On Hyperbolic Codes

O. Geil
Aalborg University
Department of Mathematics
Fr. Bajersvej 7G, 9220 Aalborg 0
Denmark
Email: olav@math.auc.dk

T. Hoholdt
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 [3] Saints and Regev considered a class of codes called hyperbolic encased Reed-Solomon codes which can be seen as an improvement of the generalized Reed-Muller codes RM_n(r, 2). The construction was further generalized by Feng and Rao in [1] to an improvement of the generalized Reed-Muller codes RM_n(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 of the codes. 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 F_q[X_1, ..., X_m] n ≥ 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(X_1, ..., X_m), ..., F(X_1, ..., X_m) \rangle \subseteq F_q[X_1, ..., X_m]

and a monomial ordering \prec on the set M_m of monomials in the variables X_1, ..., X_m. The footprint \Delta(I) of I with respect to \prec is the set of monomials in M_m that can not be found as a leading monomial of any polynomial in I.

Definition 2 Given a polynomial ring F_q[X_1, ..., X_m] and an indexing \mathbb{P}_n = \{P_1, P_2, ..., P_n\}, where n = q^m. Consider the evaluation map
\[ e : \mathbb{P}_n \rightarrow \mathbb{P}_n \]
\[ e : \left\{ F(X_1, ..., X_m) \rightarrow (F(P_1), ..., F(P_n)) \right\} .

Define the map
\[ D : \{ M \in M_m \rightarrow \mathbb{P}_n \}
\[ M \rightarrow \# \Delta(I)(\{ M, X_1^m, ..., X_m^m \}) \]

and let \( E(s) := \text{Span}_q\{ e(M) \mid M \in M_m, D(M) \leq s \} \).

Note that the value \( D(M) \) is easily calculated. It is simply the number of monomials in \( M_m \) that are not divisible by any of the monomials \( X_1^m, ..., X_m^m \).

Definition 3 We define \( M_m^r(s) := \{ M \in M_m \mid \deg_{X_i} < q \text{ for } i = 1, ..., m, \text{ and } D(M) \leq s \} \).

We have \( E(s) = \text{Span}_q\{ e(M) \mid M \in M_m^r(s) \} \). 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 \( \Delta(I) \) is a finite set. Then the size of \( \Delta(I) \) is independent of the actual choice of \( \prec \). The number of common solutions in \( F_q \) of \( F(X_1, ..., X_m), ..., F(X_1, ..., X_m) \), \( F(X_1, ..., X_m) \) is at most equal to \# \Delta(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
\[ S := \{ D(M) \mid M \in M_m, \deg_{X_i} < q, i = 1, ..., m \} \]

Theorem 7 For any \( s \in \mathbb{P}_n \) 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 \( M_m^r(s) := \{ X_1^m, ..., X_m^m \in M_m \mid \alpha_i < q \text{ for } i = 1, ..., m, \prod_{i=1}^m (\alpha_i + 1) < q^m - s \} \).

The hyperbolic codes are now defined as follows.

Definition 9 \( H_{q^m}(s, m) := \{ \in F_q \mid \langle e(M) \rangle = 0 \text{ for all } M \in M_m^r(s) \} \).

Here \( n = q^m \) and \( \langle , \rangle \) is the standard inner product in \( F_q \).
In [4] the minimum distance of these codes is estimated using the order bound. One gets \( d(H_{4}(s, m)) \geq q^m - s \). By Theorem 7 and the following result this estimate is actually equal to the true minimum distance of the hyperbolic code.

**Theorem 10** Consider \( H_{4}(X_{1}, \ldots, X_{m}) \) and \( s \in S \), then
\[
E(s) = H_{4}(s, m).
\]

It follows from Theorem 10 that we now have the generator matrices of the hyperbolic codes. For \( a \in N \) we define
\[
V(m, a) = V([x_{1}, \ldots, x_{m}] | x_{i} \in N, 1 \leq x_{i} \leq q, i = 1, \ldots, m, \prod_{i=1}^{m} x_{i} \leq a)
\]
then it follows from above that \( \text{dim}(H_{4}(s, m)) = q^m - V(m, q^m - s - 1) \). It is not obvious how to get a closed form expression for \( V(m, a) \) but since \( V(1, a) = \min \{ a, q \} \) and \( V(m, a) = \sum_{i=1}^{m} V(m-1, \lceil \frac{a}{i} \rceil) \) we can easily calculate \( V(m, a) \) recursively. One can verify that \( V(2, a) = b + \sum_{i=1}^{m} \lceil \frac{a}{i} \rceil \) where \( b := \min \{ \frac{a}{i}, q \} \) 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 \( R_{4}(r, 3) \) and 1424 different hyperbolic codes \( H_{4}(s, 3) \). These codes are of length \( n = 262,144 \). In the figure every \( \alpha \) corresponds to a generalized Reed-Muller code of the given parameters. The graph marked with \( s \) corresponds to the hyperbolic code. 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 \( 4 \)th generalized Hamming weight of the hyperbolic code \( H_{4}(s, m) \) is related to the following number.

**Definition 12**
\[
\eta_{4}(q, s, m) := \max \{ \#(M_{i}, \ldots, M_{s}, X_{i}^{q}, \ldots, X_{m}^{q}) | M_{i} \neq M_{j} \text{ for } i \neq j, M_{i} \in M_{4}^{m}(s) \text{ for } i = 1, \ldots, h \}.
\]

Note that the number \( \#(M_{i}, \ldots, M_{s}, X_{i}^{q}, \ldots, X_{m}^{q}) \) is easily calculated. It is simply the number of monomials in \( M_{4}^{m}(s) \) that are not divisible by any of the monomials \( M_{1}, \ldots, M_{s}, X_{i}^{q}, \ldots, X_{m}^{q} \). To establish the correspondence between \( \eta_{4}(q, s, m) \) and the \( 4 \)th generalized Hamming weight we will need the following definition.

**Definition 13** For \( M_{1}, \ldots, M_{s} \in M_{4}^{m}(s) \) let \( \text{gcd}(M_{1}, \ldots, M_{s}) \) denote the greatest common divisor of \( M_{1}, \ldots, M_{s} \). For a single element \( M_{i} \in M_{4}^{m}(s) \) we write \( \text{gcd}(M_{i}) := M_{i} \). The set \( D = \{ M_{1}, \ldots, M_{s} \} \subseteq M_{4}^{m}(s) \) is said to be an optimal set of size \( h \) related to \( H_{4}(s, m) \) if \( M_{i} \neq M_{j} \text{ for } i \neq j \) and
\[
\#(M_{1}, \ldots, M_{s}, X_{i}^{q}, \ldots, X_{m}^{q}) = \eta_{4}(q, s, m).
\]

We can show the following theorem concerning the \( 4 \)th generalized Hamming weight. This theorem is a generalization of Theorem 7.

**Theorem 14** The \( 4 \)th generalized Hamming weight of \( H_{4}(s, m) \) satisfies
\[
d_{4} \geq q^m - \eta_{4}(q, s, m) \tag{1}
\]
if a dense optimal set of size \( h \) related to \( H_{4}(s, m) \) exists then equality holds in (1).

We can show that for any hyperbolic code of the form \( H_{4}(s, m) \) 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 \( H_{4}(s, 2) \) of dimension at least 2 is given by \( d_{2} = q^{4} - \eta_{4}(q, s, 2) \).

**REFERENCES**