Affine variety codes are better than their reputation

Geil, Hans Olav; Martin, Stefano

Published in:
Proceedings of the 21st Symposium on Mathematical Theory of Networks and Systems

Publication date:
2014

Document Version
Early version, also known as pre-print

21st International Symposium on
Mathematical Theory of Networks and Systems
July 7-11, 2014. Groningen, The Netherlands

Affine variety codes are better than their reputation

Olav Geil[1] and Stefano Martin[2], Aalborg University

I. Affine variety codes and one-point AG-codes

In [2] Fitzgerald and Lax coined the name *affine variety code* for the following code construction. Consider an ideal $I \subseteq \mathbb{F}_q[X_1,\ldots,X_m]$ and define $I_q = I + \langle X_1^q - X_1, \ldots, X_m^q - X_m\rangle$. By $\mathbb{V}_{\mathbb{F}_q}(I_q) = \{P_1,\ldots,P_n\}$ we denote the variety of I_q. Consider a basis $\{N_1+I_q,\ldots,N_n+I_q\}$ for $\mathbb{F}_q[X_1,\ldots,X_m]/I_q$ as a vectorspace over $\mathbb{F}_q$. It is well-known that

$$\{\vec{b}_1 = \big(N_1(P_1),\ldots,N_1(P_n)\big),\ldots,\vec{b}_n = \big(N_n(P_1),\ldots,N_n(P_n)\big)\}$$

constitutes a basis for $\mathbb{F}_q^n$ as a vectorspace over $\mathbb{F}_q$.

Definition 1: Consider $L \subseteq \{1,\ldots,n\}$. We call $C(I,L) = \mathrm{Span}_{\mathbb{F}_q}\{\vec{b}_i \mid i \in L\}$ a primary affine variety code and $C^{\perp}(I,L) = \big(C(I,L)\big)^{\perp}$ a dual affine variety code.

It is not hard to prove that any linear code can be viewed as an affine variety code. More interestingly, there is a very concrete way of understanding any one-point algebraic geometric code as an affine variety code. To explain this we introduce the order domain conditions (for simplicity we consider in the present exposition only weights in $\mathbb{N}$.)

Definition 2: Consider monomials in variables $X_1,\ldots,X_m$. Given weights $w(X_1),\ldots,w(X_m) \in \mathbb{N}$ we define $w(X_1^{i_1}\cdots X_m^{i_m}) = i_1 w(X_1) + \cdots + i_m w(X_m)$. Let $\prec$ be any fixed monomial ordering. We define the weighted degree ordering $\prec_w$ by $N \prec_w M$ if either $w(N) < w(M)$ or $w(N) = w(M)$ but $N \prec M$.

Definition 3: Consider an ideal $J \subseteq k[X_1,\ldots,X_m]$, where k is a field, and a monomial ordering $\prec$. The footprint of J with respect to $\prec$ is $\Delta_{\prec}(J) = \{M \text{ is a monomial } \mid M \notin \mathrm{lm}(J)\}$.

Definition 4: Consider an ideal $J \subseteq k[X_1,\ldots,X_m]$. Let a weighted degree ordering $\prec_w$ be given. Assume that J possesses a Gröbner basis $\mathscr{F}$ with respect to $\prec_w$ such that:

- (C1) Any $F \in \mathscr{F}$ 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 $\prec_w$) satisfies the order domain conditions.

[1] olav@math.aau.dk
[2] stefano@math.aau.dk

The description of one-point algebraic geometric codes as affine variety codes follows from the below two theorems. For a reference of the first theorem see [6], [5].

Theorem 5: If Q is a rational place in an algebraic function field of transcendence degree 1 then $\cup_{s=0}^{\infty}\mathscr{L}(sQ) \simeq \mathbb{F}_q[X_1,\ldots,X_m]/I$ where I satisfies the order domain conditions. The weights involved are $w(X_i) = -\nu_Q(X_i+I)$, $i = 1,\ldots,m$.

