Hamming Weights and rational points on algebraic hypersurfaces over finite fields

Adnen SBOUI

December 15th 2010

NANYANG TECHNOLOGICAL UNIVERSITY

School of Physical and Mathematical Sciences

1. Introduction
   - Notations and definitions
   - $GRM(q, d, n)$ and $PRM(q, d, n)$ Codes
2. Results on maximum number of zeros and d_m
   - Affine Case
   - Maximal Hypersurfaces for the affine case
   - the projective case
   - Maximal Hypersurfaces for the projective case
3. weights above the minimum distance
   - The second weight
   - First weight reached by hypersurface not $\mathcal{HA}$
   - Curves with non-linear factors reaching N_3
4. Minimal Arrangement, particular weight
5. Rational points and Generalized Hamming Weight

We denote :

- $\mathbb{F}_q$ a finite field with q elements (q a power of a prime p).
- $\mathbb{F}_q[X_0, X_1, ..., X_n]_d^h \cup \{0\}$ the vector space of homogeneous polynomials in $n+1$ variables with coefficients in $\mathbb{F}_q$ and of degree d.
- $\mathbb{P}^n(\mathbb{F}_q)$ the n-dimensional projective space over $\mathbb{F}_q$.
- $\Pi_n = \#\mathbb{P}^n(\mathbb{F}_q) = \frac{q^{n+1}-1}{q-1}$, the number of rational points of $\mathbb{P}^n(\mathbb{F}_q)$.
- $\Pi_{-1} = 0$ (by convention, which meaning the number of points in the empty set).

We suppose $d \leq n(q-1)$ and $n \geq 2$.

The projective Reed-Muller code $PRM(q,d,n)$ is the image of the map :

$$\begin{array}{rccc} \Phi: & \mathbb{F}_q[X_0, X_1, ..., X_n]_d^h \cup \{0\} & \longrightarrow & \mathbb{F}_q^{\Pi_n} \\ & f & \longmapsto & (evf(v))_{v \in \mathbb{P}^n(\mathbb{F}_q)} \end{array}$$

with
$$\begin{array}{rcl} \mathrm{ev}f : \mathbb{P}^n(\mathbb{F}_q) & \longrightarrow & \mathbb{F}_q \\ v = (x_0 : ... : x_n) & \longmapsto & \frac{f(x_0,...,x_n)}{x_i^d} \end{array}$$

where x_i is the first non-zero component of $v = (x_0 : ... : x_n)$.

- a codeword $c \in PRM(q, d, n)$ is defined by the vector :

  $c = (\text{ev}f(v_1), ..., \text{ev}f(v_{\Pi_n}))$; with $f \in \mathbb{F}_q[X_0, X_1, ..., X_n]^h_d \cup \{0\}$.

- The weight of c is the number of its non-zero coordinates.

- $Z_q(f)$ the set of zeros of f, $\# Z_q(f)$ is the number of points of the hypersurface S defined by f, denoted also $\# S$.

- $N_1 = \max_{f \in \mathbb{F}_q[X_0, X_1, ..., X_n]^h_d} \# Z_q(f)$;

- $\mathcal{P}_1$: the set of non-zero polynomials f such that $\# Z_q(f) = N_1$.

- The first weight, which is the minimum distance, is $w_1 = d_m = \Pi_n - N_1$.

- $N_i = \max_{f \in \mathbb{F}_q[X_0,X_1,\ldots,X_n]_d^h \setminus \{\mathcal{P}_1 \cup \ldots \cup \mathcal{P}_{i-1}\}} \#Z_q(f)$, for $i \geq 2$.

- The i-th weight is $\boxed{w_i = \Pi_n - N_i}$, for $i \geq 1$.

- $\mathcal{P}_i^p$: the set of polynomials $f \in \mathbb{F}_q[X_0, X_1, \ldots, X_n]_d^h$ such that $\#Z_q(f) = N_i$. It is also the number of codewords of weight w_i in $PRM(q,d,n)$.

