Discrete Mathematics 81 (1990) 217–221
North-Holland

COMMUNICATION

THE PARAMETERS OF PROJECTIVE REED–MÜLLER CODES

Gilles LACHAUD
Équipe CNRS "Arithmétique & Théorie de l'Information", C.I.R.M., Luminy Case 916, 13 288 Marseille CEDEX 9, France

Communicated by P. Camion
Received 29 November 1989

Les codes de Reed–Müller projectifs sur un corps fini sont des extensions des codes de Reed–Müller généralisés. Nouse donnons les paramètres de ces codes; leur distance minimale est obtenue en utilisant une borne de Serre. On montre qu'en un certain sens, leurs performances sont meilleures que celles des codes de Reed–Müller usuels.

The projective Reed–Müller codes on a finite field are extensions of the classical generalized Reed–Müller codes. We give the parameters of these codes; we use a bound given by Serre in order to get their minimal distance. We show that in some sense their performances are better than those of the classical Reed-Müller codes.

1. Classical Reed–Müller codes

Let q be a power of a prime number. We recall the construction of the classical generalized Reed–Müller codes on $\boldsymbol{F}_q$ in the case $r < q$ after Delsarte, Goethals and MacWilliams (cf. [2]). Choose an integer $r < q$. Denote by $\boldsymbol{F}_q[X_1, \ldots, X_m]_r$ the space of polynomials of degree $\leqslant r$ with m variables and with coefficients in $\boldsymbol{F}_q$. Since $r < q$, this space can be seen as a space of polynomial functions on the affine space $\boldsymbol{A}^m(\boldsymbol{F}_q) = \boldsymbol{F}_q^m$.

The *classical generalized Reed–Müller code* of order r, which we note $\mathscr{R}_q(r, \boldsymbol{A}^m)$, is the image of the injective map

$$c : \boldsymbol{F}_q[X_1, \ldots, X_m]_r \to \boldsymbol{F}_q^V,$$

where we have put $V = \boldsymbol{A}^m(\boldsymbol{F}_q)$, defined by

$$c(P) = (P(x))_{x \in V}.$$

This code is such that

$$\text{length } \mathscr{R}_q(r, \boldsymbol{A}^m) = q^m, \qquad \dim \mathscr{R}_q(r, \boldsymbol{A}^m) = \binom{r+m}{m};$$

since the maximal number of zeroes in $\boldsymbol{A}^m(\boldsymbol{F}_q)$ of a polynomial of degree r is equal to rq^{m-1} (cf. [5], thm. 6.13 p. 275), the minimal distance of this code is equal to

$$\text{dist } \mathscr{R}_q(r, \boldsymbol{A}^m) = (q - r)q^{m-1}.$$

2. Projective Reed–Müller codes

We note $\boldsymbol{P}^m(\boldsymbol{F}_q)$ the projective space of dimension m over the finite field $\boldsymbol{F}_q$ with q elements. In order to fix the notations, recall that there is a canonical projection

$$\pi : \boldsymbol{A}^{m+1}(\boldsymbol{F}_q) - \{0\} \to \boldsymbol{P}^m(\boldsymbol{F}_q);$$

we set $(x_0 : \ldots : x_m) = \pi(x_0, \ldots, x_m)$; thus $(\lambda x_0 : \ldots : \lambda x_m) = (x_0 : \ldots : x_m)$ for any $\lambda \in \boldsymbol{F}_q^x$. For $0 \leqslant i \leqslant m$, we note x_i the coordinate function of index i on $\boldsymbol{A}^{m+1}(\boldsymbol{F}_q)$. Let U_i be the set $(x_i \neq 0)$ in $\boldsymbol{A}^{m+1} - \{0\}$, and set $V_i = \pi(U_i)$; the family $(V_i)_{0 \leqslant i \leqslant m}$ is a covering of $\boldsymbol{P}^m(\boldsymbol{F}_q)$. Let

$$W_0 = V_0, \quad W_1 = V_1 - V_0, \quad W_2 = V_2 - (V_0 \cup V_1), \quad \text{etc.},$$

thus $x = (x_0 : \cdots : x_m) \in W_i$ if and only if $x_1 = \cdots = x_{i-1} = 0$, and $x_i \neq 0$. The family $(W_i)_{0 \leqslant i \leqslant m}$ is a partition of $\boldsymbol{P}^m(\boldsymbol{F}_q)$. The set W_i is an affine subspace of dimension $m - i$, hence $\# W_i = q^{m-i}$, and we recover the familiar formula

$$\# \boldsymbol{P}^m(\boldsymbol{F}_q) = \pi_m = q^m + q^{m-1} + \cdots + 1.$$

We denote by $\boldsymbol{F}_q[X_0, \ldots, X_m]_r^0$ the vector space of those $P \in \boldsymbol{F}_q[X_0, X_1, \ldots, X_m]$ such that P is homogeneous and $\deg(P) = r$. If $P \in \boldsymbol{F}_q[X_1, \ldots, X_m]_r$, define

