Discrete Mathematics 338 (2015) 1515–1535

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

On the third weight of generalized Reed–Muller codes

Elodie Leducq

Département de Mathématiques, Bâtiment 425, Faculté des Sciences d'Orsay, Université Paris-Sud, F-91405 Orsay Cedex, France

ARTICLE INFO

Article history:
Received 23 September 2014
Received in revised form 28 December 2014
Accepted 7 March 2015
Available online 9 April 2015

Keywords:
Generalized Reed–Muller codes
Third weight codewords
Affine geometry

ABSTRACT

In this paper, we study the third weight of generalized Reed–Muller codes. Using results from Erickson, we prove under some condition that the third weight of generalized Reed–Muller codes depends on the third weight of generalized Reed–Muller codes of small order with two variables. We are able to determine the third weight and the third weight codewords of generalized Reed–Muller codes of order $r = a(q-1)+b$ with $2 \leq b \leq q-1$, for small b.

1. Introduction

In this paper, we want to determine the third weight and third weight codewords of generalized Reed–Muller codes. Th main result of this article is a description of the third weight and third weight codewords of $R_q(a(q-1)+b, m)$ the generalized Reed–Muller code of length q^m and order $a(q-1)+b$ up to those of $R_q(b, 2)$ for $2 \leq b < \frac{q+3}{2}$. We even get a full description of the third weight and the third weight codewords of $R_q(a(q-1)+b, m)$ in the case where $3 \leq b \leq \frac{q+4}{3}$.

We first introduce some notations:

Let p be a prime number, e a positive integer, $q = p^e$ and $\mathbb{F}_q$ a finite field with q elements.

If m is a positive integer, we denote by B_m^q the $\mathbb{F}_q$-algebra of the functions from $\mathbb{F}_q^m$ to $\mathbb{F}_q$ and by $\mathbb{F}_q[X_1, \ldots, X_m]$ the $\mathbb{F}_q$-algebra of polynomials in m variables with coefficients in $\mathbb{F}_q$.

We consider the morphism of $\mathbb{F}_q$-algebras $\varphi : \mathbb{F}_q[X_1, \ldots, X_m] \to B_m^q$ which associates to $P \in \mathbb{F}_q[X_1, \ldots, X_m]$ the function $f \in B_m^q$ such that

$$\forall x = (x_1, \ldots, x_m) \in \mathbb{F}_q^m, \quad f(x) = P(x_1, \ldots, x_m).$$

The morphism φ is onto and its kernel is the ideal generated by the polynomials $X_1^q - X_1, \ldots, X_m^q - X_m$. So, for each $f \in B_m^q$, there exists a unique polynomial $P \in \mathbb{F}_q[X_1, \ldots, X_m]$ such that the degree of P in each variable is at most $q-1$ and $\varphi(P) = f$. We say that P is the reduced form of f and we define the degree $\deg(f)$ of f as the degree of its reduced form. The support of f is the set $\{x \in \mathbb{F}_q^m : f(x) \neq 0\}$ and we denote by $|f|$ the cardinal of its support (by identifying canonically B_m^q and $\mathbb{F}_q^{q^m}$, $|f|$ is actually the Hamming weight of f).

For $0 \leq r \leq m(q-1)$, the rth order generalized Reed–Muller code of length q^m is

$$R_q(r, m) := \{f \in B_m^q : \deg(f) \leq r\}.$$

For $1 \leq r \leq m(q-1) - 2$, the automorphism group of generalized Reed–Muller codes $R_q(r, m)$ is the affine group of $\mathbb{F}_q^m$ (see [2]).

E-mail address: elodie.leducq@u-psud.fr.

http://dx.doi.org/10.1016/j.disc.2015.03.012
0012-365X/© 2015 Elsevier B.V. All rights reserved.

For more results on generalized Reed–Muller codes, we refer to [5].

In the following of the article, we write $r = a(q-1)+b, 0 \leq a \leq m-1, 1 \leq b \leq q-1$.

In [9], interpreting generalized Reed–Muller codes in terms of BCH codes, it is proved that the minimal weight of the generalized Reed–Muller code $R_q(r,m)$ is $(q-b)q^{m-a-1}$. The minimum weight codewords of generalized Reed–Muller codes are described in [5] (see also [11]).

