TEMA Tend. Mat. Apl. Comput., **13**, No. 3 (2012), 257-263.
doi: 10.5540/tema.2012.013.03.0257

Gröbner Bases and Minimum Distance of Affine Varieties Codes

C. CARVALHO[1], Faculdade de Matemática, Universidade Federal de Uberlândia, Av. J. N. Ávila 2121, 38.408-902 Uberlândia, MG, Brazil.

Abstract. We present a method to estimate the minimum distance of affine varieties codes. Our technique uses properties of the footprint of an ideal obtained by enlarging the defining ideal of the variety, and may be applied also to codes which do not come from the so-called weight domains.

Keywords. Affine varieties codes, Gröbner bases, footprint of an ideal, minimum distance.

AMS Classification. 13P10, 13F20, 94B27

1. Introduction

Since the appearance of the geometric Goppa codes in the eighties, many papers have dealt with improvements on the lower bound for the minimum distance of a code. One of the most successful methods for this improvement was obtained by Feng and Rao (see [6] and [7]). Many related bounds appeared after their work, one of them being a bound derived by Andersen and Geil in [1]. In that paper the authors first derive a general approach to obtain a bound for the minimum distance (actually, for the generalized Hamming weights) of a linear code, and then show how to apply their method to codes defined from weight domains. A weight domain is an $\mathbb{F}$-algebra, where $\mathbb{F}$ is a field, which admits a function to $\mathbb{N}_0 \cup \{-\infty\}$ satisfying certain properties, which makes the domain suitable to be used for defining codes, when $\mathbb{F}$ is a finite field. They were introduced in [12] by T. Høholdt, J. H. van Lint and R. Pellikaan in order to present an alternative construction for geometric Goppa codes with simple tools from commutative algebra. In the present work we show how to apply Andersen and Geil's general approach to affine variety codes. Similarly to codes obtained from weight domains, these are evaluation codes obtained from the ring of regular functions of an affine variety but weight functions play no role in this theory. Since the algebras which appear in the weight function theory are the ring of regular functions of certain type of variety (see [11]) our result applies to a more comprehensive class of rings (see Example 3.2). Thus, distinctly from recent works (see e.g. [9] and [10]) we do not need concepts like "well-behaving basis" or "one-way well behaving basis". An important set of data to obtain a bound for

[1] cicero@ufu.br. The author was supported in part by CNPq grants 302280/2011-1 and 470416/2011-4, and also by FAPEMIG proc. CEX-PPM-00127-12.

Recebido em 20 Julho 2012; Aceito em 20 Novembro 2012.

the minimum distance is the set of indexes where there is a "dimension jump" in a sequence of nested vector spaces. While in [1] there are several results on such set for the case of codes from weight domains, and in particular, one-point geometric Goppa codes, here we show that this set may be read directly from the footprint of an ideal obtained by enlarging the defining ideal of the curve.

In the next section we recall Andersen and Geil's approach to obtain a bound for the minimum distance of a linear code, we introduce the affine variety codes and recall the definition and some properties of the footprint of an ideal, then we prove our main result. Following that, we present some examples to illustrate our method, including codes obtained from an algebra which does not admit a weight function.

2. Main result

Let $\mathbb{F}_q$ be a finite field with q elements, n a positive integer and for $\mathbf{a} := (a_1, \ldots, a_n)$, $\mathbf{b} := (b_1, \ldots, b_n) \in \mathbb{F}_q^n$ define $\mathbf{a} * \mathbf{b} := (a_1 b_1, \ldots, a_n b_n)$. Let C be a vector subspace of $\mathbb{F}_q^n$. The idea of Andersen and Geil for finding a lower bound for the minimum distance of C stems from the fact that if $\mathbf{c} \in C$ and $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\} =: \mathbf{B}$ is a basis for $\mathbb{F}_q^n$ then the subspace $\mathbf{c} * \mathbf{B}$ generated by $\{\mathbf{c} * \mathbf{b}_1, \ldots, \mathbf{c} * \mathbf{b}_n\}$ has dimension equal to the weight of $\mathbf{c}$. Thus we have the following result, which is not explicitly stated in [1] but is used there.