A generalized classical Reed-Muller codes $GRM(q, d, n)$ is defined as the image of the map

$$\begin{array}{rccc} \Phi : & \mathbb{F}_q[X_1, ..., X_n]_d \cup \{0\} & \longrightarrow & \mathbb{F}_q^{q^n} \\ & f & \longmapsto & (f(v))_{v \in \mathbb{F}_q^n} \end{array}$$

Then, the equivalent numbers, N_i, w_i, $\mathcal{P}_i^a$.. already defined in the projective case follows.

The minimum distance is given firstly by Kasami, Lin and Peterson(1968)

Theorem

For $0 < d < n(q-1)$, with $d = r(q-1) + s$ and $s < q-1$:

(a) *The maximum number of zeros of polynomial in $\mathbb{F}_q[X_1, ..., X_n]_d$ is*

$$N_1 = q^n - (q-s)q^{n-r-1}$$

(b) *The minimum distance of the generalized Reed-Muller codes $GRM(q, d, n)$ is*

$$d_{min} = w_1 = (q-s)q^{n-r-1}.$$

Moreover, Delsarte, Goethals and Mac Williams characterize all polynomials having N_1 zeros.

Theorem

For $0 < d < n(q-1)$, with $d = r(q-1) + s$ and $s < q-1$:
Modulo the action of the automorphism group $G(n,q)$, whose elements acting as permutations of the n coordinates, the associated polynomial of any minimum weight codeword of $GRM(q,d,n)$ is

$$P(x_1, ..., x_n) = t_0 \prod_{i=1}^{r} [1 - (x_i - t_i)^{q-1}] \prod_{j=1}^{s} (x_{r+1} - t'_j) \qquad (1)$$

of degree $d = r(q-1) + s$, where t'_j are distinct elements of $\mathbb{F}_q$ and the t_i are arbitrary elements of $\mathbb{F}_q$, with $t_0 \neq 0$.

The maximal hypersurfaces $\mathcal{H}_1^a$ of degree $d = r(q-1) + s$, associated to the previous polynomials are hyperplane arrangements having the following geometric configuration :

(i) For r directions in $\mathbb{F}_q^n$, we have $q - 1$ parallel hyperplanes in each one,

(ii) in another direction, the $(r+1)$th one, we have s parallel hyperplanes.

➢ The number of minimum weight codewords in $GRM(q, d, n)$ is

$$\#\mathcal{P}_1^a = (q-1)q^r \frac{(q^n-1)(q^{n-1}-1)\ldots(q^{r+1}-1)}{(q^{n-r}-1)(q^{n-r-1}-1)\ldots(q-1)}\eta_s,$$

with

$$\eta_s = \begin{cases} \binom{q}{s}\frac{q^{n-r}-1}{q-1} \text{ if } 0 < s < q-1 \\ 1 \text{ if } s = 0 \end{cases}$$

The minimum distance is given :

Theorem

(a) *For* $0 < d \leq n(q-1)$, *with* $d-1 = r(q-1)+s$ *and* $s < q-1$, *(A. B. Sørensen)*
The maximum number of zeros of an homogeneous polynomial in $\mathbb{F}_q[X_0, X_1, \ldots, X_n]_d^h$ *is*

$$N_1 = \Pi_n - (q-s)q^{n-r-1} \tag{2}$$

(b) *The minimum distance of the projective generalized Reed-Muller codes* $PRM(q,d,n)$ *is*

$$d_m = w_1 = (q-s)q^{n-r-1}.$$

(c) *For* $d \leq q$ *(J.-P. Serre),*
The maximal number of $\mathbb{F}_q$*-rational points is* $N_1 = dq^{n-1} + \Pi_{n-2}$.
This number is reached only by hypersurfaces splits into d *distinct hyperplanes meeting in the same linear subspace of codimension* 2.

a characterization of maximal projective hypersurfaces is given by Rolland (SAGA 2008),

