Order Functions and Evaluation Codes

Tom Høholdt[*], Jacobus H. van Lint, and Ruud Pellikaan[†]

Appeared in *Proc. AAECC-12*, Toulouse 23-27 June, 1997,
(T. Mora and H. Mattson Eds.), *Lect. Notes Comp. Sc.*, vol. 1255,
pp. 138-150, Springer, Berlin 1997.

Abstract

Based on the notion of an order function we construct and determine the parameters of a class of error-correcting evaluation codes. This class includes the one-point algebraic geometry codes as well as the generalized Reed-Muller codes, and the parameters are determined without using heavy machinery from algebraic geometry.

1 Introduction

Suppose we have n points $P_1, \ldots, P_n$ in the affine space $AG(m, q)$ of dimension m over some finite field F_q, and a vector space of functions $f : AG(m, q) \to F_q$. We can then choose some of these functions $f_1, f_2, \ldots, f_l$, say, and define a code E_l by

$$E_l = \text{span}(f_i(P_1), f_i(P_2), \ldots, f_i(P_n)), i = 1, \ldots, l$$

and its dual code by

$$C_l = E_l^{\perp}.$$

In general nothing interesting can be said about the codes constructed in this way, but in 1977 V. D. Goppa [1] showed that it is possible to determine the parameters of such codes if the points are chosen on an algebraic curve and the functions are from a certain space associated with the curve. The proof of this uses some heavy machinery from algebraic geometry, in particular the Riemann-Roch Theorem. The subject of algebraic geometry codes exploded after Tsfasman-Vlăduţ and Zink [2] showed that in this way it is possible to get asymptotically good sequences of codes with parameters better than the Varshamov-Gilbert bound in a certain range of the rate and for large enough q. Since 1977 a lot of effort has gone into finding a more elementary way of describing these codes [3]-[8]. In this paper we give such a description based

*Tom Høholdt, Dept. of Mathematics, Technical University of Denmark, Bldg. 303, DK-2800 Lyngby, Denmark

†Jacobus H. van Lint and Ruud Pellikaan, Dept. of Mathematics and Computing Science, Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven, The Netherlands

on the so-called order functions. The paper came about when working on a chapter on algebraic geometry codes which will appear in the Handbook on Coding Theory [9].

In Section 2 we introduce the concept of an order function. Section 3 treats evaluation codes and their duals and determines the parameters and Section 4 contains some concluding remarks.

2 Order Functions

Let R be a commutative ring with a unit which contains the finite field F_q as a unitary subring. We will call R an F_q-*algebra*. Let N denote the positive integers and N_0 the nonnegative integers.

Definition 2.1 A function $\rho : R \to N_0 \cup \{-\infty\}$ is called an *order* function if it satisfies

O.0 $\rho(f) = -\infty \Leftrightarrow f = 0$
O.1 $\rho(\lambda f) = \rho(f)$ for all nonzero $\lambda \in F_q$
O.2 $\rho(f + g) \leq \max\{\rho(f), \rho(g)\}$ with equality if $\rho(f) \neq \rho(g)$
O.3 If $\rho(f) \leq \rho(g)$ and $h \in R \setminus \{0\}$ then $\rho(hf) < \rho(hg)$
O.4 If $\rho(f) = \rho(g)$ then there exists a nonzero $\lambda \in F_q$ such that $\rho(f - \lambda g) < \rho(g)$

for all $f, g, h \in R$. Here $-\infty < n$ for all $n \in N_0$.

Definition 2.2 Let R be an F_q-algebra. A *weight* function on R is an order function that furthermore satisfies

O.5 $\rho(fg) = \rho(f) + \rho(g)$

for all $f, g \in R$. Here $-\infty + n = -\infty$ for all $n \in N_0$.

Example 2.3 Let $R = F_q[x]$ and $\rho(f) = \deg f$. Then ρ is a weight function. For multivariate polynomials the degree function does not satisfy O.4.

Example 2.4 Let $R = F_q[x_1, x_2, \ldots, x_n]$. We will use the multiindex notation for monomials. This means $x^\alpha = \prod_{i=1}^m x_i^{\alpha_i}$ if $\alpha = (\alpha_1, \ldots, \alpha_m)$. The *lexicographic order* on the monomials is defined by $x^\alpha <_L x^\alpha$ if and only if $\alpha_1 = \beta_1, \ldots, \alpha_{l-1} = \beta_{l-1}$ and $\alpha_l \neq \beta_l$ for some $1 \leq l \leq m$, and the *graded lexicographic order* $<_D$ is defined by $x^\alpha <_D x^\beta$ if and only if either $\deg(x^\alpha) < \deg(x^\beta)$ or $\deg(x^\alpha) = \deg(x^\beta)$ and $x^\alpha <_L x^\beta$. The graded lexicographic order is an admissible order, and can be extended to an order function on R in the following way. Let $f_1, f_2, \ldots$ be an enumeration of the monomials such that $f_i <_D f_{i+1}$ for all i. The monomials are a basis of R over F_q, so every nonzero polynomial f can be written in a unique way as

$$f = \sum_{i=1}^{j} \lambda_i f_i$$

where $\lambda_i \in F_q$ for all i and $\lambda_j \neq 0$. Define a function

$$\rho : R \to N_0 \cup \{-\infty\}$$

by $\rho(0) = -\infty$ and $\rho(f) = j - 1$ where j is the smallest integer such that f can be written as a linear combination of the first j monomials. Then ρ is an order function, but not a weight function.

Lemma 2.5 *Let ρ be an order function on R. Then:*
1) If $\rho(f) = \rho(g)$, then $\rho(fh) = \rho(gh)$ for all $h \in R$.
2) $\rho(1) \leq \rho(f)$ for all nonzero elements $f \in R$.
3) $F = \{f \in R \mid \rho(f) \leq \rho(1)\}$.
4) If $\rho(f) = \rho(g)$, then there exists a unique nonzero $\lambda \in F$ such that $\rho(f - \lambda g) < \rho(g)$.