Theorem 6: Let $h : \mathbb{F}_q[X_1,\ldots,X_m]/I \to \mathbb{F}_q^n$ be a map such that

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

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

With a few exceptions [1], [7] all affine variety codes considered in the literature are one-point algebraic geometric codes or generalizations of such codes to algebraic structures of higher transcendence degree. For these codes the Feng-Rao bounds often give good estimates on the minimum distance and the generalized Hamming weights. However, if one wants to consider more general classes of affine variety codes, the Feng-Rao bounds no longer are enough. In the present work we consider ideals I (it is important to distinguishe between I and I_q) which satisfy the first order domain condition (C.1) but do not satisfy the second order domain condition (C.2). Our main contribution is an improvement of the Feng-Rao bound for primary codes as well as an improvement of the Feng-Rao bound for dual codes. Our bound for primary codes [4] is completely new – it relies on the well-known footprint bound from Gröbner basis theory. Our bound for dual codes [3] is an improvement of Salazar et al.'s *advisory bound* [7].

II. The new bound for primary codes

In this section we describe our new bound for primary codes. Rather than giving the full technical description we explain the idea in an example. As is well-known $\{M+J \mid M \in \Delta_{\prec}(J)\}$ constitutes a basis for $k[X_1,\ldots,X_m]/J$ as a vector space over k. As a consequence we get the following instance of the footprint bound:

Theorem 7: If $J \subseteq k[X_1,\ldots,X_m]$ is radical and zero-dimensional and if k is a perfect field then $\#\mathbb{V}(J) = \#\Delta_{\prec}(J)$.

ISBN: 978-90-367-6321-9

Note that $\mathbb{F}_q$ is perfect and that I_q is radical. We now illustrate our bound for primary codes with an example.

Example 1: Consider the ideals $I = \langle (X^4 + X^2 + X) - (Y^6 + Y^5 + Y^3) \rangle \subseteq \mathbb{F}_8[X,Y]$, $I_q = I + \langle X^8 - X, Y^8 - Y \rangle$. To define a corresponding weighted degree monomial ordering $\prec_w$ we choose weights $w(X) = 3$, $w(Y) = 2$ and we let $\prec$ be the lexicographic ordering with $Y \prec X$. Order domain condition (C.1) is satisfied for I (the monomials of highest weight are X^4 and Y^6), but as the following figure shows the order domain condition (C.2) does not hold true for I.

Y^7	XY^7	X^2Y^7	X^3Y^7	14	17	20	23
Y^6	XY^6	X^2Y^6	X^3Y^6	12	15	18	21
Y^5	XY^5	X^2Y^5	X^3Y^5	10	13	16	19
Y^4	XY^4	X^2Y^4	X^3Y^4	8	11	14	17
Y^3	XY^3	X^2Y^3	X^3Y^3	6	9	12	15
Y^2	XY^2	X^2Y^2	X^3Y^2	4	7	10	13
Y	XY	X^2Y	X^3Y	2	5	8	11
1	X	X^2	X^3	0	3	6	9
$\Delta_{\prec_w}(I_q)$				$w(\Delta_{\prec_w}(I_q))$			

Fig. 1. The footprint from Example 1

Clearly, the variety of I_q is of size 32 and we enumerate the points $\mathbb{V}(I_q) = \{P_1, \ldots, P_{32}\}$. Consider any word $\vec{c} = (F(P_1), \ldots, F(P_{32}))$. We have

$$\begin{aligned} w_H(\vec{c}) &= 32 - \#\text{ common zeros between } F \text{ and } I_q \\ &= \#\big(\Delta_{\prec_w}(I_q) \backslash \Delta_{\prec_w}(I_q + \langle F \rangle)\big) \\ &= \#\{M \in \Delta_{\prec_w}(I_q) \mid M \in \mathrm{lm}(I_q + \langle F \rangle)\}. \end{aligned}$$

We now inspect in detail the situation 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 the two monomials of the highest weight are XY^3 and X^3 (the last being the leading monomial). We consider separately two different cases corresponding to if a_{11} is zero or not.