Lemma 2.1. *The minimum distance $d(C)$ is equal to* $\min\{\dim \mathbf{c} * \mathbf{B}\,; \mathbf{c} \in C \setminus \{0\}\}$.

We will use this result to estimate the minimum distance of the so-called affine variety codes, which were introduced by J. Fitzgerald and R. F. Lax in [8]. Let $I \subset \mathbb{F}_q[X_1, \ldots, X_m]$ be an ideal, let $V_{\mathbb{F}_q}(I) = \{P_1, \ldots, P_n\}$ be the associated variety of $\mathbb{F}_q$-rational points and set $R := \mathbb{F}_q[X_1, \ldots, X_m]/I$. Consider the evaluation morphism $\varphi : R \to \mathbb{F}_q^n$ given by $f + I \mapsto (f(P_1), \ldots, f(P_n))$ and let L be an $\mathbb{F}_q$-vector subspace of R.

Definition 2.1. *The* affine variety code *$C(L)$ is the image $\varphi(L)$.*

We observe that as an $\mathbb{F}_q$-vector space R may not have finite dimension. A useful way of finding a basis for R is by means of the so-called footprint an ideal.

Definition 2.2. *Assume that $\mathbb{F}_q[X_1, \ldots, X_m]$ is endowed with a monomial order $\preccurlyeq$. The* footprint *of I (with respect to $\preccurlyeq$), denoted by $\Delta(I)$, is the set of monomials which are not leading monomials of any polynomial in I.*

Let $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}_0^m$ (where $\mathbb{N}_0$ is the set of nonnegative integers), we will denote by M_α the monomial $X_1^{\alpha_1} \cdot \cdots . X_m^{\alpha_m}$. Then the map $M_\alpha \mapsto \alpha$ gives a bijection between the set of monomials of $\mathbb{F}_q[X_1, \ldots, X_m]$ and $\mathbb{N}_0^m$. Denote by Λ the subset of $\mathbb{N}_0^m$ corresponding to the monomials which are not leading monomials of any polynomial in I with respect to a monomial order $\preccurlyeq$. Then $\Delta(I) = \{M_\lambda \mid \lambda \in \Lambda\}$ is the footprint of I (with respect to $\preccurlyeq$). One of the main properties of $\Delta(I)$ is that $\{M_\lambda + I \mid \lambda \in \Lambda\}$ is a basis for R as an $\mathbb{F}_q$-vector space (see e.g. [5, Prop. 4, § 3, Ch. 5]), and we observe that it is a basis which already carries an order.

Thus, for each $\lambda \in \Lambda$ we consider the $\mathbb{F}_q$-subspace $L_\lambda \subset R$ which is generated by all monomials in $\Delta(I)$ which are less or equal than M_λ. Clearly, if $M_\sigma \preccurlyeq M_\lambda$ then $L_\sigma \subseteq L_\lambda$, so that $C(L_\sigma) \subseteq C(L_\lambda)$. The next result shows for which values of λ we get $C(L_\sigma) \subsetneqq C(L_\lambda)$.

Theorem 2.1. *Let* $I_q := I + (X_1^q - X_1, \ldots, X_m^q - X_m)$. *Then* $\dim C(L_\lambda) > \dim C(L_\sigma)$ *(with* $M_\lambda \succ M_\sigma$*) if and only if* $M_\lambda \in \Delta(I_q)$.

