Designs, Codes and Cryptography
https://doi.org/10.1007/s10623-023-01317-2

Defects of codes from higher dimensional algebraic varieties

Mahir Bilen Can[1] · **Roy Joshua**[2] · **G. V. Ravindra**[3]

Received: 1 March 2023 / Revised: 26 September 2023 / Accepted: 4 October 2023

Abstract
An MDS code is a code which achieves equality in the singleton bound. The defect of a code measures how far it is from an MDS code. Amplifying on the relationship between the weight distribution of a code and its dual code as in the well-known MacWilliams identities, we show in this paper that there are indeed strong lower bounds on the defects of codes or the dual codes.

Keywords Defects · Algebraic geometry codes

Mathematics Subject Classification 11T71 · 94B27

1 Introduction

The *Singleton bound* provides an important relationship between the three parameters of a linear code, namely

$$d \leq n - k + 1,$$

where n denotes the length, k denotes the dimension, and d the minimum distance of the code. A linear code is said to be *Maximum Distance Separable* (MDS) if equality is attained above.

Communicated by E. Gorla.

✉ Roy Joshua
rrjoshua@gmail.com; joshua.1@math.osu.edu

Mahir Bilen Can
mahirbilencan@gmail.com

G. V. Ravindra
girivaru@gmail.com

[1] Department of Mathematics, Tulane University, New Orleans, LA, USA

[2] Department of Mathematics, Ohio State University, Columbus, OH 43210, USA

[3] Department of Mathematics, University of Missouri-St. Louis, St. Louis, MO, USA

Published online: 27 October 2023

The defect of a code, denoted by s, measures how far it is from being an MDS code and is defined to be

$$s = n - k + 1 - d.$$

The well-known MacWilliams identities (see page 131, [14]) involving the weight distribution of a code and its dual code also provide important relationships between the parameters of a code, the parameters of its dual code, and the defects. In particular, the dual of an MDS code is also an MDS code, and the cardinality of the base field is an upper bound for both $n - k + 1$ and $k + 1$ except in *degenerate cases, that is, where either the code or its dual code have dimension* 1 *or less*. Summarizing, we have (see [14, Chapter 11, section 3]):

For a non-degenerate, MDS linear code with parameters $[n, k, d]$ *that is defined over a finite field* $\mathbb{F}_q$, *we have* $n \leq 2q$.

The length of a linear evaluation code constructed by taking the sections of a line bundle on a smooth projective algebraic variety of dimension m is typically of the order q^m. It follows that apart from the case where $q^{m-1} \leq 2$, or when the code is degenerate in the sense above, such codes cannot be MDS. Thus, MDS linear codes that are non-degenerate and defined on algebraic varieties have to be defined on algebraic curves.

Since codes from higher dimensional varieties necessarily have non-trivial defects, it is important to understand how the defects depend on the parameters of codes in this context. A few preliminary remarks seem to be in order. First, one needs to observe that for all codes constructed from algebraic varieties defined over a finite field $\mathbb{F}_q$ (referred to henceforth as *algebro-geometric codes*), the length of the code, customarily denoted by n, is bounded above by the number of $\mathbb{F}_q$-rational points on the variety. The reason for this is simply that all such codes are obtained by evaluating the sections of a given line bundle at a specified set of rational points. Next, the *Hasse-Weil bound* shows that

$$n_1 \leq q + 1 + g\lfloor 2q^{1/2} \rfloor, \tag{1.0.1}$$

where, n_1 denotes the maximum number of rational points on a smooth projective curve of genus g defined over $\mathbb{F}_q$, which by the above observations is an upper bound for the length of the corresponding code, denoted n. This shows that for genus 0 curves, n is bounded above by $q + 1$, so that one way to increase n is by considering higher genus curves. One can also see from (1.0.1) that for n to be of the order q^2 (for large q), one needs the genus to be of the order $q^{3/2}$; over large fields, this means that the genus g must be very large to get n to be of the order q^2.

An alternate approach to obtain n to be of the order q^m, for any $m \geq 1$, is to start with rational algebraic varieties of dimension m over $\mathbb{F}_q$ (and therefore contain an open subvariety isomorphic to an open subvariety of an affine space), and then evaluate the sections of a line bundle over such a variety at *most* points in the above open subvariety. The most well-known examples of this strategy are the affine and projective *Reed-Muller codes* obtained from affine and projective spaces.

Indeed, there are many other varieties which satisfy the above conditions, such as higher-dimensional toric varieties and flag varieties.

A rather surprising finding made by the authors in this context is the following[1]:

As the dimension of algebraic varieties increase, the defects of the corresponding codes or their dual codes also increase in a precise and correlated manner.

[1] Despite having examined many results in the literature regarding the construction of codes from higher-dimensional algebraic varieties (see § 5), we could not find any precise statement along these lines.

In fact, we observed that the least possible *defect* (i.e., $n - k + 1 - d$) is exactly of order $m - 1$ in q, if the dimension of the algebraic variety chosen as above over $\mathbb{F}_q$ is m. For example, linear codes that are non-degenerate and obtained from rational algebraic surfaces over $\mathbb{F}_q$, or their dual codes, will have defects of order at least q. Likewise, linear codes that are non-degenerate and obtained from rational threefolds over $\mathbb{F}_q$, or their dual codes, will have defects of order at least q^2, and so on. A goal of the present paper is to systematically prove that these facts always hold true. Our analysis for proving this result and others in the following theorems is surprisingly similar to the analysis in [14, Chapter 11, section 3].

All algebraic varieties we consider in this paper are assumed to be irreducible, reduced and defined over finite fields. For a variety X defined over a field $\mathbb{F}_q$, we denote by $\mathrm{X}(\mathbb{F}_q)$ the set of $\mathbb{F}_q$-rational points, and by $|\mathrm{X}(\mathbb{F}_q)|$, the cardinality of this set. Following a suggestion from one of the referees, we have chosen to present our results initially as bounds on the defect for a single code. Consequently, our first result is as follows:

Theorem 1.1 *Let* X *denote an algebraic variety defined over a finite field* $\mathbb{F}_q$*, where* $q \geq 4$*. Let* $C := C(\mathrm{X})$ *denote an algebro-geometric code constructed from* $\mathrm{X}(\mathbb{F}_q)$ *with defect* s *and parameters* $[n, k, d]$*, where* $n \geq k \geq 2$*. Let* $C^\perp, k^\perp, d^\perp, s^\perp$ *denote the dual code, its dimension, the minimum distance, and its defect, respectively. In this notation, if* $d^\perp > 1$ *holds, then we have the following inequalities:*

(i) $s \geq \lceil d/q \rceil - 1$,
(ii) $(s + s^\perp) \geq n/(3q) \geq n/(4(q-1))$, *and*
(iii) $(s + s^\perp) \geq k/(2(q-1)) \geq k/(2q)$. *In particular, we have*

$$max\{s, s^\perp\} \geq n/(6q) \geq n/(8(q-1)),$$

and

$$max\{s, s^\perp\} \geq k/(4(q-1)) \geq k/(4q).$$

□

Notice that the condition $d^\perp > 1$ is equivalent to the condition $k > s^\perp$. Indeed, observe that if $d^\perp = 1$ holds, then $s^\perp = k$ holds, and vice versa. This observation implies that if $d^\perp = 1$, then $(s + s^\perp) \geq k$.