Case 1: Assume $a_{11} = 0$. This implies that $\mathrm{lm}\big(XF - \big((X^4 + X^2 + X) - (Y^6 + Y^5 + Y^3)\big)\big) = Y^6$ 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 as leading monomials in $I_q + \langle F \rangle$, but also Y^6, XY^6, X^2Y^6, Y^7, XY^7, X^2Y^7.

Case 2: Assume $a_{11} \neq 0$. This implies that $\mathrm{lm}\big(XF - \big((X^4 + X^2 + X) - (Y^6 + Y^5 + Y^3)\big)\big) = X^2Y^3$ 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.

If $\vec{c} = (F(P_1), \ldots, F(P_{32}))$ is a code word in a given code, then typically we will only have information about the leading monomial of the involved polynomial. If the leading monomial is X^3 then the above analysis tells us that $w_H(\vec{c}) \geq \min\{14, 13\}$.

For a general primary affine variety code $C(I,L)$ we derive a bound on the minimum distance by applying the above procedure for all possible choices of leading monomial (according to the actual choice of L). Assume that the footprint $\Delta_{\prec_w}(I_q)$ contains the same weight up to n times (in the above example we have $n = 2$). Then for each leading monomial we consider up to n different cases, and we find for each monomial the minimal value as above. In a straight forward manner one generalizes the above method to also deal with generalized Hamming weights. In the same way as the Feng-Rao bounds provide us with a method for constructing improved codes, so do our new bound for primary codes. More concretely, we can choose the L in $C(I,L)$ to be the span of only those monomials for which our bound gives a high value when these monomials are the leading monomial of F.

All the results described in this section can be reformulated at the level of general linear code. This involves a translation of the footprint bound (Theorem 7) to linear code level. Our description of a new bound for dual codes to be given in Section IV will involve a mixture of the linear code level and the affine variety code level. As a preparation we start by discussing in the next section the Feng-Rao bounds.

III. The Feng-Rao bounds

In this section we recall the Feng-Rao bounds for primary and dual codes. We start by deriving the first mentioned bound as a corollary to our new bound for primary codes.

Write $\Delta_{\prec_w}(I_q) = \{N_1, \ldots, N_n\}$, where $N_1 \prec_w \cdots \prec_w N_n$. Recall from the previous section that given a word $\vec{c} = (F(P_1), \ldots, F(P_n))$ we know that $w_H(\vec{c}) = \#\{M \in \Delta_{\prec_w}(I_q) \mid M \in \mathrm{lm}(I_q + \langle F \rangle)\}$. Let $F = \sum_{t=1}^{i} a_t N_t$, with $a_1, \ldots, a_i \in \mathbb{F}_q$ being unknown and $a_t \neq 0$. Assume that N_j is such that

$$\mathrm{lm}\big(\big(\sum_{t=1}^{i} a_t N_t\big) N_j \text{ rem } \mathscr{G}\big) = \mathrm{lm}\big(N_i N_j \text{ rem } \mathscr{G}\big) = N_l \qquad (1)$$

holds for all possible choices of $a_1, \ldots, a_i$ with $a_i \neq 0$. Obviously, then $N_l \in \Delta_{\prec_w}(I_q) \cap \mathrm{lm}(I_q + \langle F \rangle)$ and as an estimate of $w_H(\vec{c})$ we can use the number of indices l (corresponding to the number of indices j) for which (1) holds true. Clearly, this method is weaker than the method of the previous section.

