High dimensional affine codes whose square has a designed minimum distance[*]

Ignacio García-Marco[1], Irene Márquez-Corbella[1], and Diego Ruano[2]

[1] Departamento de Matemáticas, Estadística e I.O., Universidad de La Laguna, 38200 La Laguna, Tenerife, Spain. Email: iggarcia@ull.es and imarquec@ull.es
[2] IMUVA-Mathematics Research Institute, Universidad de Valladolid, 47011 Valladolid, Spain. Email: diego.ruano@uva.es

Abstract

Given a linear code $\mathcal{C}$, its square code $\mathcal{C}^{(2)}$ is the span of all component-wise products of two elements of $\mathcal{C}$. Motivated by applications in multi-party computation, our purpose with this work is to answer the following question: which families of affine variety codes have simultaneously high dimension $k(\mathcal{C})$ and high minimum distance of $\mathcal{C}^{(2)}$, $d(\mathcal{C}^{(2)})$? More precisely, given a designed minimum distance d we compute an affine variety code $\mathcal{C}$ such that $d(\mathcal{C}^{(2)}) \geq d$ and that the dimension of $\mathcal{C}$ is high. The best construction that we propose comes from hyperbolic codes when $d \geq q$ and from weighted Reed-Muller codes otherwise.

Keywords. Affine variety codes Multi-party computation Square codes Schur product of codes Minkowski sum convex set

Mathematics Subject Classification (2010). 94B05 94B75

1   Introduction

Multi-party computation studies the case where a group of persons, each holding an input for a function, wants to compute the output of it, without having each individual reveal his or her input to the other parties. Multi-party computation is possible from secret sharing schemes [12], and hence from coding theory. From now on, given a linear code $\mathcal{C}$, the dimension of $\mathcal{C}$ will be denoted by $k(\mathcal{C})$ and its minimum distance by $d(\mathcal{C})$. Moreover, if $\mathcal{C}$ is a linear code over $\mathbb{F}_q$ of length n, dimension k and minimum distance d, we call $[n, k, d]_q$ the parameters of $\mathcal{C}$.

One of the best known protocols is MiniMac [14], which evaluates boolean circuits, and its successor TinyTable [13]. These methods use a linear code $\mathcal{C}$, which should prevent cheating. The probability that a cheating player is caught depends on the minimum distance of $\mathcal{C} * \mathcal{C} = \mathcal{C}^{(2)}$, the square code of linear code [27], meaning that a high distance on the square will give a higher security. Simultaneously, it would be beneficial to have a code $\mathcal{C}$ with high rate to reduce the communications cost. Therefore, it is desirable to optimize both parameters: $d(\mathcal{C}^{(2)})$ and $k(\mathcal{C})$.

Although, in this article we are more interested in the application of the schur product to the area of secure multiparty computation, this operation has other applications. For example, component-wise products of linear codes have been used to decode linear codes [24, 25] where it is shown that a linear code of length n with a t-error correcting pair has a decoding algorithm which corrects up to t errors with complexity $\mathcal{O}\left(n^3\right)$. Moreover, the schur product is also used for cryptanalytic applications against the McEliece cryptosystem [5–7, 23, 29], which rely on two assumptions: the generic decoding is hard

on average and it is hard to distinguish the public key (a generator matrix of a code $\mathcal{C}$ with a certain structure) from a random matrix. For a summary of these applications and some others, see [27, §4].

These applications show the importance of finding linear codes, where both the code itself and the square have good parameters. Choosing a random linear code, with dimension linear in the length, will, with high probability, give a reasonable minimum distance, however, this does not hold for the square code [3]. Hence, constructing good square codes is a difficult problem. Nevertheless, good square codes exist, since there exists an asymptotic family of codes with the previous property [26]. The best binary construction available in the literature is the one in [2] obtained from cyclic codes, but their constellation is quite limited. A larger constellation can be found at [4].

Another family of codes that have been proposed for obtaining codes with a good square are *Reed-Muller codes* [27]. Reed-Muller codes can be understood as affine variety codes when one considers the ideal $I = (0)$, i.e. when one evaluates multivariate polynomials (m variables) at all the points of $\mathbb{F}_q^m$. We will restrict our attention to this case of affine variety codes in this article. One has the footprint bound [18] for estimating the minimum distance of this family of codes. The family of *hyperbolic codes* [19] was introduced to maximize the dimension of an affine variety code given a designed minimum distance from the footprint bound. In particular, a hyperbolic code has a dimension greater than or equal to a Reed-Muller code with the same minimum distance. Hence, it is natural to consider hyperbolic codes for obtaining codes where both the dimension of the code and the minimum distance of the square code are good.

Given $d \in \mathbb{Z}^+$, in this work we propose a method to obtain an affine variety code $\mathcal{C}$ satisfying that $d(\mathcal{C}^{(2)}) \geq d$ and such that $k(\mathcal{C})$ is considerably high. Our method receives as input a value $d \in \mathbb{Z}^+$ and starts by considering an affine code $\mathcal{C}_B$ associated with a set $B \subseteq \mathbb{N}^m$ such that $d(\mathcal{C}_B) \geq d$, say for example, a hyperbolic code with minimum distance at least d. Then, by means of convexity arguments, we build a set $A \subset \mathbb{N}^m$ such that the Minkowski sum $A + A$ is contained in B. The latter condition implies that $d(\mathcal{C}_A^{(2)}) \geq d(\mathcal{C}_B) \geq d$. Remarkably, the best candidate for the set $A \subseteq \mathbb{N}^m$ is not always the one related with a hyperbolic code. Indeed, when the value of the designed minimum distance d is small enough, $d < q$, we prove that there exist certain *weighted Reed-Muller codes* that outperform hyperbolic codes.

Additionally, if the minimum distance of the dual of $\mathcal{C}$ and $d(\mathcal{C}^{(2)})$ are greater than or equal to $t + 2$, then $\mathcal{C}$ can be used to construct a t-strongly multiplicative secret sharing scheme (SSS). Such a SSS is enough to construct an information theoretic secure secret sharing scheme if at most t players are corrupted [1, 8, 11]. This application shows the importance of finding linear codes where $d(\mathcal{C}^\perp)$ is also high relative to the length of the code, where $\mathcal{C}^\perp$ is the dual code of $\mathcal{C}$. Although in this work we have not focused in maximizing $d(\mathcal{C}^\perp)$ (this is also the case of other articles in the literature as [2, 4]), we note that for the affine variety codes considered in this article, the dual of $\mathcal{C}$ is again an affine variety code that can be easily constructed by [17, Proposition 1]. Moreover, its minimum distance can also be estimated using the footprint bound.

Outline of the article

Section §2 presents the notation used in the article and review some of the standard facts on affine variety codes, in particular, it provides a detailed exposition of the footprint bound, a lower bound for their minimum distance. We also describe some well known examples of affine variety codes which will be essential throughout the article, as Reed-Muller codes, weighted Reed-Muller codes and hyperbolic codes. We end this section with an original result that indicates, in the case of two variables, when the hyperbolic code has strictly higher dimension than a Reed-Muller code with the same minimum distance. Moreover, one can find in the appendix some results (some of them well known) that show when the footprint bound is sharp. We emphasize that Lemma 18 and Lemma 19 have been used in the proof of some results in the article.

Next, in Section §3 we look more closely at the operation of Schur product of affine variety codes and its relation with the Minkowski sum. Moreover, we present the key result of the article that allows us to establish a strategy to construct affine variety codes whose square code has a designed minimum distance d, this strategy is outlined in Algorithm 1. That is, given $d \in \mathbb{N}$ we construct an affine variety code $\mathcal{C}$ such that $d(\mathcal{C}^{(2)}) \geq d$.

In section §4 we will be more ambitious, this section contains the main results of the article. If our goal till this section was to obtain an affine code $\mathcal{C}$ whose square code has designed minimum distance

d i.e. $d(\mathcal{C}^{(2)}) \geq d$, throughout Section §4 our additional goal is providing a code $\mathcal{C}$ that has also high minimum distance. It seems natural to expect that a code coming from a hyperbolic code will be the best candidate for our new goal. We have called this type of codes *half hyperbolic codes* and they have been studied in detail in Section §4.1. Surprisingly, *half hyperbolic codes* are not always the best option. Indeed, we prove in Section §4.2 that, when the value of the designed minimum distance d is small enough, there exist certain weighted Reed-Muller codes that outperform half hyperbolic codes. That is, when d is small enough, then there are weighted Reed-Muller codes $\mathcal{D}$ whose square has the same designed minimum distance d than the corresponding half hyperbolic code $\mathcal{C}$ (i.e. $d(\mathcal{C}^{(2)})$, $d(\mathcal{D}^{(2)}) \geq d$) and such that $k(\mathcal{D}) > k(\mathcal{C})$.

2 Affine variety codes

Let us start this section with a brief summary on affine varieties, polynomials and ideals to set up notation and terminology. For a fuller treatment we refer the reader to [9, 10].

Let $k[X_1, \ldots, X_m]$ be a ring of polynomials over a field k and consider a monomial ordering $\succ$ on $k[X_1, \ldots, X_m]$. For a polynomial $f \in k[X_1, \ldots, X_m]$ we denote by $\mathrm{in}(f)$ its *leading term* with respect to $\succ$, that is, the largest monomial that occurs in f. For any ideal $I \subseteq k[X_1, \ldots, X_m]$ we denote by $\mathrm{in}(I)$ its *initial ideal*, which is $\mathrm{in}(I) = \langle \mathrm{in}(f) \mid f \in I \rangle$. The *radical ideal* of I, denoted $\sqrt{I}$, is the ideal $\sqrt{I} = \{f \mid f^m \in I \text{ for some integer } m \geq 1\}$. We say that I is a *radical ideal* if $I = \sqrt{I}$.

Let us recall some basics on the correspondence between ideals and varieties. Given an affine variety $V \subseteq k^m$ we can define the ideal of all polynomials vanishing on V, i.e.

$$\mathcal{I}(V) = \{f \in k[X_1, \ldots, X_m] \mid f(x) = 0 \text{ for all } x \in V\}.$$

Conversely, given an ideal $I \subseteq k[X_1, \ldots, X_m]$ we can define the affine variety

$$\mathcal{V}(I) = \{x \in k^m \mid f(x) = 0 \text{ for all } f \in I\}.$$

Hilbert's Nullstellensatz (see, e.g., [10, Theorem 6]) states that if k is algebraically closed and I is an ideal in $k[X_1, \ldots, X_m]$, then $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$. In particular, this implies that if we restrict to radical ideals, then the above maps are inverses of each other and we have a one-to-one correspondence between affine varieties and radical ideals.

Let K be the algebraic closure of k and let I be a zero-dimensional ideal, we define the quotient ring $R = K[X_1, \ldots, X_m]/I$. Then [9, Theorem 2.10] shows that the dimension of R as a K-vector space gives a bound on the number of points in $\mathcal{V}(I)$. That is,

$$\dim_K(R) \geq \#\mathcal{V}(I), \text{ with equality if and only if } I \text{ is a radical ideal;}$$

where $\#A$ denotes the cardinality of the set A.

Notice that I is a zero-dimensional ideal if and only if $\mathcal{V}(I)$ is a finite set, that is $\mathcal{V}(I) = \{P_1, \ldots, P_n\}$. The key idea to prove this result is to show that the evaluation map φ defined as

$$\varphi: \begin{array}{ccc} K[X_1, \ldots, X_m] & \longrightarrow & K^n \\ f & \mapsto & (f(P_1), \ldots, f(P_n)) \end{array} \tag{1}$$

is an epimorphism of K-vector spaces and $\mathrm{Ker}(\varphi) = \mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$.

Although we have introduced all the results for an arbitrary field, from now on we will work with the finite field with q elements, denoted as $\mathbb{F}_q$.

Let $I \subseteq \mathbb{F}_q[X_1, \ldots, X_n]$ be an ideal, we define the ideal I_q related to I as

$$I_q = I + \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle \subseteq \mathbb{F}_q[X_1, \ldots, X_m].$$

It is easy to check that I_q is radical as consequence of Seidenberg's Lemma (because I_q contains a univariate square free polynomial in each of the m-variables). Moreover, the points of the affine variety defined by I_q (over the algebraic closure of $\mathbb{F}_q$) are the $\mathbb{F}_q$-rational points of the affine variety defined by I. That is,

$$\mathcal{V}_{\overline{\mathbb{F}_q}}(I_q) = \mathcal{V}_{\mathbb{F}_q}(I_q) = \mathcal{V}_{\mathbb{F}_q}(I) = \{P_1, \ldots, P_n\}.$$

where $\overline{\mathbb{F}_q}$ denotes the algebraic closure of $\mathbb{F}_q$.

Now we consider the quotient ring $R_I = \mathbb{F}_q[X_1, \ldots, X_m]/I_q$ and denote $\mathcal{P} = V_{\mathbb{F}_q}(I) = \{P_1, \ldots, P_n\}$. By (1), the following evaluation map at the points of $\mathcal{P}$ is an isomorphism of $\mathbb{F}_q$-vector spaces:

$$\text{ev}_{\mathcal{P}} : \begin{array}{ccc} R_I & \longrightarrow & \mathbb{F}_q^n \\ f + I_q & \longmapsto & (f(P_1), \ldots, f(P_n)). \end{array} \tag{2}$$

Definition 1. Let I_q and R_q be defined as before and let L be an $\mathbb{F}_q$-vector subspace of R_q we define the affine variety code $C(I, L)$ as the image of L under the evaluation map $\text{ev}_{\mathcal{P}}$. That is:

$$C(I, L) = \text{ev}_{\mathcal{P}}(L) = \{\text{ev}_{\mathcal{P}}(f + I_q) \mid f + I_q \in L\}.$$

It is clear that $C(I, L)$ has $G = (f_i(P_j) \mid i = 1, \ldots, k \, , \, j = 1, \ldots, n)$ as generator matrix where $\{f_1, \ldots, f_k\}$ form a basis of L.

