A,C,-,, ,um,n,, ,,r,e,lle, ,r,n,e, ,,, 14 – ,,, 1,, ,,,1

On Hyperbolic Codes

O. Geil
Aalborg University
Department of Mathematics
Fr. Bajersvej 7G, 9220 Aalborg Ø
Denmark
Email: olav@math.auc.dk

T. Høholdt
Technical University of Denmark
Department of Mathematics
Bldg. 303 DK-2800 Lyngby
Denmark
Email: tom@mat.dtu.dk

Abstract — **We give a new description of the so-called hyperbolic codes from which the minimum distance and the generator matrix are easily determined. We also give a method for the determination of the dimension of the codes and finally some results on the weight hierarchy are presented.**

I. Introduction

In [5] Saints and Heegard considered a class of codes called hyperbolic cascaded Reed-Solomon codes which can be seen as an improvement of the generalized Reed-Muller codes $\mathrm{RM}_q(r,2)$. The construction was further generalized by Feng and Rao in [1] to an improvement of the generalized Reed-Muller codes $\mathrm{RM}_q(r,m)$ for arbitrary m. Feng et al. also estimated the minimum distance of the new codes. The codes were further studied in [4] and [2] where the minimum distance was estimated by means of order functions and it was shown using the theory of order domains that the codes are asymptotically bad with respect to the order bound and the codes were renamed hyperbolic codes. By use of the so-called footprint from Gröbner basis theory we construct a class of codes where the minimum distance is easy to determine. We then show that these codes are actually the hyperbolic codes, thereby obtaining generator matrices of these, and give a method for the determination of the dimension. It follows that the estimation in [4] of the minimum distance of the hyperbolic codes actually gives the correct minimum distance. We show how to estimate, and in certain cases find, the generalized Hamming weights of the codes.

II. A class of codes with known minimum distance

We give a new description of a class of codes related to $\mathbb{F}_q[X_1,\ldots,X_m]$, $m \geq 1$. The presentation of the codes relies on the Gröbner basis theoretical concept of a footprint.

Definition 1 *Assume we are given an ideal*

$$I = \langle F_1(X_1,\ldots,X_m),\ldots,F_l(X_1,\ldots,X_m)\rangle \subseteq \mathbb{F}_q[X_1,\ldots,X_m]$$

and a monomial ordering $\prec$ on the set $\mathcal{M}_m$ of monomials in the variables $X_1,\ldots,X_m$. The footprint $\Delta_\prec(I)$ of I with respect to $\prec$ is the set of monomials in $\mathcal{M}_m$ that can not be found as a leading monomial of any polynomial in I.

Definition 2 *Given a polynomial ring $\mathbb{F}_q[X_1,\ldots,X_m]$ and an indexing $\mathbb{F}_q^m = \{P_1,P_2,\ldots,P_n\}$, where $n = q^m$. Consider the evaluation map*

$$ev : \begin{cases} \mathbb{F}_q[X_1,\ldots,X_m] & \to \quad \mathbb{F}_q^n \\ F & \mapsto \quad (F(P_1),\ldots,F(P_n)) \ . \end{cases}$$

Define the map

$$D : \begin{cases} \mathcal{M}_m & \to \quad \mathbb{N}_0 \\ M & \mapsto \quad \#\Delta_\prec(\langle M, X_1^q,\ldots,X_m^q\rangle) \end{cases}$$

and let $E(s) := Span_{\mathbb{F}_q}\{ev(M) \mid M \in \mathcal{M}_m,\ D(M) \leq s\}$.

Note that the value $D(M)$ is easily calculated. It is simply the number of monomials in $\mathcal{M}_m$ that are not divisible by any of the monomials $M, X_1^q,\ldots,X_m^q$.

Definition 3 *We define $\mathcal{M}_m^{(q)}(s) := \{M \in \mathcal{M}_m \mid \deg_{X_i} < q$ for $i = 1,\ldots,m,$ and $D(M) \leq s\}$.*

We have $E(s) = \mathrm{Span}_{\mathbb{F}_q}\{\mathrm{ev}(M) \mid M \in \mathcal{M}_m^{(q)}(s)\}$. In order to estimate/find the minimum distance of the codes given in Definition 2 we will need the following result known as the footprint bound.

Theorem 4 *Assume we are given an ideal I and a monomial ordering $\prec$ such that $\Delta_\prec(I)$ is a finite set. Then the size of $\Delta_\prec(I)$ is independent of the actual choice of $\prec$. The number of common solutions in $\mathbb{F}_q^m$ of $F_1(X_1,\ldots,X_m)$,..., $F_l(X_1,\ldots,X_m)$ is at most equal to $\#\Delta_\prec(I)$.*

We get.

