# An Examination of Quaternary Higher-Dimensional Affine Variety Codes with an Improved Minimum Distance Bound

Gary L. Salazar, Diana M. Dunn, Sarah B. Graham

July 31, 2002

## 1 Introduction

This paper examines several families of affine variety codes [6] in which the minimum distance is optimal given fixed parameters of length and dimension. We also introduce a bound on the minimum distance that in some cases is an improvement of the bounds due to Feng and Rao [1] and Miura [5]. In the last section, we shall restrict our attention to quaternary affine variety codes resulting from surfaces or hypersurfaces. When necessary, the true minimum distance of codes was determined by GAP[2].

We begin with some basic definitions.

Let $\mathbb{F}_q$ denote the finite field with $q$ elements, and let $\mathbb{F}_q^k$ be the set of all $k$-tuples of elements in $\mathbb{F}_q$.

**Definition 1.1.** Let $I$ be an ideal of the polynomial ring $\mathbb{F}_q[x_1, ..., x_k]$. Then

$$I_q := I + (x_1^q - x_1, ..., x_k^q - x_k).$$

The affine variety of $I_q$, denoted $V(I_q)$, is given by

$$V(I_q) := \{(a_1, ..., a_k) \in \mathbb{F}_q^k : f(a_1, ..., a_k) = 0 \text{ for all } f \in I_q\}.$$

Let $R$ be the coordinate ring of the variety $V(I_q)$; that is, $R = \mathbb{F}_q[x_1, ..., x_k]/I_q$. Suppose that $\{P_1, ..., P_n\}$ is an ordering of the points of $V(I_q)$. We define a mapping $\phi : R \mapsto \mathbb{F}_q^k$ such that $\phi(\bar{f}) = (f(P_1), ..., f(P_n))$. It is well-known that this evaluation map $\phi$ is an isomorphism of $\mathbb{F}_q$-vector spaces.

Let $L$ denote an $\mathbb{F}_q$-vector subspace of the coordinate ring $R$.

**Definition 1.2.** The affine variety codes $C(I, L)$ and $C^{\perp}(I, L)$ are defined as follows:

$$C(I, L) = \phi(L)$$
$$C^{\perp}(I, L) = \phi(L)^{\perp},$$

where $\phi(L)^{\perp}$ is the orthogonal complement of $\phi(L)$, with respect to the usual inner product on $\mathbb{F}_q^n$.

In the field of error-correcting coding theory, maximizing the minimum distance for any code of fixed length and dimension (and thereby maximizing the error-correcting capacity of that code) is emphasized. In 1995, Feng and Rao [1] defined a lower bound on the minimum distance of the affine variety codes of the form $C^{\perp}(I, L)$. To introduce this Feng-Rao bound, we begin with the following definitions, adopting the terminology of Feng and Rao, in the context of affine variety codes.

**Definition 1.3.** Let $T^k$ denote the set of monomials of $\mathbb{F}_q[x_1, ..., x_k]$, i.e., $T^k := \{x_1^{\alpha_1}...x_k^{\alpha_k} | \alpha_i \in \mathbb{N} \text{ for } 1 \leq i \leq k\}$.

We shall define a total ordering $<_t$ on the elements of $T^k$ according to the following weighted-degree lexicographic ordering. Assign a "weight", that is, a positive integer denoted $wt(x_j)$ to each variable $x_j$ for $1 \leq j \leq k$. Then, the weight of the monomial $x_1^{\alpha_1}...x_k^{\alpha_k}$ is defined to be $wt(x_1^{\alpha_1}...x_k^{\alpha_k}) = \sum_{j=1}^{k} \alpha_j wt(x_j)$.

Moreover, $x_1^{\alpha_1}...x_k^{\alpha_k} <_t x_1^{\beta_1}...x_k^{\beta_k}$ if either
(i) $wt(x_1^{\alpha_1}...x_k^{\alpha_k}) < wt(x_1^{\beta_1}...x_k^{\beta_k})$ or
(ii) $wt(x_1^{\alpha_1}...x_k^{\alpha_k}) = wt(x_1^{\beta_1}...x_k^{\beta_k})$ and there exists an $m$ such that $\alpha_l = \beta_l$ for $1 \leq l < m$ and $\alpha_m < \beta_m$.

**Definition 1.4.** The $\Delta$-*set* of an ideal $I \subseteq \mathbb{F}_q[x_1, ..., x_k]$, denoted $\Delta(I)$, is defined to be $\Delta(I) := T^k \setminus \{lm(f) | f \in I, f \neq 0\}$ where $lm(f)$ denotes the leading monomial of $f$ under the ordering $<_t$.

Given an ideal $I$, we wish to consider two sequences resulting from $\Delta(I_q)$.

**Definition 1.5.** For $I \subseteq \mathbb{F}_q[x_1, ..., x_k]$, we define the *H-sequence* as $H := \{h_i\}_{i=1}^{n}$ the increasing sequence (under $<_t$) of the elements of $\Delta(I_q)$. The corresponding weight sequence is defined by $W := \{wt(h_i)\}_{i=1}^{n}$.

We note that $W$ is a nondecreasing sequence of integers and the elements of the set $\{\bar{h}_1, ..., \bar{h}_n\}$ form a basis for the coordinate ring $R = \mathbb{F}_q[x_1, ..., x_k]/I_q$.

**Definition 1.6.** Let $L(\underline{r})$ be the linear subspace of dimension $r$ of $R$ generated by the set $\{\bar{h}_1, ..., \bar{h}_r\}$. More generally, let $L(\underline{r}, v_1, ..., v_l)$ denote the subspace (of dimension $r + l$) generated by $\{\bar{h}_1, ..., \bar{h}_r, \bar{h}_{v_1}, ..., \bar{h}_{v_l}\}$ where $r + 1 < v_1 < ... < v_l$ for some $l \geq 0$.

Note that if $l = 0$, then we have $L(\underline{r}, v_1, ..., v_l) = L(\underline{r})$.