Proof.
1) If $\rho(f) = \rho(g)$, then there exists a nonzero $\lambda \in F$ such that $\rho(f - \lambda g) < \rho(g)$, by $(O.4)$. So $\rho(fh - \lambda gh) < \rho(gh)$, by $(O.3)$. Now $fh = (fh - \lambda gh) + \lambda gh$. Hence $\rho(fh) = \rho(\lambda gh) = \rho(gh)$, by $(O.2)$ and $(O.1)$, respectively.

2) Suppose that f is a nonzero element of R such that $\rho(f) < \rho(1)$. Then $\rho(1) > \rho(f) > \rho(f^2) > \cdots$ is a strictly decreasing sequence, by Condition $(O.3)$, but this contradicts the fact that $N_0 \cup \{-\infty\}$ is a well-order. Hence $\rho(1) \leq \rho(f)$ for all nonzero elements f in R.

3) It is clear that F is a subset of $\{f \in R \mid \rho(f) \leq \rho(1)\}$, by Conditions $(O.0)$ and $(O.1)$. If f is nonzero and $\rho(f) \leq \rho(1)$, then $\rho(f) = \rho(1)$, by 2) and hence there exists a nonzero $\lambda \in F$ such that $\rho(f - \lambda 1) < \rho(1)$, by $(O.4)$. So $f - \lambda = 0$ and $f \in F$.

4) If $\rho(f) = \rho(g)$, then there exists a nonzero $\lambda \in F$ such that $\rho(f - \lambda g) < \rho(g)$ by condition $(O.4)$. If $\rho(f - \mu g) < \rho(g)$, we get by $(O.1)$ and $(O.2)$ that $\rho(f - \lambda g - (f - \mu g)) < \rho(g)$ and therefore $\rho((\mu - \lambda)g) < \rho(g)$. Condition $(O.1)$ gives $\mu - \lambda = 0$.

Proposition 2.6 *If there exists an order function on R, then R is an integral domain.*

Proof. Suppose that $fg = 0$ for some nonzero $f, g \in R$. We may assume that $\rho(f) \leq \rho(g)$. So $\rho(f^2) \leq \rho(fg) = \rho(0) = -\infty$. So $\rho(f^2) = -\infty$, and $f^2 = 0$. Now $f \neq 0$, hence $\rho(1) \leq \rho(f)$, by Lemma 2.5. So $\rho(f) \leq \rho(f^2) = \rho(0) = -\infty$. Hence $f = 0$, which is a contradiction. Therefore R has no zero divisors.

Example 2.7 The F-algebra $R = F[X_1, X_2]/(X_1X_2 - 1)$ is an integral domain. We will show that it does not have an order function. Denote the coset of X_i modulo the ideal $(X_1X_2 - 1)$ by x_i. If ρ is an order function on R, then $\rho(1) \leq \rho(x_1)$, so $\rho(x_2) \leq \rho(x_1x_2) = \rho(1)$, hence $\rho(x_2) = \rho(1)$ and in the same way we get $\rho(x_1) = \rho(1)$. Therefore $\rho(f) \leq \rho(1)$ for all $f \in R$. Hence $F = R$ by Lemma 2.5, which is a contradiction since $x_1 \notin F$.

The following proposition and theorem show that if there exists an order function, then there exists a basis with certain properties; and conversely if such a basis exists, then one can define an order function. Although the formulation is technical, it is easy to apply. This will be shown in some examples.

Proposition 2.8 *Let R be an F-algebra with order function ρ. Then there exists a basis $\{f_i \mid i \in N\}$ of R over F such that $\rho(f_i) < \rho(f_{i+1})$ for all i. Every such basis has the property that if i is the smallest positive integer such that f can be written as a linear combination of the first i elements of that basis, then $\rho(f) = \rho(f_i)$. Furthermore, if $l(i,j)$ is the smallest positive integer l such that $\rho(f_i f_j) = \rho(f_l)$, then $l(i,j) < l(i+1,j)$ for all i and j.*

Proof. Let $(\rho_i \mid i \in N)$ be the increasing sequence of all nonnegative integers that appear as the order $\rho(f)$ of a nonzero element $f \in R$. By definition there exists an $f_i \in R$ such that $\rho(f_i) = \rho_i$ for all $i \in N$. Hence $\rho(f_i) < \rho(f_{i+1})$ for all i, and for all nonzero $f \in R$ there exists an i with $\rho(f) = \rho(f_i)$, by definition. The fact that $\{f_i \mid i \in N\}$ is a basis is proved by induction and Lemma 2.5 (4), and it has the required property by $(O.2)$. That the function $l(i,j)$ is strictly increasing in its first argument is a consequence of condition $(O.3)$.

Theorem 2.9 *Let R be an F-algebra. Let $\{f_i \mid i \in N\}$ be a basis of R as a vector space over F with $f_1 = 1$. Let L_i be the vector space generated by $f_1, \ldots, f_i$. Let $l(i,j)$ be the smallest positive integer l such that $f_i f_j \in L_l$. Suppose $l(i,j) < l(i+1,j)$ for all $i,j \in N$. Let $(\rho_i \mid i \in N)$ be a strictly increasing sequence of nonnegative integers. Define $\rho(0) = -\infty$, and $\rho(f) = \rho_i$ if i is the smallest positive integer such that $f \in L_i$. Then ρ is an order function on R. If moreover $\rho_{l(i,j)} = \rho_i + \rho_j$, then ρ is a weight function.*

Proof. The conditions $(O.0)$, $(O.1)$, $(O.2)$, and $(O.4)$ are a direct consequence of the definitions.