We now lift the above result to the level of general primary linear codes. Let $\{\vec{b}_1, \ldots, \vec{b}_n\}$ be a basis for $\mathbb{F}_q^n$. For $\vec{c} = \sum_{t=1}^{i} a_t \vec{b}_t$, $a_i \neq 0$ we define $\bar{\rho}(\vec{c}) = i$. We shall need the component wise product $*$ which is defined by $(\alpha_1, \ldots, \alpha_n) * (\beta_1, \ldots, \beta_n) = (\alpha_1\beta_1, \ldots, \alpha_n\beta_n)$.

Definition 8: If $\bar{\rho}\big(\big(\sum_{t=1}^{i} a_t\vec{b}_t\big)*\vec{b}_j\big) = \bar{\rho}(\vec{b}_i*\vec{b}_j) = l$ for all choices of $a_1,\ldots,a_i$ such that $a_i \neq 0$ then we say that (i,j) is one-way well-behaving (OWB).

Theorem 9: (The Feng-Rao bound for primary codes) If $a_i \neq 0$ then $w_H\big(\sum_{t=1}^{i} a_t\vec{b}_t\big)$ is at least equal to the number of $l \in \{1,\ldots,n\}$ for which a $j \in \{1,\ldots,n\}$ exists with (i,j) OWB and $\bar{\rho}(\vec{b}_i*\vec{b}_j) = l$.

The Feng-Rao bound for dual codes follows a similar pattern.

Definition 10: For $\vec{c} \neq 0$, let $m(\vec{c})$ be the smallest index l such that $\vec{c}\cdot\vec{b}_l \neq 0$.

Theorem 11: (The Feng-Rao bound for dual codes) If $m(\vec{c}) = l$ then $w_H(\vec{c})$ is at least equal to the number $i \in \{1,\ldots,n\}$ for which a j exists with (i,j) OWB and $\bar{\rho}(\vec{b}_i*\vec{b}_j) = l$.

Above we formulated the Feng-Rao bounds using the concept of OWB. In the literature it is more common to use the concepts of well-behaving (WB) and weakly well-behaving (WWB). However, WB is the strongest requirement followed by WWB and OWB in that order. Hence, the strongest bounds are derived by using OWB.

IV. The new bound for dual codes

The Feng-Rao bound for dual codes can be viewed to be a consequence of the following Lemma from which we derive a much stronger bound.

Lemma 12: Consider $\vec{c} \in \mathbb{F}_q^n$. Let $U \subseteq \mathbb{F}_q^n$ be a subspace of dimension δ such that for all non-zero words $\vec{u} \in U$ for some $\vec{v}$ it holds that $(\vec{u}*\vec{v})\cdot\vec{c} \neq 0$. Then $w_H(\vec{c}) \geq \delta$.

Rather than presenting our new bound in its general form we here only illustrate it with an example.

Example 2: This is a continuation of Example 1 where we considered primary affine variety codes. We now consider dual affine variety codes from the same ideal I_q. Recall that $I = \langle (X^4+X^2+X) - (Y^6+Y^5+Y^3)\rangle \subseteq \mathbb{F}_8[X,Y]$, $I_q = I + \langle X^8 - X, Y^8 - Y\rangle$. We shall write $\Delta_{\prec_w}(I_q) = \{N_1,\ldots,N_{32}\}$, with $N_1 \prec_w \cdots \prec_w N_{32}$. Using this notation we restate in Figure 2 the information from Figure 1. For $i = 1,\ldots,n$ we define $\vec{b}_i = (N_i(P_1),\ldots,N_i(P_n))$ which shall then be our basis for $\mathbb{F}_8^{32}$.