Example 1. Let $I = \langle X^{q-1} - 1 \rangle \subseteq \mathbb{F}_q[X]$. Then, $I_q = I$ and $\mathcal{V}_{\mathbb{F}_q}(I) = \mathbb{F}_q^*$. Consider $L = \langle 1, X, \ldots, X^{k-1} \rangle$, then $C(I, L)$ is the *Reed-Solomon code* of dimension k over $\mathbb{F}_q$, denoted as $\text{RS}_q(k)$. Moreover, if we set $I = (0)$, then $\mathcal{V}_{\mathbb{F}_q}(I) = \mathbb{F}_q$ and $C(I, L)$ is the *extended Reed-Solomon code* of dimension k.

Example 2. Let $I = (0) \subseteq \mathbb{F}_q[X_1, \ldots, X_m]$. Then $I_q = \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle$ and $\mathcal{V}_{\mathbb{F}_q}(I) = \mathbb{F}_q^m$. If we take $L = \{f \in \mathbb{F}_q[X_1, \ldots, X_m] \mid \deg(f) < s\}$, then $C(I, L)$ is the *q-ary Reed-Muller code of degree s in m variables*, denoted as $\text{RM}_q(s, m)$.

The reader may have already realized that some of the well-known classes of evaluation codes can be viewed as affine variety codes. Moreover in [16, Proposition 1.4] it is proved that every $\mathbb{F}_q$-linear code $\mathcal{C}$ may be represented as an affine variety code over $\mathbb{F}_{q^s}$ where we have to choose s so that q^s is greater than the length of $\mathcal{C}$.

Let $\mathcal{C} = C(I, L)$ be an affine variety code. Then, it is clear that the length of $\mathcal{C}$ is the cardinality of $\mathcal{V}_{\mathbb{F}_q}(I) = \mathcal{P} = \{P_1, \ldots, P_n\}$ and the dimension of $\mathcal{C}$ is the dimension of the subspace L - since the evaluation map $\text{ev}_{\mathcal{P}}$ is an isomorphism. In the rest of the section we will study the minimum distance of affine variety codes $\mathcal{C} = C(I, L)$ in the particular case that $I = (0)$.

Let $A \subseteq \mathbb{N}^m$ be a non-empty (finite) subset of $\mathbb{N}^m$. We denote by $\mathbb{F}_q[A] \subseteq \mathbb{F}_q[X_1, \ldots, X_m]$ the $\mathbb{F}_q$-vector space with basis:

$$\left\{ X_1^{i_1} \cdots X_m^{i_m} \mid (i_1, \ldots, i_m) \in A \right\}.$$

We will denote by $\mathcal{C}_A$ the affine variety code $C(I, L)$ with $I = (0)$ and $L = \mathbb{F}_q[A]$, in other words $\mathcal{C}_A$ consists of the evaluation of polynomials $f \in \mathbb{F}_q[A]$ in the q^m points of $\mathbb{F}_q^m$.

Remark 1. Let $A \subseteq \mathbb{N}^m$ and consider the code $\mathcal{C}_A$ as the affine variety code $C(I, L)$ with $I = (0)$ and $L = \mathbb{F}_q[A]$. Then the length of $\mathcal{C}_A$ is q^m and its dimension coincides with the cardinality of the set A.

For $a, b \in \mathbb{R}$ and $a \leq b$, we denote by $[\![a, b]\!]$ the integer interval $[a, b] \cap \mathbb{Z}$.

Remark 2. Given $A \subseteq \mathbb{N}^m$ and using the identity $z^q = z$ for every $z \in \mathbb{F}_q$, one can find a unique set $B \subseteq [\![0, q-1]\!]^m$ such that $\mathbb{F}_q[B] + I_q = \mathbb{F}_q[A] + I_q$ and, thus, A and B define the same code $\mathcal{C}_A = \mathcal{C}_B$ (see Figure 1). This set will be denoted by $B = A_q$. Throughout the article we use both sets indistinctly.

Let f be a polynomial in $\mathbb{F}_q[X_1, \ldots, X_m]$, we define the ideal

$$I_{q,f} = \langle X_1^q - X_1, \ldots, X_m^q - X_m, f \rangle$$

and the quotient ring $R_f = \mathbb{F}_q[X_1, \ldots, X_m]/I_{q,f}$.

Proposition 1. *Let f be a polynomial in $\mathbb{F}_q[X_1, \ldots, X_m]$, then the dimension of the $\mathbb{F}_q$-vector space R_f is the number of roots of f in $\mathbb{F}_q^m$. That is, $\dim_{\mathbb{F}_q}(R_f) = \#\mathcal{V}_{\mathbb{F}_q}(f)$.*

Proof. Applying (2) with $I = (f)$, then $\dim_{\mathbb{F}_q}(R_f) = \#\mathcal{V}(I_{q,f}) = \#\mathcal{V}_{\mathbb{F}_q}(f)$. $\square$

The following well-known result (see, e.g., [18]) gives a bound for the minimum distance of the particular case of affine variety codes of type $\mathcal{C}_A$. We include a short proof of this result for the sake of clarity.

Theorem 2 (Footprint bound). *Let $A \subseteq [\![0, q-1]\!]^m$. Then, the minimum distance of $\mathcal{C}_A$ satisfies that*

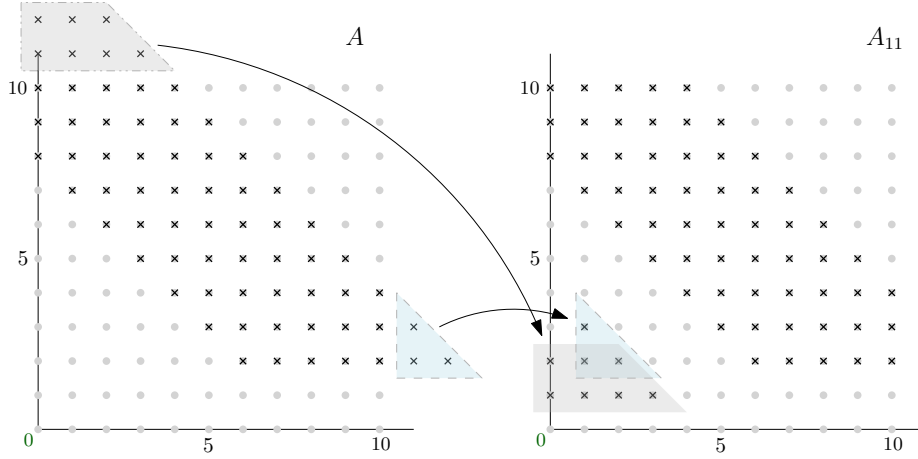$$d(\mathcal{C}_A) \geq \min_{(i_1, \ldots, i_m) \in A} \left\{ (q - i_1) \cdots (q - i_m) \right\}.$$

4

Figure 1: The sets $A \subseteq \mathbb{N}^2$ and $A_{11} \subseteq [\![0, 10]\!]^2$ define the same code over $\mathbb{F}_{11}$.

Proof. Since the codewords of $\mathcal{C}_A$ consists of the evaluation of polynomials $f \in \mathbb{F}_q[A]$ at the $n = q^m$ points of $\mathbb{F}_q^m$ and using the definition of minimum distance we have that

$$d(\mathcal{C}_A) = n - \max_{f \in \mathbb{F}_q[A]} \# \left\{ \mathbb{F}_q\text{-roots of } f \right\} = n - \max_{f \in \mathbb{F}_q[A]} \# \mathcal{V}(I_{q,f}).$$

Now using Proposition 1 and standard Gröbner basis arguments if we take $\succ$ any monomial order we have that

$$
\begin{aligned}
d(\mathcal{C}_A) &= n - \max_{f \in \mathbb{F}_q[A]} \left\{ \dim_{\mathbb{F}_q}(R_f) \right\} = n - \max_{f \in \mathbb{F}_q[A]} \left\{ \dim_{\mathbb{F}_q} \left(\mathbb{F}_q[X_1, \ldots, X_m]/\mathrm{in}(I_{q,f}) \right) \right\} \\
&\geq n - \max_{f \in \mathbb{F}_q[A]} \left\{ \dim_{\mathbb{F}_q} \left(\mathbb{F}_q[X_1, \ldots, X_m]/ \left\langle X_1^q, \ldots, X_n^q, \mathrm{in}(f) \right\rangle \right) \right\} \\
&= n - \max_{(i_1, \ldots, i_m) \in A} \left\{ \dim_{\mathbb{F}_q} \left(\mathbb{F}_q[X_1, \ldots, X_m]/ \left\langle X_1^q, \ldots, X_n^q, X_1^{i_1} \cdots X_m^{i_m} \right\rangle \right) \right\} \\
&= \min_{(i_1, \ldots, i_m) \in A} \left\{ (q - i_1) \cdots (q - i_m) \right\}.
\end{aligned}
$$

$\square$

Definition 2. Let $A \subseteq [\![0, q-1]\!]^m$. We define the *footprint-bound* of the affine code $\mathcal{C}_A$ as the integer

$$\mathrm{FB}(\mathcal{C}_A) = \min_{(i_1, \ldots, i_m) \in A} \left\{ (q - i_1) \cdots (q - i_m) \right\}.$$

By Theorem 2, we have that the minimum distance of the code $\mathcal{C}_A$ satisfies that

$$d(\mathcal{C}_A) \geq \mathrm{FB}(\mathcal{C}_A).$$

In the following lines we study some well-known families of affine codes, namely (weighted) Reed Muller and hyperbolic codes (see, e.g., [28], [15], [19]). All these codes are konwn to satisfy that their minimum distance coincides with the value of the footprint-bound. One could provide an alternative proof of this fact by a direct application of Lemma 18 in the Appendix.

Definition 3. **(Reed-Muller codes)** Let $s \in \mathbb{N}$ and

$$A = \left\{ (i_1, \ldots, i_m) \in [\![0, q-1]\!]^m \mid i_1 + \ldots + i_m \leq s \right\}.$$

Then, $\mathcal{C}_A$ is the called the q-ary *Reed-Muller* code of degree s in m variables and we denote it by $\mathrm{RM}_q(s, m)$.

The following result is known and the proof can be found in [21, Theorem 2].

Proposition 3. *Given $s \in \mathbb{N}, s \leq (q-1)m$. If we write $s = a(q-1) + b$ with $0 \leq b \leq q-1$, then the minimum distance of the Reed-Muller code $\mathcal{C} = \mathrm{RM}_q(s, m)$ is*

$$d(\mathcal{C}) = (q-b)q^{m-1-a}.$$

Definition 4. (**Weighted Reed-Muller codes**) Consider $s, s_1, \ldots, s_m > 0$ and let $A = \{(i_1, \ldots, i_m) \in [\![0, q-1]\!]^m \mid s_1 i_1 + \ldots\}$ Then, $\mathcal{C}_A$ is called the q-ary *weighted Reed-Muller* code of degree s in m variables with $\mathcal{S} = (s_1, \ldots, s_m)$ and we denote it by $\mathrm{WRM}_q(s, m, \mathcal{S})$. If $s_1 = \ldots = s_m = 1$, then $\mathrm{WRM}_q(s, m, \mathcal{S})$ is the corresponding q-ary Reed-Muller code $\mathrm{RM}_q(\lfloor s \rfloor, m)$.

Definition 5. (**Hyperbolic codes**) Let $d \in \mathbb{N}$ and

$$A = \{(i_1, \ldots, i_m) \in [\![0, q-1]\!]^m \mid (q-i_1) \cdots (q-i_m) \geq d\}.$$

Then, $\mathcal{C}_A$ is called the q-ary *hyperbolic* code of order d and we denote it by $\mathrm{Hyp}_q(d, m)$.

(a) Example of a Reed-Muller code.

(b) Example of a hyperbolic code.
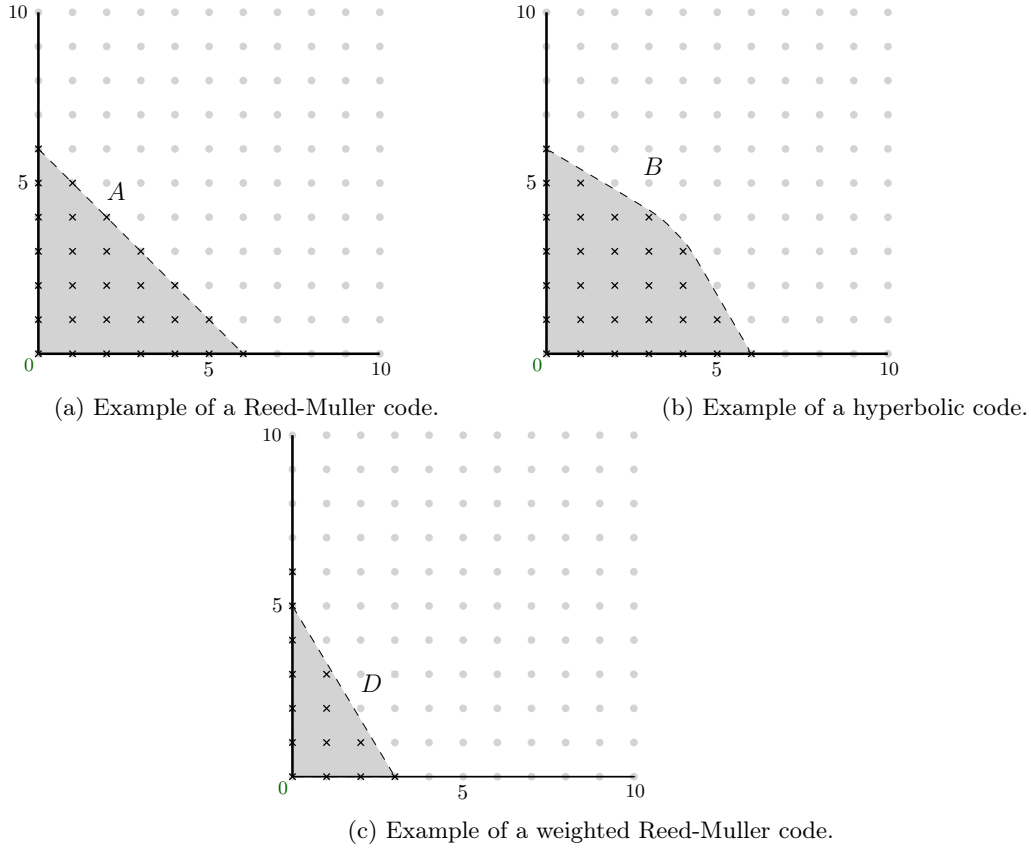
(c) Example of a weighted Reed-Muller code.