Proof. Observe initially that since $I \subset I_q$ then $\Delta(I_q) \subset \Delta(I)$, so that the claim makes sense. Denote by $\overline{\mathbb{F}_q}$ an algebraic closure of $\mathbb{F}_q$, clearly we have $V_{\mathbb{F}_q}(I) = V_{\mathbb{F}_q}(I_q)$ and denoting by $V_{\overline{\mathbb{F}_q}}(I_q) \subset \overline{\mathbb{F}_q}^m$ the variety of I_q as an ideal of $\overline{\mathbb{F}_q}[X_1, \ldots, X_m]$ we also get $V_{\mathbb{F}_q}(I_q) = V_{\overline{\mathbb{F}_q}}(I_q)$ (considering the natural inclusion $\mathbb{F}_q{}^m \subset \overline{\mathbb{F}_q}^m$). From Seidenberg's Lemma 92 (see [16] or [2, Lemma 8.13]) we get that I_q is a radical ideal, so from [2, Thm. 8.32] we get that R/I_q is an $\mathbb{F}_q$-vector space of finite dimension $\#V_{\overline{\mathbb{F}_q}}(I_q)$, and since the classes of the monomials in $\Delta(I_q)$ form a basis for R/I_q we get $\#\Delta(I_q) = n$, where $n = \#(V_{\mathbb{F}_q}(I))$. We will prove now that if $M_\lambda \in \Delta(I_q)$ then $\dim C(L_\lambda) > \dim C(L_\sigma)$ for any $M_\sigma \prec M_\lambda$. Assume that it is not the case, so there exists σ with $M_\sigma \prec M_\lambda$ such that $C(L_\lambda) = C(L_\sigma)$. In particular, there exists a nonzero finite linear combination $\sum_{M_{\sigma'} \preccurlyeq M_\sigma} a_{\sigma'} M_{\sigma'} \in L_\sigma$ such that $(\sum_{M_{\sigma'} \preccurlyeq M_\sigma} a_{\sigma'} M_{\sigma'})(P_i) = M_\lambda(P_i)$ for all $i = 1, \ldots, n$. From Hilbert's Nullstellensatz (see e.g. [5, Thm. 2, §1, Ch. 4]) we get that the polynomial $M_\lambda - \sum_{M_{\sigma'} \preccurlyeq M_\sigma} a_{\sigma'} M_{\sigma'}$ is in $\sqrt{I_q} = I_q$ and a fortiori $M_\lambda \notin \Delta(I_q)$, a contradiction. This completes the proof of the "if" assertion, for the "only if" part observe that the dimension of the spaces $\dim C(L_\lambda)$ may jump from 1 to n at most $n-1$ times, but we just proved that it will jump $n-1$ times, so every jump must correspond to an element of $\Delta(I_q)$. □

From the (proof of the) above theorem we get the following result.

Corollary 2.1.1. *Let* $\Delta(I_q) := \{M_{\lambda_1}, \ldots, M_{\lambda_n}\}$, *then* $\{\varphi(M_{\lambda_1}), \ldots, \varphi(M_{\lambda_n})\}$ *is a basis for* $\mathbb{F}_q^n$, *where* $n = \#(V_{\mathbb{F}_q}(I))$.

For simplicity we will denote by $M_1, \ldots, M_n$ the elements of $\Delta(I_q)$ and we assume that $M_1 < \cdots < M_n$. We now show how to use the above results to find a lower bound for the minimum distance of an affine variety code $C \subset \mathbb{F}_q^n$. Let $\{\mathbf{c}_1, \ldots, \mathbf{c}_\ell\}$ be a basis for C, and denote by $\mathbf{B} := \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ the (ordered) basis for $\mathbb{F}_q^n$ where $\mathbf{b}_i = \varphi(M_i + I)$, $i = 1, \ldots, n$. For all $t \in \{1, \ldots, \ell\}$ and $i \in \{1, \ldots, n\}$ write $\mathbf{c}_t * \mathbf{b}_i$ as a linear combination of the elements in $\mathbf{B}$. One way to do this is to write $\mathbf{c}_t = \varphi(f + I)$ for some $f \in \mathbb{F}_q[X_1, \ldots, X_m]$, so that $\mathbf{c}_t * \mathbf{b}_i = \varphi(fM_i + I)$. Now observe that if R_{ti} is the remainder in the division of $\mathbf{c}_t * \mathbf{b}_i$ by a Gröbner basis of I_q (with respect to $\preceq$) then R_{ti} is a linear combination of the elements in $\Delta(I_q)$ and the evaluation of fM_i at the points of $V_{\mathbb{F}_q}(I) = V_{\mathbb{F}_q}(I_q)$ coincides with the evaluation of R_{ti} at these points, which produces the desired linear combination. Let $\Gamma_{ti} \subset \Delta(I_q)$ denote the set of monomials M_j such that the coefficient of $\mathbf{b}_j$ in that linear combination is not zero. Let M_{ti} be the greatest element in Γ_{ti}. We want to find a lower bound for the weight of words of the type $\mathbf{c} = \sum_{i=1}^t a_i \mathbf{c}_i$ with $a_1, \ldots, a_t \in \mathbb{F}_q$ and $a_t \neq 0$. For this we define $D_t := \{M_{t1}\}$ and then for all