**Definition 1.7.** A monomial $h$ is *consistent with* $h_r$ if $wt(h) = wt(h_r)$ and $\bar{h} \in L(\underline{r}) \setminus L(\underline{r-1})$. If $h$ is consistent with $h_r$, then we write $h \sim h_r$.

**Lemma 1.1.** If $h <_t h_r$, then $\bar{h} \in L(\underline{r-1})$.

*Proof.* Suppose $h <_t h_r$ and $\bar{h} \in L(\underline{s})$ for some $s \geq r$. Then $h + I_q = \sum_{i=1}^{s}(k_i h_i) + I_q$ for some $k_i \in \mathbb{F}_q$ for $1 \leq i \leq s$ with $k_s \neq 0$. Thus, $f = \sum_{i=1}^{s}(k_i h_i) - h \in I_q$ and $lm(f) = h_s$ since $k_s \neq 0$ and $h <_t h_r \leq_t h_s$. This is a contradiction since the monomial $h_s \in \Delta(I_q)$. □

As a consequence, we obtain the following result.

**Corollary 1.1.** If $h \sim h_r$, then $h_r \leq_t h$.

**Definition 1.8.** A monomial $h$ is *consistent with* $h_r$ if $wt(h) = wt(h_r)$ and $\bar{h} \in L(\underline{r}) \setminus L(\underline{r-1})$. If $h$ is consistent with $h_r$, then we write $h \sim h_r$.

**Definition 1.9.** If $h_i = x_1^{i_1} x_2^{i_2} ... x_k^{i_k}$ and $h_j = x_1^{j_1} x_2^{j_2} ... x_k^{j_k}$ then define the product $h_i \cdot h_j$ by $h_{i,j} := x_1^{\alpha_1} x_2^{\alpha_2} ... x_k^{\alpha_k}$, where for $l = 1, ..., k$,

$$\alpha_l = \begin{cases} i_l + j_l & \text{if } i_l + j_l < q \\ i_l + j_l - (q-1) & \text{otherwise.} \end{cases} \tag{1}$$

**Definition 1.10.** Let $h_{i,j}$ be a monomial such that $h_{i,j} \sim h_r$ . The monomial $h_{i,j}$ is *well-behaving* if for each $(u, v)$ where $1 \leq u \leq i$ and $1 \leq v \leq j$ with $(u, v) \neq (i, j)$, we have $\bar{h}_{u,v} \in L(\underline{r-1})$.

**Definition 1.11.** Let $h_{i,j}$ be a monomial such that $h_{i,j} \sim h_r$. The monomial $h_{i,j}$ is said to be *weakly well-behaving* if for each $(u, v)$ where either $u < i$ and $v = j$ or $u = i$ and $v < j$, we have $\bar{h}_{u,v} \in L(\underline{r-1})$.

**Definition 1.12.** For each monomial $h_r \in H$, define $N_r := \{(i,j) : h_{i,j} \sim h_r$ and $h_{i,j}$ is well-behaving$\}$. Similarly, define $\tilde{N}_r = \{(i,j) : h_{i,j} \sim h_r$ and $h_{i,j}$ is weakly well-behaving$\}$.

The integer $|N_r|$ is due to Feng and Rao and the integer $|\tilde{N}_r|$ is due to Miura. Moreover, by construction, we see that $N_r \leq \tilde{N}_r$.

**Lemma 1.2.** Let $h_i, h_j$, and $h_r \in H$. If $h_{i,j} = h_r$, then $h_{i,j}$ is a well-behaving term consistent with $h_r$.

*Proof.* Suppose $h_i, h_j, h_r \in H$ such that $h_{i,j} = h_r$. Clearly, $h_{i,j} \sim h_r$. Let $(u,v)$ be such that $1 \leq u \leq i$, $1 \leq v \leq j$ and $(u,v) \neq (i,j)$. Then, $h_{u,v} <_t h_{i,j} = h_r$. Hence, by Lemma 1.1, $\bar{h}_{u,v} \in L(\underline{r-1})$. □

**Corollary 1.2.** For $h_r = x_1^{\alpha_1}...x_n^{\alpha_n} \in H$, we have $|N_r| \geq \prod_{i=1}^{n}(\alpha_i + 1)$.

That is, $N_r$ is at least the number of monomial divisors of $h_r$.

**Definition 1.13.** The parity check matrix $H_r$ for the affine variety code $C^{\perp}(I, L(\underline{r}))$ is constructed by evaluating $h_1, ..., h_r$ at each of the points of the variety. That is, $H_r := [h_i(P_j)]$ for $1 \leq i \leq r$ and $1 \leq j \leq n$, where $n$ is the number of points in the variety.

**Definition 1.14.** Let $L = L(\underline{r}, v_1, ..., v_l)$. Then $H_r^+$, the parity check matrix for $C^{\perp}(I, L)$, is defined as

$$H_r^+ := \begin{pmatrix} & H_r & \\ h_{v_1}(P_1) & \cdots & h_{v_1}(P_n) \\ \vdots & \vdots & \vdots \\ h_{v_l}(P_1) & \cdots & h_{v_l}(P_n) \end{pmatrix}.$$

Notice that if $l = 0$, then $H_r^+ = H_r$.

Given these preliminary definitions, we may now define the Feng-Rao and weakly Feng-Rao minimum distance bounds.

**Proposition 1.1.** Suppose $H_r^+$ is a parity check matrix of the linear code $C^{\perp}(I, L)$ where $L = L(\underline{r}, v_1, ..., v_l)$. Put

$$\delta_{WFR} := \min\{|\tilde{N}_v| : v \notin \{1, ..., r, v_1, ..., v_l\}\}.$$

Then, the code $C^{\perp}(I,L)$ has minimum distance at least $\delta_{WFR}$, where, $\delta_{WFR}$ will be referred to as the weakly Feng-Rao bound or the Miura bound.

The proof is found in [5].

**Definition 1.15.** Put $\delta_{FR} := min\{|N_v| : v \notin \{1, ..., r, v_1, ..., v_l\}\}$; then $\delta_{FR}$ is referred to as the Feng-Rao bound on minimum distance for the code $C^{\perp}(I,L)$ where $L = L(\underline{r}, v_1, ..., v_l)$.