Corollary 1.2 *Let* $C(\mathrm{X})$ *denote a self-dual algebro-geometric code defined over* $\mathbb{F}_q$ *(i.e.,* $C(\mathrm{X}) = C(\mathrm{X})^\perp$*), where* $q \geq 4$*, with parameters* $[n, k, d]$ *such that* $n \geq k \geq 2$*. Assume also that* $d^\perp > 1$*. If one of the following conditions*

(i) $n > 8(q-1)$, *or*
(ii) $k > 4q$

is satisfied, then the defect of the code $C(\mathrm{X})$ *must be at least 2.* □

It is interesting to observe the implications of the above theorem for families of codes constructed from families of algebraic varieties $\{\mathrm{X}_m \mid m \in \mathbb{Z}_+\}$ defined over $\mathbb{F}_q$ so that the number of rational points on X_m is of order q^{fm}, for some positive constant f. (Here $\mathbb{Z}_+$ denotes the set of all positive integers.) Remarkably, this behavior seems typical for a wide range of interesting codes constructed from families of algebraic varieties with steadily increasing dimensions. To facilitate our discussion, we will adopt the following terminology from complexity theory.

Definition 1.3 Let $\{r_m\}$ and $\{t_m\}$ be two infinite sequences of positive integers, where $m \in \mathbb{Z}_+$. We will then write that

(i) $\{r_m\} \in \Theta(\{t_m\})$ if there exists an integer $N \gg 0$ and two positive constants α, β such that $\alpha t_m \leq r_m \leq \beta t_m$ for all $m > N$. If the inequalities $\alpha t_m \leq r_m \leq \beta t_m$ hold for all $m > 1$, then we will write that $\{r_m\} \in \bar{\Theta}(\{t_m\})$.

(ii) $\{r_m\} \in \Omega(\{t_m\})$ if there exists an integer $N \gg 0$ and a constant $\alpha > 0$ such that $\alpha t_m \leq r_m$ for all $m > N$. Similarly to the previous case, we will write $\{r_m\} \in \bar{\Omega}(\{t_m\})$ if there exists a constant $\alpha > 0$ such that the inequalities $\alpha t_m \leq r_m$ hold for all $m > 1$.

We note in passing that, in Definition 1.3, the requirement that $m > 1$, rather than $m \geq 1$, is necessitated by the fact that the positive integer f in Theorems 1.4 and 1.7 could be 1, in which case the computations in Theorems 1.4 and 1.7 will hold only for $m > 1$.

Assume that we are given a family $\{\mathrm{X}_m\}$ of algebraic varieties defined over a fixed finite field $\mathbb{F}_q$ such that $\{|\mathrm{X}_m(\mathbb{F}_q)|\} \in \Omega(\{q^{fm}\})$ for some fixed positive integer $f > 0$. Let $\{C_m\}$ denote a family of evaluation codes defined on X_m. Let n_m, k_m, d_m (resp. $n_m, k_m^\perp, d_m^\perp$) denote the parameters of C_m (resp. of the dual code, $C_m^\perp$). We will assume that $n_m \geq k_m \geq 2$ for all m. Let s_m ($s_m^\perp$) denote the defect of the code C_m ($C_m^\perp$, respectively). Then we obtain the following result by applying our previous theorem to the codes in the above family.

Theorem 1.4 *In the above situation, further assume that both s_m and $s_m^\perp$ are positive for all $m > 1$. Let $q \geq 4$. Then the following assertions hold:*

(i) *If $\{d_m\} \in \bar{\Omega}(\{q^{fm}\})$, then $\{s_m + 1\} \in \bar{\Omega}(\{q^{fm-1}\})$. In fact, if there exists a positive constant α such that $d_m \geq \alpha q^m$ holds for all $m > 1$, then we have*

$$s_m + 1 \geq \alpha q^{m-1} \quad \text{for every } m > 1.$$

Moreover if $\alpha \geq 1$, where α is the positive constant above, then $s_m \geq \frac{\alpha}{2} q^{fm-1}$, for every $m > 1$.

For the next two assertions, we will assume in addition that $d_m^\perp > 1$ (equivalently $k_m > s_m^\perp$) for every integer $m > 1$.

(ii) *If $\{n_m\} \in \bar{\Omega}(\{q^{fm}\})$, then $\{s_m + s_m^\perp\} \in \bar{\Omega}(\{q^{fm-1}\})$. In fact, if α is a positive constant such that $n_m \geq \alpha q^{fm}$ for every integer $m > 1$, then*

$$s_m + s_m^\perp \geq \frac{\alpha}{3} q^{fm-1} \quad \text{for every } m > 1.$$

(iii) *If $\{k_m\} \in \bar{\Omega}(\{q^{fm}\})$, then $\{s_m + s_m^\perp\} \in \bar{\Omega}(\{q^{fm-1}\}$. In fact, if α is a positive constant such that $k_m \geq \alpha q^{fm}$ every integer $m > 1$, then*

$$s_m + s_m^\perp \geq \frac{\alpha}{2} q^{fm-1} \quad \text{for every } m > 1.$$

□

We have two remarks in order.

Remark 1.5 Under the assumptions of (ii) or (iii),

- *either* there exists a subsequence $\{s_{m_i}\}$, with $\{m_i\}$ a strictly increasing sequence of integers so that $\{s_{m_i}\} \in \Omega(\{q^{fm_i - 1}\})$,
- *or* there exists a subsequence $\{s_{m_j}^\perp\}$, with $\{m_j\}$ a strictly increasing sequence of integers so that $\{s_{m_j}^\perp\} \in \Omega(\{q^{fm_j - 1}\})$.

Remark 1.6 The implications in (i) and (iii) are strict in the sense that the conclusion may be true even if the hypothesis is false: this is shown in the examples worked out in § 4.

The aforementioned results do not apply directly to the case of codes constructed from toric varieties, primarily due to the common practice of evaluating sections (of line bundles) solely at the rational points on the dense torus. For relevant examples, we refer to [8] and [15]. For such toric codes, it is necessary to replace q^{fm} everywhere by $(q-1)^{fm}$. Consequently, we obtain the following variants of the above results.

Assume that we are given a family, $\{\mathrm{X}_m\}$, of algebraic varieties defined over the fixed finite field $\mathbb{F}_q$, such that $\{|\mathrm{X}_m(\mathbb{F}_q)|\} \in \Omega(\{(q-1)^{fm}\})$ for some fixed positive integer f. Let $\{C_m\}$ denote a family of codes, with C_m defined on X_m, so that n_m, k_m, d_m ($n_m, k_m^{\perp}, d_m^{\perp}$) denote the parameters of the code C_m (the dual code $C_m^{\perp}$, respectively). Let s_m ($s_m^{\perp}$) denote the defect of the code C_m ($C_m^{\perp}$, respectively). Then we obtain the following theorem.

Theorem 1.7 *Assume throughout that s_m and $s_m^{\perp}$ are both positive, and that $d_m^{\perp} > 1$ (equivalently, $k_m > s_m^{\perp}$), for all $m > 1$. Assume also that $q \geq 7$. Let f denote the positive integer chosen above. Then the following assertions hold:*

(i) *If $\{d_m\} \in \bar{\Omega}(\{(q-1)^{fm}\})$, then $\{s_m + 1\} \in \bar{\Omega}(\{(q-1)^{fm-1}\})$. In fact, if there exists a positive constant α such that the inequality $d_m \geq \alpha(q-1)^m$ holds for every $m > 1$, then we have*

$$s_m + 1 \geq \frac{\alpha}{2}(q-1)^{m-1} \quad \textit{for every } m > 1.$$

Moreover if $\alpha \geq 1$, where α is the positive constant above, then $s_m \geq \frac{\alpha}{3}(q-1)^{fm-1}$, for every $m > 1$.

For the next two assertions, we relax our assumption $q \geq 7$ to $q \geq 4$.