$i = 2, \dots, n$ we add M_{ti} to the set D_t if $M_{si} \prec M_{ti}$ for all $1 \le s < t$. We claim that the weight of $\mathbf{c}$ satisfies $w(\mathbf{c}) \ge \#(D_t)$. In fact, let $v = \#(D_t)$, then the $v \times n$ matrix A whose lines are the coordinates of the vectors $\mathbf{c} * \mathbf{b}_{i_1}, \dots, \mathbf{c} * \mathbf{b}_{i_v}$ in the base $\mathbf{B}$ has a $v \times v$ invertible minor. To see this, let $M_{ti_1}, \dots, M_{ti_v}$ be the distinct elements of D_t, then for each $j \in \{1, \dots, v\}$ we have $M_{ti_j} = M_{\lambda_j} \in \Delta(I_q)$, and from the construction of D_t we get that in the j-th line of A the λ_j-th entry is nonzero and all entries after it are equal to zero. This proves that $w(\mathbf{c}) \ge \#(D_t)$, so the minimum distance of C is lower bounded by $\min\{\#(D_t) \mid t = 1, \dots, \dim(C)\}$.

The above method applies to any affine variety code in $\mathbb{F}_q^n$ but to simplify the calculations in the following examples we use codes which are generated by some vectors of the base $\mathbf{B}$ induced by $\Delta(I_q)$. These examples also show that the method can yield sharp bounds, and may be applied to codes which do not come from evaluation order domains.

3. Examples

Example 3.1. *For the first example we take the hermitian curve given by $Y^3 + Y - X^4 = 0$, defined over $\mathbb{F}_9$. Codes over this curve has been studied extensively, and the minimum distance of one point geometric Goppa codes has been determined by Stichtenoth ([17]) and Yang and Kumar ([18]). Building on the experience of those who have dealt with these codes we choose a weighted lexicographic order for $\mathbb{F}_9[X, Y]$ by stating that $X^aY^b \preccurlyeq X^{a'}Y^{b'}$ if and only if $3a + 4b \le 3a' + 4b'$, and if equality holds then $X^aY^b <_{\text{lex}} X^{a'}Y^{b'}$ (with $Y <_{\text{lex}} X$). These weights come from the pole orders of the rational functions $x = X/Z$ and $y = Y/Z$ at the point at infinity $P_\infty := (0 : 1 : 0)$, which is their only pole. Using* CoCoA *([4]) or Macaulay2 ([13]) we may calculate a Gröbner basis for the ideal $I_9 := (Y^3 + Y - X^4, Y^9 - Y, X^9 - X)$ with respect to $\preccurlyeq$, which is $\{Y^3 + Y - X^4, Y^9 - Y, XY^6 - XY^4 + XY^2 - X\}$ and from that we get that the footprint of I_9 (w.r.t. $\preccurlyeq$) is $\Delta(I_9) = \{X^aY^b \mid 0 \le a \le 3, 0 \le b \le 5\} \cup \{Y^6, Y^7, Y^8\}$. The curve has 27 rational points (in the affine plane), which is the same number of elements in the footprint, as expected from the proof of theorem 2.1. When we order the monomials in $\Delta(I_9)$ we get $\{1, X, Y, X^2, XY, Y^2, X^3, X^2Y, XY^2, Y^3, X^3Y, X^2Y^2, XY^3, Y^4, X^3Y^2, X^2Y^3, XY^4, Y^5, X^3Y^3, X^2Y^4, XY^5, Y^6, X^3Y^4, X^2Y^5, Y^7, X^3Y^5, Y^8\}$ so denoting by M_i the i-th monomial in $\Delta(I_q)$ we get that $\{\mathbf{b}_i := \varphi(M_i + I) \,|\, i = 1, \dots, 27\}$ is a basis for $\mathbb{F}_9^{27}$. Let C be the code generated by the evaluation of (the class of) the first 5 elements of the basis, namely, $C = \langle \mathbf{b}_1, \dots, \mathbf{b}_5 \rangle$. We start by finding a lower bound for the weight of codewords of the type $\mathbf{c} = \sum_{i=1}^{5} a_i \mathbf{b}_i$, where $a_1, \dots, a_5 \in \mathbb{F}_9$ and $a_5 \neq 0$. Following the procedure (and the notation) described at the end of the last section, since $\mathbf{b}_1 = \varphi(1 + I)$ we must set $D_5 = \{XY\}$ to start. Then, from $\mathbf{c}_5 * \mathbf{b}_2 = \varphi(XY + I) * \varphi(X + I) = \varphi(X^2Y + I) = \mathbf{b}_8$, $\mathbf{c}_4 * \mathbf{b}_2 = \varphi(X^3 + I) = \mathbf{b}_7$, $\mathbf{c}_3 * \mathbf{b}_2 = \mathbf{b}_5$, $\mathbf{c}_2 * \mathbf{b}_2 = \mathbf{b}_4$ and $\mathbf{c}_1 * \mathbf{b}_2 = \mathbf{b}_2$ we must add X^2Y to D_5 obtaining $D_5 = \{XY, X^2Y\}$. Actually, since for any $N \in \{1, X, Y, X^2, XY\}$ and $M \in \mathcal{M} := \{X^aY^b \mid 0 \le a \le 1, 0 \le b \le 4\}$ we have $NM \in \Delta(I_q)$ and also $M \prec XM \prec YM \prec X^2M \prec XYM$, then we must add XYM to D_5 for all $M \in \mathcal{M}$, so that (so far) $\#(D_5) = 10$. We get ten other* *elements to be added to* D_5 *from the tables below*

