point AG codes in disguise.
- We introduce a much broader class of affine variety codes.
- We
  - generalise the Feng-Rao-bound/order-bound for dual codes (also simply known as the Feng-Rao-bound/order-bound). Our method builds on work by Salazar et al.
  - generalise the Feng-Rao-bound/order-bound for primary codes (sometimes called the Andersen–G bound),

We treat affine variety codes and general linear codes. We treat minimum distance and generalised Hamming weights.

Our work

- Most known affine variety codes are one-point AG codes in disguise.
- We introduce a much broader class of affine variety codes.
- We
  - generalise the Feng-Rao-bound/order-bound for dual codes (also simply known as the Feng-Rao-bound/order-bound). Our method builds on work by Salazar et al.
  - generalise the Feng-Rao-bound/order-bound for primary codes (sometimes called the Andersen–G bound),

  We treat affine variety codes and general linear codes. We treat minimum distance and generalised Hamming weights.

The footprint bound

Definition

Given an ideal $J \subseteq k[X_1, \ldots, X_m]$ and a monomial ordering $\prec$ then $\Delta_\prec(J) = \{M \text{ is a monomial } \mid M \notin \mathrm{lm}(J)\}$

Theorem

(The footprint bound:) If $J \subseteq k[X_1, \ldots, X_m]$ is radical and zero-dimensional and if k is a perfect field then $\#\mathbb{V}(J) = \#\Delta_\prec(J)$.

Theorem

(The footprint bound:) If $J \subseteq k[X_1, \ldots, X_m]$ is radical and zero-dimensional and if k is a perfect field then $\#\mathbb{V}(J) = \#\Delta_{\prec}(J)$.

- For primary order domain codes (one-point AG codes, generalised Reed-Muller codes, etc.) the order bound is a consequence of the footprint bound.
- Our new bound for primary codes relies on the footprint bound.
- Our new bound for dual codes uses Feng-Rao arguments, and the connection to the primary bound is not completely clear.

The footprint bound and other bounds

Theorem

(The footprint bound:) If $J \subseteq k[X_1, \ldots, X_m]$ is radical and zero-dimensional and if k is a perfect field then $\#\mathbb{V}(J) = \#\Delta_{\prec}(J)$.

- For primary order domain codes (one-point AG codes, generalised Reed-Muller codes, etc.) the order bound is a consequence of the footprint bound.
- Our new bound for primary codes relies on the footprint bound.
- Our new bound for dual codes uses Feng-Rao arguments, and the connection to the primary bound is not completely clear.

The rest of this talk

- Our bound for dual codes is powerful, but too technical for this talk.
- Our bound for primary codes can easily be explained for affine variety codes.

Agenda:

- We start by studying the order domain conditions and primary codes.
- Then we throw away half of the order domain conditions and consider primary codes.
- We present numerical data for both primary and dual codes.

The rest of this talk

- Our bound for dual codes is powerful, but too technical for this talk.
- Our bound for primary codes can easily be explained for affine variety codes.

Agenda:

- We start by studying the order domain conditions and primary codes.
- Then we throw away half of the order domain conditions and consider primary codes.
- We present numerical data for both primary and dual codes.

Hermitian code

$$I = \langle X^2 + X - Y^3 \rangle \subseteq \mathbb{F}_4[X, Y],\ I_q = I + \langle X^4 - X, Y^4 - Y \rangle.$$

A weighted degree lexicographic ordering

From the weight function $w(X^i Y^j) = 3i + 2j$ we define the monomial ordering $\prec_w$ by $N \prec_w M$ if

- either $w(N) < w(M)$,
- or $w(N) = w(M)$ but $\deg_X(N) < \deg_X(M)$.

$$\{P_1, \ldots, P_8\} = \mathbb{V}(I_q).$$

Consider $\vec{c} = (F(P_1), \ldots, F(P_8))$.

$$\begin{aligned} w_H(\vec{c}) &= 8 - \#\text{ common zeros between } F \text{ and } I_q \\ &= \#\big(\Delta_{\prec_w}(I_q) \backslash \Delta_{\prec_w}(I_q + \langle F \rangle)\big) \\ &= \#\{M \in \Delta_{\prec_w}(I_q) \mid M \in \mathrm{lm}(I_q + \langle F \rangle)\}. \end{aligned}$$

Hermitian code - cont.

