High dimensional affine codes whose square has a designed minimum distance

Ignacio García-Marco · Irene Márquez-Corbella · Diego Ruano

Received: 31 July 2019 / Revised: 20 February 2020 / Accepted: 2 May 2020 / Published online: 3 July 2020
© Springer Science+Business Media, LLC, part of Springer Nature 2020

Abstract
Given a linear code $C$, its square code $C^{(2)}$ is the span of all component-wise products of two elements of $C$. 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 $k(C)$ and high minimum distance of $C^{(2)}$, $d(C^{(2)})$? More precisely, given a designed minimum distance $d$ we compute an affine variety code $C$ such that $d(C^{(2)}) \geq d$ and the dimension of $C$ is high. The best constructions we propose mostly come from hyperbolic codes. Nevertheless, for small values of $d$, they come from weighted Reed–Muller codes.

Keywords Affine variety codes · Multi-party computation · Square codes · Schur product of codes · Minkowski sum · Convex set

Mathematics Subject Classification 94B05 · 94B65 · 94A60

This work was supported in part by the Spanish MICINN/FEDER Grant PGC2018-096446-B-C21, the Spanish MICINN PID2019-105896GB-I00, the Spanish MICINN PID2019-104844GB-I00, by the Spanish MINECO Grant RYC-2016-20208 (AEI/FSE/UE), MASCA (ULL Research Project) and by the Junta de CyL (Spain) Grant VA166G18.

This is one of several papers published in Designs, Codes and Cryptography comprising the “Special Issue on Codes, Cryptology and Curves”.

Irene Márquez-Corbella
imarquec@ull.es
Ignacio García-Marco
iggarcia@ull.es
Diego Ruano
diego.ruano@uva.es

1 Departamento de Matemáticas, Estadística e I.O., Universidad de La Laguna, 38200 La Laguna, Tenerife, Spain

2 IMUVA-Mathematics Research Institute, Universidad de Valladolid, 47011 Valladolid, Spain
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 (MPC) is possible from secret sharing schemes [7], and hence from coding theory. From now on, given a linear code \( C \), the dimension of \( C \) will be denoted by \( k(C) \) and its minimum distance by \( d(C) \). Moreover, if \( C \) is a linear code over the finite field \( \mathbb{F}_q \) of length \( n \), dimension \( k \) and minimum distance \( d \), we call \([n, k, d]_q \) the parameters of \( C \).

One of the best known protocols for MPC with linear codes is MiniMac [8], which evaluates boolean circuits, and its successor TinyTable [9]. These methods, which use a linear code \( C \), should prevent cheating. The probability that a cheating player is caught depends on the minimum distance of \( C \ast C = C^{(2)} \), the square code of the linear code \( C \) [19], meaning that a high distance on the square code will give a higher security. Simultaneously, it would be beneficial to have a code \( C \) with high rate to reduce the communications cost. Therefore, it is desirable to optimize both parameters: \( d(C^{(2)}) \) and \( k(C) \).

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 [17] and it is also used for cryptanalytic applications against the McEliece cryptosystem. For a summary of these applications and some others, see [19, Sect. 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 parameters. Therefore, it is desirable to optimize both parameters: \( d(C^{(2)}) \) and \( k(C) \).

Given \( d \in \mathbb{Z}^+ \), in this work we propose a method to obtain an affine variety code \( C \) satisfying that \( d(C^{(2)}) \geq d \) and such that \( k(C) \) is considerably high. Our main result, stated in Theorem 2, receives as input a value \( d \in \mathbb{Z}^+ \) and starts by considering an affine code \( C_B \) associated with a set \( B \subseteq \mathbb{N}^m \) such that \( d(C_B) \geq d \), say for example, a hyperbolic code with minimum distance at least \( d \). Then, by means of convexity arguments, we build a set \( A \subseteq \mathbb{N}^m \) such that the Minkowski sum \( A + A \) is contained in \( B \). The latter condition implies that \( d(C_A^{(2)}) \geq d(C_B) \geq d \). 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, \( d < (2 - \sqrt{2})q \), we prove that there exist certain weighted Reed–Muller codes that outperform hyperbolic codes.

Additionally, if the minimum distance of the dual of \( C \) and \( d(C^{(2)}) \) are greater than or equal to \( t + 2 \), then \( C \) 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 [1,5,6]. This application shows the importance of finding linear codes where \( d(C^{\perp}) \) is also high relative to the length of the code, where \( C^{\perp} \) is the dual code of \( C \). Although in this work we have not focused in maximizing \( d(C^{\perp}) \) (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 \( C \) is again an affine variety code that can be easily computed...
constructed by [12, 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. 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.

Next, in Sect. 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, Theorem 2, that allows us to establish a strategy to construct affine variety codes whose square code has a designed minimum distance \( d \). That is, given \( d \in \mathbb{N} \) we construct an affine variety code \( C \) such that \( d(C^{(2)}) \geq d \).

In Sect. 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 \( C \) whose square code has designed minimum distance \( d \) i.e. \( d(C^{(2)}) \geq d \), throughout Sect. 4 our additional goal is providing a code \( C \) that has also high dimension. 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 Sect. 4.1. Surprisingly, half hyperbolic codes are not always the best option. Indeed, we prove in Sect. 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.

### 2 Affine variety codes

Let us start this section with a brief summary to set up notation and terminology.