(ii) *If $\{n_m\} \in \bar{\Omega}(\{(q-1)^{fm}\})$, then $\{s_m + s_m^{\perp}\} \in \bar{\Omega}(\{(q-1)^{fm-1}\})$. In fact, if α is a positive constant such that $n_m \geq \alpha(q-1)^{fm}$ holds for every $m > 1$, then we have*

$$s_m + s_m^{\perp} \geq \frac{\alpha}{4}(q-1)^{fm-1} \quad \textit{for every } m > 1.$$

(iii) *If $\{k_m\} \in \bar{\Omega}(\{(q-1)^{fm}\})$, then $\{s_m + s_m^{\perp}\} \in \bar{\Omega}(\{(q-1)^{fm-1}\})$. In fact, if α is a positive constant such that $k_m \geq \alpha(q-1)^{fm}$ holds for every $m > 1$, then we have*

$$s_m + s_m^{\perp} \geq \frac{\alpha}{2}(q-1)^{fm-1} \quad \textit{for every } m > 1.$$

□

We have the corresponding remarks.

Remark 1.8 Under the assumptions of (ii) or (iii),

- *either* there exists a subsequence $\{s_{m_i}\}$, with $\{m_i\}$ a strictly increasing sequence of integers so that $\{s_{m_i}\} \in \Omega(\{(q-1)^{fm_i-1}\})$,
- *or* there exists a subsequence $\{s_{m_j}^{\perp}\}$, with $\{m_j\}$ a strictly increasing sequence of integers so that $\{s_{m_j}^{\perp}\} \in \Omega(\{(q-1)^{fm_j-1}\})$.

Remark 1.9 The implications in (i) and (iii) are strict in the sense that the conclusion may be true even if the hypothesis is false: this is shown in the examples worked out in § 4.

We are now ready to give a brief overview of the remaining parts of our paper. The next section begins with a concise review of fundamental terminology essential for the subsequent discussions. Proceeding to the third section, we conduct a thorough analysis of defects in connection with the MacWilliams identities, which establishes the weight distributions of

a code and its dual code. Here we also discuss the proofs of all the theorems stated in the introduction. The main goal of the fourth section is to show by explicit examples that the various implications discussed in the main results of the paper, such as in Theorem 1.4(i) and (iii) as well as in Theorem 1.7(i) and (iii) are strict. We do this by focusing on families of codes constructed primarily from projective spaces or products of projective spaces. § 5 provides a brief survey of Algebraic geometry codes constructed from surfaces and other higher dimensional algebraic varieties. Since lower bounds for the minimum distances of these codes are known, we use the Griesmer bound to provide a lower bound for their defects as in Theorem 1.1(i).

2 Basic terminology

• We fix a finite field $\mathbb{F}_q$ with characteristic p and consider only algebraic varieties defined over $\mathbb{F}_q$. Since we will only consider linear codes, a code C will denote a finite dimensional vector space over $\mathbb{F}_q$. Such codes we consider will always be obtained as follows.

• We fix a projective algebraic variety X over $\mathbb{F}_q$ along with a chosen line bundle $\mathcal{L}$.

• We also fix a set of n_1 $\mathbb{F}_q$-rational points on X, and evaluate sections of the line bundle $\mathcal{L}$ at these points to define the code C.

Therefore, the length of the code C (denoted n) will be bounded above by n_1.

The letter k will denote the dimension of the code C, which is in fact its dimension as a vector space over $\mathbb{F}_q$. The letter d will denote the minimum distance of the code C.

Definition 2.1 Given a linear code C, with parameters $[n, k, d]$, the *defect* of the code C, denoted by s, is defined by $s = n + 1 - k - d$. We will also say C is an A^sMDS-code in this case.

The terminology of Definition 2.1, which is adopted from [7], gives us a convenient way to express how far a given code is from an MDS-code. For example, one of our conclusions is that all non-degenerate surface codes, where the surfaces are defined over $\mathbb{F}_q$ and the number of rational points on them is of order q^2, seem to be A^sMDS-codes for $s \geq 1$. See the examples worked out in the last section.

Clearly an A^0MDS-code is an MDS code, and an A^1MDS-code is what is often called an *almost MDS code*. It is known (see [14, Chapter 11, section 3]) that the dual of an MDS code is necessarily an MDS code, while no such restriction remains in place for the codes with defect greater than or equal to 1.

For $i \in \{0, 1, \ldots, n\}$, we will use A_i to denote the number of code words with weight i in a given code C with parameters $[n, k, d]$. Clearly, for every $i \in \{0, \ldots, n\}$, we have $A_i \geq 0$. This simple fact will turn out to have important consequences in view of the MacWilliams-Sloane relationship between the weight distribution of the given code C and the weight distribution of the corresponding dual code $C^{\perp}$.

3 Relationship between the defect and the other code parameters

We begin with the first such relationship, which is between the minimum distance d, the defect s, and q.

Proposition 3.1 (See [7, Lemma 2].) *For a* $[n,\ k,\ d]$ *code* C *defined over a finite field* $\mathbb{F}_q$, *with* $n \geq k \geq 2$, *we have*

$$d \leq q(s+1).$$

In particular, $s \geq \lceil d/q \rceil - 1$.

Proof By the Griesmer bound, one first observes that:

$$n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil. \tag{3.0.1}$$

Therefore, if the inequality $d > q(s+1)$ was true, then it would follow that

$$n \geq d + (s+2) + \sum_{i=2}^{k-1} \lceil \frac{(s+1)}{q^{i-1}} \rceil \geq d + s + 2 + k - 2 = d + s + k = n + 1$$

since, by definition $s = n - k + 1 - d$. This contradiction proves that $d \leq q(s+1)$. Now the last statement follows readily from this. □

3.1 Proofs of part (i) of Theorems 1.1, 1.4 and 1.7

One may first of all observe that the statement $d \leq q(s+1)$ readily proves the first statement in Theorem 1.1.

Next we consider the remaining two statements. Observe that it suffices to prove the following statement: Let $\{C_m\}$ denote a family of codes defined over $\mathbb{F}_q$, so that the parameters of C_m are $[n_m, k_m, d_m]$ with s_m the corresponding defect. Let f be a positive integer so that if $\{d_m\} \in \Omega(\{q^{fm}\})$ ($\in \Omega(\{(q-1)^{fm}\})$ resp.), then $\{s_m\} \in \Omega(\{q^{fm-1}\})$ ($\in \Omega(\{(q-1)^{fm-1}\})$ for all $q \geq 7$, respectively).

We will first consider the case where $\{d_m\} \in \Omega(\{q^{fm}\})$. In this case, we first observe that, as $f > 0$ and $m > 1$,

$$(q^{fm}/q) - 1 = q^{fm-1} - 1 \geq q^{fm-1}/2, \quad q \geq 2. \tag{3.1.1}$$

Observe that, by Proposition 3.1,

$$s_m \geq d_m/q - 1.$$

Therefore, if $\{d_m\} \in \Omega(q^{fm})$, that is, $d_m \geq \alpha q^{fm}$, for some positive constant α, then,

$$\begin{aligned} &s_m + 1 \geq \alpha q^{fm-1} \text{ in general, and if } \alpha \geq 1, \text{ then,} \\ &s_m \geq \frac{\alpha}{2} q^{fm-1} \text{ for all } q \geq 2. \end{aligned}$$

This proves the statement when $\{d_m\} \in \Omega(\{q^{fm}\})$.