Figure 2: Examples of Reed-Muller, hyperbolic and weighted Reed-Muller codes.

Example 3. Consider the following codes over $\mathbb{F}_{11}$ (see Figure 2):

- the set $A = \{(i, j) \in [\![0, 10]\!]^2 \mid i + j \leq 6\}$, corresponds to the Reed-Muller code $\mathcal{C}_A = \mathrm{RM}_{11}(6, 2)$ with parameters $[11^2, 28, 55]_{11}$,

- the set $B = \{(i, j) \in [\![0, 10]\!]^2 \mid (11 - i)(11 - j) \leq 55\}$, corresponds to the hyperbollic code $\mathcal{C}_B = \mathrm{Hyp}_{11}(55, 2)$ with parameters $[11^2, 30, 55]_{11}$,

- and the set $D = \{(i, j) \in [\![0, 10]\!]^2 \mid 5i + 3j \leq 15\}$, corresponds to the weighted Reed-Muller code $\mathcal{C}_D = \mathrm{WRM}_{11}(15, 2, \{5, 3\})$ with parameters $[11^2, 13, 66]_{11}$.

The hyperbolic code $\mathrm{Hyp}_q(d,m)$ has been designed to be the code with the largest possible dimension among those affine codes $\mathcal{C}_A$ such that $\mathrm{FB}(\mathcal{C}_A) \geq d$. In the following result, we indicate in the case of two variables, when the hyperbolic code of order d has greater dimension with respect to a Reed-Muller code with the same minimum distance d.

Proposition 4. Consider $\mathcal{D} = \mathrm{RM}_q(t,2)$ and $\mathcal{E} = \mathrm{Hyp}_q(d,2)$. If $d(\mathcal{D}) = d(\mathcal{E})$, then $k(\mathcal{D}) \leq k(\mathcal{E})$. Moroever, $k(\mathcal{D}) < k(\mathcal{E})$ if and only if

$$\frac{t+5}{2} \leq q \leq \frac{(t+1)^2}{4}.$$

Proof. Since $d(\mathcal{D}) = d(\mathcal{E})$, we have that $\mathrm{FB}(\mathcal{E}) = d(\mathcal{E}) = d(\mathcal{D}) = \mathrm{FB}(\mathcal{D})$. Set $M = (m_{i,j})_{0 \leq i,j \leq q-1}$ the matrix with $m_{i,j} = (q-i)(q-j)$. We have that $\mathcal{D} = \mathcal{C}_A$ and $\mathcal{E} = \mathcal{C}_B$ with $A = \{(i,j) \in [\![0,q-1]\!] \,|\, i+j \leq t\}$ and $B = \{(i,j) \in [\![0,q-1]\!] \,|\, m_{i,j} \geq d\}$. Moreover,

$$\min\{m_{i,j} \,|\, (i,j) \in A\} = d(\mathcal{D}) = d(\mathcal{E}) = \min\{m_{i,j} \,|\, (i,j) \in B\}.$$

Hence, $A \subseteq B$ and $k(\mathcal{D}) \leq k(\mathcal{E})$; indeed, this proves that hyperbolic codes have the maximum dimension among all the codes with the same footprint-bound value.

By Proposition 3 we also have that

$$d(\mathcal{D}) = \begin{cases} m_{0,t} & \text{if } t \leq q-1, \text{ and} \\ m_{q-1,t-q+1} & \text{if } q \leq t \leq 2q-2; \end{cases}$$

and it is easy to verify that

$$\max\{m_{i,j} \,|\, (i,j) \notin A\} = \begin{cases} m_{\frac{t+1}{2},\frac{t+1}{2}} & \text{if } t \text{ is odd, and} \\ m_{\frac{t}{2},\frac{t+2}{2}} & \text{if } t \text{ is even} \end{cases}$$

We separate the proof depending on the value and the parity of t.

1. $t \leq q-1$ and

   (a) t is odd. Then $k(\mathcal{D}) < k(\mathcal{E})$ if and only if $(\frac{t+1}{2},\frac{t+1}{2}) \in B$ or, equivalently, if $m_{t,0} \leq m_{\frac{t+1}{2},\frac{t+1}{2}}$. Moreover, this happens if and only if $q \leq \left(\frac{t+1}{2}\right)^2$.

   (b) t is even. Then $k(\mathcal{D}) < k(\mathcal{E})$ if and only if $(\frac{t}{2},\frac{t+2}{2}) \in B$ or, equivalently, if $m_{t,0} \leq m_{\frac{t}{2},\frac{t+2}{2}}$. Moreover, this happens if and only if $q \leq \frac{t(t+2)}{4}$. Since t is even, this is equivalent to $q \leq \left(\frac{t+1}{2}\right)^2$.

2. $t \geq q$ and

   (a) t is odd. Then $k(\mathcal{D}) < k(\mathcal{E})$ if and only if $(\frac{t+1}{2},\frac{t+1}{2}) \in B$ or, equivalently, if $m_{q-1,t-q+1} \leq m_{\frac{t+1}{2},\frac{t+1}{2}}$. Moreover, this happens if and only if $2q - t - 1 \leq \left(q - \frac{t+1}{2}\right)^2$. This defines a quadratic inequality $p(q) > 0$ involving in the variable q. Notice that $p(q) \geq 0$ if and only if $q \leq (t+1)/2$ or $q \geq (t+5)/2$. The first option is not viable since $t \geq 2q - 1$. We conclude, thus, that $q \geq (t+5)/2$.

   (b) t is even. Then $k(\mathcal{D}) < k(\mathcal{E})$ if and only if $(\frac{t}{2},\frac{t+2}{2}) \in B$ or, equivalently, if $m_{q-1,t-q+1} \leq m_{\frac{t}{2},\frac{t+2}{2}}$. Moreover, this happens if and only if $2q - t - 1 \leq \left(q - \frac{t}{2}\right)\left(q - \frac{t+2}{2}\right)$. Proceeding as in the previous case we get that this is equivalent to $q \geq \frac{t+3+\sqrt{5}}{2}$ and since t is even, this is the same as $q \geq \frac{t+5}{2}$.

$\square$

3   Schur product of codes

The notion of Schur product of codes was first introduced in coding theory for decoding [24] [25]. But this operation turns out to have many other applications in cryptanalysis, multiparty computation, secret sharing or construction of lattices. Many of these applications are summarized in [27, §4].

Definition 6. The Schur product is the componentwise product on $\mathbb{F}_q^n$. That is, given two elements $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$:

$$\mathbf{a} * \mathbf{b} \overset{\text{def}}{=} (a_1 b_1, \ldots, a_n b_n)$$

For two codes $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_q^n$, their Schur product is the code $\mathcal{C}_1 * \mathcal{C}_2$ defined as

$$\mathcal{C}_1 * \mathcal{C}_2 \overset{\text{def}}{=} \operatorname{Span}_{\mathbb{F}_q} \{\mathbf{c}_1 * \mathbf{c}_2 \mid \mathbf{c}_1 \in \mathcal{C}_1 \text{ and } \mathbf{c}_2 \in \mathcal{C}_2\}$$

For $\mathcal{C}_1 = \mathcal{C}_2 = \mathcal{C}$, then $\mathcal{C} * \mathcal{C}$ is denoted as $\mathcal{C}^{(2)}$.

3.1   Product of codes and the Minkowski sum

Given two sets $A, B \subseteq \mathbb{N}^m$, we denote by $A + B$ its Minkowski sum, that is, $A + B = \{a + b \mid a \in A, b \in B\}$. The following property is easy to check.

Proposition 5. $\mathcal{C}_A^{(2)} = \mathcal{C}_{A+A}$.

Proof. Let $\mathbf{c} \in \mathcal{C}_A^{(2)}$, then $\mathbf{c} = \mathbf{c}_1 * \mathbf{c}_2$ with $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}_A$. Or equivalently,

$$\mathbf{c} = \operatorname{ev}_{\mathcal{P}}(f) * \operatorname{ev}_{\mathcal{P}}(g) = \operatorname{ev}_{\mathcal{P}}(fg) \text{ with } f, g \in \mathbb{F}_q[A].$$

It is easy to check that if $f, g \in \mathbb{F}_q[A]$, then $fg \in \mathbb{F}_q[A + A]$. Thus, $\mathbf{c} \in \mathcal{C}_{A+A}$.

Conversely, take notice that $\mathbb{F}_q[A + A]$ is the $\mathbb{F}_q$-vector space with basis

$$\left\{ \mathbf{X}^{\mathbf{i}} \overset{\text{def}}{=} X_1^{i_1} \cdots X_m^{i_m} \mid \mathbf{i} = (i_1, \ldots, i_m) \in A + A \right\} = \left\{ \mathbf{X}^{\mathbf{a}} \cdot \mathbf{X}^{\mathbf{b}} \mid \mathbf{a}, \mathbf{b} \in A \right\}$$

Therefore, for any $\mathbf{c} \in \mathcal{C}_{A+A}$, then $\mathbf{c} = \operatorname{ev}_{\mathcal{P}}(f)$ with $f \in \mathbb{F}_q[A + A]$, that is

$$\mathbf{c} = \operatorname{ev}_{\mathcal{P}}(f) = \operatorname{ev}_{\mathcal{P}} \left(\sum_{i=0}^{s} \lambda_i \mathbf{X}^{\mathbf{a}_i} \mathbf{X}^{\mathbf{b}_i} \right) = \sum_{i=0}^{s} \lambda_i \operatorname{ev}_{\mathcal{P}}(\mathbf{X}^{\mathbf{a}_i}) * \operatorname{ev}_{\mathcal{P}}(\mathbf{X}^{\mathbf{b}_i}) \in \mathcal{C}_A^{(2)}.$$

$\square$

It is important to highlight that even if $A \subset [\![0, q - 1]\!]^m$, it might happen that $A + A \not\subset [\![0, q - 1]\!]^m$; however $A' := (A + A)_q \subset [\![0, q - 1]\!]^m$ satisfies that $\mathcal{C}_{A'} = \mathcal{C}_{A+A}$ (see Figure 3).

Proposition 5 suggests the following way of constructing affine codes whose square has a designed minimum distance: we consider $B \subset [\![0, q - 1]\!]^m$ such that $d(\mathcal{C}_B) \geq d$ and, then, we choose A such that $(A + A)_q \subset B$. If A is chosen in this way, then we will have that $d(\mathcal{C}_A^{(2)}) = d(\mathcal{C}_{A+A}) = d(\mathcal{C}_{(A+A)_q}) \geq d(\mathcal{C}_B) \geq d$. The following lemma gives a necessary condition for such a set A.

Lemma 6. Let $A, B \subset [\![0, q - 1]\!]^m$ and for each $\epsilon = (\epsilon_1, \ldots, \epsilon_m) \in \{0, 1\}^m$ we set

$$B_\epsilon := \{\mathbf{b} + (q - 1)\epsilon \mid \mathbf{b} = (b_1, \ldots, b_n) \in B \text{ and } b_i > 0 \text{ whenever } \epsilon_i = 1\}.$$

If $(A + A)_q \subseteq B$, *then* $2A = \{2\mathbf{a} \mid \mathbf{a} \in A\}$ *is a subset of* $\cup_{\epsilon \in \{0,1\}^m} B_\epsilon$.

Proof. Assume that $(A + A)_q \subseteq B$.

We observe that whenever $\mathbf{a} = (a_1, \ldots, a_m) \in A$, then $(2\mathbf{a})_q \in (A + A)_q$,

$$\text{where } (2\mathbf{a})_q = (a'_1, \ldots, a'_m) \text{ with } a'_i = \begin{cases} 2a_i, & \text{if } 2a_i < q, \\ 2a_i - (q - 1) & \text{otherwise.} \end{cases}$$

Now, it suffices to take

$$\epsilon = (\epsilon_1, \ldots, \epsilon_m) \text{ with } \epsilon_i = \begin{cases} 0 & \text{if } 2a_i < q \\ 1 & \text{otherwise} \end{cases}$$

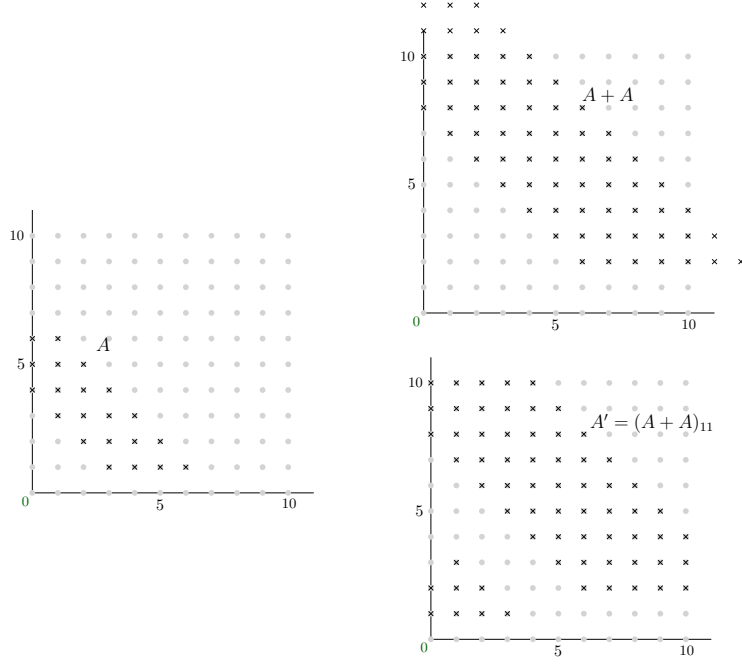to have that $2\mathbf{a} \in B_\epsilon$.

