

Available online at www.sciencedirect.com



Discrete Applied Mathematics 154 (2006) 392-398

DISCRETE APPLIED MATHEMATICS

www.elsevier.com/locate/dam

Some subsets of points in the plane associated to truncated Reed–Muller codes with good parameters

Ronan Quarez

IMR (CNRS, URA 305), Université de Rennes 1, Campus de Beaulieu, 35042 Rennes Cedex, France

Received 27 June 2003; received in revised form 27 October 2004; accepted 21 March 2005 Available online 30 September 2005

Abstract

We gives some examples of subsets of points in the projective plane associated to truncated generalized projective Reed–Muller codes with good parameters, of dimensions 6 and 10 over GF(7), GF(8) and GF(9). © 2005 Elsevier B.V. All rights reserved.

Keywords: Arcs in finite plane; Bézout's theorem; Generalized Reed-Muller codes

1. Introduction

We use the standard notation [n, k, d] to denote the parameters of a linear code C over GF(q). As usual n stands for its length, k its dimension and d its minimal distance. We say that C is an [n, k, d]-code over GF(q).

We say that the code *C* of parameters [n, k, d] is optimal if there is no [n, k, d+1]-code. We will refer to E. Brouwer's table [2] to get the known lower and upper bounds for the minimal distance (given *n* and *k*). We will say that a code meets (resp. beats) the record if it reaches the lower bound of Brouwer (resp. if it gives a better lower bound).

In this paper, we consider truncated Reed–Muller codes obtained by evaluating polynomials at a given subset of points in the projective plane.

Let PG(m, q) be the *m*-dimensional projective space over GF(q) and let $H_q(m, l)$ be the GF(q)-vector space of all homogeneous polynomials of degree l in m + 1-variables. Let $\Omega \subset PG(m, q)$ be a subset of cardinality $|\Omega| = \omega$. We consider an arbitrary ordering of the points of Ω , say $\Omega = \{A_1, \ldots, A_{\omega}\}$. Then we define a GF(q)-linear evaluation map

$$\begin{split} \Phi_{\Omega}: & H_q(m,l) & \to & GF(q)^{\,\omega} \\ & P & \mapsto & (P(A_1),\ldots,P(A_{\omega})). \end{split}$$

Its image $\Phi_{\Omega}(H_q(m, l))$ is a linear code $C_{\Omega}(m, l)$ over GF(q) of length ω . Moreover, if Φ_{Ω} is injective, then $C_{\Omega}(m, l)$ has dimension $\binom{m+l}{m}$. To shorten notations in the planar case, we will denote $C_{\Omega}(2, l)$ by $C_{\Omega}(l)$.

When $\Omega = PG(m, q)$ we get the so-called projective Reed–Muller codes [3]. If Ω is an algebraic subset then Bézout's Theorem gives a bound on the minimal distance as we see in Section 1 (following [5]).

E-mail address: ronan.quarez@univ-rennes1.fr.

⁰¹⁶⁶⁻²¹⁸X/\$ - see front matter 0 2005 Elsevier B.V. All rights reserved. doi:10.1016/j.dam.2005.03.018

The idea of the following sections is to take for Ω a (κ , ν)-arc in the projective plane which is a subset of κ points in PG(2, q) such that some ν but no $\nu + 1$ are collinear. Then, we generalize this idea and introduce the notion of a (κ , ν , 2)-arc in the projective plane and show how it produces some new codes over GF(7), GF(8), GF(9) of dimensions 6 and 10.

2. Codes from Bézout's Theorem

Let χ be an absolutely irreducible projective curve of genus g over GF(q). The Hasse–Weil bound says that its number of GF(q)-rational points satisfy $|\chi(GF(q))| \leq q + 1 + 2g\sqrt{q}$. Curves which reach the Hasse–Weil bound are called maximal.

Table 1 gives, for small q, the maximum number of GF(q)-rational points of a projective absolutely irreducible curve of given genus g:

Let $F \in H_q(2, l)$ and denote by Z(F) the locus of zeros of F in PG(2, q) and let N(F) = |Z(F)| their number. If F is absolutely irreducible of degree l over GF(q), we have

$$N(F) \leqslant q + 1 + \frac{(l-1)(l-2)}{2} \lfloor 2\sqrt{q} \rfloor,$$

since the genus g of the algebraic projective plane curve given by the equation F = 0 of degree l is such that $g \leq (l - 1)(l - 2)/2$ (equality holds if the curve is non-singular).