Note that since $N_r \subseteq \tilde{N}_r$, we have $\delta_{FR} \leq \delta_{WFR}$; this is shown in [5], although the authors indicate that they have not found an algebraic geometric code in which there was inequality.

# 2 An Improved Minimum Distance Bound for Certain Affine Variety Codes

**Definition 2.1.** Let $S_r := \{m_1, ..., m_{l_r}\}$ be the complete ordered set of monomials consistent with $h_r$ such that $m_1 <_t m_2 <_t ... <_t m_{l_r}$.

By Corollary 1.1 and Lemma 1.2, we must have $m_1 = h_r$.

In general, most affine variety codes considered in the past have had no more than 2 elements in $S_r$, for all $1 \leq r \leq n$.

**Definition 2.2.** Put $B_r := \{(i,j) : h_{i,j} = m_p \in S_r$ and there does not exist an $h_u \in H$ such that either $h_{i,u}$ or $h_{u,j}$ equals $m_v \in S_r$ for some $v < p\}$.

**Remark 2.1.** In the previous definition since $v < p$ if and only if $m_v <_t m_p$ an alternate description of $B_r$ is the following: $B_r = \{(i,j) : h_{i,j} \in S_r$ and for all $(u,v)$ such that either $u = i$ and $v < j$ or $u < i$ and $v = j$ we have that $h_{u,v} \notin S_r\}$.

**Definition 2.3.** Put $S_r^* = \{m_1, ..., m_s\}$ the ordered set of all monomials $m_j \in S_r$ such that $m_j <_t h_{r+1}$. That is, $h_r = m_1 <_t ... <_t m_s <_t h_{r+1}$.

**Definition 2.4.** Define $B_r^* := \{(i,j) : h_{i,j} = m_p \in S_r^*$ and there does not exist an $h_u \in H$ such that either $h_{i,u}$ or $h_{u,j}$ equals $m_v \in S_r^*$ for some $v < p\}$.

**Remark 2.2.** Suppose $h_r = x_1^{\alpha_1}...x_k^{\alpha_k} \in H$. Since $h_r \in S_r^*$ we have $\{(i,j) : h_{i,j} = h_r\} \subseteq B_r^*$ and $|B_r^*| \geq \prod_{i=1}^{k}(\alpha_i + 1)$.

An alternate, yet equivalent, way of viewing $B_r^*$ is provided in the following proposition.

**Proposition 2.1.** Let $h_r \in H$ and $S_r^*$ be its corresponding consistency set as in Defn 2.3. Then, $B_r^* = \{(i,j) | h_{i,j} = S_r^*$ and $h_{i,j}$ is weakly well-behaving$\}$.

*Proof.* Put $B_r' := \{(i,j) | h_{i,j} = m_p \in S_r^*$ and $h_{i,j}$ is weakly well-behaving$\}$. We shall prove by contradiction that $B_r' \subseteq B_r^*$. Suppose $(i,j) \in B_r$. Without loss of generality, assume there exists an $h_u$ such that $h_{i,u} \in S_r^*$ with $h_{i,u} <_t h_{i,j}$. Therefore, $u < j$ and $h_{i,u} \sim h_r$ implies that $\bar{h}_{i,u} \in L(\underline{r}) \setminus L(\underline{r-1})$. Hence, $h_{i,j}$ is not weakly well-behaving, which is a contradiction. Thus, $B_r' \subseteq B_r^*$.

Suppose $(i,j) \in B_r^*$. Let $(u,v)$ be such that either $u = i$ and $v < j$ or $u < i$ and $v = j$. Since $h_{u,v} <_t h_{i,j} <_t h_{r+1}$ and $wt(h_{i,j}) = wt(h_r)$, we know that $wt(h_{u,v}) \leq wt(h_r)$. If $wt(h_{u,v}) = wt(h_r)$, then $\bar{h}_{u,v} \in L(\underline{r-1})$ since $h_{u,v} \notin S_r^*$. If $wt(h_{u,v}) < wt(h_r)$, then $h_{u,v} <_t h_r$ and by Lemma 1.1, we have $\bar{h}_{u,v} \in L(\underline{r-1})$. Hence, $h_{i,j}$ is weakly well-behaving. Thus, $B_r^* \subseteq B_r'$. □

**Theorem 2.1.** For each $h_r \in H$, we have $N_r \subseteq B_r^* \subseteq \tilde{N}_r \subseteq B_r$.

*Proof.* From the description of $B_r^*$ in Proposition 2.1, we see that $B_r^* \subseteq \tilde{N}_r$.

Next, we show by contradiction that $\tilde{N}_r \subseteq B_r$. Suppose $(i,j) \in \tilde{N}_r$. Without loss of generality, assume there exists an $h_u$ such that $h_{i,u} \in S_r$ with $h_{+i,u} <_t h_{i,j}$. Therefore, $u < j$ and $h_{i,u} \sim h_r$ implies that $\bar{h}_{i,u} \in L(\underline{r}) \setminus L(\underline{r-1})$. Hence, $h_{i,j}$ is not weakly well-behaving, which is a contradiction. □

This theorem allows us to bound the somewhat cumbersome set $\tilde{N}_r$ with two sets whose cardinalities only depend on the number of monomial divisors of monomials from the consistency sets (with a certain property).

**Corollary 2.1.** Suppose $h_r \in H$ with corresponding consistency set $S_r = \{m_1, ..., m_{l_r}\}$. If $m_{l_r} <_t h_{r+1}$, then $B_r^* = \tilde{N}_r = B_r$.

Proof. Suppose that $m_{l_r} <_t h_{r+1}$. Then, $S_r = S_r^*$ implies that $B_r = B_r^*$. By the inclusion established in Theorem 2.1, this implies that $B_r^* = \tilde{N}_r = B_r$. □

**Corollary 2.2.** Let $h_r = x_1^{\alpha_1} ... x_k^{\alpha_k} \in H$. If $|S_r| = 1$, then $B_r^* = B_r = N_r = \tilde{N}_r$ with cardinality $\prod_{i=1}^{k}(\alpha_i + 1)$.