$\square$

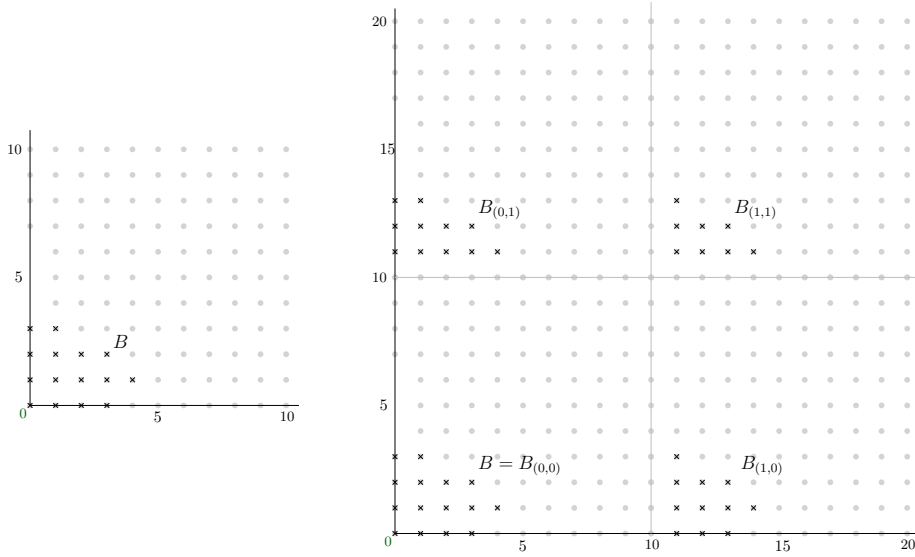Figure 3: By Proposition 5 we have that $\mathcal{C}_A^{(2)} = \mathcal{C}_{A+A} = \mathcal{C}_{A'}$.

Figure 4: Examples of sets B_ϵ for $B \subseteq [\![0, 10]\!]^2$.

The following proposition and the subsequent theorem are the key results to understand our strategy to give a code $\mathcal{C}_A$ whose square has designed minimum distance. They are both based on (simple) convexity arguments. Given a set $B \subseteq [\![0, q-1]\!]^m$, suppose that we want to find a set $A \subseteq [\![0, q-1]\!]^m$ such that $(A + A)_q \subseteq B$. If such condition happens then we will have that $(2A)_q \subseteq (A + A)_q \subseteq B$. However the following lemma allows us to construct a set A with the property that by just checking that $(2A)_q \subseteq B$, it will imply that $(A + A)_q \subseteq B$.

Proposition 7. *Let $D \subset \mathbb{R}^m$ be a convex set and consider $A := \{\mathbf{a} \in \mathbb{Z}^m \,|\, 2\mathbf{a} \in D\}$. Then, $A + A \subseteq D$.*

Proof. It suffices to check that $\mathbf{a} + \mathbf{a}' \in D$ whenever $\mathbf{a}, \mathbf{a}' \in A$. By definition of A we have that $2\mathbf{a}, 2\mathbf{a}' \in D$ and, since D is convex, the midpoint of the segment joining $2\mathbf{a}$ and $2\mathbf{a}'$, which is $\mathbf{a} + \mathbf{a}'$, also belongs to D. □

Theorem 8. *Let* $d \in \mathbb{N}$ *and let* $\mathcal{C}_B$ *be a linear code with* $B \subseteq [\![0, q-1]\!]^m$ *such that* $d \leq d(\mathcal{C}_B)$. *Consider* $C \subset \mathbb{R}^m$ *a convex set such that*

$$C \cap \{\mathbf{c} \in \mathbb{R}^m \mid 2\mathbf{c} \in [\![0, 2q-2]\!]^m \ and \ [2\mathbf{c}]_q \notin B\} = \emptyset.$$

Taking $A := C \cap [\![0, q-1]\!]^m$ *we have that* $d(\mathcal{C}_A^{(2)}) \geq d$.

Proof. To prove the statement we will just verify that $(A + A)_q \subseteq B$ and, hence, $d(\mathcal{C}_A^{(2)}) = d(\mathcal{C}_{A+A}) \geq d(\mathcal{C}_B) \geq d$. Let us take $\mathbf{a}, \mathbf{a}' \in A$, we have that $A \subset C$ and C is a convex set, so $(\mathbf{a} + \mathbf{a}')/2 \in C$. Thus, $[\mathbf{a} + \mathbf{a}']_q \in B$. $\square$

This result suggests a technique to obtain, for a given $d \in \mathbb{N}$, a set A such that $d(\mathcal{C}_A^{(2)}) \geq d$, see Algorithm 1. Indeed, it suffices to consider a linear code $\mathcal{C}_B$ such that $d \leq d(\mathcal{C}_B)$, choose a convex set $C \subset \mathbb{R}^m$ satisfying the hypotheses of the previous result and then, take $A := C \cap [\![0, q-1]\!]^m$. If one wants to have a large value of $k(\mathcal{C}_A)$ one has to choose C strategically so that it has the maximum number of integer points.

Algorithm 1: Procedure to find a set $A \subseteq [\![0, q-1]\!]^m$ with $d(\mathcal{C}_A^{(2)}) \geq d$.

Data: A set $B \subseteq [\![0, q-1]\!]^m$ such that $d(\mathcal{C}_B) \geq d$

Result: An affine variety code $\mathcal{C}_A$ such that $d(\mathcal{C}_A^{(2)}) \geq d$

Choose a convex set $C \subseteq [\![0, q-1]\!]^m$ satisfying that:

$$C \cap \{\mathbf{c} \in \mathbb{Q}^m \mid 2\mathbf{c} \in [\![0, 2q-2]\!]^m \ and \ [2\mathbf{c}]_q \notin B\} = \emptyset.$$

Take $A = C \cap \mathbb{N}^m$

In particular, if we apply the previous result to $\mathcal{C}_B$ a hyperbolic code of order d, we get the following.

Proposition 9. *Let* $C \subset \mathbb{R}^m$ *be a convex set such that* $C \cap D_\epsilon = \emptyset$ *for all* $\epsilon \in \{0, 1\}^m$, *being*

$$D_\epsilon = \{(b_1, \ldots, b_m) \mid 2b_i \in \left\{ \begin{array}{ll} [\![0, q-1]\!] & if \quad \epsilon_i = 0 \\ [\![q, 2q-2]\!] & if \quad \epsilon_i = 1 \end{array} \right. \ and \ \prod_{i=1}^m (q + \epsilon_i(q-1) - 2b_i) < d\}$$

Then, taking $A := C \cap [\![0, q-1]\!]^m$ *we have that* $d(\mathcal{C}_A^{(2)}) \geq d$.

Proof. Take $B \subseteq [\![0, q-1]\!]^m$ such that $\mathcal{C}_B = \text{Hyp}_q(d, m)$; then we have that $d(\mathcal{C}_B) \geq d$. Taking into account the following equation

$$\{\mathbf{c} \in \mathbb{R}^m \mid 2\mathbf{c} \in [\![0, 2q-2]\!]^m \ and \ [2\mathbf{c}]_q \notin B\} = \cup_{\epsilon \in [\![0,1]\!]^m} D_\epsilon.$$

and Theorem 8 the result holds. $\square$

Let us illustrate this result with an example, see Figure 5 for a graphic representation.

Example 4. Consider $q = 11$, $m = 2$ and $d = 6$. We are going to construct a code $\mathcal{C}_A$ over $\mathbb{F}_{11}$ such that $d(\mathcal{C}_A^{(2)}) \geq 6$, following Proposition 9. Consider $\mathcal{C}_B = \text{Hyp}_{11}(6, 2)$ and D_ϵ for all $\epsilon \in \{0, 1\}^2$. We choose C a convex set such that $C \cap D_\epsilon = \emptyset$ for all $\epsilon \in \{0, 1\}^2$ and take $A = C \cap [\![0, 10]\!]^2$ as in Figure 5. Then, as we proved in Proposition 9, we have that $(A + A)_{11} \subseteq B$ and, thus, $d(\mathcal{C}_A^{(2)}) = d(\mathcal{C}_{A+A}) = d(\mathcal{C}_{(A+A)_{11}}) \geq d(\mathcal{C}_B) = d(\text{Hyp}_{11}(6, 2)) = 6$.

As one can see, following the construction of Proposition 9, the number of integer points in the convex set C tuns out to be the dimension of the code A such that $d(\mathcal{C}_A^{(2)}) \geq d$. So, in order to obtain a code $\mathcal{C}_A$ with high dimension, one could look for convex sets with the most number of integer points possible. In the next section we are going to propose and compare several natural choices of the convex set C.
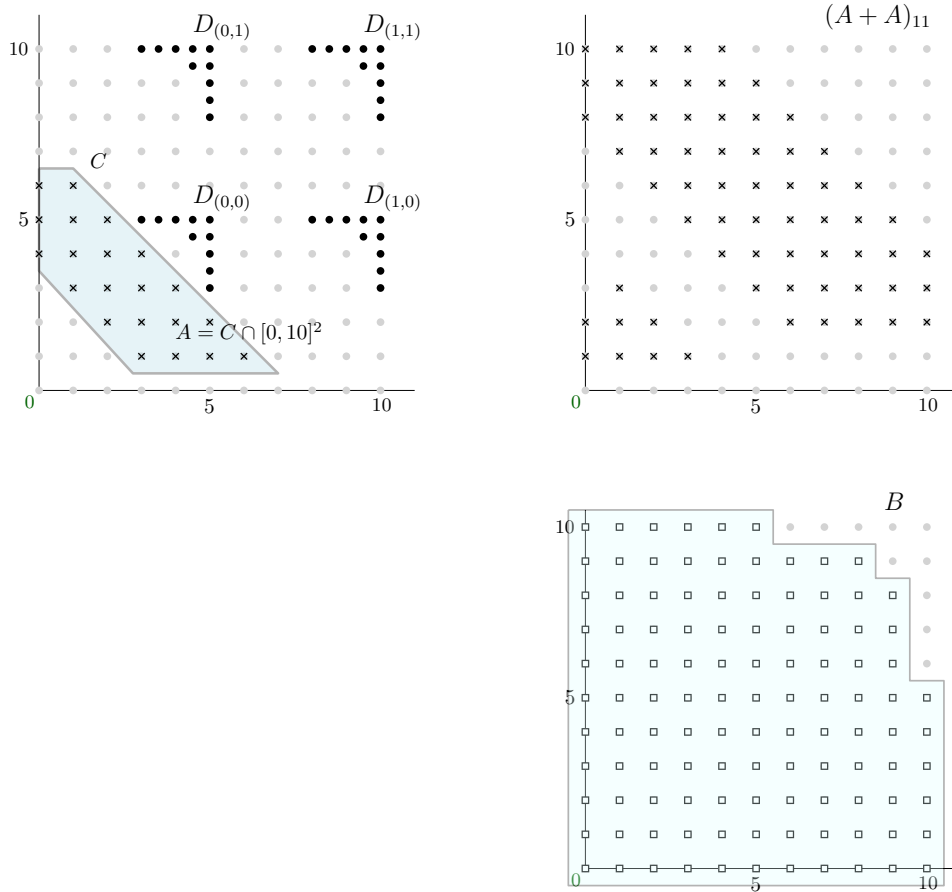
Figure 5: Example of a code $\mathcal{C}_A$ such that $(A + A)_{11} \subset B$ and, thus, $d(\mathcal{C}_A^{(2)}) \geq d(\mathcal{C}_B) = 6$ (see Example 4).

4 Choosing a convex C that gives affine codes with good parameters

In the previous section we described in Algorithm 1 a method that, given d, it returns a code $\mathcal{C}_A$ such that $d(\mathcal{C}_A^{(2)}) \geq d$. However, we would also like to find among all the codes $\mathcal{C}_A$ that verify the previous property, the one that has the highest possible dimension. For this purpose, the convex set C mentioned in Algorithm 1 must have the maximum number of integer points.

Given a fixed value d, the hyperbolic code $\mathcal{C} = \mathrm{Hyp}_q(d, m)$ of order d is, by definition, the affine variety code with the highest dimension among all the codes whose footprint-bound is $\geq d$. So it seems natural to run Algorithm 1 being $B \subset [\![0, q-1]\!]^m$ such that $\mathcal{C}_B = \mathrm{Hyp}_q(d, m)$. Now, to choose A such that $(A + A)_q \subset B$, it would be logical to expect that a certain code that behaves like a *half hyperbolic* code (see Definition 7) would be the best candidate for our goal. Surprisingly, this is not always the case. As we will prove at the end of this section, when the value of d is small enough there exist certain weighted Reed-Muller codes that outperform half hyperbolic codes.

4.1 Half hyperbolic codes

First let us introduce half hyperbolic codes.