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

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

It is easy to check that \( I_q \) is radical. Moreover, the points of the affine variety defined by \( I \) (over the algebraic closure of \( \mathbb{F}_q \)) are the \( \mathbb{F}_q \)-rational points of the affine variety defined by \( I_q \). That is,

\[
\mathbb{V}_{\mathbb{F}_q}(I_q) = \mathbb{V}_{\mathbb{F}_q}(I_q) = \mathbb{V}_{\mathbb{F}_q}(I) = \{P_1, \ldots, P_n\}.
\]

where \( \mathbb{F}_q \) denotes the algebraic closure of \( \mathbb{F}_q \).

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

\[
ev_{\mathcal{P}} : R_q \longrightarrow \mathbb{F}_q^n
\]

\[
f + I_q \longmapsto (f(P_1), \ldots, f(P_n)).
\]

**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 \( ev_{\mathcal{P}} \). That is:

\[
C(I, L) = ev_{\mathcal{P}}(L) = \{ ev_{\mathcal{P}}(f + I_q) \mid f + I_q \in L \}.
\]

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 \( L \).

The reader may have already realized that some of the well-known classes of evaluation codes can be viewed as affine variety codes. Indeed, in [11, Proposition 1.4] it is proved that
The sets $A \subseteq \mathbb{N}^2$ and $A_{11} \subseteq [0, 10]^2$ define the same code over $\mathbb{F}_{11}$

every $\mathbb{F}_q$-linear code $C$ may be represented as an affine variety code over $\mathbb{F}_q$, where we have to choose $s$ so that $q^s$ is greater than the length of $C$.

Let $C = C(I, L)$ be an affine variety code. Then, it is clear that the length of $C$ is the cardinality of $V_{\mathbb{F}_q}(I) = \mathcal{P} = \{P_1, \ldots, P_n\}$ and the dimension of $C$ is the dimension of the subspace $L$ - since the evaluation map $ev_{\mathcal{P}}$ is an isomorphism. In the rest of the section we will study the minimum distance of affine variety codes $C = C(I, L)$ 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: $\{X_1^{i_1} \cdots X_m^{i_m} \mid (i_1, \ldots, i_m) \in A\}$. We will denote by $C_A$ the affine variety code $C(I, L)$ with $I = (0)$ and $L = \mathbb{F}_q[A]$, in other words $C_A$ 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 $C_A$ as the affine variety code $C(I, L)$ with $I = (0)$ and $L = \mathbb{F}_q[A]$. Then the length of $C_A$ 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 $C_A = C_B$ (see Fig. 1). This set will be denoted by $B = A_q$.

The following well-known result gives a bound for the minimum distance of the particular case of affine variety codes of type $C_A$.

**Theorem 1** *(Footprint bound [14])* Let $A \subseteq [0, q - 1]^m$. Then, the minimum distance of $C_A$ satisfies that

$$d(C_A) \geq \min_{(i_1, \ldots, i_m) \in A} \{(q - i_1) \cdots (q - i_m)\}.$$  

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

$$\text{FB}(C_A) = \min_{(i_1, \ldots, i_m) \in A} \{(q - i_1) \cdots (q - i_m)\}.$$  

By Theorem 1, we have that the minimum distance of the code $C_A$ satisfies that

$$d(C_A) \geq \text{FB}(C_A).$$

 Springer
In the following lines we study some well-known families of affine codes, namely (weighted) Reed Muller and hyperbolic codes (see, e.g., [10,15,20]). All these codes are known 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 the following lemma, whose proof can be found in the “Appendix”. For further families of codes where the minimum distance coincides with its footprint bound, we refer the reader to [16].

**Lemma 1** Suppose that $\text{FB}(C_A) = (q - \alpha_1) \cdots (q - \alpha_m)$. Then $d(C_A) = \text{FB}(C_A)$ if all the elements $\beta = (\beta_1, \ldots, \beta_m)$ with $0 \leq \beta_i \leq \alpha_i$ belong to the set $A$.

**Definition 3** (Reed–Muller (RM) and Weighted RM codes) Consider $s, s_1, \ldots, s_m \in \mathbb{R}_{\geq 0}$ and let $A = \{(i_1, \ldots, i_m) \in [0, q - 1]^m \mid s_1i_1 + \cdots + smi_m \leq s\}$. Then, $C_A$ is called the $q$-ary weighted Reed–Muller code of degree $s$ in $m$ variables with $S = (s_1, \ldots, s_m)$ and we denote it by $\text{WRM}_q(s, m, S)$. If $s_1 = \cdots = s_m = 1$, then $\text{WRM}_q(s, m, S)$ is the corresponding $q$-ary Reed–Muller code $\text{RM}_q([s], m)$ (Fig. 2).

**Proposition 1** ([13]) 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 $C = \text{RM}_q(s, m)$ is $d(C) = (q - b)q^{m-1-a}$.

**Definition 4** (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, $C_A$ is called the $q$-ary hyperbolic code of order $d$ and we denote it by $\text{Hyp}_q(d, m)$ (See Fig. 2).

The hyperbolic code $\text{Hyp}_q(d, m)$ has been designed to be the code with the largest possible dimension among those affine codes $C_A$ such that $\text{FB}(C_A) \geq d$. 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 $d$.