Lemma

A hypersurface, defined by one maximal polynomial P, attaining $N_1 (= \Pi_n - (q - s)q^{n-r-1})$ points is such that : it exists an hyperplane H defined on $\mathbb{F}_q$ such that P vanishes on the whole H, and P restricted to the affine space $\mathbb{P}^n(\mathbb{F}_q) \setminus H$ is a maximal affine hypersurface as described in 2. Therefore P is a product of d homogeneous polynomials of degree 1.

determination of maximal polynomials and the geometric configuration of the corresponding hypersurfaces when $q < d \leq n(q-1)$ (F. ÖZBUDAK and A. SBOUI (2009))

Theorem

The maximum number of zeros $N_1 = \Pi_n - (q-s)q^{n-r-1}$ *is reached by one polynomial in the form :*

$$P(x_0, ..., x_n) = x_0 \prod_{i=1}^{r} [(x_i - t_i x_0)^{q-1} - x_0^{q-1}] \prod_{j=1}^{s} (x_{r+1} - t'_j x_0), \qquad (3)$$

which can be written as product of d linear factors :

$$P(x_0, ..., x_n) = x_0 \prod_{i=1}^{r} \prod_{\alpha \in \mathbb{F}_q \setminus \{t_i\}} (x_i - \alpha x_0) \prod_{j=1}^{s} (x_{r+1} - t'_j x_0), \qquad (4)$$

of degree d, *such that* $d - 1 = r(q-1) + s$, *where* t'_j *are distinct elements of* $\mathbb{F}_q$ *and the* t_i *are arbitrary elements of* $\mathbb{F}_q$.

The maximal hypersurfaces $\mathcal{H}_1^p$ associated to the previous polynomials are hyperplane arrangements having the following geometric configuration :

(a) One hyperplane H_0 considered as hyperplane at the infinity, we denote it often by H_∞.

(b) There are r blocks of $q-1$ hyperplanes in each one, and an $(r+1)$th block of s hyperplanes, such that the hyperplanes of each block meet in a common linear subvariety of codimension 2 contained in H_∞.

(c) The $r+1$ linear subvarieties of codimension 2 contained in H_∞ are in general position, i.e. form an arrangement of $r+1$ hyperplanes in general position in the $(n-1)$-dimensional projective space $H_\infty \cong \mathbb{P}^{n-1}(\mathbb{F}_q)$.

Number of minimum distance codewords of the generalized projective Reed-Muller codes $GRM(q, d, n)$, $d - 1 = r(q-1) + s$.

Corollary

The number of minimum weight codewords in $PRM(q, d, n)$ is

$$\#\mathcal{P}_1^p = \frac{\Pi_n}{d} \#\mathcal{P}_1^a$$

which gives

$$\mathcal{P}_1^p = \frac{(q^{n+1}-1)q^r}{d} \frac{(q^n-1)(q^{n-1}-1)...(q^{r+1}-1)}{(q^{n-r}-1)(q^{n-r-1}-1)...(q-1)} \eta_s,$$

with

$$\eta_s = \begin{cases} \binom{q}{s} \frac{q^{n-r}-1}{q-1} \ \text{if } 0 < s < q-1 \\ 1 \ \text{if } s = 0 \end{cases}$$

The second weight w_2, affine case :

- computation of the second weight $w_2 = q^n - dq^{n-1} + (d-1)q^{n-2}$, for q quite larger than d, by Rolland-Cherdieu. The result is extended by Sboui for $d < q/2$).
- using Gröbner basis theoretical methods (O. Geil (2008)) resolve the case $q/2 < d < q$

the second weight for $d < n(q-1)$ (R. Rolland (2009)) : For $d = a(q-1)+b$, $n \geq 3$, $q \geq 3$ and $q-1 < d \leq (n-1)(q-1)$, the second weight w_2 of $GRM(q,d,n)$ is given by