$$\bar{P}(X_0, X_1, \ldots, X_m) = X_0^r P(X_1/X_0, \ldots, X_m/X_0);$$

then $\bar{P} \in \boldsymbol{F}_q[X_0, \ldots, X_m]_r^0$; the map $P \to \bar{P}$ is an isomorphism

$$\boldsymbol{F}_q[X_1, \ldots, X_m]_r \xrightarrow{\sim} \boldsymbol{F}_q[X_0, \ldots, X_m]_r^0;$$

we therefore also have

$$\dim \boldsymbol{F}_q[X_0, \ldots, X_m]_r^0 = \binom{m+r}{r}.$$

Now let $V = \boldsymbol{P}^m(\boldsymbol{F}_q)$; we define a linear map

$$\boldsymbol{c} : \boldsymbol{F}_q[X_0, \ldots, X_m]_r^0 \to \boldsymbol{F}_q^V$$

in the following way: firstly for $x \in \boldsymbol{P}^m(\boldsymbol{F}_q)$ and $P \in \boldsymbol{F}_q[X_0, \ldots, X_m]_r^0$ we set

$$\boldsymbol{c}_x(P) = \frac{P(x_0, \ldots, x_m)}{x_i^r} \quad \text{if } x = (x_0 : \ldots : x_m) \in W_i;$$

the value of $\boldsymbol{c}_x(P)$ is unchanged if we replace $(x_0 : \cdots : x_m)$ by $(\lambda x_0 : \cdots : \lambda x_m)$; this value thus depends only on $x \in \boldsymbol{P}^m(\boldsymbol{F}_q)$ and not of the choosen representant of x in $\boldsymbol{A}^{m+1}(\boldsymbol{F}_q) - \{0\}$. We then define the map $\boldsymbol{c}$ as

$$\boldsymbol{c}(P) = (\boldsymbol{c}_x(P))_{x \in V}.$$

This map $\boldsymbol{c}$ is injective when $r < q$ (as is easily seen by recurrence on m); the image of $\boldsymbol{c}$ defines a code $\mathscr{R}_q(r, \boldsymbol{P}^m) \subset \boldsymbol{F}_q^V$, which we call the *projective Reed–Müller code* of order r on $\boldsymbol{P}^m$. It has been introduced in [7], in the general framework of geometric codes of Goppa (see also [4]).

J.-P. Serre has proved in [8] the following inequality, conjectured by M. Tsfasman:

Theorem 1. *If $P \in \boldsymbol{F}_q[X_0, \ldots, X_m]_r^0$ with $P \neq 0$, if $r \leqslant q+1$, and if*

$$S_P = \{x \in \boldsymbol{P}^m \mid P(x) = 0\},$$

then

$$\#S_P(\boldsymbol{F}_q) \leqslant rq^{m-1} + \pi_{m-2}.$$

Moreover, if $r \leqslant q$, the bound on the right hand side is attained only if $S_P(\boldsymbol{F}_q)$ is a union of r hyperplanes whose intersection contains a subspace of codimension 2.

The number $\#S_P(\boldsymbol{F}_q)$ is equal to the number of $x \in \boldsymbol{P}^m$ such that $\boldsymbol{c}_x(P) = 0$, i.e. to the number of null coordinates of the codeword $\boldsymbol{c}(P)$; since

$$\pi_m - (rq^{m-1} + \pi_{m-2}) = (q - r + 1)q^{m-1},$$

we have the following result, already proved in [4] in the case $r = 2$:

Theorem 2. *Assume $r < q$. The code $\mathscr{R}_q(r, \boldsymbol{P}^m)$ has parameters*

$$\text{length } \mathscr{R}_q(r, \boldsymbol{P}^m) = \pi_m, \qquad \dim \mathscr{R}_q(r, \boldsymbol{P}^m) = \binom{r+m}{r},$$

$$\text{dist } \mathscr{R}_q(r, \boldsymbol{P}^m) = (q - r + 1)q^{m-1}.$$

Examples. 1. For $r = 1$, the space $\boldsymbol{F}_q[X_0, \ldots, X_m]_1^0$ is the space of linear forms on $\boldsymbol{P}^m(\boldsymbol{F}_q)$ and we have

$$\dim \mathscr{R}_q(1, \boldsymbol{P}^m) = m + 1, \qquad \text{dist } \mathscr{R}_q(1, \boldsymbol{P}^m) = q^m;$$

this code attains the Plotkin bound. The code $\mathscr{R}_2(1, \boldsymbol{P}^{m-1})$ is equal to the *simplex code* with parameters $[2^m - 1, m, 2^{m-1}]$.