Consider $\vec{c} = (F(P_1), \ldots, F(P_8))$, say $F = a_1 + a_2 Y + X$

$w_H(\vec{c}) = \#\{M \in \Delta_{\prec_w}(I_q) \mid M \in \mathrm{Im}(I_q + \langle F \rangle)\}$.

Y^3	XY^3	6	9
Y^2	XY^2	4	7
Y	XY	2	5
1	X	0	3

$X = \mathrm{Im}(F)$, $XY = \mathrm{Im}(YF)$,
$XY^2 = \mathrm{Im}(Y^2F)$,
$XY^3 = \mathrm{Im}(Y^3F)$,
$Y^3 = \mathrm{Im}(XF - (X^2 + X - Y^3))$

In conclusion, $w_H(\vec{c}) \geq 5$.

We could also have counted the numbers in $\{0, 2, 3, 4, 5, 6, 7, 9\}$ which are being hit by $w(\mathrm{Im}(F)) = 3$.

This is due to $X^2 + X - Y^3$ having two monomials of the highest weight and all monomials in $\Delta_{\prec_w}(I)$ being of different weight.

Consider $\vec{c} = (F(P_1), \ldots, F(P_8))$, say $F = a_1 + a_2 Y + X$

$w_H(\vec{c}) = \#\{M \in \Delta_{\prec_w}(I_q) \mid M \in \mathrm{Im}(I_q + \langle F \rangle)\}$.

Y^3	XY^3	6	9
Y^2	XY^2	4	7
Y	XY	2	5
1	X	0	3

$X = \mathrm{Im}(F)$, $XY = \mathrm{Im}(YF)$,
$XY^2 = \mathrm{Im}(Y^2 F)$,
$XY^3 = \mathrm{Im}(Y^3 F)$,
$Y^3 = \mathrm{Im}(XF - (X^2 + X - Y^3))$

In conclusion, $w_H(\vec{c}) \geq 5$.

We could also have counted the numbers in $\{0, 2, 3, 4, 5, 6, 7, 9\}$ which are being hit by $w(\mathrm{Im}(F)) = 3$.

This is due to $X^2 + X - Y^3$ having two monomials of the highest weight and all monomials in $\Delta_{\prec_w}(I)$ being of different weight.

The order domain conditions

Definition

Consider an ideal $J \subseteq k[X_1, \ldots, X_m]$ where k is a field. Let a weighted degree ordering $\prec_w$ be given. Assume that J possesses a Gröbner basis $\mathcal{F}$ with respect to $\prec_w$ such that:

(C1) Any $F \in \mathcal{F}$ has exactly two monomials of highest weight.

(C2) No two monomials in $\Delta_{\prec_w}(J)$ are of the same weight.

Then we say that J and $\prec_w$ satisfy the order domain conditions.

The Feng-Rao bounds do not work well when the order domain conditions are not satisfied.

We throw away condition (C2) and introduce a method that works well for the corresponding codes.

The order domain conditions

Definition

Consider an ideal $J \subseteq k[X_1, \ldots, X_m]$ where k is a field. Let a weighted degree ordering $\prec_w$ be given. Assume that J possesses a Gröbner basis $\mathcal{F}$ with respect to $\prec_w$ such that:

(C1) Any $F \in \mathcal{F}$ has exactly two monomials of highest weight.

(C2) No two monomials in $\Delta_{\prec_w}(J)$ are of the same weight.

Then we say that J and $\prec_w$ satisfy the order domain conditions.

The Feng-Rao bounds do not work well when the order domain conditions are not satisfied.

We throw away condition (C2) and introduce a method that works well for the corresponding codes.