*Proof.* Suppose $|S_r| = 1$. Then $h_r$ is the only element of $S_r$ and $h_r <_t h_{r+1}$. So by Corollary 2.1 and Remark 2.2, $B_r^* = \tilde{N}_r = B_r = \{(i,j) : h_{i,j} = h_r\}$. From Lemma 1.2, we have $\{(i,j) : h_{i,j} = h_r\} \subseteq N_r$. On the other hand, $N_r \subseteq \tilde{N}_r$. Hence, we must have equality. □

**Definition 2.5.** We define the $n \times n$ monomial product matrix

$$M := [h_{i,j}] \text{ for } 1 \leq i, j \leq n.$$

**Definition 2.6.** For all $a \in W$, put

$$W_a := \{i : wt(h_i) = a\}.$$

**Definition 2.7.** For $a, b \in W$, let $M_{(a,b)}$ denote the submatrix of $M$ of all entries $h_{i,j}$ such that $i \in W_a$ and $j \in W_b$.

**Lemma 2.2.** If there exists at least one $h_{i,j} \in M_{(a,b)}$ such that $h_{i,j} \sim h_r$, then there exists at least one $h_{u,v} \in M_{(a,b)}$ such that $(u,v) \in B_r$.

*Proof.* Put $p' = \min\{p : m_p \in S_r \text{ and } m_p \in M_{(a,b)}\}$. Then there exists an $h_{u,v} = m_{p'} \in M_{(a,b)}$ which implies that $(u,v) \in B_r$. □

**Definition 2.8.** We shall say that the submatrix $M_{(a,b)}$ is *radical* (or *extreme*) for $h_r$ if there exists at least one $h_{i,j} \in M_{(a,b)}$ with $h_{i,j} \sim h_r$ and for all such $h_{i,j}$ we have that $h_{i,j}$ is not weakly well-behaving.

**Definition 2.9.** Define $P_r := \{(a,b) : a, b \in W \text{ and } a + b = wt(h_r)\}$. Let $\mathcal{C}_r$ denote the following collection of submatrices of $M$;

$$\mathcal{C}_r := \{M_{(a,b)} : (a,b) \in P_r\}.$$

We note that no two submatrices in $\mathcal{C}_r$ share a common row or column of $M$.

**Definition 2.10.** Put $E_r := \{(a,b) \in P_r : M_{(a,b)} \text{ is radical for } h_r\}$.

**Definition 2.11.** Put $\mathcal{A}_r := |\tilde{N}_r| + |E_r|$. We shall call $\mathcal{A}_r$ the *advisory number* for $h_r$.

We note here that since every matrix radical for $h_r$ contains an element of $B_r$ (by Lemma 2.2), but none of $\tilde{N}_r$, we then have $\mathcal{A}_r \leq |B_r|$.

**Definition 2.12.** For the code $C^{\perp}(I, L)$, where $L = L(r, v_1, ..., v_l)$ we define two numbers: $\delta_{\mathcal{A}} = \min\{\mathcal{A}_v : v \notin \{1, 2, ..., r, v_1, ..., v_l\}$ and $\delta_{\mathcal{A}^+} = \min\{|B_v| : v \notin \{1, 2, ..., r, v_1, ..., v_l\}$. We will call $\delta_{\mathcal{A}}$ the *advisory bound* and $\delta_{\mathcal{A}^+}$ the *strong advisory estimate.*

We note that since $|\tilde{N}_v| \leq \mathcal{A}_v \leq |B_r|$, we then have $\delta_{WFR} \leq \delta_{\mathcal{A}} \leq \delta_{\mathcal{A}^+}$. The number $\delta_{\mathcal{A}^+}$ seems to be a good predictor of the true minimum distance of $C^{\perp}(I, L)$. However, in the general setting it does not appear to be "provable" as a lower bound on the minimum distance. In theory, $\delta_{\mathcal{A}^+}$ may even be an overestimate of the actual minimum distance.

On the other hand, we shall prove that $\delta_{\mathcal{A}}$ is a lower bound for the minimum distance and thus an improvement of $\delta_{WFR}$. In the last section, we will examine families of codes for which we can argue that $\delta_{\mathcal{A}^+}$ may be used as a lower bound as well. The proof of $\delta_{\mathcal{A}}$ as a lower bound will resemble the proofs of those for $\delta_{FR}$ and $\delta_{WFR}$ found in [1] and [5], respectively.

**Definition 2.13.** Put $h_i' := (h_i(P_1), ..., h_i(P_n))$ and $h_{i,j}' := (h_{i,j}(P_1), ..., h_{i,j}(P_n))$. For each $c = (c_1, ..., c_n) \in \mathbb{F}_q^n$ and $1 \leq i, j \leq n$ define the following syndromes: $s_i(c) := h_i \cdot c$ and $s_{i,j}(c) := h_{i,j}' \cdot c$.

**Remark 2.3.** Note that $c$ is a codeword of $C^{\perp}(I, L)$ where $L = L(\underline{r}, v_1, ..., v_l)$ if and only if $s_i(c) = 0$ for all $i \in \{1, 2, ..., r, v_1, ..., v_l\}$. Also, $s_{i,j}(c) = 0$ if $\bar{h}_{i,j} \in L(\underline{r}, v_1, ..., v_l)$.

**Definition 2.14.** Let $\mathcal{S}_c := [s_{i,j}(c)]$ be the $n \times n$ matrix of syndromes for $c$. We shall call $\mathcal{S}_c$ the *syndrome matrix* for $c$.

**Remark 2.4.** From [1], we find that $rank\mathcal{S}_c = wt(c)$. Moreover, when $c$ is a codeword, we know that the rank of the syndrome matrix is precisely the weight of the codeword.

**Definition 2.15.** For $a, b \in W$, let $[\mathcal{S}_c]_{(a,b)}$ denote the submatrix of $\mathcal{S}_c$ of all entries $s_{i,j}(c)$ such that $i \in W_a$ and $j \in W_b$.