Next we consider the case where $\{d_m\} \in \Omega(\{(q-1)^{fm}\})$. In this case, we observe that

$$\begin{aligned} \frac{(q-1)^{fm}}{q} &\geq \frac{1}{2}(q-1)^{fm-1} \text{ for all } q \geq 2, \\ \frac{1}{2}(q-1)^{fm-1} - 1 &\geq \frac{1}{3}(q-1)^{fm-1} \text{ for all } q \geq 7. \end{aligned} \tag{3.1.2}$$

Since $d_m \geq \alpha(q-1)^{fm}$ for some $\alpha > 0$, we have that

$$s_m + 1 \geq \alpha \frac{(q-1)^{fm}}{q} \geq \frac{1}{2}\alpha(q-1)^{fm-1} \text{ for all } q \geq 2,$$

where the first inequality follows from Proposition 3.1 and the second by the (first) inequality in (3.1.2). The second inequality in (3.1.2) shows that, when $\alpha \geq 1$, s_m is bounded below by $\frac{1}{3}\alpha(q-1)^{fm-1}$, for all $q \geq 7$ and this completes the proof when $\{d_m\} \in \Omega(\{(q-1)^{fm}\})$. □

3.2. The goal of this section is to provide a proof of the statements (ii) and (iii) in Theorems 1.1, 1.4 and 1.7. However, in order to do this we need to first establish relationships between the defect s and the dimension k, as well as between s and $n-k$ (which is the dimension of the dual code). This needs a considerably deeper analysis of the weight distribution for the given code and the dual code making use of the MacWilliams-Sloane relations. We begin with the following Lemma.

Lemma 3.2 *For any positive integers n and q, the following hold:*

(i) $2\frac{q^n+\cdots+q+1}{q^{n-1}+\cdots+q+1} - 1 \in \Theta(q),\ q \geq 1,$

(i)' $2\frac{q^n+\cdots+q+1}{q^{n-1}+\cdots+q+1} - 1 \in \Theta(q-1),\ q \geq 3,$

(ii) $\frac{q^n+\cdots+q+1}{q^{n-1}+\cdots+q+1} \in \Theta(q),\ q \geq 1,$ *and,*

(ii)' $\frac{q^n+\cdots+q+1}{q^{n-1}+\cdots+q+1} \in \Theta(q-1),\ q \geq 3.$

Proof We first consider (i). Observe that

$$q^n + \ldots + 1 = (q^{n+1}-1)/(q-1) \text{ and } q^{n-1} + \ldots + 1 = (q^n-1)/(q-1).$$

Therefore:

$$\frac{q^n + \cdots + q + 1}{q^{n-1} + \cdots + q + 1} = \frac{q^{n+1}-1}{q^n - 1}.$$

Next,

$$\begin{aligned} q + (q-1)/(q^n-1) &= (q(q^n-1) + (q-1))/(q^n-1) \\ &= (q^{n+1} - q + q - 1)/(q^n-1) \\ &= (q^{n+1}-1)/(q^n-1). \end{aligned} \tag{3.2.1}$$

Therefore,

$$2((q^{n+1}-1)/(q^n-1)) - 1 = 2(q + ((q-1)/(q^n-1))) - 1 \geq 2q - 1 \geq q$$

for all $q \geq 1$. Moreover,

$$\begin{aligned} 2((q^{n+1}-1)/(q^n-1)) - 1 &= 2(q + ((q-1)/(q^n-1))) - 1 \leq 2(q+1) - 1 \\ &= 2q + 2 - 1 = 2q + 1 \leq 3q \text{ for all } q \geq 1. \end{aligned}$$

Therefore, (i) follows.

Next, we consider (i)'. For this, we observe:

$$2\frac{q^n + \cdots + q + 1}{q^{n-1} + \cdots + q + 1} - 1 = 2(q + (q-1)/(q^n-1)) - 1 \geq 2(q/2) - 1 = q - 1 \tag{3.2.2}$$

One may also see that

$$2\frac{q^n + \cdots + q + 1}{q^{n-1} + \cdots + q + 1} - 1 = 2(q + (q-1)/(q^n-1)) - 1 \leq 2q + 1 \leq 4(q-1), q \geq 3. \tag{3.2.3}$$

Taken together, these prove that

$$2\frac{q^n+\cdots+q+1}{q^{n-1}+\cdots+q+1}-1\in\Theta(q-1),\ \text{for } q\geq 3.$$

Next, we consider (ii). Clearly,

$$2q\geq q+1\geq q+(q-1)/(q^n-1)=\frac{q^n+\cdots+q+1}{q^{n-1}+\cdots+q+1}\geq q,$$

which proves (ii). Next, observe that

$$\frac{q^n+\cdots+q+1}{q^{n-1}+\cdots+q+1}=q+\frac{q-1}{q^n-1}\leq q+1\leq 2(q-1),\ \text{for } q\geq 3.$$

Clearly, $q+\frac{q-1}{q^n-1}\geq q-1$. Thus

$$\frac{q^n+\cdots+q+1}{q^{n-1}+\cdots+q+1}\in\Theta(q-1),\ \text{for } q\geq 3.$$

This proves (ii)' and completes the proof of the Lemma. □

Next, we recall the MacWilliams identities (see page 131, [14])

$$\sum_{i=0}^{n-r}\binom{n-i}{r}A_i=q^{k-r}\sum_{i=0}^{r}\binom{n-i}{r-i}A_i^{\perp},\ \text{for } r=0,\ldots,n, \tag{3.2.4}$$

where A_i (resp. $A_i^{\perp}$) denotes the number of code words of weight i in the code C (resp. the dual code $C^{\perp}$). These provide us with the following relations:

$$\sum_{i=d}^{n-r}\binom{n-i}{r}A_i=q^{k-r}\binom{n}{r}-\binom{n}{r},\ \text{for } r=0,\ldots,d^{\perp}-1. \tag{3.2.5}$$

Here $d^{\perp}$ denotes the minimum distance of the dual code. Recall that s (resp. $s^{\perp}$) denotes the defect of the given code C (resp. its dual code $C^{\perp}$). Then clearly one has:

$$\begin{aligned} d&=n-k-s+1,\ \text{and}\\ d^{\perp}&=n-(n-k)-s^{\perp}+1=k-s^{\perp}+1. \end{aligned} \tag{3.2.6}$$

Next, we let

$$\begin{aligned} s^{\perp}&=s-s',\ \text{and}\\ r&=d^{\perp}-1=k-s^{\perp}. \end{aligned} \tag{3.2.7}$$

In view of these, one may observe that the summation in (3.2.5) goes from $i=d=n-k-s+1=n-k-s^{\perp}-s'+1$ to $n-r=n-d^{\perp}+1=n-k+s^{\perp}$.We first take $r=d^{\perp}-1=k-s^{\perp}$ in (3.2.5) to obtain:

$$\begin{aligned} &\binom{k+s-1}{k-s^{\perp}}A_{n-k-s+1}+\binom{k+s-2}{k-s^{\perp}}A_{n-k-s+2}+\cdots+\binom{k-s^{\perp}}{k-s^{\perp}}\\ &A_{n-k+s^{\perp}}=(q^{s^{\perp}}-1)\binom{n}{k-s^{\perp}}. \end{aligned} \tag{3.2.8}$$

Next, we take $r = d^{\perp} - 2 = k - s^{\perp} - 1$ in (3.2.5) to obtain:

$$\binom{k+s-1}{k-s^{\perp}-1}A_{n-k-s+1} + \binom{k+s-2}{k-s^{\perp}-1}A_{n-k-s+2} + \cdots + \binom{k-s^{\perp}-1}{k-s^{\perp}-1}A_{n-k+s^{\perp}+1} = (q^{s^{\perp}+1}-1)\binom{n}{k-s^{\perp}-1}. \tag{3.2.9}$$