Definition 7. **(Half hyperbolic codes)** Let $\mathcal{C}_B = \mathrm{Hyp}_q(d, m)$ be an hyperbolic code with $B = \{(i_1, \ldots, i_m) \in [\![0, q-1]\!]^m \mid (q - i_1) \cdots (q - i_m) \geq d\}$ and let

$$A = \left\{ (i_1, \ldots, i_m) \in \left[\!\!\left[0, \frac{q-1}{2}\right]\!\!\right]^m \mid (q - 2i_1) \cdots (q - 2i_m) \geq d \right\}.$$

11

In other words, for $\mathbf{a} \in \left[0, \frac{q-1}{2}\right]^m$, then $\mathbf{a} \in A$ if and only if $2\mathbf{a} \in B$. Then, $\mathcal{C}_A$ is the q-ary *half hyperbolic* code of order d and we denote it by $\mathrm{HalfHyp}_q(d, m)$.
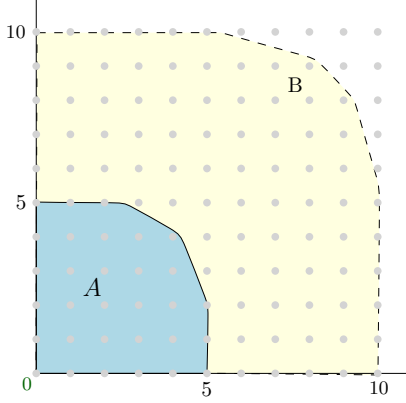

Figure 6: Figure illustrating Example 5.

Example 5. Let $B = \left\{(i,j) \in [\![0,10]\!]^2 \mid (11-i)(11-j) \geq 6\right\}$ then $\mathcal{C}_B = \mathrm{Hyp}_{11}(6,2)$. The code $\mathcal{C}_B$ has parameters $[11^2, 111, 6]_{11}$. Now we consider

$$A = \left\{(i,j) \in [\![0,5]\!]^2 \mid (11-2i)(11-2j) \geq 6\right\}$$

then $\mathcal{C}_A$ is the half hyperbolic code of order 6 and we denote it by $\mathrm{HalfHyp}_{11}(6,2)$. The code $\mathcal{C}_A$ has parameters $[11^2, 25, 49]_{11}$ and $d(\mathcal{C}_A^{(2)}) \geq 6$. See Figure 6 for a graphic representation of this example.

In the following result we use Proposition 9 to prove that the square of a half-hyperbolic code of order d has minimum distance $\geq d$.

Proposition 10. *Let* $d \in \mathbb{Z}^+$ *such that* $d < q^m$, *then* $d(\mathrm{HalfHyp}_q(d,m)^{(2)}) \geq d$.

Proof. Taking $C = \left\{\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{R}^m \mid 0 \leq a_i \leq \frac{q-1}{2}, \prod_{i=1}^{m}(q - 2a_i) \geq d\right\}$ we have that C is a convex set. Moreover, by definition of this set $C \cap D_\epsilon = \emptyset$ for all $\epsilon \in \{0,1\}^m$ (where D_ϵ is defined as in Proposition 9). Thus, taking $A = C \cap [\![0, q-1]\!]^m$, Proposition 9 guarantees that $d(\mathcal{C}_A^{(2)}) \geq d$. To finish the proof it suffices to observe that $\mathcal{C}_A$ coincides with $\mathrm{HalfHyp}_q(d,m)$. □

Providing a formula for the dimension of a half hyperbolic code is not an easy task. Nevertheless, we provide an expression for the dimension of a half hyperbolic code when $m = 2$:

Lemma 11. *Let* $d \in \mathbb{Z}^+$ *such that* $d < q^2$, *then*

$$k(\mathrm{HalfHyp}_q(d,2)) = \sum_{i=0}^{\lfloor \frac{q^2-d}{2q} \rfloor} \left\lfloor \frac{d + (q+2)(2i-q)}{4i - 2q} \right\rfloor$$

Proof. Since $\mathrm{HalfHyp}_q(2,d) = \mathcal{C}_A$ with $A = \{(i,j) \in \mathbb{N}^2 \mid 0 \leq i, j \leq (q-1)/2 \text{ and } (q-2i)(q-2j) \geq d\}$, then

$$k(\mathrm{HalfHyp}_q(2,d)) = |A|.$$

Moreover, setting $A_i := \{j \mid (i,j) \in A\}$ for all $i \in [\![0, (q-1)/2]\!]$, one has that $|A| = \sum_{i=0}^{(q-1)/2} |A_i|$ and

$$
\begin{aligned}
A_i &= \{j \mid 0 \leq j \leq (q-1)/2 \text{ and } (q-2i)(q-2j) \geq d\} \\
&= \{j \mid 0 \leq j \leq (q-1)/2 \text{ and } q - 2j \geq d/(q-2i)\} \\
&= \left\{j \mid 0 \leq j \leq \frac{d + q(2i-q)}{4i - 2q}\right\}.
\end{aligned}
$$

Hence $A_i = \emptyset$ whenever $i > (q^2 - d)/2q$; and $|A_i| = \left\lfloor \frac{d + q(2i-q)}{4i - 2q} \right\rfloor + 1$ otherwise. □

12

When $d \geq q$, the sets D_ϵ in Proposition 9 seem to 'divide' $[\![0, q-1]\!]^m$ into 2^m regions. For this reason, we propose $\mathcal{C} = \mathrm{HalfHyp}_q(d, m)$, the half hyperbolic code of order d, as a code with high dimension $k(\mathcal{C})$ and satisfying that $d(\mathcal{C}^{(2)}) \geq d$ (see Figure 7). As we will see in the following subsection, when $d < q$ one can find better options in the family of weighted Reed-Muller codes.
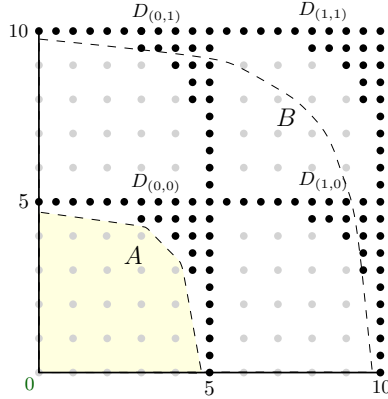

Figure 7: Example over $\mathbb{F}_{11}$ with $m = 2$ and $d = 12$. The sets D_ϵ described in Theorem 8 seem to divide $[\![0, 10]\!]^2$ into 4 regions. The code $\mathcal{C}_A = \mathrm{HalfHyp}_{11}(11, 2)$, which has parameters $[11^2, 24, 56]_{11}$ is a code with high dimension and $d(\mathcal{C}_A^{(2)}) \geq 11$.

4.2   Weighted Reed-Muller codes

It is not difficult to see that when $d \geq q$ and $\mathcal{C}$ is a weighted Reed-Muller code with $d(\mathcal{C}^{(2)}) \geq d$, then $\mathrm{FB}(\mathcal{C}) \geq \mathrm{FB}(\mathrm{HalfHyp}_q(m, d))$ and, hence, $k(\mathcal{C}) \leq k(\mathrm{HalfHyp}_q(m, d))$. As we will see at the end of this section, this is no longer true for all the values $d < q$, where some weighted Reed-Muller codes outperform half hyperbolic ones when d is small enough (see Propositions 16 and 17). For simplicity this section concerns the case $m = 2$. Before proving Propositions 16 and 17, we characterize which is the weighted Reed-Muller code with highest dimension among those verifying that the minimum distance of its square is at least d, provided $d < q$. It happens that the choice of this code depends on the parity of d (see Theorem 13 for d odd, and Theorem 15 for d even).

A first observation is that if $\mathcal{C}$ is a weighted Reed-Muller code then $\mathcal{C}^{(2)}$ is not necessarily a weighted Reed-Muller code as the following example shows.
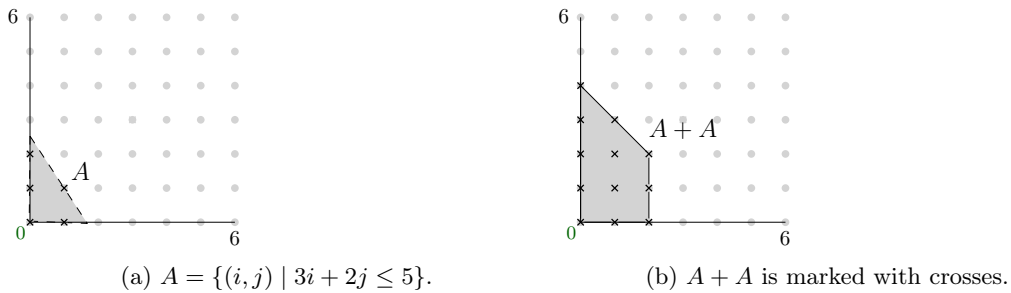

(a) $A = \{(i, j) \mid 3i + 2j \leq 5\}$.

(b) $A + A$ is marked with crosses.

Figure 8: Figure illustrating Example 6.

Example 6. Consider the weighted Reed-Muller code $\mathcal{C}_A$ over $\mathbb{F}_7$ with

$$A = \{(i, j) \mid 3i + 2j \leq 5\}.$$

Then the code $\mathcal{C}_{A+A}$ is the affine variety code that consists of the evaluation of polynomials $f \in \mathbb{F}_q[A+A]$ in the points of $\mathbb{F}_7^2$, where

$$A + A = \{(i, j) \mid 0 \leq i, j \leq 2\} \cup \{(0, 3), (0, 4), (1, 3)\}$$

13

(see Figure 8b). It is easy to check that there is no weighted Reed-Muller code $\mathcal{C}_B$ such that $(2,2) \in B$, but $(0,5),(3,0) \notin B$. Thus, $\mathcal{C}_{A+A}$ is not a weighted Reed-Muller code.

Despite the fact that the square of a weighted Reed-Muller is not necessarily a weighted Reed-Muller code, they verify the following property which will be important in the proofs of the main results.

Lemma 12. *If $\mathcal{C}$ is a weighted Reed-Muller code then $d(\mathcal{C}^{(2)}) = \mathrm{FB}(\mathcal{C}^{(2)})$.*

Proof. Let $\mathcal{C}_A$ be a weighted Reed-Muller code with $A \subset [\![0, q-1]\!]^m$ and suppose that

$$\mathrm{FB}(\mathcal{C}^{(2)}) = \prod_{i=1}^{m}(q - \alpha_i),$$

for some $\mathbf{a} = (\alpha_1, \ldots, \alpha_m) \in A + A$. Then $\mathbf{a} = \mathbf{b} + \mathbf{c}$ for some $\mathbf{b}, \mathbf{c} \in A$. Taking the componentwise partial order $\leq$ in $[\![0, q-1]\!]^m$ and $\mathbf{b}' \leq \mathbf{b}$ and $\mathbf{c}' \leq \mathbf{c}$, one has that $\mathbf{b}', \mathbf{c}' \in A$ because $\mathcal{C}_A$ is a weighted Reed-Muller code. Then one easily gets that $\mathbf{a}' \in A + A$ for all $\mathbf{a}' \leq \mathbf{a}$ and applying Lemma 18 we complete the proof. $\square$

When $d \geq q$, it is easy to verify that the weighted Reed-Muller code with maximum dimension and designed minimum distance is a Reed-Muller code. Now we are going to characterize which are the weighted Reed-Muller codes with maximum dimension and designed minimum distance when $d < q$. We will have that it is also a Reed-Muller code when d is odd, but instead, it is a weighted Reed-Muller one when d is even.

Theorem 13. *Let $\mathbb{F}_q$ be a finite field and $d \in \mathbb{Z}^+$ be an odd integer with $d < q$ and let $s := q - \frac{d+1}{2}$. If $\mathcal{C}$ is a weighted Reed-Muller code over $\mathbb{F}_q$ with $d(\mathcal{C}^{(2)}) \geq d$, then $k(\mathcal{C}) \leq k(\mathrm{RM}_q(2, s))$.*

Proof. Let $\mathcal{C}$ be a weighted Reed-Muller code over $\mathbb{F}_q$ with $d(\mathcal{C}^{(2)}) \geq d$. We assume without loss of generality that $\mathcal{C} = \mathrm{WRM}_q(\lambda, 2, (w_1, 1))$ for some $\lambda, w_1 > 0$. Taking

$$A := \{(i,j) \in [\![0, q-1]\!] \mid w_1 i + j \leq \lambda\}$$

we have that $\mathcal{C} = \mathcal{C}_A$.

In this proof we denote $a := (q-1)/2$ and $b := (q-d+1)/2$; and observe that $(2a, 2b) \in \mathbb{N}^2$ and that $s = a + b - \frac{1}{2}$.

We divide the proof in two cases depending on the value of λ.

Case I: $\lambda \leq a + b + \frac{1}{2}$. If we consider $B := \{(i,j) \in \mathbb{N}^2 \mid i + j \leq s\}$, then $\mathrm{RM}_q(2, s) = \mathcal{C}_B$. To prove that $|A| = k(\mathcal{C}) \leq k(\mathrm{RM}_q(2, s)) = |B|$ we are going to prove that either $A \subseteq B$, or the symmetry through the point (a, b):

$$\varphi: \quad \begin{array}{ccc} A - B & \longrightarrow & B - A \\ (\alpha, \beta) & \mapsto & (2a - \alpha, 2b - \beta) \end{array}$$

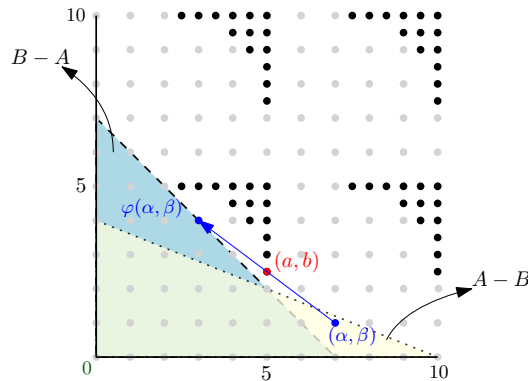is an injective map (see Figure 9 for a graphic representation of this idea).

Figure 9: Figure illustrating the proof of Theorem 13 for $d = 7$, $q = 11$, $(a, b) = (5, 2.5)$, $A = \{(i,j) \in \mathbb{N}^2 \mid 0.4i + j \leq 4\}$ and $B = \{(i,j) \in \mathbb{N}^2 \mid i + j \leq 7\}$.

Since the injectivity of φ is easy to check, we are proving that φ is well defined in three steps:

(a) if $(\alpha, \beta) \in A$, then $(2a - \alpha, 2b - \beta) \notin A$,

(b) if $(\alpha, \beta) \in A - B$, then $(2a - \alpha, 2b - \beta) \in \mathbb{N}^2$, and

(c) if $(\alpha, \beta) \in A - B$, then $(2a - \alpha, 2b - \beta) \in B$.