---

Fig. 2 Examples of Reed–Muller, hyperbolic and weighted Reed–Muller codes over $\mathbb{F}_{11}$. a corresponds to the RM code $C_A = \text{RM}_{11}(6, 2)$ with parameters $[11^2, 28, 55]_{11}$ and the set $A = \{(i, j) \in [0, 10]^2 \mid i + j \leq 6\}$. b corresponds to the hyperbolic code $C_B = \text{Hyp}_{11}(55, 2)$ with parameters $[11^2, 30, 55]_{11}$ and the set $B = \{(i, j) \in [0, 10]^2 \mid (11 - i)(11 - j) \leq 55\}$. c corresponds to the weighted Reed–Muller code $C_D = \text{WRM}_{11}(15, 2, [5, 3])$ with parameters $[11^2, 13, 66]_{11}$ and the set $D = \{(i, j) \in [0, 10]^2 \mid 5i + 3j \leq 15\}$.
Proposition 2 Consider $D = \text{RM}_q(t, 2)$ and $E = \text{Hyp}_q(d, 2)$. If $d(D) = d(E)$, then $k(D) \leq k(E)$. Moreover, $k(D) < k(E)$ if and only if
\[ \frac{s + 5}{2} \leq q \leq \left(\frac{s + 1}{2}\right)^2. \]

Proof Since $d(D) = d(E)$, we have that $FB(E) = d(E) = d(D) = FB(D)$. 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 $D = C_A$ and $E = C_B$ with $A = \{(i, j) \in [0, q - 1]| i + j \leq s\}$ and $B = \{(i, j) \in [0, q - 1]| m_{i, j} \geq d\}$. Moreover,
\[ \min\{m_{i, j} | (i, j) \in A\} = d(D) = d(E) = \min\{m_{i, j} | (i, j) \in B\}. \]

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

By Proposition 1 we also have that
\[ d(D) = \begin{cases} m_{0, s} & \text{if } s \leq q - 1, \\ m_{q-1, s-q+1} & \text{if } q \leq s \leq 2q - 2; \end{cases} \]
and it is easy to verify that
\[ \max\{m_{i, j} | (i, j) \notin A\} = \begin{cases} m_{\frac{s+1}{2}, \frac{s+1}{2}} & \text{if } s \text{ is odd}, \\ m_{\frac{s+2}{2}, \frac{s+2}{2}} & \text{if } s \text{ is even}. \end{cases} \]

We separate the proof depending on the value and the parity of $s$.

1. $t \leq q - 1$ and
   (a) $s$ is odd. Then $k(D) < k(E)$ if and only if $(\frac{s+1}{2}, \frac{s+1}{2}) \in B$ or, equivalently, if $m_{s, 0} \leq m_{\frac{s+1}{2}, \frac{s+1}{2}}$. This happens if and only if $q \leq (\frac{s+1}{2})^2$.
   (b) $s$ is even. Then $k(D) < k(E)$ if and only if $(\frac{s}{2}, \frac{s+2}{2}) \in B$ or, equivalently, if $m_{s, 0} \leq m_{\frac{s}{2}, \frac{s+2}{2}}$. That is, if and only if $q \leq \frac{s(s+2)}{4}$, which is equivalent to $q \leq (\frac{s+1}{2})^2$, since $s$ is even.

2. $s \geq q$ and
   (a) $s$ is odd. Then $k(D) < k(E)$ if and only if $(\frac{s+1}{2}, \frac{s+1}{2}) \in B$ or, equivalently, if $m_{q-1, s-q+1} \leq m_{\frac{s+1}{2}, \frac{s+1}{2}}$. This happens if and only if $2q - s - 1 \leq (q - \frac{s+1}{2})^2$. This defines a quadratic inequality $p(q) > 0$ involving in the variable $q$. Notice that $p(q) \geq 0$ if and only if $q \leq (s + 1)/2$ or $q \geq (s + 5)/2$. The first option is not viable since $s \geq 2q - 1$. Thus, $q \geq (s + 5)/2$.
   (b) $s$ is even. Then $k(D) < k(E)$ if and only if $(\frac{s}{2}, \frac{s+2}{2}) \in B$ or, equivalently, if $m_{q-1, s-q+1} \leq m_{\frac{s}{2}, \frac{s+2}{2}}$. That is, if and only if $2q - s - 1 \leq (q - \frac{s+2}{2})(q - \frac{s+2}{2})$. Proceeding as in the previous case we get that this is equivalent to $q \geq \frac{s+3}{2}$ and since $s$ is even, this is the same as $q \geq \frac{s+5}{2}$.

\[ \square \]
3 Schur product of codes

The notion of Schur product of codes was first introduced in coding theory for decoding [17]. 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 [19, Sect. 4].

Definition 5 The Schur product is the componentwise product on $\mathbb{F}_q^n$. That is, given two elements $a, b \in \mathbb{F}_q^n$, $a \ast b \triangleq (a_1 b_1, \ldots, a_n b_n)$. For two codes $C_1, C_2 \subseteq \mathbb{F}_q^n$, their Schur product is the code $C_1 \ast C_2$ defined as

$$C_1 \ast C_2 \triangleq \text{Span}_{\mathbb{F}_q} \{c_1 \ast c_2 \mid c_1 \in C_1 \text{ and } c_2 \in C_2\}$$

For $C_1 = C_2 = C$, then $C \ast C$ is denoted as $C^{(2)}$. □

3.1 Product of codes and the Minkowski sum

Given two sets $A, B \subseteq \mathbb{N}^m$, we denote by $A + B$ their Minkowski sum, that is, $A + B = \{a + b \mid a \in A, b \in B\}$.

We observe that if $f, g \in \mathbb{F}_q[A]$ then, $\text{ev}_P(f) \ast \text{ev}_P(g) = \text{ev}_P(fg)$ and $fg \in \mathbb{F}_q[A + A]$. With these considerations the following property is easy to check.

Proposition 3 $C^{(2)}_A = C_{A+A}$.

It is important to highlight that even if $A \subseteq [[0, q-1]]^m$, it might happen that $A + A \not\subseteq [[0, q-1]]^m$; however $A' := (A + A)_q \subseteq [[0, q-1]]^m$ satisfies that $C_{A'} = C_{A+A}$.