Next, we proceed to compare the terms on the left-hand-side of (3.2.8) with the corresponding terms on the left-hand-side of (3.2.9). We have the binomial coefficient $\binom{k+s-i}{k-s^{\perp}-1}$ on the left-hand-side of (3.2.9), while the corresponding term on the left-hand-side of (3.2.8) is $\binom{k+s-i}{k-s^{\perp}}$. Now we obtain (with $*$ denoting multiplication):

$$\begin{aligned}
\binom{k+s-i}{k-s^{\perp}-1} &= \binom{k+s^{\perp}+s'-i}{k-s^{\perp}-1} \\
&= \frac{(k+s^{\perp}+s'-i)!}{(k-s^{\perp}-1)!(2s^{\perp}+s'-i+1)!} \\
&= \frac{(k+s^{\perp}+s'-i)!(k-s^{\perp})}{(k-s^{\perp})!(2s^{\perp}+s'-i)!(2s^{\perp}+s'-i+1)} \\
&= \frac{(k+s^{\perp}+s'-i)!}{(k-s^{\perp})!(2s^{\perp}+s'-i)!} * \frac{(k-s^{\perp})}{(2s^{\perp}+s'-i+1)} \\
&= \binom{k+s^{\perp}+s'-i}{k-s^{\perp}} * \frac{(k-s^{\perp})}{(2s^{\perp}+s'-i+1)} \\
&\geq \binom{k+s^{\perp}+s'-i}{k-s^{\perp}} * \frac{(k-s^{\perp})}{2s^{\perp}+s'} = \binom{k+s-i}{k-s^{\perp}} * \frac{(k-s^{\perp})}{2s^{\perp}+s'},
\end{aligned} \tag{3.2.10}$$

where one obtains the last inequality from the observation that $2s^{\perp}+s'-i+1 \leq 2s^{\perp}+s'$ and since we will assume $k > s^{\perp}$ (which, in view of (3.2.7) is equivalent to $d^{\perp} > 1$) and $i \geq 1$.

Therefore, a comparison of the left-hand-side of (3.2.9) and (3.2.8) shows that the sum of all the terms on the left-hand-side of (3.2.9) except the last term is greater than or equal to the sum of all the terms on the left-hand-side of (3.2.8) multiplied by the factor $\frac{k-s^{\perp}}{2s^{\perp}+s'}$. Clearly the last term equals the sum of all the terms on the right-hand-side of (3.2.8) multiplied by the factor $\frac{k-s^{\perp}}{2s^{\perp}+s'}$. Moreover, the latter equals

$$(q^{s^{\perp}}-1)\binom{n}{k-s^{\perp}}\frac{k-s^{\perp}}{2s^{\perp}+s'} = (q^{s^{\perp}}-1)\binom{n}{k-s^{\perp}-1}\frac{(n-k+s^{\perp}+1)(k-s^{\perp})}{(k-s^{\perp})(2s^{\perp}+s')}.$$

One may also observe from (3.2.6) that $s' = s - s^{\perp}$, so that $2s^{\perp}+s' = s+s^{\perp}$.

Therefore, from (3.2.8) and (3.2.9), we obtain:

$$\begin{aligned}
0 \leq A_{n-k+s^{\perp}+1} &\leq (q^{s^{\perp}+1}-1)\binom{n}{k-s^{\perp}-1} \\
&\quad - (q^{s^{\perp}}-1)\binom{n}{k-s^{\perp}-1} * \frac{(n-k+s^{\perp}+1)}{s+s^{\perp}} \\
&= (q-1)\binom{n}{k-s^{\perp}-1}
\end{aligned}$$

$$\left[(q^{s^\perp}+\cdots+q^1+1)-(q^{s^\perp-1}+\cdots+q^1+1)*\frac{(n-k+s^\perp+1)}{s+s^\perp}\right]. \tag{3.2.11}$$

Since $A_{n-k+s^\perp+1}\geq 0$, it follows that

$$(s+s^\perp)\frac{q^{s^\perp}+\cdots+q^1+1}{q^{s^\perp-1}+\cdots+q^1+1}\geq n-k+s^\perp+1. \tag{3.2.12}$$

Bringing the term $s^\perp$ to the left-hand-side provides us with the inequality,

$$(s+s^\perp)\frac{q^{s^\perp}+\cdots+q^1+1}{q^{s^\perp-1}+\cdots+q^1+1}-s^\perp\geq n-k+1. \tag{3.2.13}$$

Replacing the given code C by its dual code $C^\perp$, and observing that for $C^\perp$, the dimension of the code is $n-k$, while the defect for the code C is s, we also obtain from (3.2.12):

$$(s+s^\perp)\frac{q^{s}+\cdots+q^1+1}{q^{s-1}+\cdots+q^1+1}\geq k+s+1\geq k. \tag{3.2.14}$$

Bringing the term s to the left-hand-side, then provides us with the inequality,

$$(s+s^\perp)\frac{q^{s}+\cdots+q^1+1}{q^{s-1}+\cdots+q^1+1}-s\geq k+1. \tag{3.2.15}$$

These results set the framework for completing the proofs of parts (ii) and (iii) of Theorems 1.1, 1.4 and 1.7, which we discuss next.

Proofs of parts (ii) and (iii) of Theorems 1.1, 1.4 **and** 1.7. Without loss of generality, we may assume that $s^\perp\geq s$ (if necessary, by renaming C as $C^\perp$). Then, on adding the left-hand-sides of the two inequalities in (3.2.13) and (3.2.15), we obtain:

$$(s+s^\perp)\left(2\frac{q^{s^\perp}+\cdots+q^1+1}{q^{s^\perp-1}+\cdots+q^1+1}-1\right)\geq n. \tag{3.2.16}$$

From Lemma 3.2(i), we have that

$$2\frac{q^{s^\perp}+\cdots+q^1+1}{q^{s^\perp-1}+\cdots+q^1+1}-1\in\Theta(q).$$

In fact, the proof of Lemma 3.2(i) shows that

$$q\leq 2\frac{q^{s^\perp}+\cdots+q^1+1}{q^{s^\perp-1}+\cdots+q^1+1}-1\leq 3q,\quad \text{since } q\geq 1.$$

In view of (3.2.16), these prove both statements in Theorems 1.1(ii) and 1.4(ii), since $q\geq 4$ by assumption. Next, from Lemma 3.2(i)', we have that

$$2\frac{q^{s^\perp}+\cdots+q^1+1}{q^{s^\perp-1}+\cdots+q^1+1}-1\in\Theta(q-1),\quad \text{where } q\geq 3.$$

In fact, the proof of Lemma 3.2(i)' shows that

$$q-1\leq 2\frac{q^{s^\perp}+\cdots+q^1+1}{q^{s^\perp-1}+\cdots+q^1+1}-1\leq 4(q-1),\quad (q\geq 3).$$

In view of (3.2.16), this proves the statement in Theorem 1.7(ii).

Next, we observe from Lemma 3.2(ii) that

$$\frac{q^s + \cdots + q^1 + 1}{q^{s-1} + \cdots + q^1 + 1} \in \Theta(q)$$

(and from Lemma 3.2(ii)', that it belongs to $\Theta(q-1)$, for $q \geq 3$, respectively). In fact, the proof of Lemma 3.2(ii) and (ii)' show that

$$q - 1 \leq q \leq \frac{q^s + \cdots + q^1 + 1}{q^{s-1} + \cdots + q^1 + 1} \leq 2(q-1) \leq 2q, \quad (q \geq 3).$$

Therefore, in view of the above observations, (3.2.14) proves the statements in Theorems 1.1(iii), 1.4(iii) and 1.7(iii). □

Proofs of the statements in Remarks 1.5 and 1.8. Assume towards a contradiction that the statement in Remark 1.5 is false. Then it follows that $\lim_{m\to\infty} s_m/q^{fm-1} = 0 = \lim_{m\to\infty} s_m^{\perp}/q^{fm-1}$, so that $\lim_{m\to\infty}(s_m + s_m^{\perp})/q^{fm-1} = 0$, which contradicts the conclusion that $\{s_m + s_m^{\perp}\} \in \Omega(\{q^{fm-1}\})$. One may prove the statement in Remark 1.8 in a similar manner.