We illustrate the construction given in [5, Theorem 2.27], writing down the result obtained by Bézout's Theorem:

Theorem 2.1. Let $F \in H_q(3, l')$ be such that F = 0 is the equation of an irreducible non-singular plane curve. Let $\Omega = Z(F)$ and let l be an integer such that $|\Omega| > ll'$. Then, $C_{\Omega}(l)$ is a linear code over GF(q) with parameters:

- $n = |\Omega|,$
- $d \ge n ll'$

•
$$k = \begin{cases} \left(\frac{l+2}{2}\right) & \text{if } l < l' \\ ll' + 1 - \left(\frac{l'-1}{2}\right) & \text{if } l \ge l' \end{cases}$$

To use Theorem 2.1, we are obviously interested in curves with many points (maximal curves for instance) in order to get codes with good parameters.

Example. We take as an example, $\Omega = Z(X^3Y + Y^3Z + Z^3X)$ where $X^3Y + Y^3Z + Z^3X = 0$ is the equation of a projective non-singular maximal plane curve over GF(8). Then $C_{\Omega}(l)$, with l = 2, 3, 4, 5, are codes of parameters [24, 6, ≥ 16], [24, 10, ≥ 12], [24, 14, ≥ 8], [24, 18, ≥ 4]. To compare with the parameters of records [24, 6, 16], [24, 10, 12], [24, 14, 8], [24, 18, 5].

Table 1 Maximal number of GF(q)-rational points

q	2	3	4	5	7	8	9	11	13	16
g = 1	5	7	9	10	13	14	16	18	21	25
g = 2	6	8	10	12	16	18	20	24	26	33
g = 3	7	10	14	16	20	24	28	28	32	38

3. Configuration of lines in the plane

3.1. Arcs in the plane

Concerning all the notions of this section we refer to [1,4,6] for a survey. A κ -arc in PG(2, q) is a set of κ points no three of which are collinear. The maximum number of points in a κ -arc is denoted by m(2, q). A maximal plane κ -arc is called an *oval*. We have

$$m(2,q) = \begin{cases} q+1 & \text{for } q \text{ odd,} \\ q+2 & \text{for } q \text{ even.} \end{cases}$$

More generally, a (κ, v) -arc in PG(2, q) is a subset of κ points such that some v but no v + 1 are colinear. Again, we denote by $m_v(2, q)$ the maximum number of points in a (κ, v) -arc. We have the trivial values: $m_2(2, q) = m(2, q)$, $m_{q+1}(2, q) = q^2 + q + 1$ and $m_q(2, q) = q^2$ [4]. And for $v \leq q - 1$ "Table 2" is the table of values $m_v(2, q)$ for small q:

We have also the inequality: $m_v(2, q) \leq (v-1)q + v$, and there are many upper bounds when we add some conditions on v. A (κ , v)-arc which satisfies $m_v(2, q) = (v-1)q + v$ is said to be *maximal*. However, we are mostly interested in lower bound, and for instance let us state the following:

Proposition 3.1. We have

- (1) if $q = 2^h$, v = q 2, then $m_v(2, q) \ge (v 1)q + 2$,
- (2) if q is a square, then $m_v(2,q) \ge (q + \sqrt{q} + 1)(v \sqrt{q})$,
- (3) if q is a square and $v = q \sqrt{q}$, then $m_v(2, q) \ge (v 1)q + \sqrt{q}$.

3.2. Truncated Reed-Muller codes

Let $N_q(l, \Omega)$ be the maximal number of zeros in $\Omega \subset PG(2, q)$ of a polynomial in $H_q(2, l)$. We also define arc (Ω) to be the lowest integer v such that Ω does not contain any $(\kappa, v + 1)$ -arc. We have the following:

Proposition 3.2. Let $\Omega \subset PG(2, q)$ and set $\omega = |\Omega|$. If $N_q(l, \Omega) < \omega$, then the evaluation map Φ_Ω is injective and its image $C_{\Omega}(l)$ is a code of parameters

$$\left[\omega, \frac{(l+1)(l+2)}{2}, \omega - N_q(l, \Omega)\right]$$

over GF(q).