With every nonzero element $f \in R$ the smallest positive integer $\iota(f)$ is associated such that $f \in L_{\iota(f)}$. Let f and g be nonzero elements of R. Then

$$f = \sum_{i \leq \iota(f)} \lambda_i f_i, \; g = \sum_{j \leq \iota(g)} \nu_j f_j \;\text{ and }\; fg = \sum_{l \leq \iota(fg)} \mu_l f_l,$$

with $\lambda_{\iota(f)} \neq 0$, $\nu_{\iota(g)} \neq 0$ and $\mu_{\iota(fg)} \neq 0$. There exist $\mu_{ijl} \in F$ such that

$$f_i f_j = \sum_{l \leq l(i,j)} \mu_{ijl} f_l$$

and $\mu_{ijl(i,j)} \neq 0$. Hence

$$\mu_l = \sum_{l(i,j)=l} \lambda_i \nu_j \mu_{ijl}.$$

The function $l(i,j)$ is strictly increasing in both arguments, by assumption and symmetry. So $l(i,j) < l(\iota(f), \iota(g))$ if $i < \iota(f)$ or $j < \iota(g)$. Furthermore, if $i = \iota(f)$ and $j = \iota(g)$, then

$$\lambda_i \nu_j \mu_{ijl(i,j)} \neq 0,$$

This element is therefore equal to $\mu_{\iota(fg)}$, and we have proved that $\iota(fg) = l(\iota(f), \iota(g))$.

If moreover $\rho_{l(i,j)} = \rho_i + \rho_j$, then

$$\rho(fg) = \rho_{\iota(fg)} = \rho_{l(\iota(f),\iota(g))} = \rho_{\iota(f)} + \rho_{\iota(g)} = \rho(f) + \rho(g).$$

Example 2.10 Let $\mathbf{w} = (w_1, \ldots, w_m)$ be an m-tuple of positive integers called *weights*. The *weighted degree* of $\alpha \in N_0^m$ and of the corresponding monomial X^α is defined by

$$\mathrm{wdeg}(X^\alpha) = \mathrm{wdeg}(\alpha) = \sum \alpha_l w_l,$$

and of a nonzero polynomial $F = \sum \lambda_\alpha X^\alpha$ by

$$\mathrm{wdeg}(F) = \max\{\ \mathrm{wdeg}(X^\alpha) \mid \lambda_\alpha \neq 0\ \}.$$

This gives a degree function wdeg on the ring $F[X_1, \ldots, X_m]$. The *weighted graded lexicographic order* $\prec_{\mathbf{w}}$ on N_0^m is defined by

$$\alpha \prec_{\mathbf{w}} \beta \text{ if and only if } \mathrm{wdeg}(\alpha) < \mathrm{wdeg}(\beta) \text{ or } \mathrm{wdeg}(\alpha) = \mathrm{wdeg}(\beta) \text{ and } \alpha \prec_L \beta\ ,$$

and similarly for the monomials. For $m = 2$ with $X = X_1$, $Y = X_2$, $\mathrm{wdeg}(X) = 4$ and $\mathrm{wdeg}(Y) = 5$, the begining of this total graded lexicographic order looks like:

$$\begin{array}{lllllllllllll}
1 & \prec & & & & & & & & & & & \\
X & \prec & Y & \prec & & & & & & & & & \\
X^2 & \prec & XY & \prec & Y^2 & \prec & & & & & & & \\
X^3 & \prec & X^2Y & \prec & XY^2 & \prec & Y^3 & \prec & & & & & \\
X^4 & \prec & X^3Y & \prec & X^2Y^2 & \prec & XY^3 & \prec & Y^4 & \prec & & & \\
X^5 & \prec & X^4Y & \prec & X^3Y^2 & \prec & X^2Y^3 & \prec & XY^4 & \prec & X^6 & \prec & Y^5
\end{array}$$

Example 2.11 Let I be the ideal in $F[X, Y]$ generated by a polynomial

$$X^a + Y^b + G(X, Y)$$

with $\deg(G) < b < a$ and $\gcd(a, b) = 1$. Let $R = F[X, Y]/I$. Denote the cosets of X and Y modulo I by x and y, respectively. Then $x^a = -y^b - g(x, y)$ and therefore x^a is a linear combination of elements of the form $x^\alpha y^\beta$ with $0 \leq \alpha < a$, since $\deg(G) < a$. By recursion one shows that the set

$$\{x^\alpha y^\beta \mid 0 \leq \alpha < a\}$$

is a basis for R. Suppose there exists a weight function ρ on R such that $\gcd(\rho(x), \rho(y)) = 1$. We will show that $\rho(x) = b$ and $\rho(y) = a$. Let $x^i y^j$ be the monomial in g with the largest weight. Then $\rho(g) \leq i\rho(x) + j\rho(y)$ by $(O.2)$ and $(O.5)$ and therefore either $\rho(g) \leq (i+j)\rho(x)$ or $\rho(g) \leq (i+j)\rho(y)$ from which we get $\rho(g) < ag(x)$ or $\rho(g) < b\rho(y)$ since $i + j < b < a$. But $\rho(x^a) = \rho(y^b + g)$ and $\rho(y^b) = \rho(x^a + g)$ by $(O.1)$ so we conclude $\rho(x^a) = \rho(y^b)$ using $(O.2)$ and $(O.5)$, and therefore $a\rho(x) = b\rho(y)$. Since $\gcd(\rho(x), \rho(y)) = 1$, the result follows.

In the following it is shown that indeed such a weight function exists.