Proof of Corollary 1.2. If $C(\mathrm{X})$ is self-dual then $s = s^{\perp}$. Theorem 1.1 (ii) implies that $(s + s^{\perp}) \geq n/(4(q-1))$. If $C(\mathrm{X})$ is self-dual and $s \leq 1$, then $s + s^{\perp} \leq 2$. In this case, our claim follows from the inequality $2 \geq (s + s^{\perp}) \geq n/(4(q-1))$. Likewise, under our assumptions, Theorem 1.1 (iii) implies that $2 \geq k/(2q)$. Hence, our claim follows in this case also. □

4 Examples of codes from projective spaces

The main goal of this section is to show by explicit examples that the various implications discussed in the main results of the paper such as in Theorem 1.4(i) and (iii) as well as in Theorem 1.7(i) and (iii) are strict. For this purpose, we will consider the following three families of codes constructed from algebraic varieties defined over $\mathbb{F}_q$:

- $\mathrm{X}_m = \mathbb{P}^m$, $m \geq 2$,
- $\mathrm{X}_m = (\mathbb{P}^2)^{\times m}$, and
- $\mathrm{X}_m = (\mathbb{P}^1)^{\times m}$.

Example 4.1 Let $\mathrm{X}_m = \mathbb{P}^m$ and $\mathcal{O}(r)$ the r-th tensor power of the structure sheaf $\mathcal{O}(1)$ on $\mathbb{P}^m$. The polytope corresponding to the line bundle $\mathcal{O}(r)$ is the regular r-simplex with a side given by r and all but one face along the coordinate planes, one vertex at the origin and the other vertices being

$$(r, 0, \ldots, 0), (0, r, 0, \ldots, 0), \ldots, (0, \ldots, 0, r).$$

We also require that $r \leq q - 1$.

Now we will compute the parameters of the corresponding codes, where we evaluate sections of the line bundle $\mathcal{O}(r)$ at all the $\mathbb{F}_q$-rational points on the open affine subspace $\mathbb{A}^m$.

Therefore, $n = q^m$, that is, $f = 1$. The bound worked out in [11, Theorem 6.13] shows that the maximum number of zeros of a degree r polynomial in m-variables is rq^{m-1}. These are the maximum number of zeros on an affine space of dimension m. Therefore, the minimum distance is given by

$$d_m = q^m - rq^{m-1}.$$

It follows that $\{d_m\} \in \Theta(\{q^m\})$. To see that $q^m - rq^{m-1} > \alpha q^m$, just choose $0 < \alpha < 1/q$.

The volume of the hyper-pyramid gives the dimension of the corresponding code. Therefore, it is given by $k_m = r^m/m!$, which is the formula for the volume of the above r-simplex with side given by r. Clearly, the limit of this term is 0, as $m \to \infty$. Therefore

$$s_m = n_m + 1 - d_m - k_m = q^m + 1 - (q^m - rq^{m-1}) - r^m/m! = rq^{m-1} - r^m/m! + 1.$$

As $\lim_{m\to\infty} r^m/m! = 0$, it follows that $\{s_m\} \in \Omega(\{q^{m-1}\})$ (and hence $\{s_m + s_m^{\perp} | m\} \in \Omega(\{q^{m-1}\})$), *for each fixed* q. However, observe that $\{k_m\}$ clearly does *not* belong to $\Omega(\{q^m\})$. This shows that the implication in Theorem 1.4(iii) is indeed strict.

Next, we consider the same example, but where the sections of the line bundle $\mathcal{O}(r)$ are evaluated only at the rational points on the dense torus. In this case, $n = (q-1)^m$. The same argument as in [11, Theorem 6.13] (see also [15, Theorem 2.1]), but where one evaluates only at the rational points on the dense torus, shows that the maximum number of zeroes of a degree r polynomial in m variables, when evaluated at the rational points of a split torus of dimension m is $r(q-1)^{m-1}$. Therefore, the minimum distance is given by

$$d_m = (q-1)^m - r(q-1)^{m-1}.$$

It follows that $\{d_m\} \in \Theta(\{(q-1)^m\})$. To see that $(q-1)^m - r(q-1)^{m-1} > \alpha(q-1)^m$, just choose $0 < \alpha < 1/(q-1)$. Then we obtain

$$\begin{aligned} s_m &= n_m + 1 - d_m - k_m \\ &= (q-1)^m + 1 - (q-1)^m + r(q-1)^{m-1} - r^m/m! \\ &= r(q-1)^{m-1} - r^m/m! + 1. \end{aligned}$$

As $\lim_{m\to\infty} r^m/m! = 0$, it is clear that $\{s_m\} \in \Omega(\{(q-1)^{m-1}\})$, *for each fixed* q. However, observe that $\{k_m\}$ clearly does *not* belong to $\Omega(\{(q-1)^m\})$. This shows that the implication in Theorem 1.7(iii) is also indeed strict.

Example 4.2 Here, the variety X_m will be $(\mathbb{P}^2)^{\times m}$. The line bundle we use on $\mathbb{P}^2$ will be $\mathcal{O}(r)$ which corresponds to the triangle with vertices $(0,0)$, $(r,0)$, $(0,r)$. We will choose $r \ll q$, where r is a positive integer. We evaluate sections of the above line bundle at all points of the affine subspace $\mathbb{A}^{2m}$. Therefore, the parameters of the resulting code on $\mathbb{P}^2$ are:

$$n = q^2, \quad k = (r+1)(r+2)/2, \quad \text{and } d = q^2 - rq.$$

Invoking [16, 2.5], the parameters of the resulting product code on $\mathrm{X}_m = (\mathbb{P}_2)^{\times m}$ are then given by

$$[n_m, k_m, d_m] \;=\; [q^{2m}, ((r+1)^m(r+2)^m)/2^m, (q^2 - rq)^m].$$

Therefore, in this case $\{n_m\} \in \Theta(\{q^{2m}\})$ and $\{d_m\} \in \Omega(\{q^{2m}\})$ for q sufficiently large and for a fixed $m > 1$ (for then, viewing d_m as a polynomial in q, the complexity is determined by the leading term in q). Clearly, we have $f = 2$ in this example. Since $r \ll q$ by assumption, we have

$$k_m = ((r+1)^m(r+2)^m)/2^m \ll (q(q+1))^m/2^m.$$

Therefore, $\{k_m\}$ does not belong to $\Omega(\{q^{2m}\})$.

Now, we have

$$s_m = q^{2m} + 1 - (q^2 - rq)^m - ((r+1)^m(r+2)^m)/2^m$$

$$= q^{2m-1} + \text{ lower order terms in } q.$$

In other words, we have $\{s_m\} \in \Omega(\{q^{2m-1}\})$ for all sufficiently large q. This example also shows that the implication in Theorem 1.4(iii) is indeed strict.