If (a) does not hold, then both (α, β) and $(2a - \alpha, 2b - \beta) \in A$. Hence, $(2a, 2b) = (\alpha, \beta) + (2a - \alpha, 2b - \beta) \in A + A$ and $\mathcal{C}_A^{(2)} = \mathcal{C}_{A+A}$. Since $\mathcal{C}_A$ is a weighted Reed-Muller code, by Lemma 12 we have that $d \le d(\mathcal{C}^{(2)}) = \mathrm{FB}(\mathcal{C}^{(2)}) \le (q - 2a)(q - 2b) = d - 1$, a contradiction.

We observe that $(2a - \alpha, 2b - \beta) \in \mathbb{Z}^2$ and that $\alpha \le q - 1 = 2a$, so to prove (b) we just need to see that $2b - \beta \ge 0$. Assume that $2b < \beta$ and let us prove that

(b.1) $P_1 = (a, b + \frac{1}{2})$, $Q_1 = (a, b - \frac{1}{2}) \in A$ if q is odd, or

(b.2) $P_2 = (a + \frac{1}{2}, b)$, $Q_2 = (a - \frac{1}{2}, b) \in A$ if q is even.

If $\alpha > a$, then $\alpha \ge a + \frac{1}{2}$ since $\beta \ge 2b + 1 > b + \frac{1}{2}$ we have that $P_1, Q_1 \in A$ in case (b.1) and $P_2, Q_2 \in A$ in case (b.2). If $\alpha \le a$, from one side we have that $(\alpha, \beta) \notin B$, so

$$\alpha + \beta \ge s + 1 = a + b + \frac{1}{2} \tag{3}$$

and, from the other side we have that $(\alpha, \beta) \in A$, which implies that

$$w_1 \alpha + \beta \le \lambda. \tag{4}$$

From (3) and (4) we get that

$$(w_1 - 1)\alpha + a + b + \frac{1}{2} \le (w_1 - 1)\alpha + \alpha + \beta \le w_1\alpha + \beta \le \lambda \le a + b + \frac{1}{2}$$

and, thus, $w_1 \le 1$. Hence, using that $\alpha \le a$, (3) and (4) we get that

$$
\begin{aligned}
w_1(a + \frac{1}{2}) + b \ &\le\ w_1 a + b + \frac{1}{2} \\
&=\ a + b + \frac{1}{2} + (w_1 - 1)a \\
&\le\ a + b + \frac{1}{2} + (w_1 - 1)\alpha \\
&\le\ \alpha + \beta + (w_1 - 1)\alpha = \\
&=\ w_1\alpha + \beta \le \lambda
\end{aligned}
$$

and we conclude that $P_1, Q_1 \in A$ in case (b.1) and $P_2, Q_2 \in A$ in case (b.2). Moreover, since $P_1 + Q_1 = P_2 + Q_2 = (2a, 2b)$, in both cases we obtain that $(2a, 2b) \in A + A$ and $\mathcal{C}_A^{(2)} = \mathcal{C}_{A+A}$. Since $\mathcal{C}_A$ is a weighted Reed-Muller code, by Lemma 12 we have that $d \le d(\mathcal{C}^{(2)}) = \mathrm{FB}(\mathcal{C}^{(2)}) \le (q - 2a)(q - 2b) = d - 1$, a contradiction.

Let us prove now (c). Whenever $(\alpha, \beta) \in A - B$, then $\alpha + \beta \ge s + 1$. Since $a + b = s + \frac{1}{2}$, we have that $2a - \alpha + 2b - \beta \le s$ and $(2a - \alpha, 2b - \beta) \in \mathbb{N}^2$ by (b), so $(2a - \alpha, 2b - \beta) \in B$.

Case II: $\lambda > a + b + \frac{1}{2}$. We claim that $\frac{\lambda}{w_1} < a + b + \frac{1}{2}$. Otherwise, we have that $(a + \frac{1}{2}, b), (a - \frac{1}{2}, b) \in A$ if q is even, or $(a, b + \frac{1}{2}), (a, b - \frac{1}{2}) \in A$ if q is odd. In both cases $(2a, 2b) \in A + A$ and $\mathcal{C}_A^{(2)} = \mathcal{C}_{A+A}$. Since $\mathcal{C}_A$ is a weighted Reed-Muller code, by Lemma 12 we have that $d \le d(\mathcal{C}^{(2)}) \le (q - 2a)(q - 2b) = d - 1$, a contradiction.

Since $\frac{\lambda}{w_1} < a + b + \frac{1}{2}$, then $A = \{(i, j) \in \mathbb{N}^2 \,|\, 0 \le i, j \le q - 1 \text{ and } i + \frac{1}{w_1}j \le \frac{\lambda}{w_1}\}$ and a symmetric argument to *Case I* applies here. $\square$

Since $(\mathrm{RM}_q(2, s)^{(2)}) = d$, this means that $\mathrm{RM}_q(2, s)$ has the highest dimension among all the weighted Reed-Muller codes $\mathcal{C}$ such that $d(\mathcal{C}^{(2)}) \ge d$.

Lemma 14. *Let $\mathbb{F}_q$ be a finite field and $d \in \mathbb{Z}^+$ be an even integer with $d < q$ and let $s := q - \frac{d}{2}$. Let*

$$
\begin{aligned}
B_1 \ &:=\ \{(i, j) \in \mathbb{N}^2 \,|\, i + j < s\} \cup \{(i, j) \in \mathbb{N}^2 \,|\, i + j = s \text{ and } j < (q - d + 1)/2\}, \text{ and} \\
B_2 \ &:=\ \{(i, j) \in \mathbb{N}^2 \,|\, i + j < s\} \cup \{(i, j) \in \mathbb{N}^2 \,|\, i + j = s \text{ and } i < (q - d + 1)/2\}
\end{aligned}
$$

then, $\mathcal{C}_{B_1}$ and $\mathcal{C}_{B_2}$ are weighted Reed-Muller codes and $k(\mathcal{C}_{B_1}) = k(\mathcal{C}_{B_2})$.

Proof. It suffices to perturb slightly the line $x + y = s$ to get that both $\mathcal{C}_{B_1}$ and $\mathcal{C}_{B_2}$ are weighted Reed-Muller codes. Indeed it is easy to check that

$$k(\mathcal{C}_{B_1}) = |B_1| = \frac{(q - \frac{d}{2} + 2)(q - \frac{d}{2} + 1)}{2} + \frac{q - \frac{d}{2}}{2} - 1 = k(\mathcal{C}_{B_2})$$
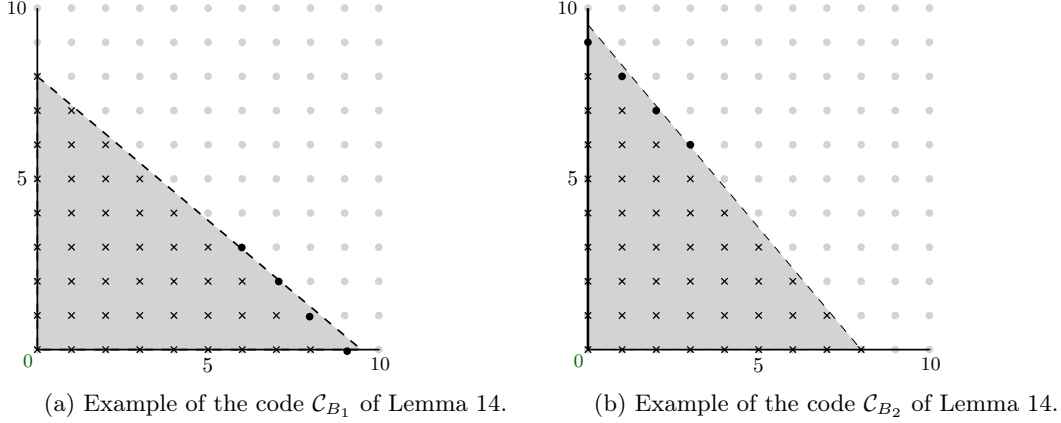
See an illustration in Figure 10. □

(a) Example of the code $\mathcal{C}_{B_1}$ of Lemma 14. (b) Example of the code $\mathcal{C}_{B_2}$ of Lemma 14.

Figure 10: Example illustrating Lemma 14 with $q = 11$ and $d = 4$.

We can now consider the case when the minimum distance is even.

Theorem 15. Let $\mathbb{F}_q$ be a finite field and $d \in \mathbb{Z}^+$ be an even integer with $d < q$. If $\mathcal{C}$ is a weighted Reed-Muller code over $\mathbb{F}_q$ with $d(\mathcal{C}^{(2)}) \geq d$, then $k(\mathcal{C}) \leq k(\mathcal{C}_B)$, where $\mathcal{C}_B$ is any of the weighted Reed-Muller codes described in Lemma 14.

Proof. This proof will follow the same ideas in Theorem 13. Let $\mathcal{C}$ be a weighted Reed-Muller code over $\mathbb{F}_q$ with $d(\mathcal{C}^{(2)}) \geq d$. We assume without loss of generality that $\mathcal{C} = \mathrm{WRM}_q(\lambda, 2, w_1, 1)$ for some $\lambda, w_1 > 0$. Taking

$$A := \{(i, j) \in [\![0, q-1]\!] \mid w_1 i + j \leq \lambda\}$$

we have that $\mathcal{C} = \mathcal{C}_A$.

In this proof we denote $a := (q-1)/2$ and $b := (q - d + 1)/2$; and observe that either $(a, b) \in \mathbb{N}^2$ or both $(a - \frac{1}{2}, b + \frac{1}{2}), (a + \frac{1}{2}, b - \frac{1}{2}) \in \mathbb{N}^2$. We divide the proof in two cases depending on the value of λ.

Case I: $\lambda \leq a + b$. We take $B = B_1$ as in Lemma 14. To prove that $|A| = k(\mathcal{C}) \leq k(\mathcal{C}_B) = |B|$ we are going to prove that either $A \subseteq B$, or

$$\varphi : \quad A - B \quad \longrightarrow \quad B - A$$
$$\quad (\alpha, \beta) \quad \mapsto \quad (2a - \alpha, 2b - \beta)$$

is an injective map (see Figure 11 for a graphic representation of this idea).

Since the injectivity of φ is easy to check, we are showing that φ is well defined in three steps:

(a) if $(\alpha, \beta) \in A$, then $(2a - \alpha, 2b - \beta) \notin A$,

(b) if $(\alpha, \beta) \in A - B$, then $(2a - \alpha, 2b - \beta) \in \mathbb{N}^2$, and

(c) if $(\alpha, \beta) \in A - B$, then $(2a - \alpha, 2b - \beta) \in B$.

If (a) does not hold, then both (α, β) and $(2a - \alpha, 2b - \beta) \in A$. Hence, $(2a, 2b) = (\alpha, \beta) + (2a - \alpha, 2b - \beta) \in A + A$ and $\mathcal{C}_A^{(2)} = \mathcal{C}_{A+A}$. Since $\mathcal{C}_A$ is a weighted Reed-Muller code, by Lemma 12 we have that

$$d \leq d(\mathcal{C}^{(2)}) = \mathrm{FB}(\mathcal{C}^{(2)}) \leq (q - 2a)(q - 2b) = d - 1,$$

a contradiction.

We observe that $(2a - \alpha, 2b - \beta) \in \mathbb{Z}^2$ and that $\alpha \leq q - 1 = 2a$, so to prove (b) we just need to see that $2b - \beta \geq 0$. Assume that $2b < \beta$ and let us prove that
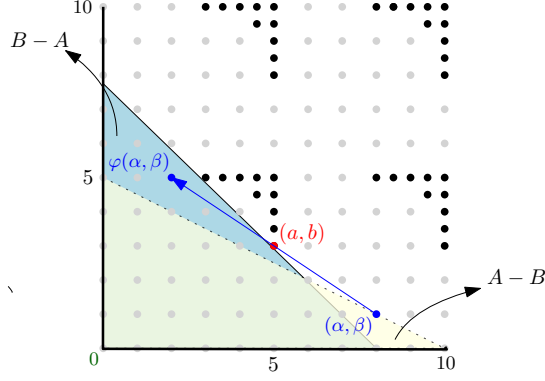
16

Figure 11: Figure illustrating the proof of Theorem 15 for $d = 6$, $q = 11$, $(a, b) = (5, 3)$, $A = \{(i, j) \in \mathbb{N}^2 \mid 0.4i + j \leq 4\}$ and $B = \{(i, j) \in \mathbb{N}^2 \mid i + j < 8\} \cup \{(i, j) \in \mathbb{N}^2 \mid i + j = 8 \text{ and } j < 3\}$.

(b.1) $P = (a, b) \in A$ if q is odd, or

(b.2) $Q_1 = (a - \frac{1}{2}, b + \frac{1}{2})$, $Q_2 = (a + \frac{1}{2}, b - \frac{1}{2}) \in A$ if q is even.

If $\alpha > a$, then $\alpha \geq a + \frac{1}{2}$ since $\beta \geq 2b + 1 > b + \frac{1}{2}$ we have that $P \in A$ in case (b.1) and $Q_1, Q_2 \in A$ in case (b.2). If $\alpha \leq a$, from one side we have that $(\alpha, \beta) \notin B$, so

$$\alpha + \beta \geq a + b \tag{5}$$

and, if we have equality, then $\beta \geq b$. From the other side we have that $(\alpha, \beta) \in A$, which implies that

$$w_1 \alpha + \beta \leq \lambda. \tag{6}$$

From (5) and (6) we get that

$$(w_1 - 1)\alpha + a + b \leq (w_1 - 1)\alpha + \alpha + \beta = w_1 \alpha + \beta \leq \lambda \leq a + b$$

and, thus, $w_1 \leq 1$. Hence, we separate three cases:

Subcase I.I. If $\alpha + \beta > a + b$.

$$
\begin{aligned}
w_1(a + \tfrac{1}{2}) + b - \tfrac{1}{2} &\leq w_1 a + b \leq w_1(a - \tfrac{1}{2}) + b + \tfrac{1}{2} \\
&< w_1 a + b + \tfrac{1}{2} \\
&= a + b + \tfrac{1}{2} + (w_1 - 1)a \\
&\leq a + b + \tfrac{1}{2} + (w_1 - 1)\alpha \\
&< \alpha + \beta + (w_1 - 1)\alpha \\
&= w_1 \alpha + \beta \leq \lambda.
\end{aligned}
$$

So, $P \in A$ if q is odd, or both $Q_1, Q_2 \in A$ if q is even.

