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
e-mail : ronan.quarez@univ-rennes1.fr

Keywords : Arcs in finite plane - Bézout's Theorem - Generalized Reed-Muller Codes

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 $H_q(m,l)$ be the $GF(q)$-vector space of all homogeneous polynomials of degree l in m-variables. Let $\Omega \subset PG(m,q)$ be a subset of cardinal $|\Omega| = \omega$. We consider an arbitrary order on the points of Ω, say $\Omega = \{A_1, \ldots, A_\omega\}$. Then we define a $GF(q)$-linear evaluation map

$$\begin{array}{rccc} \Phi_\Omega : & H_q(m+1,l) & \to & GF(q)^\omega \\ & P & \mapsto & (P(A_1), \ldots, P(A_\omega)) \end{array}$$

Its image $\Phi_\Omega(H_q(m+1,l))$ is a linear code $C_\Omega(m+1,l)$ over $GF(q)$ of length ω. Moreover, if Φ_Ω is injective, then $C_\Omega(m+1,l)$ has dimension $\binom{m+l}{m}$. To shorten notations in the planar case, we will denote $C_\Omega(3,l)$ by $C_\Omega(l)$.

When $\Omega = PG(m,q)$ we recover 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 [6]).

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 $(\kappa,\nu,2)$-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.

1 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.

The following table gives, for small q, the precise upper bound for the maximum number of $GF(q)$-rational points of a projective absolutely irreducible curve of given genus g :

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

Table 1: maximal number of $GF(q)$-rational points

Let $F \in H_q(3,l)$ and denote by $Z(F)$ the locus of zeros of F in $PG(2,q)$ and $N(F) = |Z(F)|$ their number. If F is absolutely irreducible of degree l over $GF(q)$, we have $N(F) \leq q+1+\frac{(l-1)(l-2)}{2}\lfloor 2\sqrt{q}\rfloor$, since the genus g of the algebraic projective plane curve given by the equation $F=0$ of degree l is such that $g \leq \frac{(l-1)(l-2)}{2}$ (the equality holds if the curve defined by the equation $F=0$ is non-singular).

We illustrate the construction given in [6, Th 2.27], writing down the result obtained by Bézout's theorem :

Theorem 1.1 *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 l be an integer such that $|\Omega| > ll'$. Then, $C_\Omega(l)$ is a linear code over $GF(q)$ with parameters :*

- $n = |\Omega|$,
- $d \geq n - ll'$
- $k = \begin{cases} \binom{l+2}{2} & if\ l < l' \\ ll' + 1 - \binom{l'-1}{2} & if\ l \geq l' \end{cases}$

To use 1.1, we are obviously interested in curves with many points (maximal curves for instance) in order to get codes with good parameters.

Examples Take $GF(7)$ as ground field.

Let $\Omega = Z(F)$ where $F=0$ is the equation of a projective non-singular maximal plane curve of degree 3 (for instance we may take $F = Y^3 - X^2Z + 3Z^3$). Then $C_\Omega(2)$ is a $[13,6,7]$-code which is optimal.

Likewise, if $\Omega = Z(F)$ where $F=0$ is the equation of a plane maximal curve of degree 4, then $C_\Omega(l)$ with $l = 2,3,4$ are codes of parameters respectively $[20,6,\geq 12]$, $[20,10,\geq 8]$, $[19,15,\geq 4]$. To compare with the parameters of records $[20,6,12]$, $[20,10,9]$, $[19,15,4]$.

2 Configuration of lines in the plane

2.1 Arcs in the plane

Concerning all the notions of this section we refer to [1], [5] and [7] for a survey. A κ-*arc* in $PG(2,q)$ is a set of κ points no three of which are colinear. The maximum number of points in a κ-arc is denoted by $m(2,q)$. 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 $(\kappa,\nu)-arc$ in $PG(2,q)$ is a subset of κ points such that some ν but no $\nu+1$ are colinear. Again, we denote by $m_\nu(2,q)$ the maximum number of points in a (κ,ν)-arc. We have the trivial values : $m_2(2,q) = m(2,q)$, $m_{q+1}(2,q) = q^2+q+1$ and $m_q(2,q) = q^2$ ([5]). And for $\nu \leq q-1$ here is the table of values $m_\nu(2,q)$ for small q :

ν \ 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

Table 2: $m_\nu(2,q)$

2.2 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 $H_q(3,l)$. We also define arc (Ω) to be the lowest integer ν such that Ω does not contain any $(\kappa,\nu+1)$-arc. We have the following :

Proposition 2.1 *Let $\Omega \subset PG(2,q)$ and set $\omega = |\Omega|$. If $N_q(l,\Omega) < \omega$, then the evaluation map Φ_Ω restricted to $H_q(3,l)$ is injective and its image $C_\Omega(l)$ is a code of parameters $[\omega, \frac{(l+1)(l+2)}{2}, \omega - N_q(l,\Omega)]$ over $GF(q)$.*

The difference between 2.1 and 1.1 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 $\kappa = m_\nu(2,q)$.