Next, we consider the same example, but where we evaluate sections of the line bundle $\mathcal{O}(r)$ only at the rational points in the dense torus in $\mathbb{P}^2$. Therefore, the parameters of the resulting code on $\mathbb{P}^2$ are given by

$$n = (q-1)^2, \quad k = (r+1)(r+2)/2, \quad \text{and } d = (q-1)^2 - r(q-1).$$

Invoking [16, 2.5] (see also [15, Theorem 2.1]), the parameters of the resulting product code on $\mathrm{X}_m = (\mathbb{P}_2)^{\times m}$ are then given by

$$[n_m, k_m, d_m] \;=\; [(q-1)^{2m}, ((r+1)^m(r+2)^m)/2^m, ((q-1)^2 - r(q-1))^m].$$

Therefore, in this case $\{n_m\} \in \Theta(\{(q-1)^{2m}\})$ and $\{d_m\} \in \Omega(\{(q-1)^{2m}\})$ for q sufficiently large and for a fixed $m > 1$ (for then, viewing d_m as a polynomial in q, the complexity is determined by the leading term in q). Clearly, we have $f = 2$ in this example. Moreover,

$$k_m \;=\; ((r+1)^m(r+2)^m)/2^m \;\ll\; ((q-1)q)^m/2^m.$$

Consequently, $\{k_m\}$ does not belong to $\Omega(\{(q-1)^{2m}\})$.

We observe that

$$\begin{aligned} s_m &= (q-1)^{2m} + 1 - ((q-1)^2 - r(q-1))^m - ((r+1)^m(r+2)^m)/2^m \\ &= (q-1)^{2m-1} + \text{ lower order terms in } q. \end{aligned}$$

It follows that $\{s_m\} \in \Omega(\{(q-1)^{2m-1}\})$, where q is a sufficiently large prime power. This example also shows that the implication in Theorem 1.7(iii) is indeed strict.

Example 4.3 In this final example, we will let $\mathrm{X}_m = (\mathbb{P}^1)^{\times m}$. The code we choose on $\mathbb{P}^1$ will be a Reed-Solomon code with parameters

$$n = q, \; k = q-1, \; d = 2,$$

which is clearly an MDS code. Here we are assuming $q \gg 2$. Invoking [16, 2.5] once more, we compute the parameters of the resulting product codes to be given by

$$n_m = q^m, \; k_m = (q-1)^m, \; \text{and } d_m = 2^m.$$

In this case, clearly $\{k_m\}$ belongs to $\Omega(\{(q-1)^m\})$, and therefore to $\Omega(\{q^m\})$ for q sufficiently large, but $\{d_m\}$ does *not* belong to $\Omega(\{q^m\})$, for any $q > 2$. We compute:

$$s_m = q^m + 1 - (q-1)^m - 2^m.$$

One can see that on expanding $(q-1)^m$ using the binomial theorem in powers of q, the leading term in q, which is q^m, cancels off leaving terms in q^{m-1} and lower order terms. (One may also observe that as $q \gg 2$, the term $q^{m-2} > 2^m$.) Therefore, $\{s_m\} \in \Omega(\{q^{m-1}\})$ for q sufficiently large and $m > 1$. Moreover, the resulting family of codes are all non-MDS codes for $m > 1$. This example shows that the implication in Theorem 1.4(i) is indeed strict. (Clearly, in this example $f = 1$.)

Next we consider the same example, but where we evaluate sections of the line bundle $\mathcal{O}(r)$ only at the rational points in the dense torus in $\mathbb{P}^1$. The code we choose on $\mathbb{P}^1$ will be a Reed-Solomon code with parameters

$$n = (q-1), \; k = q-2, \; d = 2,$$

which is clearly an MDS code. Invoking again [16, 2.5], we compute the parameters of the resulting product codes to be given by

$$[n_m, k_m, d_m] \;=\; [(q-1)^m, (q-2)^m, 2^m].$$

In this case, clearly $\{k_m\}$ belongs to $\Omega(\{(q-2)^m\})$, and therefore to $\Omega(\{(q-1)^m\})$ for q sufficiently large, but $\{d_m\}$ does *not* belong to $\Omega(\{(q-1)^m\})$, for any $q > 2$. We compute:

$$s_m = (q-1)^m + 1 - (q-2)^m - 2^m.$$

Therefore, $\{s_m\} \in \Omega(\{(q-1)^{m-1}\})$ for q sufficiently large and for a fixed $m > 1$. Moreover, the resulting family of codes are all non-MDS codes for $m > 1$. This example shows that the implication in Theorem 1.7(i) is indeed strict. (Clearly, in this example also, $f = 1$.)

Remark 4.1 It is important that we consider only families of codes all of which are not MDS, that is, whose defects are positive. Otherwise, the conclusions will not hold, as can be seen by taking degenerate MDS codes. For example, one may take $n = q$, $k = q$ and $d = 1$ as an example of a degenerate MDS code constructed from $\mathbb{P}^1$. Then the resulting product codes on $\mathrm{X}_m = (\mathbb{P}^1)^{\times m}$ will also be degenerate MDS codes and therefore, in these cases both s_m and $s_m^{\perp}$ will be 0 for all m.

5 Examples of codes from higher dimensional algebraic varieties

In this section, we will discuss various examples of codes that are constructed from higher dimensional algebraic varieties, for which good estimates for code parameters are known. There are in fact many papers that work out explicit bounds for the parameters of algebro-geometric codes constructed from surfaces: rational surfaces (see [4]), low rank surfaces (see [13], [17]), del Pezzo surfaces (see [3, 12]), Abelian surfaces (see [2]), families of surfaces with special conditions (see [1]), any surfaces (see [6]). There are also a few papers, such as [12] and [9], that work out explicit bounds for the parameters of algebro-geometric codes constructed from other higher dimensional varieties.

We will then observe that Theorem 1.1(i) applies to provide lower bounds for their defects. We will assume that $q \geq 4$, $n \geq k \geq 2$ and $d^{\perp} > 1$ in all these examples, so that we are able to invoke Theorem 1.1(i). Observe that the inequality $q(s+1) \geq d$ implies $s \geq \lceil d/q \rceil - 1$.

Example 5.1 **The Grassmann code** (See, for example, [12, Theorem 7.22].) Here, we consider the Grassmannian of ℓ planes in m-space over the finite field $\mathbb{F}_q$. For $a \in \mathbb{Z}_+$, let

$$[a]_q := \frac{q^a - 1}{q - 1}.$$

Then it is well-known that the parameters of the resulting code are given by

- $n = \begin{bmatrix} m \\ l \end{bmatrix}_q := \frac{[m]_q [m-1]_q \cdots [m-l+1]_q}{[1]_q [2]_q \cdots [l]_q}$,
- $k = \binom{m}{\ell}$,
- $d = q^{\ell(m-\ell)}$.

Now we make use of the inequality $q(s+1) \geq d = q^{\ell(m-\ell)}$ to obtain

$$s \geq q^{\ell(m-\ell)-1} - 1.$$

Example 5.2 **The higher Grassmann code** (See [5]).) Once again, we start with $Gr(\ell, m)$, the Grassmannian of ℓ-planes in $\mathbb{A}^m$, defined over $\mathbb{F}_q$. However, we will consider higher embeddings instead of the usual Plücker embedding, so that we consider the degree ν code $C_{Gr(\ell,m)}(\nu)$, where $\nu - 1 = r(q-1) + \tau$, $0 \leq \tau \leq q-1$. Then clearly n is the same as in the last example. It is shown that d is bounded below by $(q-\tau)q^{\ell(m-\ell)-r-1}$ (Theorem 6.2, *op. cit.*). Therefore, again making use of the inequality $q(s+1) \geq d$, we obtain:

$$s \geq (q-\tau)q^{\ell(m-\ell)-r-2} - 1.$$

One may observe that the projective Reed-Muller codes are special cases of the Higher Grassmann codes, obtained by taking $\ell = 1$.