Proposition 3 suggests the following way of constructing affine codes whose square has a designed minimum distance: we consider $B \subseteq [[0, q-1]]^m$ such that $d(C_B) \geq d$. Then, we choose $A$ such that $(A + A)_q \subseteq B$. If $A$ is chosen in this way, then we will have that $d(C^{(2)}_A) = d(C_{A+A}) = d(C_{(A+A)_q}) \geq d(C_B) \geq d$. The following lemma gives a necessary condition for such a set $A$.

Lemma 2 Let $A, B \subseteq [[0, q-1]]^m$ and for each $\epsilon = (\epsilon_1, \ldots, \epsilon_m) \in \{0, 1\}^m$ we set

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

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

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

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

where $(2a)_q = (a'_1, \ldots, a'_m)$ 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 $2a \in B_\epsilon$. □

The following proposition and the subsequent theorem are the key results to understand our strategy to give a code $C_A$ whose square has a designed minimum distance. They are
both based on (simple) convexity arguments. Given a set \( B \subseteq \mathbb{Z}^{m} \), suppose that we want to find a set \( A \subseteq \mathbb{Z}^{m} \) 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 4** Let \( D \subseteq \mathbb{R}^{m} \) be a convex set and consider \( A := \{a \in \mathbb{Z}^{m} \mid 2a \in D\} \). Then, \( A + A \subseteq D \).

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

**Theorem 2** Let \( d \in \mathbb{N} \) and let \( C_{B} \) be a linear code with \( B \subseteq \mathbb{Z}^{m} \) such that \( d \leq d(C_{B}) \). Consider \( C \subseteq \mathbb{R}^{m} \) a convex set such that

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

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

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

In particular, if we apply the previous result to a hyperbolic code \( C_{B} \) of order \( d \), we get the following.

**Proposition 5** Let \( C \subseteq \mathbb{R}^{m} \) be a convex set such that \( C \cap D_{\epsilon} = \emptyset \) for all \( \epsilon \in \{0, 1\}^{m} \), being

\[
D_{\epsilon} = \{(b_{1}, \ldots, b_{m}) \in \mathbb{R}^{m} \mid 2b_{i} \in \begin{cases} [0, q - 1] & \text{if } \epsilon_{i} = 0 \\ [q, 2q - 2] & \text{if } \epsilon_{i} = 1 \end{cases} \text{ and } \prod_{i=1}^{m} (q + \epsilon_{i}(q - 1) - 2b_{i}) < d \}
\]

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

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

\[
\{c \in \mathbb{R}^{m} \mid 2c \in [0, 2q - 2]^{m} \text{ and } [2c]_{q} \notin B\} = \bigcup_{\epsilon \in \{0, 1\}^{m}} D_{\epsilon}.
\]

and by Theorem 2 the result holds.

**Example 1** Consider \( q = 11 \), \( m = 2 \) and \( d = 6 \). We are going to construct a code \( C_{A} \) over \( \mathbb{F}_{11} \) such that \( d(C_{A}^{(2)}) \geq 6 \), following Proposition 5. Consider \( C_{B} = \text{Hyp}_{11}(6, 2) \) and \( D_{\epsilon} \) 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 \( A = C \cap [0, 10]^{2} \). Then, by Proposition 5, we have that \((A + A)_{11} \subseteq B\) and, thus, \( d(C_{A}^{(2)}) = d(C_{A + A}) \geq d(C_{B}) = d(\text{Hyp}_{11}(6, 2)) = 6 \).

As one can see, following the construction of Proposition 5, the number of integer points in the convex set \( C \) turns out to be the dimension of the code \( A \) such that \( d(C_{A}^{(2)}) \geq d \). So, in order to obtain a code \( C_{A} \) 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 \( C \).
In the previous section we described a method that, given $d$, it returns a code $C_A$ such that $d(C_A^{(2)}) \geq d$. However, we would also like to find among all the codes $C_A$ that verify the previous property, the one that has the highest possible dimension. For this purpose, the convex set $C$ mentioned in this method must have the maximum number of integer points.

Given a fixed value $d$, the hyperbolic code $C = \text{Hyp}_q(d, m)$ 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 the method used in Theorem 2 being $B \subset [0, q-1]_m^m$ such that $C_B = \text{Hyp}_q(d, m)$. 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 6) 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

Definition 6 (Half hyperbolic codes) Let $C_B = \text{Hyp}_q(d, m)$ 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

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

In other words, for $a \in \left[0, \frac{q-1}{2}\right]^m$, then $a \in A$ if and only if $2a \in B$. Then, $C_A$ is the $q$-ary half hyperbolic code of order $d$ and we denote it by $\text{HalfHyp}_q(d, m)$ (Fig. 3).
Proof Taking $C = \{a = (a_1, \ldots, a_m) \in \mathbb{R}^m \mid 0 \leq a_i \leq \frac{q-1}{2}, \prod_{i=1}^{m} (q-2a_i) \geq d\}$ 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 $D_\epsilon$ is defined as in Proposition 5). Thus, taking $A = C \cap [0,q-1]^m$, Proposition 5 guarantees that $d(C^{(2)}_A) \geq d$. To finish the proof it suffices to observe that $C_A$ coincides with $\text{HalfHyp}_q(d,m)$.

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 3 Let $d \in \mathbb{Z}^+$ such that $d < q^2$, then

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

Proof Since $\text{HalfHyp}_q(d,2) = C_A$ 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

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

Moreover, setting $A_i := \{j \mid (i,j) \in A\}$ for all $i \in [0, (q - 1)/2]$, one has that $|A| = \sum_{i=0}^{(q-1)/2} |A_i|$ with $A_i = \{j \mid 0 \leq j \leq (q - 1)/2 \text{ and } (q - 2i)(q - 2j) \geq d\}$. Hence $A_i = \emptyset$ whenever $i > (q^2 - d)/2q$; and $|A_i| = \left\lceil \frac{d + q(2i - q)}{4i - 2q} \right\rceil + 1$ otherwise.