Table	2
$m_v(2,$	q)

v	q							
	3	4	5	7	8	9		
2	4	6	6	8	10	10		
3		9	11	15	15	17		
4			16	22	28	28		
5				29	33	37		
6				36	42	48		
7					49	55		
8						65		

Since it is difficult to compute $N_q(l, \Omega)$ in general, we may bound it. Let $I_q(l)$ be the maximal numbers of zeros in PG(2, q) of an absolutely irreducible polynomial in $H_q(2, l)$. Note that we clearly have

 $I_q(l) \leq q + 1 + (l - 1)(l - 2)\sqrt{q}$

by the Hasse-Weil bound.

The following result handle the situation where the maximal numbers of zeros of a polynomial on Ω is bounded by those of a product of linear factors.

Lemma 3.3. Let $\Omega \subset PG(2, q)$ and set $\omega = |\Omega|$. Let $\operatorname{arc}(\Omega) = a$. If $I_a(j) \leq ja$ for all $j \in \{2, \ldots, l\}$, then $N_a(l, \Omega) \leq la$.

Proof. Let $F \in H_q(2, s)$ with $s \leq l$ and let N(F) be its number of zeros. If s = 1 then we obviously have $N(F) \leq a$ since $N_q(1, \Omega) = \operatorname{arc}(\Omega) = a$. Assume now that s > 1.

It is enough to show that $N(F) \leq sa$. We proceed by induction on s. Let $F = f_1 \cdots f_r$ be the decomposition of F into absolutely irreducible factors. If r = 1 then $N_q(F) \leq I_q(s) \leq sa$ by assumption. Then, we may assume that r > 1.

The polynomial f_i has coefficients in a given extension $GF(q^{u(i)})$ of degree u(i) of GF(q). Considering a basis of the GF(q)-vector space $GF(q^{u(i)})$, the equation $f_i = 0$ splits into a system of u(i) polynomial equations over GF(q) which are either the zero equation or equations of degree equal to deg f_i . Pick one such nonzero equation $\tilde{f}_i = 0$. We obviously have $N_q(f_i) \leq N_q(\tilde{f}_i)$ and hence by the induction hypothesis $N(f_i) \leq N(\tilde{f}_i) \leq a \deg f_i$. This concludes the proof. \Box

In the following, the difference between our use of Proposition 3.2 in place of Theorem 2.1 is that, instead of taking Ω to be all the GF(q)-rational points of a maximal curve, we consider for Ω a (κ, ν) -arc with κ as big as possible, namely $\kappa = m_{\nu}(2, q)$.

For instance, when l = 1, we have an easy bound for $N_q(1, \Omega)$. Thus, when l = 1, we may compare codes of dimension 3 obtained by Theorem 2.1 (the Bézout construction with l' = 2) and those obtained from Proposition 3.2 (the arc construction with v = 2).

Examples. 1. Over GF(q), the Bézout construction gives [q + 1, 3, q - 1]-codes, whereas the arc construction gives [q + 1, 3, q - 1]-codes for q odd and [q + 2, 3, q]-codes for q even.

2. For greater length, we can produce a lot of examples where the arc construction (together with Table 2) give better result than the Bézout construction (together with Table 1).

For instance, over GF(7), the Bézout construction yields [13, 3, 10] and [20, 3, 16]-codes, whereas the arc construction yields [15, 3, 12] and [22, 3, 18]-codes.

4. Quadric-arcs and codes

As an application of Proposition 3.2 to codes of dimension 6, we have to bound $N_q(2, \Omega)$, namely to bound the number of zeros of a polynomial P of degree 2 in a subset Ω of PG(2, q).

If *P* is absolutely irreducible (*P* is a conic) then we know that it has at most q + 1 zeros in PG(2, q). And if *P* is reducible, namely a product of two linear factors, then the number of its zeros in Ω is bounded by 2 arc (Ω). So we get

 $N_q(2, \Omega) \leq \max(q+1, 2 \operatorname{arc}(\Omega)),$

which leads to the following result:

Proposition 4.1. If $2v \ge q+1$ then $m_v(2, q) \ge q+1$ and there is a code with parameters $[m_v(2, q), 6, \ge m_v(2, q)-2v]$ over GF(q).