**Definition 2.16.** Let $\mathcal{C}_r'$ denote the following collection of submatrices of $\mathcal{S}_c$, $\mathcal{C}_r' = \{[\mathcal{S}_c]_{(a,b)} : (a, b) \in P_r\}$.

We note that every submatrix $[\mathcal{S}_c]_{(a,b)}$ of $\mathcal{C}_r'$ corresponds in a natural way to the submatrix $M_{(a,b)}$ of $\mathcal{C}_r$. Furthermore, no two submatrices of $\mathcal{C}_r'$ share a common row or column of $\mathcal{S}_c$.

**Theorem 2.3.** Suppose $c = (c_1, ..., c_n)$ is a nonzero codeword of $C^{\perp}(I, L)$ with parity check matrix $H_r^*$. Suppose $s_w(c) \neq 0$ and $s_v(c) = 0$ for all $v < w$. Then, the minimum distance is at least $\mathcal{A}_w$.

*Proof.* Note that we have $wt(c) = rank\mathcal{S}_c \geq \sum_{(a,b)\in P_w} rank[\mathcal{S}_c]_{(a,b)} = \sum_{(a,b)\in P_w \setminus E_w} rank[\mathcal{S}_c]_{(a,b)} + \sum_{(a,b)\in E_w} rank[\mathcal{S}_c]_{(a,b)}$ by the above remarks.

For each $(i, j) \in \tilde{N}_w$, we know that for all $(u, v)$ such that either $u < i$ and $v = j$ or $u = i$ and $v < j$, we have $\bar{h}_{u,v} \in L(\underline{w-1})$ and therefore $s_{u,v}(c) = 0$. On the other hand, $h_{i,j} \sim h_w$ and $s_w(c) \neq 0$ imply that $s_{i,j}(c) \neq 0$. Therefore, there exists $|\tilde{N}_w|$ rows of $\mathcal{S}_c$ that have their first nonzero entry in different columns. Hence, $\sum_{(a,b)\in P_w \setminus E_w}$ rank $[\mathcal{S}_c]_{(a,b)} \geq |\tilde{N}_w|$.

Since each matrix $M_{(a,b)}$ radical for $h_w$ contains an entry consistent with $h_w$, we know that $[\mathcal{S}_c]_{(a,b)}$ is nonzero and hence $rank[\mathcal{S}_c]_{(a,b)} \geq 1$. Therefore, we have $\sum_{(a,b)\in E_w} rank[\mathcal{S}_c]_{(a,b)} \geq |E_w|$. Thus, we have $wt(c) \geq |\tilde{N}_w| + |E_w| = \mathcal{A}_w$.

**Remark 2.5.** If it can be shown that $|B_w| \leq \sum_{(a,b)\in P_w} rank[\mathcal{S}_c]_{(a,b)}$, then we could restate Theorem 2.2, with $|B_w|$ in place of $\mathcal{A}_w$. In the last section, we give an example in which $|B_w|$ can be used instead.

In the next section we will give examples of codes in which $N_r \subset \tilde{N}_r$ and $\tilde{N}_r \subset \mathcal{A}_r$.

Let $[n,\kappa,d]$ denote a code of length $n$, dimension $\kappa$, and minimum distance $d$. This paper examines several families of affine variety codes generated by polynomials $\{p_1, ..., p_m\} \in \mathbb{F}_4[x_1, ..., x_k]$. Polynomials considered in our study satisfy two criteria.

*i)* The polynomials generate affine varieties of at least 20 points. Thus, $\Delta(I_4)$ contains at least 20 elements.

*ii)*For some $n$ and $\kappa$, the advisory bound on minimum distance ties the highest known distance for that particular code length and dimension, and there is a gap between the highest known distance and the theoretical upper bound on distance.

The highest known minimum distance and upper bounds on distance were determined by the *Linear Bounds server* [3].

# 3 Family Ties

The remainder of this paper describes certain "families" of polynomials. We shall say that codes $C^{\perp}(I, L)$ and $C^{\perp}(I', L)$ are members of the same family if the two corresponding $\Delta$-*sets*, namely $\Delta(I)$ and $\Delta(I')$ are the same and for each monomial in the $\Delta$-*set*, the corresponding consistency sets are equal as well. The discussion surrounding our first family will include a comprehensive example of the methods that were employed to study each family.

**Definition 3.1.** A polynomial $f(x_1, ..., x_k) \in F_4[x_1, ..., x_k]$ is called an $(\mathbb{F}_4^k, \mathbb{F}_2)$-polynomial if for each $\gamma \in \mathbb{F}_4^k$, we have $f(\gamma) \in \mathbb{F}_2 = \{0, 1\}$.

## 3.1 A [32,9,15] Family

Our first family consists of those polynomials of the form $f(x_1)+g(x_2)+h(x_3)$, where $f, g, h$ are $(\mathbb{F}_4, \mathbb{F}_2)$ polynomials with $deg(f) = deg(h) = 3$ and $deg(g) = 2$.

By the comprehensive classification of $(\mathbb{F}_4^k, \mathbb{F}_2)$ polynomials in [4], and by simple combinatorics, the family can be shown to have 96 members. Furthermore, since any $(\mathbb{F}_4^k, \mathbb{F}_2)$ polynomial of the form $f(x_1, ..., x_{j-1}, x_{j+1}, ..., x_k) + (x_j^2 + x_j)$ over $\mathbb{F}_4$ has $\frac{1}{2}(4^k)$ solutions, each member of our polynomial family has $\frac{1}{2}(64) = 32$ solutions. We shall let $I = \langle f(x_1) + g(x_2) + h(x_3)\rangle$.

Assigning $wt(x_1) = 2, wt(x_2) = 3$, and $wt(x_3) = 2$, we obtain $wt(x_2^2) = wt(x_1^3)$ and $wt(x_1x_2^2) = wt(x_1x_3^3)$. Notice that for any member of the family, $x_2^2$ is in the linear span of $x_1^3$ and smaller terms, while $x_1x_2^2$ is in the linear span of $x_1x_3^3$ and smaller terms. Hence we see that $x_1^3 \sim x_2^2$ and $x_1x_2^2 \sim x_1x_3^3$.