Subcase I.II. If $\alpha + \beta = a + b$ and q is odd. Since $\beta \geq b$ and $w_1 < 1$, we have that $w_1(\alpha - a) + \beta - b \geq w_1(\alpha - a + \beta - b) = 0$. As a consequence,

$$w_1 a + b \leq w_1 a + b + w_1(\alpha - a) + \beta - b = w_1 \alpha + \beta \leq \lambda.$$

Therefore $P \in A$.

Subcase I.III. If $\alpha + \beta = a + b$ and q is even. Since $\beta \geq b$ and $b \notin \mathbb{N}$, then $\beta \geq b + \frac{1}{2}$; moreover, $w_1 < 1$, then we have that $w_1(\alpha - a + \frac{1}{2}) + \beta - b - \frac{1}{2} \geq w_1(\alpha - a + \frac{1}{2} + \beta - b - \frac{1}{2}) = 0$. As a consequence,

$$
\begin{aligned}
w_1(a + \tfrac{1}{2}) + b - \tfrac{1}{2} &\leq w_1(a - \tfrac{1}{2}) + b + \tfrac{1}{2} \\
&\leq w_1(a - \tfrac{1}{2}) + b + \tfrac{1}{2} + w_1(\alpha - a + \tfrac{1}{2}) + \beta - b - \tfrac{1}{2} \\
&= w_1 \alpha + \beta \leq \lambda
\end{aligned}
$$

17

and we conclude that $Q_1, Q_2 \in A$.

Moreover, since $P + P = Q_1 + Q_2 = (2a, 2b)$, in both cases we obtain that $(2a, 2b) \in A + A$ and $\mathcal{C}_A^{(2)} = \mathcal{C}_{A+A}$. Since $\mathcal{C}_A$ is a weighted Reed-Muller code, by Lemma 12 we have that $d \leq d(\mathcal{C}^{(2)}) \leq (q - 2a)(q - 2b) = d - 1$, a contradiction.

Let us prove now (c). Take $(\alpha, \beta) \in A - B$, then either

(c.1) $\alpha + \beta > a + b$, or

(c.2) $\alpha + \beta = a + b$ and $\beta \geq b$.

In (c.1) we have that $2a - \alpha + 2b - \beta < a + b$, so $(2a - \alpha, 2b - \beta) \in B$. In (c.2) we observe that $\beta \neq b$ because $(a, b) \notin A$. Then, we have that $2a - \alpha + 2b - \beta = a + b$ and $2b - \beta < b$, so $(2a - \alpha, 2b - \beta) \in B$.

Case II: $\lambda \geq a + b$. We claim that $\frac{\lambda}{w_1} < a + b$. Otherwise, we have that $P \in A$ if q is odd, or $Q_1, Q_2 \in A$ if q is even. In both cases $(2a, 2b) \in A + A$ and $\mathcal{C}_A^{(2)} = \mathcal{C}_{A+A}$. Since $\mathcal{C}_A$ is a weighted Reed-Muller code, by Lemma 12 we have that $d \leq d(\mathcal{C}^{(2)}) \leq (q - 2a)(q - 2b) = d - 1$, a contradiction. Since $\frac{\lambda}{w_1} < a + b$, then $A = \{(i, j) \in \mathbb{N}^2 \mid 0 \leq i, j \leq q - 1 \text{ and } i + \frac{1}{w_1} j \leq \frac{\lambda}{w_1}\}$ and a symmetric argument to **Case I** using $B = B_2$ with B_2 as in Lemma 14 applies here. $\square$

Finally, we are proving that when d is small enough (more precisely, when $d < (2 - \sqrt{2})q$), then there are weighted Reed-Muller codes that have more dimension and whose square has the same designed minimum distance as the corresponding half hyperbolic code.

Proposition 16. *If $d < (2 - \sqrt{2})q$ and d odd, then*

$$k\left(\mathrm{RM}_q\left(2, q - \frac{d - 1}{2}\right)\right) > k(\mathrm{HalfHyp}_q(2, d)).$$

Proof. Take notice that

$$
\begin{aligned}
k\left(\mathrm{RM}_q\left(2, q - \frac{d - 1}{2}\right)\right) &= \frac{(q - \frac{d-1}{2} + 2)(q - \frac{d-1}{2} + 1)}{2} \\
&= \frac{(2q - d + 5)(2q - d + 3)}{8} = A
\end{aligned}
$$

$$k(\mathrm{HalfHyp}_q(2, d)) < \left(\frac{q + 1}{2}\right)^2 - 2\left(\frac{d - 1}{2}\right) + 1 = B$$

Therefore if $A - B > 0$ then our claim holds. Now $A - B > 0$ if $p(d) = d^2 - 4qd + (2q^2 + 12q + 13) > 0$. This defines a quadratic function whose vertex represent its minimum value. That is, $p(d) > 0$ if $d > 2q + \sqrt{2q^2 - 12q - 13}$ or $d < 2q - \sqrt{2q^2 - 12q - 13}$. Take notice that if

$$d < (2 - \sqrt{2})q < 2q - \sqrt{2q^2 - 12q - 13}$$

then: $k\left(\mathrm{RM}_q\left(2, q - \frac{d-1}{2}\right)\right) > k(\mathrm{HalfHyp}_q(2, d))$. $\square$

Proposition 17. *If $d < (2 - \sqrt{2})q$ and d even, then $k(\mathcal{C}_B) > k(\mathrm{HalfHyp}_q(2, d))$ where $\mathcal{C}_B$ is one of the weighted Reed-Muller codes defined in Lemma 14.*

Proof. Take notice that

$$
\begin{aligned}
k(\mathcal{C}_B) &= \frac{(q - \frac{d-1}{2} + 2)(q - \frac{d-1}{2} + 1)}{2} + \frac{q - \frac{d}{2}}{2} - 1 \\
&= \frac{1}{8}d^2 - \frac{1}{2}dq + \frac{1}{2}q^2 - d + 2q = A
\end{aligned}
$$

$$k(\mathrm{HalfHyp}_q(2, d)) < \left(\frac{q + 1}{2}\right)^2 - 2\left(\frac{d - 1}{2}\right) + 1 = B$$

Therefore if $A - B > 0$ then our claim is true. Now $A - B > 0$ if $p(d) = d^2 - 4dq + (2q^2 + 12q - 18) > 0$. This defines a quadratic function whose vertex represent its minimum value. That is, $p(d) > 0$ if $d > 2q + \sqrt{2q^2 - 12q + 18}$ or $d < 2q - \sqrt{2q^2 - 12q + 18}$. Take notice that if

$$d < (2 - \sqrt{2})q < 2q - \sqrt{2q^2 - 12q + 18},$$

then: $k(\mathcal{C}_B) > k(\mathrm{HalfHyp}(2, d))$. $\qquad\square$

Example 7. We continue with Example 5. That is, consider $\mathcal{C}_B = \mathrm{Hyp}_{11}(6, 2)$ with $B = \left\{ (i, j) \in [\![0, 10]\!]^2 \mid (11 - i)(11 - j) \right.$
We recall that the half hyperbolic code of order 6 has parameters $[11^2, 25, 49]_{11}$ and $d(\mathcal{C}_A^{(2)}) \geq 6$.

Taking A_1 as in Figure 12a, then $\mathcal{C}_{A_1}$ is a weighted Reed-Muller code with parameters $[11^2, 34, 9]_{11}$ such that $d(\mathcal{C}_{A_1}^{(2)}) \geq 6$. Take notice that this example already gives an affine variety code with higher dimension than the half hyperbolic code.

Moreover, by Theorem 15, we know that if we take the set A_2 defined in Figure 12b then the weighted Reed-Muller code $\mathcal{C}_{A_2}$ has higher dimension than any other weighted Reed-Muller code $\mathcal{C}$ such that $d(\mathcal{C}^{(2)}) \geq 6$. In particular, we know by Theorem 15 that $k(\mathcal{C}_{A_2}) \geq k(\mathcal{C}_{A_1})$. Note that $\mathcal{C}_{A_2}$ is defined as in Lemma 14 and has parameters $[11^2, 39, 33]_{11}$.

(a) Set A_1 of Example 7.
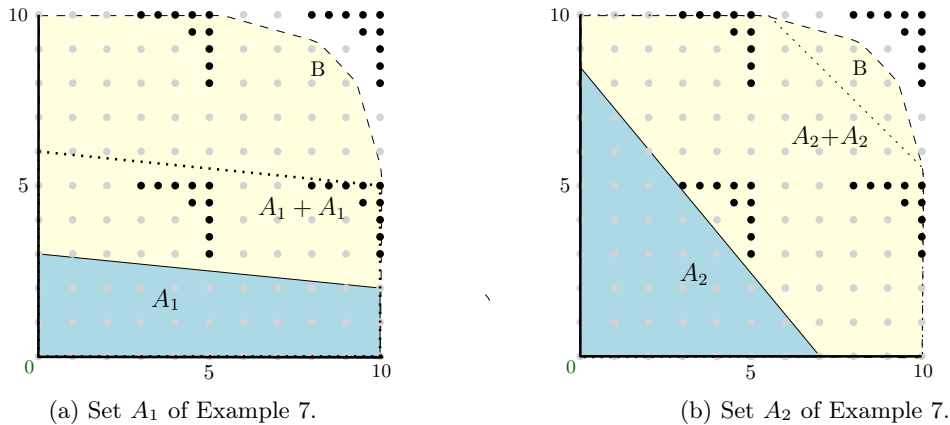
(b) Set A_2 of Example 7.

Figure 12: Figure illustrating Example 7.

References

[1] M. Ben-Or, S. Goldwasser, and A. Wigderson. *Completeness theorems for non-cryptographic fault-tolerant distributed computation.* In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, pages 1–10, NY, USA, 1988.

[2] I. Cascudo. *On squares of cyclic codes.* IEEE Trans. Inform. Theory, 65(2):1034–1047, 2019.

[3] I. Cascudo, R. Cramer, D. Mirandola, and G. Zémor. *Squares of random linear codes.* IEEE Trans. Inform. Theory, 61(3):1159–1173, 2015.

[4] I. Cascudo, J. S. Gundersen, and D. Ruano. *Squares of matrix-product codes.* arXiv, abs/1903.05494, 2019.

[5] A. Couvreur, P. Gaborit, V. Gauthier-Umaña, A. Otmani and J.-P. Tillich. *Distinguisher-based attacks on public-key cryptosystems using Reed-Solomon codes.* Des. Codes Cryptogr., 73(2):641–666, 2014.

[6] A. Couvreur, A. Otmani, and J.-P. Tillich. *Polynomial time attack on wild McEliece over quadratic extensions.* In Advances in cryptology, EUROCRYPT 2014, volume 8441 of Lecture Notes in Comput. Sci., pages 17–39. Springer, Heidelberg, 2014.

[7] A. Couvreur, I. Márquez-Corbella, R. Pellikaan. *Cryptanalysis of McEliece Cryptosystem Based on Algebraic Geometry Codes and Their Subcodes.* IEEE Trans. Inform. Theory, 63(8):5404 - 5418, 2017.

[8] D. Chaum, C. Crépeau, and I. Damgård. *Multiparty unconditionally secure protocols.* In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, pages 11–19, NY, USA, 1988.

[9] D.A. Cox, J. Little and D. O'Shea. *Using Algebraic Geometry.* Second Edition. Graduate Texts in Mathematics, Springer New York, 2005.

[10] D.A. Cox, J. Little and D. O'Shea. *Ideals, Varieties and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Third Edition. Graduate Texts in Mathematics, Springer New York, 2007.

[11] R. Cramer, I. Damgå rd, and U. Maurer. *General secure multi-party computation from any linear secret-sharing scheme.* In *Advances in cryptology EUROCRYPT 2000 (Bruges)*, volume 1807 of *Lecture Notes in Comput. Sci.*, pages 316–334. Springer, Berlin, 2000.

[12] R. Cramer, I. Damgård, and J. B. Nielsen. *Secure Multiparty Computation and Secret Sharing.* Cambridge University Press, New York, NY, USA, 1st edition, 2015.

[13] I. Damgård, J. B. Nielsen, M. Nielsen, and S. Ranellucci. *The TinyTable protocol for 2-party secure computation, or: Gate-scrambling revisited.* In *Advances in cryptology CRYPTO 2017. Part I*, volume 10401 of *Lecture Notes in Comput. Sci.*, pages 167–187. Springer, Cham, 2017.

[14] I. Damgård and S. Zakarias. *Constant-overhead secure computation of boolean circuits using pre-processing.* In *Proceedings of the 10th Theory of Cryptography Conference on Theory of Cryptography*, TCC'13, pages 621–641, Berlin, Heidelberg, Springer-Verlag, 2013.

[15] G.-L. Feng, T. R. N. Rao. *Improved geometric Goppa codes.* I. Basic theory. Special issue on algebraic geometry codes. IEEE Trans. Inform. Theory, 41(6):1678–1693, 1995.

[16] J. Fitzgerald and R. F. Lax, *Decoding affine variety codes using Gröbner bases.* Des. Codes Cryptogr., vol. 13, 1998.