In his Ph.D. thesis [6], Erickson proves that if we know the second weight of $R_q(b,2)$, then we know the second weight for all generalized Reed–Muller codes. From a conjecture on blocking sets, Erickson conjectures that the second weight of $R_q(b,2)$ is $(q-b)q+b-1$. Bruen proves the conjecture on blocking set in [3]. Geil also proves this result in [7] using Groebner basis. An alternative approach can be found in [14] where the second weight of most $R_q(r,m)$ is established without using Erickson's results. Second weight codewords have been studied in [4,15] and finally completely described in [12].

For $q = 2$, small weights and small weight codewords are described in [10], the third weight for $r > (m-1)(q-1)+1$ is given in [7], we can find results on small weight codewords in [1]. In the following, we consider only $q \geq 3$ and $r \leq m(q-1)+1$.

We first give some tools that we will use through all the paper. Then we give an upper bound on the third weight of generalized Reed–Muller codes. In Section 4 is the main result of this article: we describe the third weight of generalized Reed–Muller codes with some restrictive condition. In Section 5, we study more particularly the case of two variables which is quite essential in the determination of the third weight. In Section 6, we described the codewords reaching the third weight. In Section 7, we summarize the results obtain in this article.

2. Preliminaries

2.1. Notation and preliminary remark

Let $f \in B_m^q$, $\lambda \in \mathbb{F}_q$. We define $f_\lambda \in B_m^q$ by

$$\forall x = (x_2, \dots, x_m) \in \mathbb{F}_q^m, \quad f_\lambda(x) = f(\lambda, x_2 \dots, x_m).$$

Let $0 \leq r \leq (m-1)(q-1)$ and $f \in R_q(r,m)$. We denote by S the support of f. Consider H an affine hyperplane in $\mathbb{F}_q^m$, by an affine transformation, we can assume $x_1 = 0$ is an equation of H. Then $S \cap H$ is the support of $f_0 \in R_q(r, m-1)$ or the support of $(1-x_1^{q-1})f \in R_q(r+(q-1), m)$.

2.2. Useful lemmas

Lemma 2.1. *Let $q \geq 3$, $m \geq 3$ and S a set of points of $\mathbb{F}_q^m$ such that $\#S = uq^n < q^m$, $u \not\equiv 0 \mod q$. Then there exists H a hyperplane such that $\#(S \cap H) < uq^{n-1}$.*

Proof. Assume for all H hyperplane, $\#(S \cap H) \geq uq^{n-1}$. Consider an affine hyperplane H; then for all H' hyperplane parallel to H, $\#(S \cap H') \geq u.q^{n-1}$. Since $u.q^n = \#S = \sum_{H'//H} \#(S \cap H')$, we get that for all H hyperplane, $\#(S \cap H) = u.q^{n-1}$.

Now consider A an affine subspace of codimension 2 and the $(q+1)$ hyperplanes through A. These hyperplanes intersect only in A and their union is equal to $\mathbb{F}_q^m$. So

$$uq^n = \#S = (q+1)u.q^{n-1} - q\#(S \cap A).$$

Finally we get a contradiction if $n = 1$ since $u \not\equiv 0 \mod q$. Otherwise, $\#(S \cap A) = u.q^{n-2}$. Iterating this argument, we get that for all A affine subspace of codimension $k \leq n$, $\#(S \cap A) = u.q^{n-k}$.

Let A be an affine subspace of codimension $n+1$ and A' an affine subspace of codimension $n-1$ containing A. We consider the $(q+1)$ affine subspaces of codimension n containing A and included in A', then

$$u.q = \#(S \cap A') = (q+1)u - q\#(S \cap A)$$

which is absurd since $\#(S \cap A)$ is an integer and $u \not\equiv 0 \mod q$. So there exists H_0 a hyperplane such that $\#(S \cap H_0) \leq uq^{n-1}$

The following lemma is proved in [5].

Lemma 2.2. *Let $m \geq 1$, $q \geq 2$, $f \in B_m^q$ and $w \in \mathbb{F}_q$. If for all $(x_2, \dots, x_m)$ in $\mathbb{F}_q^{m-1}$, $f(w, x_2, \dots, x_m) = 0$ then for all $(x_1, \dots, x_m) \in \mathbb{F}_q^m$,*

$$f(x_1, \dots, x_m) = (x_1 - w)g(x_1, \dots, x_m)$$

with $\deg_{x_1}(g) \leq \deg_{x_1}(f) - 1$ *and* $\deg(g) \leq \deg(f) - 1$.

The following lemmas are proved in [6].