Now the $\Delta$-*set* for each polynomial is identical (because each has the same leading term in $x_1, x_2$, and $x_3$). To obtain the Feng-Rao, weak Feng-Rao, and advisory bounds for a fixed dimension, $N_r, \tilde{N}_r, \mathcal{A}_r$, and $A_r^+$ were computed for each $h_r$ in the $\Delta$-*set*, as shown in the table below. To simplify notation, we write $x_1 = x$, $x_2 = y$, $x_3 = z$.

| Bound Comparison | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $h_r$ | 1 | $z$ | $x$ | $y$ | $z^2$ | $xz$ | $x^2$ | $yz$ |
| $N_r$ | 1 | 2 | 2 | 2 | 3 | 4 | 3 | 4 |
| $\tilde{N}_r$ | 1 | 2 | 2 | 2 | 3 | 4 | 3 | 4 |
| $\mathcal{A}_r$ | 1 | 2 | 2 | 2 | 3 | 4 | 3 | 4 |
| $\mathcal{A}_r^+$ | 1 | 2 | 2 | 2 | 3 | 4 | 3 | 4 |
| $h_r$ | $xy$ | $z^3$ | $y^2$ | $xz^2$ | $x^2z$ | $yz^2$ | $xyz$ | $x^2y$ |
| $N_r$ | 4 | 4 | 3 | 6 | 6 | 6 | 8 | 6 |
| $\tilde{N}_r$ | 4 | 4 | 3 | 6 | 6 | 6 | 8 | 6 |
| $\mathcal{A}_r$ | 4 | 4 | 5 | 6 | 6 | 6 | 8 | 6 |
| $\mathcal{A}_r^+$ | 4 | 4 | 5 | 6 | 6 | 6 | 8 | 6 |
| $h_r$ | $y^2z$ | $xz^3$ | $x^2z^2$ | $yz^3$ | $y^3$ | $xyz^2$ | $x^2yz$ | $y^2z^2$ |
| $N_r$ | 6 | 10 | 9 | 8 | 4 | 12 | 12 | 9 |
| $\tilde{N}_r$ | 6 | 10 | 9 | 8 | 4 | 12 | 12 | 9 |
| $\mathcal{A}_r$ | 7 | 10 | 9 | 8 | 8 | 12 | 12 | 9 |
| $\mathcal{A}_r^+$ | 10 | 10 | 9 | 8 | 8 | 12 | 12 | 15 |
| $h_r$ | $x^2yz^3$ | $y^3z^3$ | $x^2z^3$ | $y^3z$ | $xyz^3$ | $x^2yz^2$ | $y^2z^3$ | $y^3z^2$ |
| $N_r$ | 15 | 8 | 16 | 18 | 12 | 12 | 24 | 16 |
| $\tilde{N}_r$ | 15 | 8 | 16 | 18 | 20 | 12 | 24 | 32 |
| $\mathcal{A}_r$ | 15 | 10 | 16 | 18 | 20 | 12 | 24 | 32 |
| $\mathcal{A}_r^+$ | 15 | 16 | 16 | 18 | 20 | 24 | 24 | 32 |

**Example 3.1.** Arranging the *N-numbers* in ascending order, we obtain the sequence {1, 2, 2, 2, 3, 3, 3, 4, 4, 4, 4, 4, 6, 6, 6, 6, 6, 6, 8, 8, 8, 9, 9, 10, 10, 12, 12, 12, 12, 15, 16, 16, 18, 24}. From this sequence, we can determine $\delta_{FR}$ for various dimensions of $C^{\perp}(I,L)$. For instance, since the removal of the monomials $1$,$x, y, z, x^2, y^2$, and $z^2$ leaves only monomials with *N-numbers* 4 or higher, $\delta_{FR} = 4$ for dimension 32-7=25. Thus, we have a [32,25,$\geq$ 4] code. This particular code is, in fact, a [32,25,4] code, as verified by [2].

Two interesting results arise from a closer inspection of the chart.

Letting $r = \{h_v \in \Delta(I) : A_v \leq 15\}$, we see that the dual code $C^{\perp}(I,L)$ for $L = (\underline{r})$ is [32,6,$\geq$15]. However, if it can be shown that the rank of the syndrome matrix for $b$ additional monomials in $L$ is actually 15 or greater, then $C^{\perp}(I,L)$ must indeed be a [32,6+$b$,$\geq$15] code.

Consider the following monomials: $y^2z$, $y^2z^2$, $y^3z$, $y^3z^2$. We demonstrate that each of these has syndrome matrix rank higher than its $A$ number. Of these, three monomials have rank 15 or higher, yielding $C^{\perp}(I,L) = [32, 9, 15]$. Notice that this is, in fact, the prediction of the strong advisory estimate.

Since $S_{i,j} = 0$ for all $h_j$ where $h_j \in L(\underline{r-1})$, non-zero entries are first found in $P_r$, the weight box consisting of all monomials of equivalent weight to $h_r$. Clearly, the rank of the syndrome matrix can be no less than the sum of the ranks of these boxes.

Take, as an example, the weight boxes of $y^2z$, shown below.

$$\boxed{\begin{array}{c} y^2z \\ xz^3 \\ x^2z^2 \end{array}} \quad \boxed{\begin{array}{cc} z^4 & xz^3 \\ y^2z & xy^2 \\ xz^3 & x^2z^2 \\ x^2z^2 & x^3z \end{array}} \quad \boxed{\begin{array}{c} y^2z \\ xy^2 \end{array}} \quad \boxed{\begin{array}{ccc} z^4 & xz^3 & x^2z^2 \\ xz^3 & x^2z^2 & x^3z \\ x^2z^2 & x^3z & x^4 \end{array}} \quad \boxed{\begin{array}{cc} y^2z & xy^2 \end{array}}$$

$$\boxed{\begin{array}{cccc} z^4 & y^2z & xz^3 & x^2z^2 \\ xz^3 & xy^2 & x^2z^2 & x^3z \end{array}} \quad \boxed{\begin{array}{ccc} y^2z & xz^3 & x^2z^2 \end{array}}$$

Boxes 1, 3, 5, and 7 have only one row or column and an entry of $y^2z$ each; hence, the row for each of these boxes must be 1.