When $d \geq q$, the sets $D_\epsilon$ in Proposition 5 split $[0,q-1]^m$ into $2^m$ regions. For this reason, we propose $C = \text{HalfHyp}_q(d,m)$, the half hyperbolic code of order $d$, as a code with high dimension $k(C)$ and satisfying that $d(C^{(2)}_q) \geq d$ (see Fig. 4). As we will see in the following subsection, when $d < q$ one can find better options in the family of weighted Reed–Muller codes.

\(\square\) Springer
Consider the weighted Reed–Muller code $C_A$ over $F_7$ with $A = \{(i, j) \mid 3i + 2j \leq 5\}$. Then the code $C_{A+A}$ is the affine variety code that consists of the evaluation of polynomials $f \in F_q[A+A]$ in the points of $F^n_2$, where $A + A = \{(i, j) \mid 0 \leq i, j \leq 2\} \cup \{(0, 3), (0, 4), (1, 3)\}$ (see Fig. 5b). It is easy to check that there is no weighted Reed–Muller code $C_B$ such that $(2, 2) \in B$, but $(0, 5), (3, 0) \notin B$. Thus, $C_{A+A}$ is not a weighted Reed–Muller code.

4.2 Weighted Reed–Muller codes

It is not difficult to see that when $d \geq q$ and $C$ is a weighted Reed–Muller code with $d(C^{(2)}) \geq d$, then $FB(C) \geq FB(\text{HalfHyp}_q(m, d))$ and, hence, $k(C) \leq k(\text{HalfHyp}_q(m, d))$. 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 Proposition 7). This section concerns the case $m = 2$ but we believe that it might be extended to several variables. Before proving Proposition 7, 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 3).

A first observation is that if $C$ is a weighted Reed–Muller code then $C^{(2)}$ is not necessarily a weighted Reed–Muller code as Fig. 5 shows.

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 proof of the main result.

Lemma 4 If $C$ is a weighted Reed–Muller code then $d(C^{(2)}) = FB(C^{(2)})$.

Proof Let $C_A$ be a weighted Reed–Muller code with $A \subset [0, q-1]^m$ and suppose that

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

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 $C_A$ 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 1 we complete the proof.

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.
Lemma 5 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

\[
B_1 := \{(i, j) \in \mathbb{N}^2 \mid i + j < s\} \cup \{(i, j) \in \mathbb{N}^2 \mid i + j = s \text{ and } j < (q - d + 1)/2\}, \quad \text{and} \quad B_2 := \{(i, j) \in \mathbb{N}^2 \mid i + j < s\} \cup \{(i, j) \in \mathbb{N}^2 \mid i + j = s \text{ and } i < (q - d + 1)/2\}
\]

then, \( C_{B_1} \) and \( C_{B_2} \) are weighted Reed–Muller codes and \( k(C_{B_1}) = k(C_{B_2}) \).

**Proof** It suffices to rotate slightly the line \( x + y = s \) to get that both \( C_{B_1} \) and \( C_{B_2} \) are weighted Reed–Muller code (see Fig. 6). Indeed it is easy to check that

\[
k(C_{B_1}) = |B_1| = \frac{(q - \frac{d}{2} + 2)(q - \frac{d}{2} + 1)}{2} + \frac{q - \frac{d}{2}}{2} - 1 = k(C_{B_2})
\]

\( \square \)

Theorem 3 Let \( \mathbb{F}_q \) be a finite field and \( d \in \mathbb{Z}^+ \) with \( d < q \). Let \( C \) is a weighted Reed–Muller code over \( \mathbb{F}_q \) with \( d(C^{(2)}) \geq d \).

1. If \( d \) is an odd integer then, \( k(C) \leq k(\text{RM}_q(s, 2)) \) with \( s := q - \frac{d+1}{2} \).
2. If \( d \) is an even integer then, \( k(C) \leq k(C_B) \), where \( C_B \) is any of the weighted Reed–Muller codes described in Lemma 5.

**Proof** We will study the case when \( d \) is odd. The case when \( d \) is even is similar and details can be found in the appendix.

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

\[
A := \{(i, j) \in \lfloor 0, q-1 \rfloor \mid w_1i + j \leq \lambda\}
\]

we have that \( C = C_A \).

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 \( \lambda \).

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

\[
\varphi : A - B \rightarrow B - A \\
(\alpha, \beta) \mapsto (2a - \alpha, 2b - \beta)
\]
is an injective map (see Fig. 7 for a graphic representation of this idea).

Since the injectivity of \( \varphi \) is easy to check, we are proving that \( \varphi \) 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 \( (\alpha, \beta) \) and \( (2a - \alpha, 2b - \beta) \in A \). Hence, \( (2a, 2b) = (\alpha, \beta) + (2a - \alpha, 2b - \beta) \in A + A \) and \( C_A^{(2)} = C_{A+A} \). Since \( C_A \) is a weighted Reed–Muller code, by Lemma 4 we have that \( d \leq d(C_A^{(2)}) = FB(C_A^{(2)}) \leq (q - 2a)(q - 2b) = d - 1 \), a contradiction.