An affine variety code over $\mathbb{F}_8$.

$$I = \langle (X^4 + X^2 + X) - (Y^6 + Y^5 + Y^3) \rangle \subseteq \mathbb{F}_8[X, Y].$$
$$I_q = I + \langle X^8 - X, Y^8 - Y \rangle.$$

Define $\prec_w$ on the basis of $w(X^iY^j) = 3i + 2j$.

Y^7	XY^7	X^2Y^7	X^3Y^7
Y^6	XY^6	X^2Y^6	X^3Y^6
Y^5	XY^5	X^2Y^5	X^3Y^5
Y^4	XY^4	X^2Y^4	X^3Y^4
Y^3	XY^3	X^2Y^3	X^3Y^3
Y^2	XY^2	X^2Y^2	X^3Y^2
Y	XY	X^2Y	X^3Y
1	X	X^2	X^3

$\Delta_{\prec_w}(I_q)$

14	17	20	23
12	15	18	21
10	13	16	19
8	11	14	17
6	9	12	15
4	7	10	13
2	5	8	11
0	3	6	9

Corresponding weights

An affine variety code over $\mathbb{F}_8$ - cont.

14	17	20	23
12	15	18	21
10	13	16	19
8	11	14	17
6	9	12	15
4	7	10	13
2	5	8	11
0	3	6	9

$$\mathbb{V}(I_q) = \{P_1, \ldots, P_{32}\}$$

$$\vec{c} = (F(P_1), \ldots, F(P_{32}))$$

where

$$F = a_1 + a_2Y + a_3X + a_4Y^2 + a_5XY + a_6Y^3 + a_7X^2 + a_8XY^2 + a_9Y^4 + a_{10}X^2Y + a_{11}XY^3 + X^3$$

Observe that $w(XY^3) = w(X^3) = 9$. Hence, we must be careful.

An affine variety code over $\mathbb{F}_8$ - cont.

$F = a_1 + a_2Y + a_3X + a_4Y^2 + a_5XY + a_6Y^3 + a_7X^2 + a_8XY^2 + a_9Y^4 + a_{10}X^2Y + a_{11}XY^3 + X^3$.

14	17	20	23
12	15	18	21
10	13	16	19
8	11	14	17
6	9	12	15
4	7	10	13
2	5	8	11
0	3	6	9

Case 1: $a_{11} = 0$

$\text{Im}\left(XF - ((X^4 + X^2 + X) - (Y^6 + Y^5 + Y^3))\right) = Y^6$ and therefore we find not only X^3, X^3Y, X^3Y^2, X^3Y^3, X^3Y^4, X^3Y^5, X^3Y^6, X^3Y^7 but also Y^6, XY^6, X^2Y^6, Y^7, XY^7, X^2Y^7 as leading monomials.

Remember: $w_H(\vec{c}) = \#\{M \in \Delta_{\prec_w}(I_q) \mid M \in \text{Im}(I_q + \langle F \rangle)\}$.

An affine variety code over $\mathbb{F}_8$ - cont.

$F = a_1 + a_2Y + a_3X + a_4Y^2 + a_5XY + a_6Y^3 + a_7X^2 + a_8XY^2 + a_9Y^4 + a_{10}X^2Y + a_{11}XY^3 + X^3.$

14	17	20	23
12	15	18	21
10	13	16	19
8	11	14	17
6	9	12	15
4	7	10	13
2	5	8	11
0	3	6	9

Case 2: $a_{11} \neq 0$

$\mathrm{lm}\left(XF - ((X^4+X^2+X) - (Y^6+Y^5+Y^3))\right) = X^2Y^3$ and therefore we find not only X^3, X^3Y, X^3Y^2, X^3Y^3, X^3Y^4, X^3Y^5, X^3Y^6, X^3Y^7 but also X^2Y^3, X^2Y^4, X^2Y^5, X^2Y^6, X^2Y^7 as leading monomials.

Case 1 gave $w_H(\vec{c}) \geq 14$ and Case 2 gave $w_H(\vec{c}) \geq 13$.

Hence, $w_H(\vec{c}) \geq 13$. (The Feng-Rao bound gives $w_H(\vec{c}) \geq 8$)

An affine variety code over $\mathbb{F}_8$ - cont.