- for $q = 3$
  - (a) if $1 \leq a \leq n-1$ and $b = 0$ then $w_2 = 4 \times 3^{n-a-1}$;
  - (b) if $1 \leq a < n-1$ and $b = 1$ then $7 \times 3^{n-a-2} \leq w_2 \leq 8 \times 3^{n-a-2}$;
- for $q \geq 4$
  - (a) if $1 \leq a < n-1$ and $2 \leq b < q-1$ then $w_2 = q^{n-a-2}(q-1)(q-b+1)$;
  - (b) if $1 \leq a \leq n-1$ and $b = 0$, then $w_2 = 2q^{n-a-1}(q-1)$;
  - (c) if $1 \leq a < n-1$ and $b = 1$, then $q^{n-a} - 2q^{n-a-2} \leq w_2 \leq q^{n-a}$. ? w_2

Second and third weights w_2, w_3, projective case :
(F. Rodier and A. Sboui) :

- $w_2 = q^n - (d-1)q^{n-1} + (d-2)q^{n-2}$, with $q \geq 2d$.
  This result is extended to $q > d$ when ($q = p$ prime).
- $w_3 = q^n - (d-1)q^{n-1} + 2(d-3)q^{n-2}$, with $q \geq 3d$.
  This result is extended to $q > d + 2$ ($q = p$ prime).

- For $d < \frac{q+1}{2} + 2$, the second and the third weights are reached only by algebraic hypersurfaces which are arrangement of d hyperplanes.
- For $\frac{q+1}{2} + 2 \leq d < q$, the third weight w_3 is also reached by hypersurfaces containing an irreducible quadric.

Example

$$S : f(x_0, ..., x_n) = (x_2^2 - x_0 x_1) x_0 x_1 \prod_{i=1}^{d-4} (x_0 - \alpha_i x_1),$$

where $d = \frac{q+1}{2} + 3$, q odd, the α_i are $d - 4$ $(= \frac{q-1}{2})$ non-squares.

Proposition, case q even

Let C a projective plane curve of degree d over $\mathbb{F}_q$, $d = \frac{q}{2} + t$ and $3 \leq t \leq \frac{q}{2}$, composed of $d-2$ concurrent lines to the same point ω, and a conic $\mathscr{C}$ of nucleus distinct from ω.

If among these lines

- $\frac{q}{2}$ do not intersect $\mathscr{C}$;
- and there is a tangent line to $\mathscr{C}$.

Then $\underline{\#C = N_3}$.

Proposition, case q odd

Let C a projective plane curve of degree d over $\mathbb{F}_q$, $d = \frac{q+1}{2} + t$, $2 \leq t \leq \frac{q-1}{2}$, composed of $d-2$ concurrent lines to the same point ω and a conic $\mathscr{C}$.

If we are in the two following situations :

(a) $\omega \in Int(\mathscr{C})$: among the $d-2$ lines $\frac{q+1}{2}$ do not intersect $\mathscr{C}$;

(b) $\omega \in Ext(\mathscr{C})$: among the $d-2$ lines $\frac{q-1}{2}$ do not intersect $\mathscr{C}$ and two lines are tangent to $\mathscr{C}$.

Then $\underline{\#C = N_3}$.

(Rodier and Sboui)

Projectif case

$\mathcal{A}^d_{min}$: a minimal arrangement of d hyperplanes is such that : for every $1 \leq i, j \leq d$, $i \neq j$, we have $H_i \cap H_j = K^i_j$, where the K^i_j are $\binom{d}{2}$ subspaces of dimension $n-2$ all distinct, and meeting in a common subspace of dimension $n-3$. (2-dimension linear system of hyperplane)

Consequence of $\mathcal{A}^d_{min}$

For $q > \frac{d(d-1)}{2}$

➢ $tr_{H_i}(\mathcal{A}^{d+1}_{min} \setminus H_i) = \mathcal{A}^d_1$ (pencil of hyperplanes) in $\mathbb{P}^{n-1}(\mathbb{F}_q)$

$N(\mathcal{A}^d_{min}) = dq^{n-1} + \Pi_{n-2} - \frac{(d-1)(d-2)}{2} q^{n-2}.$

For $q > \frac{d(d-1)}{2}$

Any algebraic projective hypersurface S of degree d, not union of d hyperplanes, contains less points than any algebraic hypersurface which is the union of d hyperplanes.