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

(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 \( \alpha \geq a + \frac{1}{2} \) since \( \beta \geq 2b + 1 > b + \frac{1}{2} \) 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 \( \alpha \leq a \), from one side we have that \( (\alpha, \beta) \notin B \), so

\[
\alpha + \beta \geq s + 1 = a + b + \frac{1}{2}
\]

(2)
and, from the other side we have that \( (\alpha, \beta) \in A \), which implies that

\[
w_1\alpha + \beta \leq \lambda.
\]

(3)

From (2) and (3) we get that

\[
(w_1 - 1)a + a + b + \frac{1}{2} \leq (w_1 - 1)a + \alpha + \beta \leq w_1\alpha + \beta \leq \lambda \leq a + b + \frac{1}{2}
\]

and, thus, \( w_1 \leq 1 \). Hence, using that \( \alpha \leq a \), (2) and (3) we get that

\[
w_1(a + \frac{1}{2}) + b \leq w_1a + b + \frac{1}{2} \leq a + b + \frac{1}{2} + (w_1 - 1)a = w_1\alpha + \beta \leq \lambda.
\]
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 $C^{(2)}_A = C_{A+A}$ and, as before, using Lemma 4 we get a contradiction.

Let us prove now (c). Whenever $(\alpha, \beta) \in A - B$, then $\alpha + \beta \geq s + 1$. Since $a + b = s + \frac{1}{2}$, we have that $2a - \alpha + 2b - \beta \leq s$ 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 $\frac{\lambda}{2} < a + b + \frac{1}{2}$. Otherwise, we have that $(\frac{\lambda}{2}, b), (a - \frac{1}{2}, b) \in A$ 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 $C^{(2)}_A = C_{A+A}$ and, as before, using Lemma 4 we get a contradiction.

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

Since $(RM_q(s, 2)^{(2)}) = d$, this means that $RM_q(s, 2)$ has the highest dimension among all the weighted Reed–Muller codes $C$ such that $d(C^{(2)}) \geq d$.

Finally, we will prove 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 7** Let $d < (2 - \sqrt{2})q$.

1. If $d$ is odd, then $k(RM_q(q - \frac{d-1}{2}, 2)) < k(\text{HalfHyp}_q(d, 2))$.
2. If $d$ is even, then $k(C_B) > k(\text{HalfHyp}_q(d, 2))$ where $C_B$ is one of the weighted Reed–Muller codes defined in Lemma 5.

**Proof** Take notice that

\[
k(RM_q(q - \frac{d-1}{2}, 2)) = \frac{(q - \frac{d-1}{2} + 2)(q - \frac{d-1}{2} + 1)}{2} = A_1
\]

\[
k(C_B) = \frac{(q - \frac{d-1}{2} + 2)(q - \frac{d-1}{2} + 1)}{2} + \frac{q - \frac{d}{2}}{} - 1 = A_2
\]

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

Therefore if $A_1 - B > 0$ and $A_2 - B > 0$ then our claims holds.

Now $A_1 - B > 0$ 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: $k(RM_q(q - \frac{d-1}{2}, 2)) > k(\text{HalfHyp}_q(d, 2))$.

By similar arguments it is easy to check that $k(C_B) > k(\text{HalfHyp}(d, 2))$ (see Fig. 8 for an example). \square

**A For which affine codes $C_A$ is it verified that $FB(C_A) = d(C_A)$?**

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

**Lemma 6** Suppose that $FB(C_A) = (q - \alpha_1) \cdots (q - \alpha_m)$. Then $d(C_A) = FB(C_A)$ 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 $FB(C_A) = (q - \alpha_1)(q - \alpha_2)$. 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:

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

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 $c = ev_{\mathcal{P}}(f) \in C_A$ of weight $q^2 - (\alpha_1 + \alpha_2)q - \alpha_1 \alpha_2 = FB(C_A)$. Hence the minimum distance of $C_A$ is $FB(C_A)$.

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 $C_A$ of weight $FB(C_A)$, hence $d(C_A) = FB(C_A)$.

\[\square\]
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 \( C_A \) by just checking that a very small number of points belongs to the set \( A \).

**Lemma 7** Let \( \alpha \) 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 root 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 \( \alpha^j \) is an \( \mathbb{F}_q \)-root of \( f(X) \), then \( f(\alpha^j) = 0 \), that is \( \alpha^{lj} = \alpha^j \) which implies that the order of \( \alpha \), 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 these equations has the form:

\[
(x - \frac{l}{\gcd(l, q - 1)} y, y + \frac{q - 1}{\gcd(l, q - 1)}) \quad \text{with} \quad \lambda \in \mathbb{Z}
\]

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 1** Suppose that \( \text{FB}(C_A) = (q - l)q^{m-1} \) with \( l \) a divisor of \( q - 1 \). Then, \( d(C_A) = \text{FB}(C_A) \) if \( \{1, X_1^l\} \subseteq \mathbb{F}_q[A] \) for some \( i \in \{1, \ldots, m\} \).

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

\[
f(X) = X_1^l - \beta \quad \text{for certain} \quad \beta \in \mathbb{F}_q.
\]

Then, by Lemma 7, \( f(X) \) has \( lq^{m-1} \) \( \mathbb{F}_q \)-roots. That is, we have found a codeword of \( C_A \) of weight \( \text{FB}(C_A) \), hence \( d(C_A) = \text{FB}(C_A) \). \( \square \)

**Lemma 8** Suppose that \( \text{FB}(C_A) = (q - kl)q^{m-1} \) with \( l \) a divisor of \( q - 1 \). Then, \( d(C_A) = \text{FB}(C_A) \) if \( \{1, X_1^l, X_1^{2l}, \ldots, X_1^{kl}\} \subseteq \mathbb{F}_q[A] \) for some \( i \in \{1, \ldots, m\} \).