$F = a_1 + a_2Y + a_3X + a_4Y^2 + a_5XY + a_6Y^3 + a_7X^2 + a_8XY^2 + a_9Y^4 + a_{10}X^2Y + a_{11}XY^3 + X^3$.

14	17	20	23
12	15	18	21
10	13	16	19
8	11	14	17
6	9	12	15
4	7	10	13
2	5	8	11
0	3	6	9

Case 2: $a_{11} \neq 0$

$\text{lm}\left(XF - ((X^4+X^2+X)-(Y^6+Y^5+Y^3))\right) = X^2Y^3$ and therefore we find not only X^3, X^3Y, X^3Y^2, X^3Y^3, X^3Y^4, X^3Y^5, X^3Y^6, X^3Y^7 but also X^2Y^3, X^2Y^4, X^2Y^5, X^2Y^6, X^2Y^7 as leading monomials.

Case 1 gave $w_H(\vec{c}) \geq 14$ and Case 2 gave $w_H(\vec{c}) \geq 13$.

Hence, $w_H(\vec{c}) \geq 13$. (The Feng-Rao bound gives $w_H(\vec{c}) \geq 8$)

Terminology for general linear code

Feng-Rao introduced the concept of well-behaving pairs (WB),

Miura the concept of weakly well-behaving pairs (WWB),

G–Thommesen the concept of one-way well-behaving pairs (OWB).

OWB $\Leftarrow$ WWB $\Leftarrow$ WB
Therefore OWB gives the strongest bounds.

OWB becomes crucial when we skip the second order domain condition.

Results for dual codes

$$I = \langle (X^9 + X^3 + X) - (Y^{12} + Y^{10} + Y^4) \rangle \subseteq \mathbb{F}_{27}[X, Y].$$

Code length $n = 243$.

	Feng-Rao WB	Feng-Rao WWB	Feng-Rao OWB	"Advisory bound"	Our bound
$d_1(C(75))$	15	15	21	29	33
$d_2(C(75))$	16	16	24	34	38
$d_1(C(76))$	15	15	21	33	36
$d_2(C(76))$	16	16	24	38	39
$d_1(C(83))$	16	16	24	34	38
$d_2(C(83))$	17	17	27	39	41

A method for constructing many examples

Definition

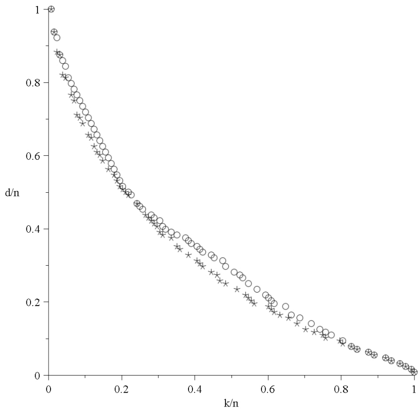
An $(\mathbb{F}_{q^t}, \mathbb{F}_q)$-polynomial is a polynomial $F(T) \in \mathbb{F}_{q^t}[T]$ such that $F(\gamma) \in \mathbb{F}_q$ holds for all $\gamma \in \mathbb{F}_{q^t}$.

Theorem

Consider the cyclotomic coset C_i modulo $q^t - 1$. Then $F(T) = \sum_{s \in C_i} X^s$ is an $(\mathbb{F}_{q^t}, \mathbb{F}_q)$-polynomial.

Corollary

Let $F(T)$ be a polynomial as in the above theorem and different from the trace-polynomial. Then $Tr_{\mathbb{F}_{q^t}/\mathbb{F}_q}(X) - F(Y)$ has exactly q^{2t-1} zeros.



Improved codes over $\mathbb{F}_{16}$ of length $n = 128$.
Using the trace-polynomial and the polynomial corresponding to the cyclotomic coset C_{10} we get $w(X) = 5$ and $w(Y) = 4$. These are the $\circ$s.
Using the trace-polynomial and the norm-polynomial we get the $*$s.