2. When $m = 1$, the projective Reed–Müller codes are *generalized Reed–Solomon codes* (cf. [6], p. 303). More precisely, take a set $X \subset \boldsymbol{P}^1(\boldsymbol{F}_q)$, with $\#X = n > r$, and define as before a map

$$\boldsymbol{c} : \boldsymbol{F}_q[X_0, X_1]_r^0 \to \boldsymbol{F}_q^X$$

by $\boldsymbol{c}(P) = (\boldsymbol{c}_x(P))_{x \in X}$. The map $\boldsymbol{c}$ is injective (because $\#X > r$), and we then get an MDS code C with

$$\text{length } C = n = \#X, \qquad \dim C = r + 1, \qquad \text{dist } C = n - r.$$

3. Relative parameters and comparison of the two kinds of Reed–Müller codes

The transmission rate

$$R(C) = \frac{\dim C}{\text{length } C}$$

of $\mathcal{R}_q(r, \boldsymbol{P}^m)$ is worse than that of $\mathcal{R}_q(r, \boldsymbol{A}^m)$, since the dimension of these codes is the same; but the relative distance

$$\delta(C) = \frac{\text{dist } C}{\text{length } C}$$

is better, as it is easily seen. For any code C, let

$$\lambda(C) = R(C) + \delta(C) = (\dim C + \text{dist } C)/\text{length } C.$$

The number $\lambda(C)$ can be taken as a measure of the performance of the code C. In this respect, the following result, deduced from Theorem 2, expresses that the performances of projective Reed–Müller codes are better than the classical generalized Reed–Müller codes.

Corollary. *If* $r + 1 \leqslant q$, *if* $m \geqslant 2$, *and* $r \geqslant 2m/(m-1)$, *then*

$$\lambda(\mathcal{R}_q(r, \boldsymbol{P}^m)) > \lambda(\mathcal{R}_q(r, \boldsymbol{A}^m)).$$

Examples. If we take $q = 4$, $m = 3$, $r = 2$, then $\mathcal{R}_4(2, \boldsymbol{A}^3)$ has parameters $[64, 10, 32]$, hence $R = 0.156\ldots$ and $\delta = 0.5$ for this code; on the other hand $\mathcal{R}_4(2, \boldsymbol{P}^3)$ has parameters $[85, 10, 48]$, hence $R = 0.118\ldots$ and $\delta = 0.565\ldots$ for that one; we thus have

$$\lambda(\mathcal{R}_4(2, \boldsymbol{A}^3)) = 0.656\ldots < \lambda(\mathcal{R}_4(2, \boldsymbol{P}^3)) = 0.682\ldots.$$

Also, if we take $q = 8$, $m = 2$, $r = 2$, then $\mathcal{R}_8(2, \boldsymbol{A}^2)$ has parameters $[64, 6, 48]$, here $R = 0.094\ldots$, $\delta = 0.75$; but $\mathcal{R}_8(2, \boldsymbol{P}^2)$ has parameters $[73, 6, 56]$, hence there $R = 0.082\ldots$, $\delta = 0.767\ldots$, and

$$\lambda(\mathcal{R}_8(2, \boldsymbol{A}^2) = 0.844\ldots < \lambda(\mathcal{R}_8(2, \boldsymbol{P}^2)) = 0.849\ldots, \text{ etc.}$$

4. Congruences for the weights of projective Reed–Müller codes

From Ax' theorem (cf. [1], and also [3]), we get:

Theorem 3. *With the notations of Theorem* 1, *assume moreover that* $r < m$. *Then*

$$\#S_P(\boldsymbol{F}_q) \equiv \pi_{b-1} \pmod{q^b},$$

where b *is the greatest integer strictly less than* $(m+1)/r$.

This theorem implies immediately:

Theorem 4. *Assume $r \leq q$ and $r \leq m$. The weights of the projective Reed–Müller code $\mathcal{R}_q(r, \boldsymbol{P}^m)$ satisfy*

$$w \equiv 0 \,(\mathrm{mod}\, q^b),$$

$$(q + 1 - r)q^{m-1} \leq w \leq q^m + \cdots + q^b.$$

Theorem 4 is the analog for projective Reed–Müller codes in any degree and any characteristic of the Corollary 13 in Chapter 15, p. 447 in [6] about affine Reed–Müller codes $\mathcal{R}_q(2, \boldsymbol{A}^m)$, where q is even.

Acknowledgement

I would like to thank S.N. Litsyn, R. Rolland and J. Wolfmann for their interest on this work.

References

[1] J. Ax, Zeroes of polynomials in finite fields, Amer. J. Math. 86 (1964) 255–261.
[2] P. Delsarte, J.M. Goethals and F.J. MacWilliams, On generalized Reed–Müller codes and their relatives, Inform. and Control 16 (1970) 403–442.
[3] J.R. Joly, Équations et variétés algébriques sur un corps fini, Enseign. Math. 19 (1973) 1–117.
[4] G. Lachaud, Projective Reed–Müller codes, in Coding Theory and Applications, Proc. 2nd Int. Colloq., Paris 1986, Lect. Notes Comput. Sci. 311 (1988) 125–129.
[5] R. Lidl and H. Niederreiter, Finite Fields, Enc. of Math. and its Appl., Vol. 20 (Cambridge University Press, Cambridge, 1983).
[6] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-correcting Codes (North-Holland, Amsterdam, 1977).
[7] Yu.I. Manin and S.G. Vladut, Linear codes and modular curves, Itogi Nauki i Tekhniki 25 (1984) 209–257 J. Soviet Math. 30 (1985) 2611–2643.
[8] J.-P. Serre, Letter to M. Tsafasman, dated July 29, 1989.