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

\[
f(X) = (X_1^l - \beta)(X_1^{2l} - \beta^2) \cdots (X_1^{kl} - \beta^k) \quad \text{for certain} \quad \beta \in \mathbb{F}_q.
\]

Then, by Lemma 7, \( f(X) \) has \( klq^{m-1} \) \( \mathbb{F}_q \)-roots. That is, we have found a codeword of \( C_A \) of weight \( \text{FB}(C_A) \), hence \( d(C_A) = \text{FB}(C_A) \). \( \square \)

**Lemma 9** Suppose that \( \text{FB}(C_A) = (q - l_1) \cdots (q - l_m) \) with \( l_i \) a divisor of \( q - 1 \). Then, \( d(C_A) = \text{FB}(C_A) \) if \( \{1, X_1^{l_1}, \ldots, X_m^{l_m}\} \subseteq \mathbb{F}_q[A] \).

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

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

Then, by Lemma 7, \( f(X) \) has \( (l_1 + \cdots + l_m)q^{m-1} - \sum_{1 \leq i < j \leq m} l_il_jq^{m-2} - \sum_{1 \leq i < j < k \leq m} l_il_jl_kq^{m-3} - \cdots - l_1 \cdots l_m \) \( \mathbb{F}_q \)-roots. That is, we have found a codeword of \( C_A \) of weight \( \text{FB}(C_A) \), hence \( d(C_A) = \text{FB}(C_A) \). \( \square \)
Lemma 10 Suppose that $FB(C_A) = (q - k_1 l_1) \cdots (q - k_m l_m)$ with $l_i$ a divisor of $q - 1$. Then, $d(C_A) = FB(C_A)$ if $\{1, X_1^{l_1}, \ldots, X_1^{m l_1}, \ldots, X_m^{l_m}, \ldots, X_m^{a m l_m}\} \subseteq F_q[A]$.

**Proof** By hypothesis we can define the following polynomial in $F_q[A]$:

$$f(X) = \prod_{i=1}^{m} (X_i^{l_i} - \beta_i)(X_i^{2l_i} - \beta_i^2) \cdots (X_i^{k_i l_i} - \beta_i^{k_i})$$

for certain $\beta_1, \ldots, \beta_m \in F_q$. Then, by Lemma 7, we have found a codeword of $C_A$ of weight $FB(C_A)$, hence $d(C_A) = FB(C_A)$.

Lemma 11 Suppose that $FB(C_A) = (q - l)q^{m-1}$ with $l - 1$ a divisor of $q - 1$. Then, $d(C_A) = FB(C_A)$ if $\{X_i, X_i^j\} \subseteq F_q[A]$ for some $i \in \{1, \ldots, m\}$.

**Proof** By hypothesis we can define the following polynomial in $F_q[A]$:

$$f(X) = (X_i^{l} - \beta X_i) = X_i(X_i^{l-1} - \beta)$$

for certain $\beta \in F_q$. Then, by Lemma 7, $f(X)$ has $lq^{m-1}$ $F_q$-roots. That is, we have found a codeword of $C_A$ of weight $FB(C_A)$, hence $d(C_A) = FB(C_A)$.

Lemma 12 Let $A \subseteq \{0, q - 1\}^m$ and $s \in \{0, q - 1\}$. If for all $f \in F_q[A]$ we have that $X_s$ is a divisor of $f(X)$, then $d(C_A) = d(C_B)$ 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 $f \in F_q[A]$ can be written as $f = X_i^j g$ with $g \in F_q[B]$. And both polynomials $f$ and $g$ have exactly the same number of $F_q$-roots.

B Proof of Theorem 3 when $d$ is even

We consider now the case of Theorem 3 when the minimum distance $d$ is even.

**Theorem 4** Let $F_q$ be a finite field and $d \in \mathbb{Z}^+$ be an even integer with $d < q$. If $C$ is a weighted Reed–Muller code over $F_q$ with $d(C(2)) \geq d$, then $k(C) \leq k(C_B)$, where $C_B$ is any of the weighted Reed–Muller codes described in Lemma 5.

**Proof** This proof will follow the same ideas in Theorem 3. Let $C$ be a weighted Reed–Muller code over $F_q$ with $d(C(2)) \geq d$. We assume without loss of generality that $C = WRM_q(\lambda, 2, \{w_1, 1\})$ for some $\lambda, w_1 > 0$. Taking

$$A := \{(i, j) \in \{0, q - 1\} \mid w_1i + j \leq \lambda\}$$

we have that $C = C_A$.

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 $\lambda$.

Case 1: $\lambda \leq a + b$. We take $B = B_1$ as in Lemma 5. To prove that $|A| = k(C) \leq k(C_B) = |B|$ we are going to prove that either $A \subseteq B$, or

$$\varphi : A - B \longrightarrow B - A$$

$$(\alpha, \beta) \mapsto (2a - \alpha, 2b - \beta)$$
Fig. 9 Figure illustrating the proof of Theorem 4 for \( d = 6 \), \( q = 11 \), \((a, b) = (5, 3)\), \( A = \{(i, j) \in \mathbb{N}^2 \mid 0.4i + j \leq 4\}\) and \( B = \{(i, j) \in \mathbb{N}^2 \mid i + j < 8\} \cup \{(i, j) \in \mathbb{N}^2 \mid i + j = 8 \text{ and } j < 3\}\)

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

Since the injectivity of \( \varphi \) is easy to check, we are showing that \( \varphi \) 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 \((\alpha, \beta)\) and \((2a - \alpha, 2b - \beta) \in A\). Hence, \((2a, 2b) = (\alpha, \beta) + (2a - \alpha, 2b - \beta) \in A + A\) and \(C_A^{(2)} = C_{A+A}\). Since \(C_A\) is a weighted Reed–Muller code, by Lemma 4 we have that \(d \leq d(C^{(2)}) = FB(C^{(2)}) \leq (q - 2a)(q - 2b) = d - 1\), 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