Proposition 2.12 *Let I be the ideal in $F[X,Y]$ generated by a polynomial of the form $X^a + Y^b + G(X,Y)$ with $\deg(G) < b < a$ and $\gcd(a,b) = 1$. Let $R = F[X,Y]/I$. Then there exists a weight function ρ on R. The ring R is an integral domain, I is a prime ideal and $X^a + Y^b + G(X,Y)$ is absolutely irreducible.*

Proof. Consider the total weighted degree lexicographic order $\prec_{\mathbf{w}}$ on the monomials in X and Y with respect to the weights $\mathrm{wdeg}(X) = b$ and $\mathrm{wdeg}(Y) = a$. This weight function is injective on the set $\{X^\alpha Y^\beta \mid 0 \le \alpha < a\}$, since $\gcd(a,b) = 1$. Let $f_1, f_2, \dots$ be an enumeration of the elements $x^\alpha y^\beta$ of the basis of R, and let $\rho_1, \rho_2, \dots$ be an enumeration of the nonnegative integers of the form $\alpha b + \beta a$ with $0 \le \alpha < a$, in such a way that $\rho_i < \rho_{i+1}$ and $f_i = x^\alpha y^\beta$ if $\rho_i = \alpha b + \beta a$ and $0 \le \alpha < a$, for all i. Let $L_l = \langle f_1, \dots, f_l \rangle$.

It is proved by induction that $\rho_{l(i,j)} = \rho_i + \rho_j$. The induction is with respect to the well-order $\prec_{\mathbf{w}}$ on N^2. Now $f_1 = 1$ and $\rho_1 = 0$. So $l(1,1) = 1$ and the start of the induction is satisfied. Suppose that the claim is proved for all $(i', j') \prec_{\mathbf{w}} (i,j)$. Let $f_i = x^\alpha y^\beta$, $\rho_i = \alpha b + \beta a$ with $0 \le \alpha < a$. Let $f_j = x^\gamma y^\delta$, $\rho_j = \gamma b + \delta a$ with $0 \le \gamma < a$. Then $f_i f_j = x^{\alpha+\gamma} y^{\beta+\delta}$ and $\rho_i + \rho_j = (\alpha+\gamma)b + (\beta+\delta)a$.

If $\alpha+\gamma < a$, then $f_i f_j$ is a basis element. So $f_{l(i,j)} = f_i f_j$ and $\rho_{l(i,j)} = \rho_i + \rho_j$.

If $\alpha + \gamma \ge a$, then $\alpha + \gamma = a + \epsilon$ with $0 \le \epsilon < a$. Hence

$$\rho_i + \rho_j = (\alpha+\gamma)b + (\beta+\delta)a = \epsilon b + (b + \beta + \delta)a$$

and

$$f_i f_j = -x^\epsilon y^{b+\beta+\delta} - x^\epsilon g(x,y).$$

The term $x^\epsilon y^{b+\beta+\delta}$ is a basis element f_l. We may assume by induction that $x^\epsilon g(x,y) \in L_{l-1}$, since $\deg(G) < b < a$. Hence $f_i f_j = f_l$, $l(i,j) = l$ and $\rho_l = \epsilon b + (b+\beta+\delta)a = \rho_i + \rho_j$. This concludes the proof that $\rho_{l(i,j)} = \rho_i + \rho_j$. Therefore $l(i,j) < l(i+1,j)$.

Hence there exists a weight function ρ on R such that $\rho(x^\alpha y^\beta) = \alpha b + \beta a$, by Theorem 2.9. So R is an integral domain by Proposition 2.6 and I is therefore a prime ideal.

The general question under what conditions on the ideal I it is possible to find an order function on $R = F[x_1, \dots, x_m]/I$ is difficult. Some results relating this to the existence of Groebner bases for I with certain properties are given by R. Pellikaan in [8].

3 Evaluation Codes and Their Duals

Let R be an F_q-algebra with an order function ρ. Let $(f_i \mid i \in N)$ be a basis of R over F_q such that $\rho(f_i) < \rho(f_{i+1})$ for all $i \in N$, and for all nonzero $f \in R$ there exists a j with $\rho(f) = \rho(f_j)$. The existence of such a basis is guaranteed by Proposition 2.8. Let L_l be the vector space generated by $f_1, \dots, f_l$. Hence for all nonzero $f \in R$ we have that $\rho(f) = \rho(f_l)$ if and only if l is the smallest integer such that $f \in L_l$. Let $l(i,j)$ be the smallest positive integer l such that $f_i f_j \in L_l$. So $l(i,j) < l(i+1,j)$ for all $i,j \in N$.

The coordinatewise multiplication on F_q^n is defined by $\mathbf{a}*\mathbf{b} = (a_1b_1, \ldots, a_nb_n)$ for $\mathbf{a} = (a_1, \ldots, a_n)$ and $\mathbf{b} = (b_1, \ldots, b_n)$. The vector space F_q^n becomes an F_q-algebra with the multiplication $*$.

Definition 3.1 The map

$$\varphi : R \longrightarrow F_q^n,$$

is called a morphism of F_q-algebras if φ is F_q-linear and

$$\varphi(fg) = \varphi(f) * \varphi(g).$$

Let $\mathbf{h}_i = \varphi(f_i)$. Define the *evaluation code* E_l and its dual C_l by

$$E_l = \varphi(L_l) = \langle \mathbf{h}_1, \ldots, \mathbf{h}_l \rangle,$$

$$C_l = \{\mathbf{c} \in F_q^n \mid \mathbf{c} \cdot \mathbf{h}_i = 0 \ \text{ for all } \ i \le l\}.$$

We will consider only those algebra morphisms φ that are surjective. Hence there exists a positive integer N such that $E_l = F_q^n$ and $C_l = 0$ for all $l \ge N$.

Let the set $\mathcal{P}$ consist of n distinct points $P_1, \ldots, P_n$ in F_q^m. Consider the evaluation map

$$ev_{\mathcal{P}} : F[X_1, \ldots, X_m] \longrightarrow F^n,$$

defined by $ev_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n))$. This is a morphism of F_q-algebras from R to F_q^n, since $FG(P) = F(P)G(P)$ for all polynomials F and G, and all points P.