Example. We have

- 1. Let Ω be a (29, 5)-arc in PG(2, 7) (such an arc exists by Table 2). By the Hasse–Weil bound, we have $I_7(2) \leq 7+1=8$ and hence $I_7(2) \leq 2 \operatorname{arc}(\Omega) = 10$. Which defines a [29, 6, 19]-code over GF(7) meeting the record.
- 2. Together with Proposition 3.1, Proposition 4.1 yields the existence of codes over GF(q) with parameters: $[(q + \sqrt{q} + 1)(v \sqrt{q}), 6, (q + \sqrt{q} + 1)(v \sqrt{q}) 2v]$ if q is a square.

Next, to get a more precise bound on $N_q(2, \Omega)$ we introduce the notion of quadric-arc.

Definition. A quadric arc or a $(\kappa, \nu, 2)$ -arc is a set of κ points in PG(2, q) such that some ν but no $\nu + 1$ are the zeros (not counted with multiplicity) of a polynomial of degree 2. Let $m_{\nu,2}(2, q)$ be the maximal number of points in a $(\kappa, \nu, 2)$ -arc.

Of course, we have the following result, which can be seen as a straightforward generalization of Proposition 4.1:

Theorem 4.2. There is a code of parameters $[m_{\nu,2}(2,q), 6, \ge m_{\nu,2}(2,q) - \nu]$ over GF(q).

Since it is difficult to get exact values for $m_{v,2}(2,q)$ in general, we give the following simple ones:

Proposition 4.3. For all q, we have $m_{4,2}(2, q) = 4$, $m_{2q,2}(2, q) = q^2$ and $m_{2q+1,2}(2, q) = q^2 + q + 1$. Furthermore, for very small q, the values of $m_{\nu,2}(2, q)$ are given by Table 3:

Proof. The values of $m_{4,2}(2,q)$ and $m_{2q+1,2}(2,q)$ are obvious. So we will focus on $m_{2q,2}(2,q)$. We need the following elementary result:

Lemma 4.4. Let a be such that $m_{v-1}(2, q) < a \leq m_v(2, q)$ and $a - v > m_{v'}(2, q)$. Then $m_{v+v',2}(2, q) < a$.

Proof. Let $\Omega \subset PG(2, q)$ be such that $|\Omega| = a$. Then, there is a line *L* containing *v* points of Ω . Since $|\Omega \setminus L| = a - v$, there is a line *K* containing v' + 1 points of $\Omega \setminus L$. Thus, the union of the two lines $L \cup K$ contains at least v + v' + 1 points of Ω . \Box

By the inequality $m_v(2, q) \leq (v - 1)q + v$ and Lemma 4.4 (with $(a, v, v') = (q^2 + 1, q + 1, q - 1)$) we deduce that $m_{2q,2} \leq q^2$.

For the converse inequality, we consider q parallel lines in the affine plane, and obviously get $m_{2q,2}(2,q) \ge q^2$. In fact it is the generic example since all (q^2, q) -arcs are projectively equivalent to subsets $\Omega = PG(2, 4) \setminus l$ where l is a line in PG(2, 4) [4, 12.2.1(ii)].

Now, we compute the values of $m_{\nu,2}(2,4)$ for $\nu \in \{5, 6, 7\}$. By Lemma 4.4 with $(a, \nu, \nu') = (10, 4, 1)$ we have $m_{5,2}(2,4) \leq 9$. Likewise $m_{6,2}(2,4) \leq 10$ (take $(a, \nu, \nu') = (10, 4, 1)$) and $m_{7,2}(2,4) \leq 13$ (take $(a, \nu, \nu') = (10, 4, 1)$). Let

$$\begin{split} \Omega_5 &= \{(0, 0, 1), (0, 1, 1), (1, a, 1), (a, 1, 1), (a, 0, 1), (a + 1, a, 1), (1, 1, 1), \\ &\quad (0, 1, 0)\}, \\ \Omega_6 &= \{(0, 0, 1), (0, 1, 1), (1, 0, 1), (0, a, 1), (a, 0, 1), (1, 1, 1), (a + 1, a, 1), \\ &\quad (1, 1, 0), (1, a, 0), (a, 1, 0)\}, \\ \Omega_7 &= \{(0, 0, 1), (0, 1, 1), (1, 0, 1), (0, a, 1), (a, 0, 1), (1, 1, 1), (a + 1, a, 1), \\ &\quad (1, 1, 0), (1, 1, 0), (1, 1, 0), (1, 0, 1), (1, 0, 1), (1, 0, 0), (1, 1, 1), (1, 0$$

(1, a, 1), (a, 1, 1), (a, 1, 1), (1, 1, 0), (1, a, 0), (a, 1, 0).