$w(\Delta_{\prec_w}(I_q))$				$\Delta_{\prec_w}(I_q)$			
14	17	20	23	N_{21}	N_{26}	N_{30}	N_{32}
12	15	18	21	N_{17}	N_{23}	N_{28}	N_{31}
10	13	16	19	N_{13}	N_{19}	N_{25}	N_{29}
8	11	14	17	N_9	N_{15}	N_{22}	N_{27}
6	9	12	15	N_6	N_{11}	N_{18}	N_{24}
4	7	10	13	N_4	N_8	N_{14}	N_{20}
2	5	8	11	N_2	N_5	N_{10}	N_{16}
0	3	6	9	N_1	N_3	N_7	N_{12}

Fig. 2. The footprint of Example 2

Consider a word $\vec{c}$ with $m(\vec{c}) = 21$. That is, $l = 21$ is the smallest index such that $\vec{c}\cdot\vec{b}_l \neq 0$. Observe, that $w(N_{21}) = 14 = w(N_{22})$. We shall consider two cases according to if $\vec{c}\cdot\vec{b}_{22}$ is zero or not.

Case 1: Assume $\vec{c}\cdot\vec{b}_{22} = 0$
If we choose $U = \mathrm{Span}\{\vec{b}_1, \vec{b}_2, \vec{b}_4, \vec{b}_6, \vec{b}_9, \vec{b}_{13}, \vec{b}_{17}, \vec{b}_{21}, \vec{b}_3, \vec{b}_{12}, \vec{b}_5, \vec{b}_{16}, \vec{b}_7, \vec{b}_{10}\}$ then indeed for each $\vec{u} \in U\backslash\{\vec{0}\}$ there exists a $\vec{b}_j$ such that $(\vec{u}*\vec{b}_j)\cdot\vec{c} \neq 0$.

Case 2: Assume $\vec{c}\cdot\vec{b}_{22} \neq 0$
If we choose $U = \mathrm{Span}\{\vec{b}_1,\vec{b}_2,\vec{b}_4,\vec{b}_6,\vec{b}_9,\vec{b}_{13},\vec{b}_{17},\vec{b}_{21}, \vec{b}_3,\vec{b}_5,\vec{b}_8,\vec{b}_{11},\vec{b}_{15}\}$ then indeed for each $\vec{u} \in U\backslash\{\vec{0}\}$ there exists a $\vec{b}_j$ such that $(\vec{u}*\vec{b}_j)\cdot\vec{c} \neq 0$.

From Case 1 we get $w_H(\vec{c}) \geq 14$ and from Case 2 $w_H(\vec{c}) \geq 13$. Hence, $w_H(\vec{c}) \geq \min\{14,13\} = 13$. For comparison the Feng-Rao bound with WB or WWB gives $w_H(\vec{c}) \geq 8$. The same bound, but with OWB, produces $w_H(\vec{c}) \geq 10$. Finally, the Advisory bound (equiped with OWB) gives $w_H(\vec{c}) \geq 12$.

For a general dual affine variety code $C^{\perp}(I,L)$ we derive a bound on the minimum distance by applying the above procedure for all possible choices of $l = m(\vec{c})$ (according to the actual choice of L). Assume that the footprint $\Delta_{\prec_w}(I_q)$ contains the same weight up to n times (in the above example we have $n = 2$). Then for each choice of l we consider up to n different cases, and we find for each monomial the minimal value as above. One can generalize the above method to also deal with generalized Hamming weights. In the same way as the Feng-Rao bounds provide us with a method for constructing improved codes, so do our new bound for dual codes.

As reflected by Example 1 and Example 2, when $\Delta_{\prec_w}(I_q)$ is a box, our bounds for primary and dual codes produce similar code parameters. When $\Delta_{\prec_w}(I_q)$ is not a box the estimated code parameters are often very different.

V. The case of two variables

Our method from Section II and Section IV works well for any ideal I which satisfies the order domain condition (C.1). Clearly, there are many more such ideals than there are ideals which satisfy in addition condition (C.2). In our work we have given particular attention to the case $I = \langle F(X,Y)\rangle \subseteq \mathbb{F}_q[X,Y]$. Using cyclotomic cosets we can construct polynomials $F(X,Y) = G(X) - H(Y)$ with

maximal possible number of zeros according to the values of $\mathrm{lm}(G)$ and $\mathrm{lm}(H)$. This provides us with many new examples of good affine variety codes that are not one-point algebraic geometric codes. We refer to [4] for closed formula expressions of the parameters of these codes.