Proposition 5 *The code $E(s)$ is of length $n = q^m$ and minimum distance $d \geq q^m - s$.*

Whenever s is chosen properly we can say even more.

Definition 6 *Define*

$$S := \{D(M) \mid M \in \mathcal{M}_m, \deg_{X_i} < q,\ i = 1,\ldots,m\} \ .$$

Theorem 7 *For any $s' \in \mathbb{N}_0$ there exists a unique $s \in S$ such that $E(s') = E(s)$. The minimum distance of $E(s)$ is given by $d = q^m - s$.*

III. Hyperbolic codes

In [4, p. 922] the so-called hyperbolic codes are considered.

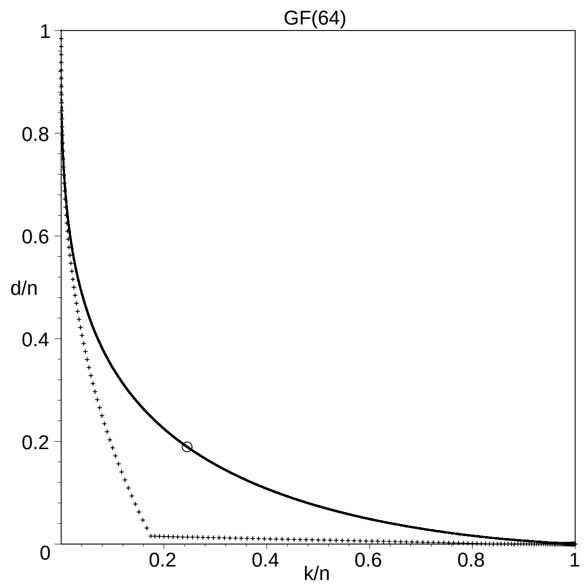
Definition 8 *Let $\mathcal{N}_m^{(q)}(s) := \{X_1^{a_1}\cdots X_m^{a_m} \in \mathcal{M}_m \mid a_i < q$, for $i = 1,\ldots,m,\ \prod_{i=1}^m (a_i+1) < q^m - s\}$.*

The hyperbolic codes are now defined as follows.

Definition 9

$$Hyp_q(s,m) := \{\underline{c} \in \mathbb{F}_q^n \mid \langle \underline{c}, ev(M)\rangle = 0 \text{ for all } M \in \mathcal{N}_m^{(q)}(s)\}.$$

Here $n = q^m$ and $\langle\ ,\ \rangle$ is the standard inner product in $\mathbb{F}_q^n$.



In [4] the minimum distance of these codes is estimated using the order bound. One gets $d(\mathrm{Hyp}_q(s,m)) \geq q^m - s$. By Theorem 7 and the following result this estimate is actually equal to the true minimum distance of the hyperbolic code.

Theorem 10 *Consider* $\mathbb{F}_q[X_1,\ldots,X_m]$ *and* $s \in S$, *then* $E(s) = Hyp_q(s,m)$.

It follows from Theorem 10 that we now have the generator matrices of the hyperbolic codes. For $a \in \mathbb{N}$ we define

$$V(m,a) := \#\{(x_1,\ldots,x_m) \mid x_i \in \mathbb{N}, 1 \leq x_i \leq q, \\ i=1,\ldots,m,\ \textstyle\prod_{i=1}^{m} x_i \leq a\}$$

then it follows from above that $\dim(\mathrm{Hyp}_q(s,m)) = q^m - V(m,q^m-s-1)$. It is not obvious how to get a closed form expression for $V(m,a)$ but since $V(1,a) = \min\{a,q\}$ and $V(m,a) = \sum_{j=1}^{q} V(m-1, \lfloor \frac{a}{j} \rfloor)$ we can easily calculate $V(m,a)$ recursively. One can verify that $V(2,a) = bq + \sum_{j=b+1}^{\min\{a,q\}} \lfloor \frac{a}{j} \rfloor$ where $b := \min\{\lfloor \frac{a}{q} \rfloor, q\}$ and the last sum is zero if $b \geq q$.

The description in [4] of the hyperbolic codes is based on order domain theory. From the theory in [4] it is clear that the hyperbolic code construction is an improvement of the generalized Reed-Muller code construction.

Example 11 *There are* 190 *different generalized Reed-Muller codes* $RM_{64}(r,3)$ *and* 14 224 *different hyperbolic codes* $Hyp_{64}(s,3)$. *These codes are of length* $n = 262\,144$. *In the figure every* + *corresponds to a generalized Reed-Muller code of the given parameters. The graph marked with a* $\circ$ *corresponds to the hyperbolic codes. It appears that given a generalized Reed-Muller code, then in almost all cases there are hyperbolic codes that are of larger minimum distance and are of larger dimension.*

It is well-known that generalized Reed-Muller codes are asymptotically bad and it follows from [2, Corollary 2] that the hyperbolic codes are also asymptotically bad since their minimum distance as we have shown equals the order bound.