Remainder in the division of $\mathbf{c}_i * \mathbf{b}_j$ *by the Gröbner basis of* I_q					
	$\mathbf{b}_4 = X^2$	$\mathbf{b}_7 = X^3$	$\mathbf{b}_8 = X^2Y$	$\mathbf{b}_{11} = X^3Y$	$\mathbf{b}_{12} = X^2Y^2$
XY	X^3Y	Y^4+Y^2	X^3Y^2	Y^5+Y^3	X^3Y^3
X^2	Y^3+Y	XY^3+XY	Y^4+Y^2	XY^4+XY^2	Y^5+Y^3
Y	X^2Y	X^3Y	X^2Y^2	X^3Y^2	X^2Y^3
X	X^3	Y^3+Y	X^3Y	Y^4+Y^2	X^3Y^2
1	X^2	X^3	X^2Y	X^3Y	X^2Y^2

Remainder in the division of $\mathbf{c}_i * \mathbf{b}_j$ *by the Gröbner basis of* I_q					
	$\mathbf{b}_{15} = X^3Y^2$	$\mathbf{b}_{16} = X^2Y^3$	$\mathbf{b}_{19} = X^3Y^3$	$\mathbf{b}_{20} = X^2Y^4$	$\mathbf{b}_{23} = X^3Y^4$
XY	Y^6+Y^4	X^3Y^4	Y^7+Y^5	X^3Y^5	Y^8+Y^6
X^2	XY^5+XY^3	Y^6+Y^4	$-XY^4-XY^2+X$	Y^7+Y^5	$-XY^5-XY^3+XY$
Y	X^3Y^3	X^2Y^4	X^3Y^4	X^2Y^4	X^3Y^4
X	Y^5+Y^3	X^3Y^3	Y^6+Y^4	X^3Y^4	Y^7+Y^5
1	X^3Y^2	X^2Y^3	X^3Y^3	X^2Y^4	X^3Y^4