In general, it is difficult to compute $N_q(l,\Omega)$. But when $l=1$, we have an easy bound. Indeed, when $l=1$, we may compare codes of dimension 3 obtained by Theorem 1.1 (Bézout construction with $l'=2$) and those obtained from Proposition 2.1 (Arc construction with $\nu=2$).

Examples

- Over $GF(q)$, Bézout construction gives $[q+1, 3, q-1]$-codes, whereas Arc construction gives $[q+1, 3, q-1]$-codes for q odd and $[q+2, 3, q]$-codes for q even.
- For greater length, we can produce a lot of examples where Arc construction (together with table 2) give better result than Bézout construction (together with table 1).

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

3 Quadric-arcs and codes

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 $H_q(3, l)$. We clearly have $I_q(l) \leq q + 1 + (l-1)(l-2)\sqrt{q}$ by the Hasse-Weil bound.

As an application of 2.1 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 $2\,\mathrm{arc}\,(\Omega)$.

So we get $N_q(2, \Omega) \leq \max(q+1, 2\,\mathrm{arc}\,(\Omega))$, which lead to the following result :

Proposition 3.1 *If $2\nu \geq q+1$ then $m_\nu(2, q) > q+1$ and there is a code with parameters $[m_\nu(2, q), 6, \geq m_\nu(2, q) - 2\nu]$ over $GF(q)$.*

Example Let Ω be a $(29, 5)$-arc in $PG(2, 7)$ (such an arc exists by Table 2). Since $I_7(2) \leq 7 + 1 = 8$ by the Hasse-Weil bound, we have $I_7(2) \leq 2\,\mathrm{arc}\,(\Omega) = 10$ and hence we find a $[29, 6, 19]$-code over $GF(7)$ which meet the record.

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

Définition *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 degree 2 polynomial. Let $m_{\nu,2}(2, q)$ be the maximal number of points in a $(\kappa, \nu, 2)$-arc.*

It is difficult to get in general exact values for $m_{\nu,2}(2, q)$. We give the following simple ones :

Proposition 3.2 *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, we have the table of $m_{\nu,2}(2, q)$ for very small values of q :*

ν \ q	2	3	4
5	7	7	8
6		9	10
7		13	13
8			16
9			21

Table 3: $m_{\nu,2}(2,q)$

For the proof and also in the following, we need the elementary result :

Lemma 3.3 *Let a be such that $m_{\nu-1}(2,q) < a \leq m_\nu(2,q)$ and $a - \nu > m_{\nu'}(2,q)$. Then $m_{\nu+\nu',2}(2,q) < a$.*

Of course, we have the straightforward generalization of proposition 3.1 :

Proposition 3.4 *There is a code of parameters $[m_{\nu,2}(2,q), 6, \geq m_{\nu,2}(2,q) - \nu]$ over $GF(q)$.*

4 Examples and results

4.1 Codes of dimension 6

All the codes of this section are constructed using Proposition 3.4.

Remark that we have explicit generating matrices of the codes given below, since the construction of maximal (κ,ν)-arcs and $(\kappa,\nu,2)$-arcs we used, can be in tables 2 and 3 can be made explicit.

- Over $GF(7)$:
  We have the elementary inequalities $13 \leq m_{6,2}(2,7) \leq 15$. Since there is no code of parameters $[15,6,9]$ we deduce that $m_{6,2}(2,7) \leq 14$. 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 $m_{6,2}(7,2) \geq 13$.

  We have also $m_{8,2}(2,7) \geq 22$ 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 $14 \leq m_{6,2}(2,8) \leq 15$.

  We have also the elementary inequalities $24 \leq m_{8,2}(2,8) \leq 28$. 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 $m_{8,2}(2,8) \geq 27$.

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

  We also construct 19 codes of dimension 6 and length ≤ 43 which meet the record.

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

  We have also $m_{8,2}(2,9) = 28$.

  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 also construct 41 codes of dimension 6 and length ≤ 65 which meet the record.

4.2 Codes of dimension 10

Using Proposition 2.1 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

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

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.

References

[1] S.M. Ball, Multiple blocking sets and arcs in finite planes, Journal of the London Mathematical Society 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.

[5] J.W.P. Hirschfeld, Projective Geometries over Finite Fields (Oxford Univ. Press, Oxford, 1979).

[6] T. Hoholt, J. H. van Lint, R. Pellikaan, Algebraic geometry codes, in Handbook of Coding Theory, vol. 1 (Elsevier 1998) 871-961.

[7] I.N. Landjev, Linear codes over finite fields and finite projective geometries, Discrete Mathematics 213 (2000) 211-244