By a Maple computation on Ω_5 , Ω_6 , Ω_7 , we respectively deduce that $m_{5,2}(2, 4) \ge 8$, $m_{6,2}(2, 4) = 10$ and $m_{7,2}(2, 4) = 13$. So it only remains to show that $m_{5,2}(2, 4) \ne 9$.

The full list of projectively distinct (9, 3)-arcs in PG(2, 4) is given in [4, pp. 355]: a (9, 3)-arc is either of the form $PG(2, 4) \setminus (l_1 \cup l_2 \cup l_3)$ or $PG(2, 4) \setminus (O \cup l \cup l')$ where l_1, l_2, l_3 are distinct lines, O an oval, l = (PQ), l' = (PQ')

Table 3 $m_{v,2}(2,q)$			
ν	q		
	2	3	4
5	7	7	8
6		9	10
7		13	13
8			16
9			21

with $P, Q, Q' \in O$.

- First case: Ω = PG(2, 4)\(l₁ ∪ l₂ ∪ l₃). Send l₃ to infinity. Then consider the parallel lines of l₁ in the affine plane AG(2, 4) = PG(2, 4)\{l₃}. They intersect l₁ ∪ l₂ ∪ l₃ at most in one point in AG(2, 4). And hence a product of two of them contains at least 6 points of Ω, a contradiction.
- Second case: $\Omega = PG(2, 4) \setminus (O \cup l \cup l')$. After a change of coordinates, we may assume that P = (0, 0, 1), Q = (0, 1, 0) and (QQ') is the line at infinity (i.e. of equation z = 0). Let D_i be the line of equation x = iz, $i \in GF(4)$. Then the oval O contains exactly 3 points in $AG(2, 4) \setminus D_0$, where AG(2, 4) is the affine plane $PG(2, 4) \setminus \{(QQ')\}$. Necessarily we can find a union of two lines D_i , D_j , where $i, j \in GF(4) \setminus \{0\}$, which contains six points of $\Omega \cap AG(2, 4)$.

This concludes the proof. \Box

5. Further examples and results

5.1. Codes of dimension 6

All the codes of this section are constructed using Theorem 4.2. Our estimates of $m_{2\nu,2}(2,q)$ mainly comes from Lemma 4.4, and sometimes using Bézout's Theorem (to get lower bounds), or even by a direct explicit computation.

Note that we have explicit generating matrices of the codes given below, since the construction of maximal (κ , ν)-arcs and (κ , ν , 2)-arcs of Tables 2 and 3 can be made explicit.

• Over GF(7): We have the elementary inequalities $13 \le m_{6,2}(2,7) \le 15$. Since there is no code of parameters [15, 6, 9] we deduce that $m_{6,2}(2,7) \le 14$. Furthermore, if $m_{6,2}(2,7) = 14$ then we would get a new code [14, 6, 8]. Although, all the computation we have done show only $m_{6,2}(7,2) \ge 13$. We have also $m_{8,2}(2,7) \ge 22$ since $I_7(2) = 8$.

Results: We construct 10 codes of dimension 6 and length ≤ 29 which meet the record.