which are $\{X^3Y, Y^4, X^3Y^2, Y^5, X^3Y^3, Y^6, X^3Y^4, Y^7, X^3Y^5, Y^8\}$*, so that now* $\#(D_5) = 20$*. The product of the elements in the basis of* C *with* $\mathbf{b}_{18}, \mathbf{b}_{21}, \mathbf{b}_{22}, \mathbf{b}_{24}, \mathbf{b}_{25}, \mathbf{b}_{26}$ *and* $\mathbf{b}_{27}$ *will not yield any monomial to be added to* D_5*; for example, the remainders in the division of* $\mathbf{c}_1 * \mathbf{b}_{25}$*,* $\mathbf{c}_2 * \mathbf{b}_{25}$*,* $\mathbf{c}_3 * \mathbf{b}_{25}$*,* $\mathbf{c}_4 * \mathbf{b}_{25}$ *and* $\mathbf{c}_5 * \mathbf{b}_{25}$ *by the Gröbner basis of* I_9 *are respectively* $Y^7, XY^5 - XY^3 + XY, Y^8, X^2Y^5 - X^2Y^3 + X^2Y$ *and* X*, so we cannot add* X *to* D_5 *(because, for instance,* $X \prec Y^8$*). Likewise, we compute* $\#(D_4)$*,* $\#(D_3)$*,* $\#(D_2)$ *and* $\#(D_1)$ *obtaining respectively 21, 22, 24 and 27. Thus our bound for the minimum distance is 20 but this is the actual value of the minimum distance, which we may check by observing that the code corresponds to the geometric Goppa code generated by a basis of* $L(7P_\infty)$*, see [17].*

Example 3.2. *In this example we deal with the affine curve defined over* $\mathbb{F}_9$ *by the equation* $X^6Y^4 + X^8 + 1 = 0$*. Observe that the closure of the curve in* $\mathbb{P}^2(\mathbb{F}_9)$ *has two nonsingular points, namely,* $P_1 := (0 : 1 : 0)$ *and* $P_2 := (1 : 0 : 0)$ *so* $R = \mathbb{F}_9[X, Y]/(X^6Y^4 + X^8 + 1)$ *is* not *a weight domain (see [14], see also [3] for results on codes defined by means of near weight domains, which include the ring* R*). The pole divisor of the functions* x *and* y *in the function field of the curve are respectively,* $\mathrm{div}_\infty(x) = 2P_1 + 2P_2$ *and* $\mathrm{div}_\infty(y) = 5P_1 + 5P_2$ *(calculations done with KASH/KANT - [15]) so we choose a weighted lexicographic order for* $\mathbb{F}_9[X, Y]$ *by stating that* $X^aY^b \preccurlyeq X^{a'}Y^{b'}$ *if and only if* $2a + 5b \leq 2a' + 5b'$*, and if equality holds then* $X^aY^b <_{\mathrm{lex}} X^{a'}Y^{b'}$ *(with* $Y <_{\mathrm{lex}} X$*). Using* CoCoA *([4]) or Macaulay2 ([13]) we may calculate a Gröbner basis for* $I_9 = (X^6Y^4 + X^8 + 1, Y^9 - Y, X^9 - X)$ *obtaining* $\{X^4 - 1, Y^4 - X^6\}$ *so that the footprint is* $\Delta(I_9) = \{X^aY^b \mid 0 \leq a \leq 3, 0 \leq b \leq 3\}$*, and we conclude that there are 16 rational points in the affine curve. Let* C *be the code generated by evaluating the classes* $\{1 + I, X + I, X^2 + I, Y + I, X^3 + I, XY + I\}$ *at the rational points in the affine plane (hence, from the above theorem we know* *that this code has dimension 6). Observe that this is the geometric Goppa code generated by a base of* $L(7P_1 + 7P_2)$*, or in other words, the geometric Goppa code associated with the divisors* $G = 7P_1 + 7P_2$ *and* D*, where* D *is the sum of all rational points. Let* $f = a_1 + a_2X + a_3X^2 + a_4Y + a_5X^3 + a_6XY$*, with* $a_1, \ldots, a_6 \in \mathbb{F}_9$ *and let* $j \in \{1, \ldots, 6\}$ *be greatest index for which* $a_j \neq 0$*. Denoting by* $\mathbf{B}$ *the (ordered) basis* $\{\varphi(X^aY^b + I) \mid 0 \leq a \leq 3, 0 \leq b \leq 3\}$ *of* $\mathbb{F}_9^{16}$ *and proceeding as in the example above we see that* $\varphi(f + I) * \mathbf{B}$ *has dimension at least 9 (respectively, 4, 12, 8, 12, 16) if* $j = 6$ *(respectively, 5, 4, 3, 2, 1), so our bound for the minimum distance is 4, and one may check that this is the actual bound. We also see that if we discard* X^3 *and consider the code generated by evaluating the classes* $\{1 + I, X + I, X^2 + I, Y + I, XY + I\}$ *at the rational points, then the bound for the minimum distance is now 8, and again one may check that this is the actual bound.*

Acknowledment. The author would like to express his warm thanks to the referees for their careful reading and many suggestions which have improved very much the readability of this text.