Example 5.3 **Codes from del Pezzo surfaces** (See [12, Theorem 7.24].) A *del Pezzo surface* X is a projective surface of degree m in $\mathbb{P}^m$ on which the anti-canonical line bundle K_{X}^{-1} is ample. It is shown in [12, Theorem 7.24] that associated to one of the integers $\ell = 0, 1, \ldots, 6$, one can construct an associated del Pezzo surface, denoted X_ℓ, over $\mathbb{F}_q$, with $q > 4$. The resulting code $C(\mathrm{X}_\ell)$ has parameters $n = q^2 + q + 1 + \ell q$, $k = 10 - \ell$ and d given such that there is a positive constant α so that $d \geq \alpha q^2$. Therefore, again making use of the inequality $q(s+1) \geq d$, we obtain:

$$s \geq \alpha q - 1.$$

Example 5.4 **Codes from Quadric hypersurfaces in projective space** (See [12, 7.4.1].) These are the zero sets of degree 2 homogeneous polynomials in $\mathbb{F}_q[x_0, \cdots, x_m]$. Given such a hypersurface X, the number of rational points on it is well-known:

$$|\mathrm{X}(\mathbb{F}_q)| = q^{m-1} + \cdots + q + 1 + (w-1)q^{(m-1)/2},$$

where w is an integer called the character of X. For codes constructed on such varieties, one may take $n = |\mathrm{X}(\mathbb{F}_q)|$. It is known that $k = m + 1$ and that

$$d = \begin{cases} q^{m-1} & \text{if } w = 2 \\ q^{m-1} - q^{(m-2)/2} & \text{if } w = 1 \\ q^{m-1} - q^{(m-1)/2} & \text{if } w = 0. \end{cases}$$

Once again using the bound $q(s+1) \geq d$, we see that

$$s \geq \begin{cases} q^{m-2} - 1 & \text{if } w = 2 \\ q^{m-2} - q^{\frac{(m-2)}{2}-1} - 1 & \text{if } w = 1 \\ q^{m-2} - q^{\frac{(m-1)}{2}-1} - 1 & \text{if } w = 0. \end{cases}$$

Example 5.5 **Codes from Surfaces obtained by restriction of scalars from elliptic and hyperelliptic curves** (See [17, §4 and §5].) One may start with the prime field $\mathbb{F}_7$ and consider the finite Galois extension $\mathbb{F}_{7^2}$. Then starting with an elliptic or hyperelliptic curve over $\mathbb{F}_{7^2}$ one considers the surface over $\mathbb{F}_7$ obtained by the restriction of scalars from Spec $\mathbb{F}_{7^2}$ to Spec $\mathbb{F}_7$. A table of parameters of various codes constructed on the resulting surfaces are discussed in [17, section 5]. In each case, one may obtain a lower bound for the defect s, making use of the inequality $q(s+1) \geq d$. As an example, one finds a code with parameters $[50, 11, 27]$, for which $s \geq \lceil 27/7 \rceil - 1 \geq 3$. (The actual defect in this case is $50-11-27+1 = 13$.) The reader may work out lower bounds for s in a similar manner for the remaining examples of codes considered there and conclude that it is at least 1 in all cases (i.e., these are all $A^s MDS$-codes for $s \geq 1$), while the actual defect in all these examples may be even a bit higher.

Example 5.6 **Bounds on surface codes with special conditions** (See [1].) Let X denote an algebraic surface defined over $\mathbb{F}_q$. Let S be a set of rational points on X, H be a rational effective ample divisor on X avoiding S, and let r a positive integer. Then a lower bound for the minimum distance of the corresponding algebraic geometry code $d(\mathrm{X}, r\mathrm{H}, \mathrm{S})$ is given under various conditions on the canonical divisor $\mathrm{K_X}$. For example, if $\mathrm{K_X}$ is nef, then it is found that

$$d(\mathrm{X}, r\mathrm{H}, \mathrm{S}) \geq |\mathrm{S}| - r\mathrm{H}^2(q + 1 + m) - m(\pi_{r\mathrm{H}} - 1),$$

where H^2 denotes the self-intersection number of H, $\pi_{r\mathrm{H}}$ is the virtual arithmetic genus of $r\mathrm{H}$, and $m = \lfloor 2q^{1/2} \rfloor$. Making use of the inequality $q(s + 1) \geq d(\mathrm{X}, r\mathrm{H}, \mathrm{S})$, one obtains

$$s \geq d(\mathrm{X}, r\mathrm{H}, \mathrm{S})/q - 1 \geq |\mathrm{S}|/q - r\mathrm{H}^2(1 + (1 + m)/q) - m/q(\pi_{r\mathrm{H}} - 1) - 1.$$

When $|\mathrm{S}|$ is of order q^m, one can see from these inequalities that $|\mathrm{S}|/q$ is of order q^{m-1}.

Acknowledgements The authors would like to thank both the reviewers for providing valuable comments that were very helpful to the authors in revising the manuscript.

Funding This study was funded by Simons Foundation (Grant No. 830817).

References

1. Aubr Y., Berardini E., Herbaut F., Perret M.: Bounds on the minimum distance of Algebraic Geometry codes defined over some families of surfaces, in Arithmetic, geometry, cryptography and coding theory, 11–28. Contemp. Math. **770**, American Math. Society (2021).
2. Aubry Y., Berardini E., Herbaut F., Perret M.: Algebraic geometry codes over Abelian surfaces containing no absolutely irreducible curves of low genus. Finite Fields Appl. **70**, 101791, 20 (2021).
3. Blache R., Couvreur A., Hallouin E., Madore D., Nardi J., Rambaud M., Randriam H.: Anti-canonical codes from del Pezzo surfaces with Picard rank one. Trans. Am. Math. Soc. **373**(8), 5371–5393 (2020).
4. Couvreur A.: Construction of rational surfaces yielding good codes. Finite Fields Appl. **17**(5), 424–441 (2011).
5. Can M.B., Joshua R., Ravindra G.V.: Higher Grassmann Codes II. Finite Fields Appl. **89**, 1–21 (2023).
6. Couvreur A., Lebacque P., Perret M.: Toward good families of codes from towers of surfaces, in Arithmetic, geometry, cryptography and coding theory. Contemp. Math. **770**, 59–93 (2021).
7. Faldum A., Willems W.: Codes of small defect. Des. Codes Cryptogr. **10**, 341–350 (1997).
8. Hansen J.P.: Toric varieties, Hirzebruch surfaces and error-correcting codes, applicable algebra in engineering. Commun. Comput. **13**, 289–300 (2002).
9. Hansen S.H.: Error-correcting codes from higher-dimensional varieties. Finite Fields Appl. **7**(4), 531–552 (2001).
10. Huffman W.C., Pless V.: Fundamentals of Error Correcting Codes. Cambridge University Press, Cambridge (2003).
11. Lidl R., Niederreiter H.: Finite Fields, vol. 20, 2nd edn Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge (1997).
12. Little J.: Algebraic Geometry codes from Higher dimensional varieties. In: Advances in Algebraic Geometry Codes, pp. 258–293. World Scientific, Singapore (2008).
13. Little J., Schenck H.: Codes from surfaces with small Picard number. SIAM J. Appl. Algebra Geom. **2**(2), 242–258 (2018).
14. MacWilliams F.J., Sloane N.J.A.: The Theory of Error-Correcting Codes, vol. 16. North Holland, North Holland Mathematical Library (1977).
15. Soprunov I., Soprunova J.: Bringing Toric codes to the next dimension. SIAM J. Discrete Math. **24**(2), 655–665 (2010).
16. van Lint J.H.: Coding Theory, vol. 201. Lecture Notes in Mathematics. Springer, New York (1982).
17. Zarzar M.: Error correcting codes on low rank surfaces. Finite Fields Appl. **13**, 727–737 (2007).