IV. The generalized Hamming weights

As demonstrated below the hth generalized Hamming weight of the hyperbolic code $\mathrm{Hyp}_q(m,s)$ is related to the following number.

Definition 12

$$\eta_h(q,s,m) := \max\{\#\Delta_\prec(\langle M_1,\ldots,M_h,X_1^q,\ldots,X_m^q\rangle) \mid \\ M_i \neq M_j \textit{ for } i \neq j,\ M_i \in \mathcal{M}_m^{(q)}(s) \textit{ for } i=1,\ldots,h\}\ .$$

Note that the number $\#\Delta_\prec(\langle M_1,\ldots,M_h,X_1^q,\ldots,X_m^q\rangle)$ is easily calculated. It is simply the number of monomials in $\mathcal{M}_m$ that are not divisible by any of the monomials $M_1,\ldots,M_h,X_1^q,\ldots,X_m^q$. To establish the correspondence between $\eta_h(q,s,m)$ and the hth generalized Hamming weight we will need the following definition.

Definition 13 *For* $M_1,\ldots,M_h \in \mathcal{M}_m$ *where* $h \geq 2$, *let* $gcd(M_1,\ldots,M_h)$ *denote the greatest common divisor of* $M_1,\ldots,M_h$. *For a single element* $M_1 \in \mathcal{M}_m$ *we write* $\gcd(M_1) := M_1$. *The set* $D = \{M_1,\ldots,M_h\} \subseteq \mathcal{M}_m^{(q)}(s)$ *is said to be a dense set related to* $Hyp_q(s,m)$ *if*

$$\{X_1^{b_1}\cdots X_m^{b_m} \in \Delta_\prec(\langle M_1\ldots,M_h,X_1^q,\ldots,X_m^q\rangle) \mid \\ a_i \leq b_i, i=1,\ldots,m\} \subseteq \mathcal{M}_m^{(q)}(s)\ ,$$

where $X_1^{a_1}\cdots X_m^{a_m} = \gcd(M_1,\ldots,M_h)$. *A set* $D = \{M_1,\ldots,M_h\} \subseteq \mathcal{M}_m^{(q)}(s)$ *is said to be an optimal set of size* h *related to* $Hyp_q(s,m)$ *if* $M_i \neq M_j$ *for* $i \neq j$ *and*

$$\#\Delta_\prec(\langle M_1,\ldots,M_h,X_1^q,\ldots,X_m^q\rangle) = \eta_h(q,s,m)\ .$$

We can show the following theorem concerning the hth generalized Hamming weight. This theorem is a generalization of Theorem 7.

Theorem 14 *The* h*th generalized Hamming weight of* $Hyp_q(s,m)$ *satisfies*

$$d_h \geq q^m - \eta_h(q,s,m)\ . \quad (1)$$

If a dense optimal set of size h *related to* $Hyp_q(s,m)$ *exists then equality holds in (1).*

We can show that for any hyperbolic code of the form $\mathrm{Hyp}_q(s,2)$ and of dimension at least two there exists a related dense and optimal set of size two. Therefore we have the following proposition.

Proposition 15 *The second generalized Hamming weight of a hyperbolic code* $Hyp_q(s,2)$ *of dimension at least* 2 *is given by* $d_2 = q^2 - \eta_2(q,s,2)$.

References

[1] G.-L. Feng and T.R.N. Rao, “Improved Geometric Goppa Codes, Part I:Basic theory,” *IEEE Trans. Inform. Theory*, vol. 41, pp. 1678-1693, Nov. 1995.

[2] O. Geil, “On the Construction of Codes from Order Domains”, submitted to *IEEE Trans. Inform. Theory*, Sep. 2000.

[3] O. Geil, and T. Høholdt, “Footprints or Generalized Bezout's Theorem”, *IEEE Trans. Inform. Theory*, vol. 46, pp. 635-641, Mar. 2000.

[4] T. Høholdt, J. H. van Lint, and R. Pellikaan, “Algebraic Geometry Godes”, in *Handbook of Coding Theory*, (V. S. Pless, and W. C. Hufman Eds.), vol 1, pp. 871-961, Elsevier, Amsterdam 1998.

[5] K. Saints, and C. Heegard, “On Hyperbolic Cascaded Reed-Solomon codes”, *Proc. AAECC-10, Lecture Notes in Comput. Sci.* Vol. 673, pp. 291-303, Springer, Berlin 1993.