Lemma 3.2 *The map $ev_{\mathcal{P}}$ is surjective.*

Proof. Let $P_j = (x_{j1}, \ldots, x_{jm})$. Let $A_{il} = \{x_{jl} \mid j = 1, \ldots, n\} \setminus \{x_{il}\}$. Define the polynomial f_i by

$$f_i = \prod_{l=1}^{m} \prod_{x \in A_{il}} (X_l - x).$$

Then $f_i(P_j) = 0$ for all $i \neq j$. Furthermore $f_i(P_i) \neq 0$, since the points $P_1, \ldots, P_n$ are mutually distinct. Let $g_i = f_i/f_i(P_i)$. Then $ev_{\mathcal{P}}(g_i)$ is the ith standard basis element of F_q^n. Hence $ev_{\mathcal{P}}$ is surjective.

Suppose that I is an ideal in the ring $F[X_1, \ldots, X_m]$. Let $P_1, \ldots, P_n$ be in the zeroset of I with coordinates in F. Hence $f(P_j) = 0$ for all $f \in I$ and all $j = 1, \ldots, n$. Then the evaluation map induces a well-defined linear map

$$ev_{\mathcal{P}} : F[X_1, \ldots, X_m]/I \longrightarrow F^n,$$

which is also a surjective morphism of F-algebras.

In the above setting the codes are very general and nothing specific can be said about the minimum distance of the codes E_l and C_l. We will show that certain order and weight functions on the affine ring R give a bound on the minimum distance which is in many cases the actual minimum distance.

Suppose that ρ is a weight function. Condition $(O.5)$ implies that the subset $S = \{\rho(f) \mid f \in R,\ f \neq 0\ \}$ of N_0 has the property that, $0 \in S$, and $x + y \in S$ for all $x, y \in S$.

Definition 3.3 A subset S of the nonnegative integers N_0 is called a *semigroup* if $0 \in S$ and for all $x, y \in S$ also the sum $x + y \in S$. Elements of $N_0 \setminus S$ are called *gaps* of S and elements of S are called *nongaps* of S. If all elements of S are divisible by an integer $d > 1$, then there are infinitely many gaps. The *number of gaps* is denoted by $g = g(S)$. If $g < \infty$, then $l_g(S) = l_g$ is both the *largest gap* of S and the gth gap.

Lemma 3.4 *Let S be a semigroup with finitely many gaps and $s \in S$. Then the number of elements of $S \setminus (s + S)$ is equal to s.*

Proof. Let $s \in S$. Let l_g be the largest gap of S. Let $T = \{t \in N_0 \mid t > s + l_g\}$. Then T is contained in S and in $s + S$. Let $U = \{u \in S \mid u \leq s + l_g\}$. Then the number of elements of U is equal to $s + l_g + 1 - g$, and S is the disjoint union of T and U. Let $V = \{v \in s + S \mid s \leq v \leq s + l_g\}$. Then the number of elements of V is equal to $l_g + 1 - g$, and $s + S$ is the disjoint union of V and T. Furthermore $V \subseteq U$, since $s \in S$ and S is a semigroup. Hence

$$\#(S \setminus (s + S)) = \#U - \#V = (s + l_g + 1 - g) - (l_g + 1 - g) = s.$$

Lemma 3.5 *Let f be a nonzero element of an F_q-algebra R with a weight function ρ. Then*

$$\dim(R/(f)) = \rho(f).$$

Proof. Let S be the semigroup of the weight function ρ. Let $s = \rho(f)$. Let $(\rho_i \mid i \in N)$ be the sequence of the elements of S in increasing order. The image under ρ of the set of nonzero elements of the ideal (f) is equal to $s + S$. So for every $\rho_i \in S$ there exists an $f_i \in R$ such that $\rho(f_i) = \rho_i$, and $f_i \in (f)$ if $\rho_i \in s + S$. The sets $\{f_i \mid i \in N\}$ and $\{f_i \mid i \in N,\ \rho_i \in s + S\}$ are bases of the algebra R and the ideal (f), respectively, by the same argument as 2.8. Hence the classes of f_i modulo (f) with $i \in N$ and $\rho_i \in S \setminus (s+S)$ form basis for $R/(f)$. So the dimension of $R/(f)$ is equal to the number of elements of $S \setminus (s + S)$, which is $\rho(f)$ by Lemma 3.4.

Suppose that we have a weight function ρ on an affine F_q-algebra $R = F_q[X_1, \ldots, X_m]/I$. Let $\mathcal{P}$ consist of n distinct points of F_q^m in the zero set of I, and let $ev_{\mathcal{P}} : R \to F_q^n$ be the corresponding evaluation map.

Lemma 3.6 *Let f be a nonzero element of R. Then the number of zeros of f is at most $\rho(f)$.*

Proof. Let $\mathcal{Q}$ be the set of zeros of f and let $t = |\mathcal{Q}|$. The map $ev_{\mathcal{Q}} : R \rightarrow F_q^t$ is linear and surjective by Lemma 3.2. Furthermore $g(Q) = 0$ for all $Q \in \mathcal{Q}$ and $g \in (f)$. This induces a well-defined map $ev_{\mathcal{Q}} : R/(f) \rightarrow F_q^t$ which is linear and surjective. Hence the number of zeros of f is at most the dimension of $R/(f)$ which is equal to $\rho(f)$ by Lemma 3.5.

Theorem 3.7 *Let ρ be a weight function. Then the minimum distance of E_l is at least $n - \rho_l$. If $\rho_l < n$, then $\dim(E_l) = l$.*

Proof. Let $\mathbf{c}$ be a nonzero element of E_l. Then there exists a nonzero element $f \in R$ such that $\rho(f) \leq \rho_l$ and $\mathbf{c} = ev_{\mathcal{P}}(f)$. So $c_i = f(P_i)$ for all i. The number of zeros of f is at most ρ_l, by Lemma 3.6. Hence $wt(\mathbf{c}) \geq n - \rho_l$.

Suppose moreover that $\rho_l < n$. E_l is the image under the evaluation map of the vector space L_l of dimension l. If $f \in L_l$ and $ev_{\mathcal{P}}(f) = 0$, then f has at least n zeros. Hence $f = 0$ by Lemma 3.6, since $\rho_l < n$. So the map $ev_{\mathcal{P}} : L_l \rightarrow E_l$ is a linear isomorphism, so $\dim(E_l) = l$.