$S : f \in \mathbb{F}_q[X_0, X_1, ..., X_n]^h_d$, not product of d linear factors :

$$\#Z_q(f) < N_1 - \frac{(d-1)(d-2)}{2} q^{n-2}$$

Application : Highest weight obtained by an hyperplane arrangement

$$w_{i?} = q^n - (d-1)q^{n-1} + \frac{(d-1)(d-2)}{2} q^{n-2}.$$

Which is the highest weight given by an hyperplane arrangement.

Let C be a $[n, k]$ linear code and D be a subcode.
The support of D, denoted $\chi(D)$, is the set of not-always-zero coordinate positions of D, i.e., $\chi(C) := \{i : \exists(x_1, x_2, ..., x_n) \in C, x_i \neq 0\}$.

A one-dimensional subcode D of C consists of two codewords : the zero codeword, and a nonzero codeword.
The support of D equals to the Hamming weight of the nonzero codeword.

Based on this perspective, we define the rth generalized Hamming weight of C, denoted $d_r(C)$, to be the size of the smallest support of an r-dimensional subcode of C, i.e.,

$d_r(C) := min\{|\chi(D)| : D \text{ is a subcode of } C \text{ with rank } r\}$.

Note that $d_1(C)$ equals to the traditional minimum Hamming d_m weight of C.

The weight hierarchy of a linear code C is defined to be the set of integers $\{d_r(c), 1 \leq r \leq k\}$

Theorem

(Monotonicity) : For an $[n, k]$ linear code C with $k > 0$, we have $0 < d_1(C) < d_2(C) < ... < d_k(C) \leq n$.

The study of generalized Hamming weights has been motivated by several applications in cryptography :

- application to t-resilient functions
- application to cryptography of wire-tap channel of type II. In fact, the generalized Hamming weights characterize the performance of a linear code used for that channel

Geometric interpretation of Generalized Weights

The minimum distance equals the minimal number of points of a projective system lying outside a hyperplane

$d_1 = n - max\{|X \cap H| : H \text{ a hyperplane in } \mathbb{P}^{k-1}(\mathbb{F}_q)\}$

---

and the rth generalized weight equals the minimal number of points outside a linear subspace of codimension r :

$d_r = n - max\{|X \cap \Pi| :$
$\Pi \text{ a projective subspace of codimension r } in\ \mathbb{P}^{k-1}(\mathbb{F}_q)\}$

Generalized Weights for the case of Reed-Muller codes

For higher order Reed-Muller codes the problem is much more subtle and reduces to the following geometric question :

Problem (a) : Let $f_1, ..., f_r$ be linearly independent polynomials in n variables of degree d or less. What is the maximum possible number of solutions in $\mathbb{F}_q^n$ of the system

$$f_1 = ... = f_r = 0$$

For projective Reed-Muller codes the problem reads as follows :

Problem (b) : Let $F_1, ..., F_r$, be linearly independent homogeneous forms in $n+1$ variables of degree d.
What is the maximum possible number of $\mathbb{F}_q$-points on an algebraic set defined by

$$F_1 = ... = F_r = O \ ?$$

Some results

Picture of what is known on the subject :

Corollary

The second generalized Hamming weight of a projective q-ary Reed-Muller codes $PRM(q, d, n)$ of order $d < q - 1$ is equal to

$$d_2 = \Pi_n - (d-1)q^{n-1} - \pi_{n-2} - q^{n-2}$$

Conjecture (Boguslavsky)

the weight hierarchy of a projective q-ary Reed-Muller codes $PRM(q, d, n)$ of order $d < q$ is given by

$$d_r = \Pi_n - \sum_{i=j}^{n} \alpha_i (\Pi_{n-1} - \Pi_{n-i-j}) + \Pi_{n-2}$$

where α_i are such that $x_0^{\alpha_0} x_1^{\alpha_1} ... x_n^{\alpha_n}$ is the rth (in lexicographical order) monomial of degree d in $n+1$ variables, and j is the smallest integer such that $\alpha_j \neq 0$.