Consider Box 2. Monomials $<_t y^2z$ receive an entry of zero; $y^2z$ and monomials consistent to it receive a one (simply representing a non-zero entry), and other monomials have an unknown value.

Notice that some entries are not monomials in the footprint, but can either be reduced by (1) or by a consistency relationship to a monomial in the linear span of monomials less than $y^2z$. For example, $z^4 = z$ by (1); since $h_r = y^2z$, $z \in L(\underline{r-1})$ – hence its assignment of 0 in the syndrome matrix. Also, $xy^2$ is consistent to $xz^3 = h_{r+1}$ – hence its assignment of $S_{r+1}$ in the syndrome matrix. So the syndrome matrix for Box 2 becomes

$$\boxed{\begin{array}{cc} 0 & S_{r+1} \\ 1 & S_{r+1} \\ S_{r+1} & S_{r+2} \\ S_{r+2} & 1 \end{array}}\,.$$

Suppose that $S_{r+1} = 0$. Then the 2nd and 4th rows must be linearly independent; hence, the rank of the box is greater than or equal to 2. Supposing instead that $S_{r+1} \neq 0$, the 1st and 4th rows are linearly independent, so again, the rank is at least 2. Observe that Box 4 is simply the transpose of Box 2 – that is, the rows of Box 2 are the columns of Box 4. Thus, the rank of Box 4 must also be at least 2.

Employing the same strategy with Box 5, we find that the matrix

$$\boxed{\begin{array}{ccc} 0 & S_{r+1} & S_{r+2} \\ S_{r+1} & S_{r+2} & 1 \\ S_{r+2} & 1 & 0 \end{array}}$$

has rank at least 2. To see this, notice that if either $S_{r+1} = 0$ or $S_{r+1} \neq 0$, then the 2nd and 3rd rows are linearly independent. So the rank of the syndrome matrix for this monomial is at least 10, rather than 7, as our bound had indicated.

Likewise, the syndrome matrices for the monomials $y^2z^2$, $y^3z$, $y^3z^2$ have ranks at least 15, 16, and 24, respectively. Given these improved values, we find that we have a [32, 9,≥15] code, verified to be a [32,9,15] code.

An examination of the monomials $y^2z^3$ and $y^3z^3$ yields interesting results as well. The boxes of equivalent weight for $y^3z^3$ are shown below.

$$\boxed{y^3z^3} \quad \boxed{\begin{array}{cc} y^3z^3 & xy^3z^2 \\ x^2yz^4 & x^3yz^3 \end{array}} \quad \boxed{y^3z^3} \quad \boxed{\begin{array}{ccc} y^3z^3 & xy^3z^2 & x^2y^3z \\ xyz^5 & x^2yz^4 & x^3yz^3 \\ x^2yz^4 & x^3yz^3 & x^4yz^2 \end{array}} \quad \boxed{\begin{array}{cc} y^3z^3 & xy^3z^2 \\ x^2yz^4 & x^3yz^3 \end{array}}$$

$$\boxed{\begin{array}{cccc} yz^6 & y^3z^3 & xyz^5 & x^2yz^4 \\ y^3z^3 & y^5 & xy^3z^2 & x^2y^3z \\ xyz^5 & xy^3z^2 & x^2yz^4 & x^3yz^3 \\ x^2yz^4 & x^2y^3z & x^3yz^3 & x^4yz^2 \end{array}} \quad \boxed{\begin{array}{ccc} y^3z^3 & xy^3z^2 & x^2y^3z \\ xyz^5 & x^2yz^4 & x^3yz^3 \\ x^2yz^4 & x^3yz^3 & x^4yz^2 \end{array}} \quad \boxed{\begin{array}{ccc} y^3z^3 & xyz^5 & x^2yz^4 \\ xy^3z^2 & x^2yz^4 & x^3yz^3 \\ x^2y^3z & x^3yz^3 & x^4yz^2 \end{array}}$$

$$\boxed{\begin{array}{cccc} yz^6 & y^3z^3 & xyz^5 & x^2yz^4 \\ y^3z^3 & y^5 & xy^3z^2 & x^2y^3z \\ xyz^5 & xy^3z^2 & x^2yz^4 & x^3yz^3 \\ x^2yz^4 & x^2y^3z & x^3yz^3 & x^4yz^2 \end{array}} \quad \boxed{\begin{array}{cc} y^3z^3 & x^2yz^4 \\ xy^3z^2 & y^3z^3 \end{array}} \quad \boxed{\begin{array}{ccc} y^3z^3 & xyz^5 & x^2yz^4 \\ xy^3z^2 & x^2yz^4 & x^3yz^3 \\ x^2y^3z & x^3yz^3 & x^4yz^2 \end{array}}$$

$$\boxed{y^3z^3} \quad \boxed{\begin{array}{cc} y^3z^3 & x^2yz^4 \\ xy^3z^2 & x^3yz^3 \end{array}} \quad \boxed{y^3z^3}$$

Observe that, after reducing monomials as detailed above, each of the 12 $x^3yz^3$ entries is the highest ranked monomial in its respective row or column up to that entry. Thus, by definition, $x^3yz^3$ is weakly well behaving, although in no box is $x^3yz^3$ well behaving. So, the $\tilde{N}$ number associated with $x^3yz^3$ is 32, while the $N$-number is only 16.

Likewise, $y^2z^3$ has 12 well-behaving terms, but adds 8 more weakly well-behaving terms. Hence, its $\tilde{N}$ number is 20.