Corollary 3.8 *Let ρ be a weight function with g gaps. If $\rho_k < n$, then E_k is an $[n, k, d]$ code such that $k + d \geq n + 1 - g$.*

Proof. This follows from Theorem 3.7 and the fact that $l \geq \rho_l + 1 - g$.

Remark 3.9 If ρ is an order function but not a weight function, then in general $R/(f)$ is not finite dimensional and there is not a straightforward bound on the minimum distance for E_l.

We will now give a bound on the minimum distance of C_l and repeat the main definitions. Let R be an F_q-algebra with an order function ρ. Let $\{f_i \mid i \in N\}$ be a basis of R over F_q such that $\rho(f_i) < \rho(f_{i+1})$ for all $i \in N$. Let $\varphi : R \rightarrow F_q^n$ be a surjective morphism of F_q-algebras. Let L_l be the vector space with $f_1, \ldots, f_l$ as a basis. The number $l(i,j)$ was defined as the smallest positive integer l such that $f_i f_j \in L_l$. The function $l(i,j)$ is strictly increasing in both arguments. Let $\mathbf{h}_i = \varphi(f_i)$. Let $E_l = \varphi(L_l)$ and C_l its dual. There exists a positive integer N such that $E_l = F_q^n$ for all $l > N$. So $C_l = 0$ for all $l > N$. Let $\mathbf{H}$ be the $N \times n$ matrix with $\mathbf{h}_i$ on the i^{th} row for $1 \leq i \leq N$.

Definition 3.10 Consider the *syndromes*

$$s_i(\mathbf{y}) = \mathbf{y} \cdot \mathbf{h}_i \quad \text{and} \quad s_{ij}(\mathbf{y}) = \mathbf{y} \cdot (\mathbf{h}_i * \mathbf{h}_j).$$

Then $\mathbf{S}(\mathbf{y}) = (s_{ij}(\mathbf{y}) \mid 1 \leq i, j \leq N)$ is the *matrix of syndromes* of $\mathbf{y}$.

Lemma 3.11 *Let* $\mathbf{y} \in F_q^n$. *Let* $\mathbf{D}(\mathbf{y})$ *be the diagonal matrix with* $\mathbf{y}$ *on the diagonal. Then*

$$\mathbf{S}(\mathbf{y}) = \mathbf{H}\mathbf{D}(\mathbf{y})\mathbf{H}^T,$$

and

$$\mathrm{rank}(\mathbf{S}(\mathbf{y})) = \mathrm{wt}(\mathbf{y}).$$

Proof. The matrix of syndromes $\mathbf{S}(\mathbf{y})$ is equal to $\mathbf{H}\mathbf{D}(\mathbf{y})\mathbf{H}^T$, since

$$s_{ij}(\mathbf{y}) = \mathbf{y} \cdot (\mathbf{h}_i * \mathbf{h}_j) = \sum_l y_l h_{il} h_{jl},$$

where h_{il} is the l^{th} entry of $\mathbf{h}_i$. The rank of the diagonal matrix $\mathbf{D}(\mathbf{y})$ is equal to the number of nonzero entries of $\mathbf{y}$, which is $wt(\mathbf{y})$. The rows of $\mathbf{H}$ generate F_q^n, since $E_N = F_q^n$. Hence the matrices $\mathbf{H}$ and $\mathbf{H}^T$ both have full rank n. Therefore $\mathrm{rank}(\mathbf{S}(\mathbf{y})) = \mathrm{rank}(\mathbf{D}(\mathbf{y})) = \mathrm{wt}(\mathbf{y})$.

Definition 3.12 Define

$$N_l = \{\ (i,j) \in N^2 \ \mid\ l(i,j) = l+1\ \}.$$

Let ν_l be the number of elements of N_l.

Lemma 3.13
1) *If* $\mathbf{y} \in C_l$ *and* $l(i,j) \le l$, *then* $s_{ij}(\mathbf{y}) = 0$.
2) *If* $\mathbf{y} \in C_l \setminus C_{l+1}$ *and* $l(i,j) = l+1$, *then* $s_{ij}(\mathbf{y}) \neq 0$.

Proof.
1) Let $\mathbf{y} \in C_l$. If $l(i,j) \le l$. Then $f_i f_j \in L_l$. So $\mathbf{h}_i * \mathbf{h}_j = \varphi(f_i f_j)$ is an element of $\varphi(L_l)$, which is the dual of C_l. Hence $s_{ij}(\mathbf{y}) = \mathbf{y} \cdot (\mathbf{h}_i * \mathbf{h}_j) = 0$.
2) Let $\mathbf{y} \in C_l \setminus C_{l+1}$. If $l(i,j) = l+1$, then $f_i f_j \in L_{l+1} \setminus L_l$. So $f_i f_j \equiv \mu f_{l+1}$ modulo L_l for some nonzero $\mu \in F_q$. Hence $\mathbf{h}_i * \mathbf{h}_j \equiv \mu \mathbf{h}_{l+1}$ modulo $\varphi(L_l)$. Now $\mathbf{y} \notin C_{l+1}$, so $s_{l+1}(\mathbf{y}) \neq 0$. Therefore $s_{ij}(\mathbf{y}) \neq 0$

Lemma 3.14 *If* $t = \nu_l$ *and* $(i_1, j_1), \ldots, (i_t, j_t)$ *is an enumeration of the elements of* N_l *in increasing order with respect to the lexicographic order on* N^2, *then* $i_1 < \cdots < i_t$ *and* $j_t < \cdots < j_1$. *If moreover* $\mathbf{y} \in C_l \setminus C_{l+1}$, *then*

$$s_{i_u j_v}(\mathbf{y}) = \begin{cases} 0 & \text{if} \quad u < v \\ \text{not zero} & \text{if} \quad u = v. \end{cases}$$

Proof. The sequence $(i_1, j_1), \ldots, (i_t, j_t)$ is ordered in such a way that $i_1 \le \ldots \le i_t$ and $j_u < j_{u+1}$ if $i_u = i_{u+1}$. If $i_u = i_{u+1}$, then $j_u < j_{u+1}$, and therefore

$$l+1 = l(i_u, j_u) < l(i_u, j_{u+1}) = l(i_{u+1}, j_{u+1}) = l+1,$$

which is a contradiction. Hence the sequence $i_1, \ldots, i_t$ is strictly increasing. A similar argument shows that $j_{u+1} < j_u$ for all $u < t$.