• Over GF(8) = GF(2)[b] with $b^3 = b + 1$: We have $14 \le m_{6,2}(2, 8) \le 15$. We have also the elementary inequalities $24 \le m_{8,2}(2, 8) \le 28$. In fact, a computation on the set

$$\{ (0, 1, 0), (b^2, b, 1), (b, 1, 1), (b + b^2, b, 1), (1, b + b^2, 1), (1 + b^2, 1 + b^2, 1), (1 + b, b + b^2, 1), (1 + b + b^2, 1 + b^2, 1), (1, 1, 0), (0, 1 + b, 1), (b^2, b + b^2, 1), (b, 1 + b, 1), (b + b^2, b + b^2, 1), (1, 1, 1), (1 + b^2, b^2, 1), (1 + b, 1, 1), (1 + b + b^2, b^2, 1), (0, b^2, 1), (b^2, 1 + b, 1), (b, b^2, 1), (b + b^2, 1 + b, 1), (1, 1 + b^2, 1), (1 + b^2, b, 1), (1 + b, 1 + b^2, 1), (1 + b + b^2, b, 1), (b^2 + b, 1, 0), (b^2 + b + 1, 1, 0) \}$$

shows that $m_{8,2}(2, 8) \ge 27$.

Results: We construct codes with parameters [27 - i, 6, 19 - i] which beat the record for $i \in \{0, 1, 2\}$,

• Over GF(9): We have the elementary inequalities $16 \leq m_{6,2}(2,9) \leq 17$.

Table /

$m_{\nu,2}(2,q)$	$n_{v,2}(2,q)$							
v	q							
	2	3	4	5	7	8	9	
6		9	10	11	13–14	14–15	16–17	
7		13	13	12-15	14-19	15-19	17-21	
8			16	16	22	27-28	28	
9			21	17-24	23-27	29-33	29-33	
10				25	29	33-34	37	
11				31	30-35	34–39	38-43	
12					36	42	48	

We have also $m_{8,2}(2, 9) = 28$ and $m_{12,2}(2, 9) = 48$, $m_{13,2}(2, 9) \ge 49$. *Results*: We construct codes of parameters [48 - i, 6, 36 - i] for $i \in \{0, 1, 2\}$, and also [49, 6, 36], which beat the record.

We end this section by a table of very loose possible ranges of values for $m_{\nu,2}(2,q)$ (Table 4):

To get these values, we mainly used Lemma 4.4 and Table 2.

5.2. Codes of dimension 10

Using Proposition 3.2 with l = 3, we may construct codes of dimension 10. To estimate the minimal distance, we have to bound $N_q(3, \Omega)$ for $\Omega \subset PG(2, q)$. For instance, the Hasse–Weil bound gives

$$N_q(3, \Omega) \leq \max(q + 1 + 2\sqrt{q}, \operatorname{arc}(\Omega) + N_q(2, \Omega)).$$

good bound on $N_q(l, \Omega)$ by Bézout's Theorem.

and also

 $N_q(3, \Omega) \leq \max(q + 1 + 2\sqrt{q}, \operatorname{arc}(\Omega) + q + 1, 3 \operatorname{arc}(\Omega)).$

Results: Over GF(8), we construct [27 - i, 10, 15 - i]-codes which beat the record for $i \in \{0, 1, 2\}$.

We construct also, over GF(7), GF(8) and GF(9), few other codes of dimension 10 which meet the record. It would be natural to try to apply Proposition 3.2 to get codes of higher dimensions (namely of dimension (l + 1)(l + 2)/2 when $l \ge 4$). But when l grows, the Hasse–Weil bound gives a poor bound on $N_q(l)$, and we get codes far from the record. This is in contrast to the Bézout construction where the algebraic nature of the subset Ω ensures a

References

- [1] S.M. Ball, Multiple blocking sets and arcs in finite planes, J. London Math. Soc. 54 (1996) 581-593.
- [2] A.E. Brouwer, Server for bounds on the minimum distance of q-ary linear codes, q = 2, 3, 4, 5, 7, 8, 9, available online at http://www.win.tue.nl/~aeb/voorlincod.html.
- [3] P. Delsarte, J.M. Goethals, F.J. Mac Williams, On generalized Reed–Muller codes and their relatives, Inform. and Control 16 (1970) 403–442.
- [4] J.W.P. Hirschfeld, Projective Geometries over Finite Fields, Oxford University Press, Oxford, 1979.
- [5] T. Hoholt, J.H. van Lint, R. Pellikaan, Algebraic geometry codes, in: Handbook of Coding Theory, vol. 1, Elsevier, Amsterdam, 1998, pp. 871–961.
- [6] I.N. Landjev, Linear codes over finite fields and finite projective geometries, Discrete Math. 213 (2000) 211-244.