Resumo. Nesse trabalho apresentamos um método para estimar a distância mínima de códigos de variedades afins. Nossa técnica usa propriedades da pegada de um ideal obtido através do aumento do ideal de definição da variedade em questão, e também pode ser aplicada a códigos de que não são produzidos utilizando-se domínios-pesos.

Palavras-chave. Códigos de variedade afim, bases de Gröbner, pegada de um ideal, distância mínima.

References

[1] H.E. Andersen, O. Geil, Evaluation codes from order domain theory, *Finite Fields Appl.*, **14**, (1) (2008), 92-123.

[2] T. Becker, V. Weispfenning, "Gröbner Bases - A computational approach to commutative algebra", Springer Verlag, Berlin, 1993.

[3] C. Carvalho, E. Silva, On algebras admitting a complete set of near weights, evaluation codes, and Goppa codes, Des. Codes Cryptography 53 (2) (2009), 99-110.

[4] CoCoA Team - CoCoA: a system for doing Computations in Commutative Algebra. Available at `http://cocoa.dima.unige.it`.

[5] D. Cox, J. Little, D. O'Shea, "Ideals, Varieties, and Algorithms", Third ed., Springer, New York, 2007.

[6] G.-L. Feng, T.R.N. Rao, A simple approach for construction of algebraic-geometric codes from affine plane curves, *IEEE Trans. In- form. Theory*, **40** (1994), 1003-1012.

[7] G.-L. Feng, T.R.N. Rao, Improved geometric Goppa codes, Part I:Basic theory, *IEEE Trans. Inform. Theory*, **41)**, (1995), 1678-1693.

[8] J. Fitzgerald, R.F. Lax, Decoding affine variety codes using Göbner bases, *Designs, Codes and Cryptography*, **13**, (2) (1998), 147-158.

[9] O. Geil, "Algebraic geometry codes from order domains, in Gröbner Bases, Coding, and Cryptography, Springer", 2009, Eds.: Sala, Mora, Perret, Sakata, Traverso, 121-141

[10] O. Geil, Evaluation Codes from an Affine Variety Code Perspective, in Advances in algebraic geometry codes, Ser. Coding Theory Cryptol., 5, World Sci. Publ., Hackensack, NJ, 2008, Eds.: E. Martinez-Moro, C. Munuera, D. Ruano, 153-180

[11] O. Geil, R. Pellikaan, On the Structure of Order Domains, *Finite Fields Appl.*, **8** (2002), 369-396.

[12] T.Høholdt, J.H. van Lint, R. Pellikaan, Algebraic geometric codes, in: V. Pless, W. C. Huffman (Eds.), Handbook of Coding Theory, Elsevier, 1998, pp. 871-961.

[13] D. Grayson, M. Stillman, Macaulay2, a software system for research in algebraic geometry, available at `http://www.math.uiuc.edu/Macaulay2/`.

[14] R. Matsumoto, Miuras's generalization of one-point AG codes is equivalent to Høholdt, van Lint and Pellikaan's generalization, *IEICE Trans. Fundamentals*, **E82-A** (1999), 665-670.

[15] M.E. Pohst, et al., The Computer Algebra System KASH/KANT, available at `http://www.math.tu-berlin.de/∼kant`.

[16] A. Seidenberg, Constructions in algebra, *Transactions of the American Mathematical Society*, 197 (1974), 273-313.

[17] H. Stichtenoth, A note on Hermitian codes over $GF(q^2)$, *IEEE Trans. Inform. Theory*, 34 (1988), 1345-1348.

[18] K. Yang, P.V. Kumar, On the true minimum distance of Hermitian codes, Lectures Notes in *Math.*,**1518** (1992), 99-107.