Let $\mathbf{y} \in C_l$. If $u < v$, then $l(i_u, j_v) < l(i_v, j_v) = l + 1$. Lemma 3.13 implies that $s_{i_u j_v}(\mathbf{y}) = 0$.

Moreover, let $\mathbf{y} \notin C_{l+1}$. If $u = v$, then $l(i_u, j_v) = l + 1$. Lemma 3.13 implies that $s_{i_u j_v}(\mathbf{y}) \neq 0$.

Proposition 3.15 *If* $\mathbf{y} \in C_l \setminus C_{l+1}$, *then* $\mathrm{wt}(\mathbf{y}) \geq \nu_l$.

Proof. This follows from Lemmas 3.11 and 3.14.

Definition 3.16

$$d_{ORD}(l) = \min\{\nu_{l'} \mid l' \geq l\},$$

$$d_{ORD,\varphi}(l) = \min\{\nu_{l'} \mid l' \geq l, C_{l'} \neq C_{l'+1}\},$$

If R is an affine algebra of the form $F_q[X_1, \ldots, X_m]/I$ and φ is the evaluation map $ev_{\mathcal{P}}$ of the set $\mathcal{P}$ of n points in F_q^m, then we denote $d_{ORD,\varphi}$ by $d_{ORD,\mathcal{P}}$.

Theorem 3.17 *The numbers* $d_{ORD}(l)$ *and* $d_{ORD,\varphi}(l)$ *are lower bounds for the minimum distance of* C_l*:*

$$d(C_l) \geq d_{ORD,\varphi}(l) \geq d_{ORD}(l).$$

Proof. The theorem is a direct consequence of Definition 3.16 and Proposition 3.15.

Remark 3.18 The set N_l and the numbers ν_l and d_{ORD} depend only on the order function ρ and neither on the choice of the basis $\{f_i \mid i \in N\}$ nor on the choice of the set of points. The number $d_{ORD,\mathcal{P}}$ depends on the order function and the choice of the set of points, but not on the choice of the basis.

If $\mathcal{P} \subseteq \mathcal{P}'$, then $d_{ORD,\mathcal{P}} \geq d_{ORD,\mathcal{P}'}$.

Example 3.19 Let $R = F_q[X]$ and let ρ, with $\rho(f) = \deg(f)$, be the order function of Example 2.3. Let $f_i = X^{i-1}$. For a primitive element α of F_q and $n = q - 1$, let $\varphi : R \to F_q^n$ be defined by $\varphi(f) = (f(\alpha^0), f(\alpha^1), \ldots, f(\alpha^{n-1}))$. Then $C_l = \{\mathbf{c} \in F_q^n | \mathbf{c} \cdot \varphi(f_i) = 0,\ 1 \leq i \leq l\}$ and C_l is a cyclic code with defining set $\alpha^0, \alpha, \ldots, \alpha^{l-1}$. The order bound gives $d_{ORD}(l) = l+1$ from which the BCH bound may be derived.

Example 3.20 Let $R = F_{16}[x, y]/ < x^5 + y^4 + y >$. The polynomial $x^5 + y^4 + y$ has 64 zeros in F_{16}^2. The monomials $\{x^i y^j | 0 \leq i, 0 \leq j \leq 3\}$ constitute a basis for R and $\rho(x^i y^j) = 4i + 5j$ gives a weight function on R. The table gives a list of the functions f_l, the nongaps ρ_l, the numbers ν_l and the bound $d_{ORD}(l)$ from Theorem 3.17. The number of gaps is $g = 6$ and the largest gap is $l_g = 11$.

l	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
f_l	1	x	y	x^2	xy	y^2	x^3	x^2y	xy^2	y^3	x^4	x^3y	x^2y^2	xy^3	x^5
ρ_l	0	4	5	8	9	10	12	13	14	15	16	17	18	19	20
ν_l	2	2	3	4	3	4	6	6	4	5	8	9	8	9	10
$d_{ORD}(l)$	2	2	3	3	3	4	4	4	4	5	8	8	8	9	10

The above example can be generalized to treat all the so-called Hermitian codes.

Example 3.21 *Reed-Muller codes* Let $R = F_q[X_1, \ldots, X_m]$. Let ρ be the order function associated to the graded lexicographic order on the monomials of R. Let f_i be the i^{th} monomial with respect to this order. Let $n = q^m$. Let $P_1, \ldots, P_n$ be an enumeration of the n points of $F_q^m = \mathcal{P}$. Then $RM_q(r, m)$ is by definition the code obtained by evaluating all $f \in F_q[X_1, \ldots, X_m]$ of degree at most r at all points of $\mathcal{P}$. If $f_l = X_1^r$, then $f_{l+1} = X_m^{r+1}$ and $\{f_i \mid i \leq l\}$ is the set of all monomials of degree at most r. So $RM_q(r, m) = ev_{\mathcal{P}}(L_l) = E_l$. Hence C_l is the dual of $RM_q(r, m)$, which is equal to $RM_q(m(q-1) - r - 1, m)$. The minimum distance of Reed-Muller codes is well-known. It is also a consequence of the theory developed above, as we will now demonstrate.