Example 3: From the ideal $I = \langle (X^9 + X^3 + X) - (Y^{12} + Y^{10} + Y^4) \rangle \subseteq \mathbb{F}_{27}[X,Y]$ we derive dual codes of length $n = 243$ with estimated minimum distance and second generalized Hamming weight as follows (we refer to [4] for the meaning of the notation $C(s)$):

	Feng-Rao WB	Feng-Rao WWB	Feng-Rao OWB	Advisory bound	The new 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

The codes are of dimensions 168, 167, and 160, respectively. The corresponding footprint is a box. Hence, the Feng-Rao bounds and our new bounds produce similar results for primary codes (there does not seem to be a counter part of the Advisory bound to primary codes).

Example 4: In Figure 3 we consider improved codes over $\mathbb{F}_{64}$ of length $n = 2048$ (for the considered ideals the performance of dual and primary codes are the same). The lower graph corresponds to the improved norm-trace codes (Feng-Rao improved one-point algebraic geometric codes). The upper graph corresponds to improved affine variety codes defined from an ideal $I = \langle G(X) - H(Y) \rangle$ where $\mathrm{lm}(G) = X^{32}$ and $\mathrm{lm}(H) = Y^{42}$. Note that I does not satisfy order domain condition (C.2) as 32 and 42 are not relatively prime.

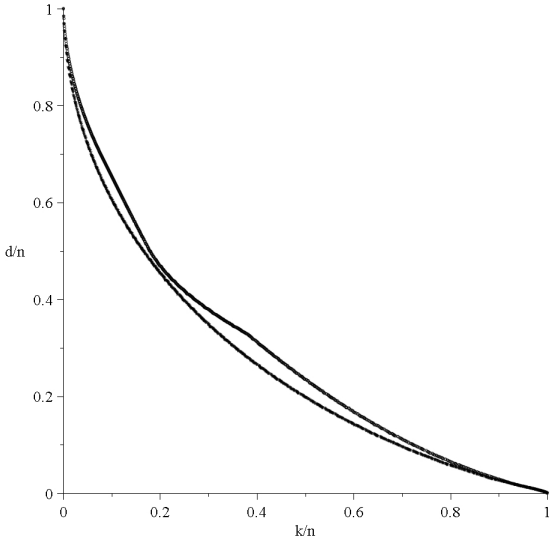

Fig. 3. The codes from Example 4.

REFERENCES

[1] Gui Liang Feng and T. R. N. Rao. A simple approach for construction of algebraic-geometric codes from affine plane curves. *IEEE Trans. Inform. Theory*, 40(4):1003–1012, 1994.

[2] J. Fitzgerald and R. F. Lax. Decoding affine variety codes using Gröbner bases. *Des. Codes Cryptogr.*, 13(2):147–158, 1998.

[3] Olav Geil and Stefano Martin. Further improvements on the Feng-Rao bound for dual codes. *arXiv preprint arXiv:1305.1091*, 2013.

[4] Olav Geil and Stefano Martin. An improvement of the Feng-Rao bound for primary codes. *arXiv preprint arXiv:1307.3107*, 2013.

[5] Ryutaroh Matsumoto and Shinji Miura. On construction and generalization of algebraic geometry codes. *Proc. Algebraic Geometry, Number Theory, Coding Theory, and Cryptography*, pages 3–15, 2000.

[6] Ruud Pellikaan. On the existence of order functions. *Journal of Statistical Planning and Inference*, 94(2):287–301, 2001.

[7] G. Salazar, D. Dunn, and S. B. Graham. An improvement of the Feng-Rao bound on minimum distance. *Finite Fields Appl.*, 12:313–335, 2006.