(b.1) \( P = (a, b) \in A \) if \( q \) is odd, or
(b.2) \( Q_1 = (a - \frac{1}{2}, b + \frac{1}{2}), \quad Q_2 = (a + \frac{1}{2}, b - \frac{1}{2}) \in A \) 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

\[
\alpha + \beta \geq a + b
\]

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

\[
w_1\alpha + \beta \leq \lambda.
\]

From (4) and (5) 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 \( \alpha + \beta > a + b \).

\[
w_1(a + \frac{1}{2}) + b - \frac{1}{2} \leq w_1a + b < w_1a + b + \frac{1}{2} < \alpha + \beta + (w_1 - 1)\alpha = w_1\alpha + \beta \leq \lambda.
\]

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,

\[
w_1a + b \leq w_1a + b + w_1(\alpha - a) + \beta - b = w_1\alpha + \beta \leq \lambda.
\]

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 $w_1(a - a - \frac{1}{2}) + \beta - b - \frac{1}{2} \geq w_1(\alpha - a + \frac{1}{2} + \beta - b - \frac{1}{2}) = 0$. As a consequence,

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

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 $C_A^{(2)} = C_{A+A}$. Since $C_A$ is a weighted Reed–Muller code, by Lemma 4 we have that $d \leq d(C_A^{(2)}) \leq (q - 2a)(q - 2b) = d - 1$, 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 $C_A^{(2)} = C_{A+A}$. Since $C_A$ is a weighted Reed–Muller code, by Lemma 4 we have that $d \leq d(C_A^{(2)}) \leq (q - 2a)(q - 2b) = d - 1$, a contradiction. Since $\frac{\lambda}{w_1} < a + b$, then $A = \{i, j\} \in \mathbb{N}^2 | 0 \leq i, j \leq q - 1$ 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 5 applies here.

References

1. Ben-Or M., Goldwasser S., Wigderson A.: Completeness theorems for non-cryptographic fault-tolerant distributed computation. In: Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing, STOC ’88, pp. 1–10, NY, USA (1988).
2. Cascudo I.: On squares of cyclic codes. IEEE Trans. Inf. Theory 65(2), 1034–1047 (2019).
3. Cascudo I., Cramer R., Mirandola D., Zémor G.: Squares of random linear codes. IEEE Trans. Inf. Theory 61(3), 1159–1173 (2015).
4. Cascudo I., Gundersen J.S., Ruano D.: Squares of matrix-product codes. Finite Fields Appl. 62, 101606 (2020).
5. Chaum D., Crépeau C., Damgård I.: Multiparty unconditionally secure protocols. In: Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing, STOC ’88, pp. 11–19, NY, USA (1988).
6. Cramer R., Damgård I., Maurer U.: 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., pp. 316–334. Springer, Berlin (2000).
7. Cramer R., Damgård I., Nielsen J.B.: Secure Multiparty Computation and Secret Sharing, 1st edn. Cambridge University Press, New York (2015).
8. Damgård I., Zakarias S.: Constant-overhead secure computation of boolean circuits using preprocessing. In: Proceedings of the 10th Theory of Cryptography Conference on Theory of Cryptography, TCC’13, pp. 621–641, Springer, Berlin (2013).
9. Damgård I., Nielsen J.B., Nielsen M., Ranellucci S.: 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., pp. 167–187. Springer, Cham (2017).
10. Feng G.-L., Rao T.R.N.: Improved geometric Goppa codes. I. Basic theory. Special issue on algebraic geometry codes. IEEE Trans. Inf. Theory 41(6), 1678–1693 (1995).
11. Fitzgerald J., Lax R.F.: Decoding affine variety codes using Gröbner bases. Des. Codes Cryptogr. 13, 147–158 (1998).
12. Galindo C., Hernando F., Ruano D.: Stabilizer quantum codes from $J$-affine variety codes and a new Steane-like enlargement. Quantum Inf. Process. 14(9), 3211–3231 (2015).
13. Geil O.: On the second weight of generalized Reed-Muller codes. Des. Codes Cryptogr. 48, 323–330 (2008).
14. Geil O., Høholdt T.: Footprints or generalized Bezout’s theorem. IEEE Trans. Inf. Theory 46(2), 635–641 (2000).
15. Geil O., Høholdt T.: On hyperbolic codes. Applied algebra, algebraic algorithms and error-correcting codes (Melbourne, 2001), pp. 159–171, Lecture Notes in Comput. Sci., 2227, Springer, Berlin (2001).
16. Martínez-Bernal J., Pitones Y., Villarreal R.H.: Minimum distance functions of complete intersections. J. Algebra Appl. 17(11), 1850204 (2018).
17. Pellikaan R.: On decoding by error location and dependent sets of error positions. Discret. Math. 106–107, 369–381 (1992).
18. Randriambololona H.: Asymptotically good binary linear codes with asymptotically good self-intersection spans. IEEE Trans. Inf. Theory 59(5), 3038–3045 (2013).
19. Randriambololona H.: On products and powers of linear codes under component wise multiplication. In: Algorithmic Arithmetic, Geometry and Coding Theory, volume 637 of Contemp. Math., pp. 3-78, Amer. Math. Soc., Providence, RI (2015).
20. Sørensen A.B.: Weighted Reed-Muller codes and algebraic-geometric codes. IEEE Trans. Inf. Theory 38(6), 1821–1826 (1992).

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.