### 3.2 Two cousins: a [48,41,4] and a [48,36,6] family

Consider the four $(\mathbb{F}_4, \mathbb{F}_2)$-polynomials belonging to the set $S = \{x_1^3+1, x_1^3+x_1^2+x_1, x_1^3+\alpha^2x_1^2+\alpha x$, and $x_1^3+\alpha x_1^2+\alpha^2x_1\}$. Let $I = \langle f(x)\rangle$, for $f \in S$. $V(I)$ has 48 members and since there are no consistency relationships, $N_r = \tilde{N}_r = \mathcal{A} = \mathcal{A}^+$=number of divisors of $h_r$ for each $h_r \in \Delta(I)$. For codes of this family with dimension 41, the advisory bound $\delta_{\mathcal{A}} = 4$; with dimension 36, $\delta_{\mathcal{A}} = 6$; both bounds are ties with the best known codes.

### 3.3 A [46,39,4] family

This family consists of polynomials of the form $x_1x_2x_3(1+c\cdot x^ix^jx^k)$, where $0 \le i,j,k \le 2$, $(i,j,k) \ne (1,1,1)$, and $c \in \{1, \alpha, \alpha^2\}$. Thus there are 76 family members, each of which has 46 solutions. Because there are no consistency relationships, all bounds coincide and yield a tie in minimum distance (=4) for dimension 39.

### 3.4 More cousins: an [85,77,4] and a [67,59,4] family

This family consists of polynomials of the form $\{x_1x_2x_4^{e1} + x_1^{e2}x_2^{e3}x_3^{e4}, x_4^2 + x_3^{e5}x_4\}$. Of the 243 members of this family, 9 have 85 solutions and the remaining 234 have 67 solutions. All tie the best known minimum distance: the 85 solution codes at dimension 77 and the 67 solution codes at dimension 59.

### 3.5 Another [32,9,15] family

Consider polynomials of the form $cx_1^2x_3 + c^2x_1x_3^2 + f(x_2) + g(x_1,x_3)$, where $c \in \{1,\alpha,\alpha^2\}$, $f \in (\mathbb{F}_4,\mathbb{F}_2)$, $deg(f) = 2$, and $g(x,z) = h(x) + l(x)$, where $h, l \in (\mathbb{F}_4, \mathbb{F}_2)$ and $deg(h) \le 2, deg(l) \le 3$. The family has 576 members, each with 32 solutions. Clearly, $x_1^2x_3 \sim x_2^2$. We wish to employ the methods of section 3.1, with slight variation. For this family, select the following weights: $wt(x_1) = 8$, $wt(x_2) = 9$, $wt(x_3) = 2$. Notice, then, that the weight of each $h_r \in H$ is distinct.

**Remark 3.1.** If $wt(h_r)$ is distinct in $H$ for each $h_r$ in $H$, then $N_r = \tilde{N}_r = \mathcal{A}_r = \mathcal{A}_r^+$ for each $h_r$ in $H$.

To see this, notice first that if $h_{i,j} \sim h_r$ is the only entry in $M_{(a,b)}$, then $(i,j) \in N_r$. This follows because $h_{i,j} \sim h_r$, where $h_{i,j}$ is alone in $M_{(a,b)}$, implies that for all $(u,v)$ such that $1 \leq u \leq i$ and $1 \leq v \leq j$, $(u,v) \neq (i,j)$, $h_{u,v} \in L(\underline{r-1})$. Hence, $h_{i,j}$ is well-behaving, so by definition, $(i,j) \in N_r$.

Now if for each $h_r \in H$, $wt(h_r)$ is distinct, then each $M_{(a,b)} \in \mathcal{C}_r$ has one entry. So, in this case, $N_r = \{(i,j) : h_{i,j} \sim h_r\}$. But then, $N_r = B_r$, which by the inequalities given in Section 2, implies that $N_r = \tilde{N}_r = \mathcal{A}_r = \mathcal{A}_r^+$ for each $h_r$ in $H$.

Thus, the following chart results.

Another Bound Comparison Example

| $h_r$ | $1$ | $z$ | $x$ | $z^2$ | $y$ | $xz$ | $z^3$ | $yz$ |
|---|---|---|---|---|---|---|---|---|
| $N_r$ | 1 | 2 | 2 | 3 | 2 | 4 | 4 | 4 |
| $h_r$ | $x^2$ | $xz^2$ | $xy$ | $yz^2$ | $y^2$ | $xz^3$ | $xyz$ | $x^3$ |
| $N_r$ | 3 | 6 | 4 | 6 | 3 | 6 | 8 | 4 |
| $h_r$ | $yz^3$ | $y^2z$ | $x^2y$ | $xyz^2$ | $xy^2$ | $y^2z^2$ | $y^3$ | $xyz^3$ |
| $N_r$ | 8 | 6 | 9 | 8 | 4 | 12 | 12 | 9 |
| $h_r$ | $xy^2z$ | $x^3y$ | $y^3z$ | $xy^2z^2$ | $xy^3$ | $y^3z^2$ | $xy^3z$ | $xy^3z^2$ |
| $N_r$ | 15 | 8 | 16 | 18 | 12 | 12 | 24 | 16 |

# References

[1] G. L. Feng and T. R. N. Rao, "Improved Geometric Goppa Codes Part 1, Basic Theory," IEEE Trans. Inf. Theory, vol. 41, no.6, pp. 1678-1686, 1995.

[2] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.3*; 2002, (`http://www.gap-system.org`).

[3] *Bounds on the minimum distance of linear codes.* Technische Universiteit Eindhoven. 14 July 2002 <http://www.win.tue.nl/∼ aeb/voorlincod.html>.

[4] Jamie Lamb, "Classifications of $(\mathbb{F}_4^k, \mathbb{F}_2)$-polynomials," April 25, 2002.

[5] Ryutaroh Matsumoto and Shinji Miura, “On the Feng-Rao Bound for the $\mathcal{L}$-construction of Algebraic Geometry Codes”, IEICE Trans. Fundamentals, vol. E83-A, no. 5, May 2000

[6] J. Fitzgerald and R.F. Lax, “Decoding Affine Variety Codes Using Groebner Bases,” Designs, Codes and Cryptography, vol.? 13, 147-158, 1998.