Proposition 3.22
1) *If* $f_{l+1} = X^\gamma$, *then* $\nu_l = \prod_{t=1}^m (\gamma_t + 1)$.
2)

$$d_{ORD}(l) = \begin{cases} \deg(f_l) + 2 & \textit{if } f_l = X_1^r, \\ \deg(f_l) + 1 & \textit{otherwise.} \end{cases}$$

3) *Let* $f_l = X_1^r$. *Write* $r + 1 = \nu(q-1) + \mu$ *with* $\nu, \mu \in N_0$ *such that* $\mu < q - 1$. *Then* $d(C_l) = d_{ORD,\mathcal{P}}(l) = (\mu + 1)q^\nu$.

Proof.
1) If $f_i = X^\alpha$, $f_j = X^\beta$, then $f_l = X^{\alpha+\beta}$ for some l. So $l(i, j) = l$. So if $f_{l+1} = X^\gamma$, then ν_l is equal to the number of pairs (i, j) such that $f_i f_j = f_{l+1}$, which is equal to the number of all $\alpha \in N_0^m$ such that $0 \leq \alpha_t \leq \gamma_t$ for all t, $1 \leq t \leq m$, which is $\prod(\gamma_t + 1)$.
2) If $f_l = X_1^r$, then $f_{l+1} = X_m^{r+1}$. So $\nu_l = r + 2 = \deg(f_l) + 2$, and

$$\nu_{l'} = \prod(\gamma_t + 1) \geq (\sum \gamma_t) + 1 = \deg(f_{l'+1}) + 1 \geq \deg(f_l) + 2,$$

where $f_{l'+1} = \prod X^\gamma$, for all $l' \geq l$. Hence $d_{ORD}(l) = \deg(f_l) + 2$.
If f_l is not of the form X_1^r, then $f_{l_0+1} = X_1^r$ for some $l_0 \geq l$ and $r = \deg(f_l)$. So $\nu_{l_0} = r + 1$ and $\nu_{l'} \geq r + 1$ for all $l' \geq l$. Hence $d_{ORD}(l) = \deg(f_l) + 1$.
3) If $f_{l'+1} = X^\gamma$, then the code $C_{l'}$ is not equal to $C_{l'+1}$ if and only if $0 \leq \gamma_t \leq q - 1$ for all t. Hence

$$d_{ORD,\mathcal{P}}(l) = \min\{ \prod(\gamma_t + 1) \mid \sum \gamma_t \geq r + 1 \text{ and } 0 \leq \gamma_t \leq q - 1 \text{ for all } t \},$$

if $f_l = X_1^r$. Consider f defined by $f(\mathbf{x}) = \prod(x_t + 1)$ as a real function on the domain $\{\mathbf{x} \in R^m \mid \sum \gamma_t \geq r + 1 \text{ and } 0 \leq x_t \leq q - 1 \text{ for all } t \}$. The method of the multipliers of Lagrange gives that the minimum of f is obtained in the corner $(0, \ldots, 0, \mu, q - 1, \ldots, q - 1)$, where the last ν coordinates are equal to $q - 1$. Hence $d_{ORD,\mathcal{P}}(l) = (\mu + 1)q^\nu$. We refer to the literature for the fact that there are codewords in C_l with this weight.

4 Concluding Remarks

Let $P_1, P_2, \ldots, P_n, P_\infty$ be a set of F_q-rational points on a nonsingular, irreducible curve of genus g defines over F_q. The algebraic geometry codes $C_L(D,G)$ and $C_L(D,G)^\perp$ where $D = P_1 + \cdots + P_n$, $G = mP_\infty$, are a subclass of the codes E_l and C_l respectively. In this case $R = \bigcup_{m=1}^{\infty} L(mP_\infty)$ and $\rho : R \to N_0 \cup \{-\infty\}$ is defined by $\rho(f) = -\nu_{P_\infty}(f)$, where ν_{P_∞} is the valuation at infinity. It then follows from properties of valuations that this ρ indeed is a weight function. This implies that the so-called one-point algebraic geometry codes can be understood as a special case of the codes treated in section 3. Many other classes of codes can also be treated and it is indeed possible to give fast decoding algorithms as well. For further results on this we refer to [9].

References

[1] V.D. Goppa, "Codes associated with divisors," *Probl. Peredachi Inform.* vol. 13 (1), pp. 33-39, 1977. Translation: *Probl. Inform. Transmission*, vol. 13, pp. 22-26, 1977.

[2] M.A. Tsfasman, S.G. Vlăduţ and T. Zink, "Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilbert bound," *Math. Nachrichten*, vol. 109, pp. 21-28, 1982.

[3] J. Justesen, K.J. Larsen, H. Elbrønd Jensen, A. Havemose and T. Høholdt, "Construction and decoding of a class of algebraic geometric codes," *IEEE Trans. Inform. Theory*, vol. IT-35, pp. 811-821, July 1989.

[4] G.-L. Feng and T.R.N. Rao, "Decoding of algebraic geometric codes up to the designed minimum distance," *IEEE Trans. Inform. Theory*, vol. IT-39, pp. 37-45, Jan. 1993.

[5] G.-L. Feng and T.R.N. Rao, "A simple approach for construction of algebraic-geometric codes from affine plane curves," *IEEE Trans. Inform. Theory*, vol. IT-40, pp. 1003-1012, July 1994.

[6] G.-L. Feng, V. Wei, T.R.N. Rao and K.K. Tzeng, "Simplified understanding and efficient decoding of a class of algebraic-geometric codes," *IEEE Trans. Inform. Theory*, vol. IT-40, pp. 981-1002, July 1994.

[7] G.-L. Feng and T.R.N. Rao, "Improved geometric Goppa codes," Part I: Basic Theory, *IEEE Trans. Inform. Theory*, pp. 1678-1693, Nov. 1995.

[8] R. Pellikaan, "On the existence of order functions," Proceedings of the 2nd Shanghai conference on designs, codes and finite geometries, to appear 1997.

[9] R.A. Brualdi, W.C. Huffmann and V.S. Pless eds.: Handbook on Coding Theory, Elsevier Amsterdam, to appear.