[17] C. Galindo, F. Hernando, and D. Ruano. *Stabilizer quantum codes from J-affine variety codes and a new Steane-like enlargement. Quantum Inf. Process.*, 14(9):3211–3231, 2015.

[18] O. Geil, T. Hholdt. *Footprints or generalized Bezout's theorem.* IEEE Trans. Inform. Theory, 46(2):635–641, 2000.

[19] O. Geil, and T. Hholdt. *On hyperbolic codes.* Applied algebra, algebraic algorithms and error-correcting codes (Melbourne, 2001), 159–171, Lecture Notes in Comput. Sci., 2227, Springer, Berlin, 2001.

[20] O. Geil. *On codes from norm-trace curves.* Finite Fields Appl. 9, 351-371, 2003.

[21] O. Geil. *On the second weight of generalized Reed-Muller codes.* Des. Codes Cryptogr. 48, 323-330, 2008.

[22] T. Hholdt, J. M. van Lint, R. Pellikaan. *Algebraic geometry codes.* Handbook of coding theory, Vol. I, II, 871–961, North-Holland, Amsterdam, 1998.

[23] I. Márquez-Corbella, E. Martínez-Moro, R. Pellikaan, and D. Ruano. *Computational aspects of retrieving a representation of an algebraic geometry code.* J. Symbolic Comput., 64:67–87, 2014.

[24] R. Pellikaan. *On decoding by error location and dependent sets of error positions.* Discrete Math., 106-107:369-381, 1992.

[25] R. Pellikaan. *On the existence of error-correcting pairs.* Statistical Planning and Inference, 51: 229-242, 1996.

[26] H. Randriambololona. *Asymptotically good binary linear codes with asymptotically good self-intersection spans.* IEEE Trans. Inform. Theory, 59(5):3038–3045, 2013.

[27] H. Randriambololona. *On products and powers of linear codes under component wise multiplication.* In *Algorithmic arithmetic, geometry and coding theory*, volume 637 of Contemp. Math., pages 3-78, Amer. Math. Soc., Providence, RI, 2015.

[28] A. B. Srensen. *Weighted Reed-Muller codes and algebraic-geometric codes.* IEEE Trans. Inform. Theory 38(6): 1821–1826, 1992.

[29] C. Wieschebrink. *Crytanalysis of the Niederreiter public key scheme based on GRS subcodes.* In Post-Quatum Cryptography, volume 6061 of Lecture Notes in Comput. Sci. pages 61-72. Springer-Verlag Berlin Heidelberg, 2010.

A   For which affine codes $\mathcal{C}_A$ is it verified that $\mathrm{FB}(\mathcal{C}_A) = d(\mathcal{C}_A)$?

Let $A \subseteq [\![0, q-1]\!]^m$ and consider the code $\mathcal{C}_A$ as the affine variety code $C(I, L)$ with $I = (0)$ and $L = \mathbb{F}_q[A]$. Then, we know that the length of $\mathcal{C}_A$ is q^m and its dimension coincides with the cardinality of the set A. Moreover its minimum distance, denoted as $d(\mathcal{C}_A)$, satisfies that $d(\mathcal{C}_A) \geq \mathrm{FB}(\mathcal{C}_A)$. In this section we will study when these two values coincide. More concretely, we provide sufficient conditions to have the equality $d(\mathcal{C}_A) = \mathrm{FB}(\mathcal{C}_A)$.

Lemma 18. Suppose that $\mathrm{FB}(\mathcal{C}_A) = (q - \alpha_1) \cdots (q - \alpha_m)$. Then $d(\mathcal{C}_A) = \mathrm{FB}(\mathcal{C}_A)$ if all the elements $\beta = (\beta_1, \ldots, \beta_m)$ with $0 \leq \beta_i \leq \alpha_i$ belong to the set A.

Proof. First, to simplify the proof let us suppose that $m = 2$. Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be the ordered enumeration of the q^2 different points of $\mathbb{F}_q^2$. Suppose that $\mathrm{FB}(\mathcal{C}_A) = (q - \alpha_1)(q - \alpha_2)$. Now we can define the polynomial

$$f(x) = (X_1 - P_1) \cdots (X_1 - P_{\alpha_1}) \cdot (X_2 - P_1) \cdots (X_2 - P_{\alpha_2}).$$

Take notice that by hypothesis $f(X_1, X_2) \in \mathbb{F}_q[A]$ since all the elements $\beta = (\beta_1, \beta_2)$ with $0 \leq \beta_1 \leq \alpha_1$ and $0 \leq \beta_2 \leq \alpha_2$ belongs to the set A. Moreover, the $\mathbb{F}_q$-roots of f are all the points of form:

$$(P_i, z_2) \quad \text{and} \quad (z_1, P_j) \quad \text{with } i \in \{1, \ldots, \alpha_1\}, \, j \in \{1, \ldots, \alpha_2\} \text{ and } z_1, z_2 \in \mathbb{F}_q.$$

That is, the number of $\mathbb{F}_q$-roots of $f(x)$ is $(\alpha_1 + \alpha_2)q - \alpha_1\alpha_2$. Therefore, we have found a codeword $\mathbf{c} = \mathrm{ev}_\mathcal{P}(f) \in \mathcal{C}_A$ of weight $q^2 - (\alpha_1 + \alpha_2)q - \alpha_1\alpha_2 = \mathrm{FB}(\mathcal{C}_A)$. Hence the minimum distance of $\mathcal{C}_A$ is $\mathrm{FB}(\mathcal{C}_A)$.

The generalization to m variables is straightforward. Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be the ordered enumeration of the q^m different points of $\mathbb{F}_q^m$. Then, using all the hypothesis we can define the following polynomial in $\mathbb{F}_q[A]$:

$$f(X_1, \ldots, X_m) = \prod_{i=1}^{m} (X_i - P_1) \cdots (X_i - P_{\alpha_i}) \in \mathbb{F}_q[A].$$

Thus, we have found a codeword of $\mathcal{C}_A$ of weight $\mathrm{FB}(\mathcal{C}_A)$, hence $d(\mathcal{C}_A) = \mathrm{FB}(\mathcal{C}_A)$. ☐

The following result shows that if l is a divisor of $q-1$ then, there exists a polynomial $f(x) = X^l - \alpha \in \mathbb{F}_q[X]$ with small support but a large number of $\mathbb{F}_q$-roots. This result will be useful for computing the minimum distance of codes of type $\mathcal{C}_A$ by just checking that a very small number of points belongs to the set A.

Lemma 19. Let α be a primitive element of $\mathbb{F}_q^*$. Consider the polynomial $f(X) = X^l - \alpha^j \in \mathbb{F}_q[X]$. Then $X^l - \alpha^j$ has at least one roots in $\mathbb{F}_q$ if and only if $\gcd(l, q-1)$ divides j. In such case, the exactly number of $\mathbb{F}_q$-roots of $f(X)$ is $\gcd(l, q-1)$.

Proof. Suppose that α^i is an $\mathbb{F}_q$-root of $f(X)$, then $f(\alpha^i) = 0$, that is $\alpha^{il} = \alpha^j$ which implies that the order of α, which is $q-1$, divides $il-1$. In other words, there exists an integer x such that $x(q-1)+il = j$. Take notice that such x exists if and only if $\gcd(l, q-1)$ divides j.

In such case, if (x, y) is a solution of the equation $x(q-1) + yl = j$. Then, all solutions of this equations has the form:

$$\left(x - \lambda \frac{l}{\gcd(l, q-1)}, y + \lambda \frac{q-1}{\gcd(l, q-1)}\right) \text{ with } \lambda \in \mathbb{Z}$$

Therefore, if $f(X)$ has at least one root in $\mathbb{F}_q$, then it will have exactly $\gcd(l, q-1)$ $\mathbb{F}_q$-roots. $\square$

Corollary 20. Suppose that $\mathrm{FB}(\mathcal{C}_A) = (q-l)q^{m-1}$ *with l a divisor of $q-1$. Then, $d(\mathcal{C}_A) = \mathrm{FB}(\mathcal{C}_A)$ if* $\{1, X_i^l\} \subseteq \mathbb{F}_q[A]$ *for some $i \in \{1, \ldots, m\}$.*

Proof. By hypothesis we can define the following polynomial in $\mathbb{F}_q[A]$:

$$f(X) = X_i^l - \beta \text{ for certain } \beta \in \mathbb{F}_q.$$

Then, by Lemma 19, $f(X)$ has lq^{m-1} $\mathbb{F}_q$-roots. That is, we have found a codeword of $\mathcal{C}_A$ of weight $\mathrm{FB}(\mathcal{C}_A)$, hence $d(\mathcal{C}_A) = \mathrm{FB}(\mathcal{C}_A)$. $\square$

Lemma 21. Suppose that $\mathrm{FB}(\mathcal{C}_A) = (q - kl)q^{m-1}$ *with l a divisor of $q-1$. Then, $d(\mathcal{C}_A) = \mathrm{FB}(\mathcal{C}_A)$ if* $\{1, X_i^l, X_i^{2l}, \ldots, X_i^{kl}\} \subseteq \mathbb{F}_q[A]$ *for some $i \in \{1, \ldots, m\}$.*

Proof. By hypothesis we can define the following polynomial in $\mathbb{F}_q[A]$:

$$f(X) = (X_i^l - \beta)(X_i^{2l} - \beta^2) \cdots (X_i^{kl} - \beta^k) \text{ for certain } \beta \in \mathbb{F}_q.$$

Then, by Lemma 19, $f(X)$ has klq^{m-1} $\mathbb{F}_q$-roots. That is, we have found a codeword of $\mathcal{C}_A$ of weight $\mathrm{FB}(\mathcal{C}_A)$, hence $d(\mathcal{C}_A) = \mathrm{FB}(\mathcal{C}_A)$. $\square$

Lemma 22. Suppose that $\mathrm{FB}(\mathcal{C}_A) = (q-l_1) \cdots (q-l_m)$ *with l_i a divisor of $q-1$. Then, $d(\mathcal{C}_A) = \mathrm{FB}(\mathcal{C}_A)$ if* $\{1, X_1^{l_1}, \cdots, X_m^{l_m}\} \subseteq \mathbb{F}_q[A]$.

Proof. By hypothesis we can define the following polynomial in $\mathbb{F}_q[A]$:

$$f(X) = \prod_{i=1}^{m} (X_i^{l_i} - \beta_i) \text{ for certain } \beta_1, \ldots, \beta_m \in \mathbb{F}_q.$$

Then, by Lemma 19, $f(X)$ has

$$(l_1 + \ldots l_m)q^{m-1} - \sum_{1 \le i < j \le m} l_i l_j q^{m-2} - \sum_{1 \le i < j < k \le m} l_i l_j l_k q^{m-3} - \ldots - l_1 \cdots l_m$$

$\mathbb{F}_q$-roots. That is, we have found a codeword of $\mathcal{C}_A$ of weight $\mathrm{FB}(\mathcal{C}_A)$, hence $d(\mathcal{C}_A) = \mathrm{FB}(\mathcal{C}_A)$. $\square$

Lemma 23. Suppose that $\mathrm{FB}(\mathcal{C}_A) = (q - k_1 l_1) \cdots (q - k_m l_m)$ *with l_i a divisor of $q-1$. Then, $d(\mathcal{C}_A) = \mathrm{FB}(\mathcal{C}_A)$ if* $\{1, X_1^{l_1}, \ldots, X_1^{m l_1}, \cdots, X_m^{l_m}, \ldots, X_m^{k_m l_m}\} \subseteq \mathbb{F}_q[A]$.

Proof. By hypothesis we can define the following polynomial in $\mathbb{F}_q[A]$:

$$f(X) = \prod_{i=1}^{m} (X_i^{l_i} - \beta_i)(X_i^{2l_i} - \beta_i^2) \cdots (X_i^{k_i l_i} - \beta_i^{k_i}) \text{ for certain } \beta_1, \ldots, \beta_m \in \mathbb{F}_q.$$

Then, by Lemma 19, we have found a codeword of $\mathcal{C}_A$ of weight $\mathrm{FB}(\mathcal{C}_A)$, hence $d(\mathcal{C}_A) = \mathrm{FB}(\mathcal{C}_A)$. $\square$

Lemma 24. Suppose that $\mathrm{FB}(\mathcal{C}_A) = (q-l)q^{m-1}$ *with $l-1$ a divisor of $q-1$. Then, $d(\mathcal{C}_A) = \mathrm{FB}(\mathcal{C}_A)$ if* $\{X_i, X_i^l\} \subseteq \mathbb{F}_q[A]$ *for some $i \in \{1, \ldots, m\}$.*

Proof. By hypothesis we can define the following polynomial in $\mathbb{F}_q[A]$:

$$f(X) = (X_i^l - \beta X_i) = X_i(X_i^{l-1} - \beta) \text{ for certain } \beta \in \mathbb{F}_q.$$

Then, by Lemma 19, $f(X)$ has lq^{m-1} $\mathbb{F}_q$-roots. That is, we have found a codeword of $\mathcal{C}_A$ of weight $FB(\mathcal{C}_A)$, hence $d(\mathcal{C}_A) = FB(\mathcal{C}_A)$. $\square$

Lemma 25. Let $A \subseteq [\![0, q-1]\!]^m$ and $s \in [\![0, q-1]\!]$. If for all $f \in \mathbb{F}_q[A]$ we have that X_1^s is a divisor of $f(X)$, then $d(\mathcal{C}_A) = d(\mathcal{C}_B)$ with

$$B = \{(i_1 - s - 1, i_2, \ldots, i_m) \mid (i_1, \ldots, i_m) \in A\}.$$

The result can be generalized to any other coordinate X_i with $i = 2, \ldots, m$.

Proof. By hypothesis every polynomial $f \in \mathbb{F}_q[A]$ can be written as $f = X_1^s g$ with $g \in \mathbb{F}_q[B]$. And both polynomials f and g have exactly the same number of $\mathbb{F}_q$-roots. $\square$