Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Pure and Applied Algebra 196 (2005) 91–99

JOURNAL OF PURE AND APPLIED ALGEBRA

www.elsevier.com/locate/jpaa

Cayley–Bacharach and evaluation codes on complete intersections

Leah Gold[a,*], John Little[b], Hal Schenck[a]

[a] *Mathematics Department, Texas A&M University, College Station, TX 77843-3368, USA*
[b] *Department of Mathematics and Computer Science, College of the Holy Cross, Worcester, MA 01610, USA*

Received 15 January 2004; received in revised form 2 June 2004
Communicated by J. Walker
Available online 27 September 2004

Abstract

Hansen (Appl. Algebra Eng. Comm. Comput. 14 (2003) 175) uses cohomological methods to find a lower bound for the minimum distance of an evaluation code determined by a reduced complete intersection in $\mathbb{P}^2$. In this paper, we generalize Hansen's results from $\mathbb{P}^2$ to $\mathbb{P}^m$; we also show that the hypotheses of Hansen (2003) may be weakened. The proof is succinct and follows by combining the Cayley–Bacharach Theorem and the bounds on evaluation codes obtained in Hansen (Zero-Dimensional Schemes (Ravello, 1992), de Gruyter, Berlin, 1994, pp. 205–211).

MSC: Primary: 14G50; secondary: 94B27

1. Introduction

In [3], Duursma, Rentería, and Tapia-Recillas compute the block length and dimension of the Reed–Muller (or evaluation) code determined by a zero-dimensional complete intersection $\Gamma \subset \mathbb{P}^m$. The words of the code $C(\Gamma)_a$ are obtained by evaluating homogeneous polynomials of degree a at the points of Γ. When Γ is determined by two polynomials of degrees d_1, d_2 in $R = \mathbb{K}[x, y, z]$, Hansen [8] obtains a lower bound for the minimum

* Corresponding author.
E-mail addresses: lgold@math.tamu.edu (L. Gold), little@mathcs.holycross.edu (J. Little), schenck@math.tamu.edu (H. Schenck).

0022-4049/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.jpaa.2004.08.015

distance of the code. In particular, if $d_i \geqslant 3$ and

$$\max\{d_1 - 2, d_2 - 2\} \leqslant a \leqslant d_1 + d_2 - 3,$$

then the code $C(\Gamma)_a$ has minimum distance $d \geqslant d_1 + d_2 - a - 1$. The key point is the observation that when one evaluates polynomials of degree a with $a \leqslant d_1 + d_2 - 3$, then the resulting evaluation vectors will be linearly dependent. In algebraic–geometric terms, this reflects the fact that the points of Γ fail to impose independent conditions on polynomials of degree a. It turns out that this failure gives one some room to correct transmission errors.

The main theme of this paper is that using the modern Cayley–Bacharach Theorem due to Davis, Geramita, and Orecchia [2] streamlines the proof in [8] substantially, and makes it easy to generalize the results from $\mathbb{P}^2$ to $\mathbb{P}^m$. In the $m = 2$ case, the Cayley–Bacharach Theorem also allows us to drop the hypotheses $\max\{d_1 - 2, d_2 - 2\} \leqslant a$ and $d_i \geqslant 3$ of [8], so, in particular, our result applies to Reed–Solomon codes. We start off with a quick review of evaluation codes, and a discussion of residual schemes and the Cayley–Bacharach Theorem.

1.1. Background on evaluation codes

Let V be a variety in $\mathbb{P}^m$ defined over the finite field $\mathbb{F}_q$, with $\Gamma = \{p_1, \ldots, p_n\}$ a set of $\mathbb{F}_q$-rational points on V. Let $R = \mathbb{F}_q[x_0, \ldots, x_m]$, and let R_a denote the vector space of homogeneous polynomials of degree a. Choose a degree a and $f_0 \in R_a$ such that $f_0(p_i) \neq 0$ for all $i \in \{1, \ldots, n\}$. The evaluation map $e_a(\Gamma)$ is defined to be the linear map

$$\begin{aligned} e_a(\Gamma) : R_a &\to \mathbb{F}_q^n \\ f &\mapsto \left(\frac{f(p_1)}{f_0(p_1)}, \ldots, \frac{f(p_n)}{f_0(p_n)}\right). \end{aligned}$$

The image of $e_a(\Gamma)$ is a linear code of block length n, which we will denote as $C(\Gamma)_a$. The codes $C(\Gamma)_a$ are called *evaluation codes* associated to Γ. The minimum distance of $C(\Gamma)_a$ is

$$d = d(C(\Gamma)_a) = \min_{w_1 \neq w_2 \in C(\Gamma)_a} |w_1 - w_2|,$$

where $|\cdot|$ denotes the norm corresponding to the *Hamming distance*, that is, the number of nonzero entries in a word. Since $C(\Gamma)_a$ is closed under sums, the minimum distance is also equal to the minimum over all the nonzero codewords of the number of nonzero entries, or equivalently the length of the words minus the largest number of zero entries in any nonzero codeword.

The Singleton bound implies that the minimum distance d, the block length n, and the dimension k of a linear code satisfy $d \leqslant n - k + 1$. Codes for which the upper bound are achieved are known as maximum distance separable, or MDS, codes.

1.2. Background on the Cayley–Bacharach Theorem

Let $\mathbb{K}$ be a field and suppose $\Gamma = \{p_1, \ldots, p_n\}$ is a set of distinct points in $\mathbb{P}^m_{\mathbb{K}}$. As above, let e_a be the evaluation map from the vector space R_a of homogeneous polynomials of

degree a to $\mathbb{K}^n$. The kernel of this map consists of polynomials of degree a which vanish on Γ, so the kernel is simply the degree a piece of the ideal I_Γ. Hence, we have an exact sequence of vector spaces

$$0 \longrightarrow (I_\Gamma)_a \longrightarrow R_a \xrightarrow{e_a} \mathbb{K}^n \longrightarrow \operatorname{coker}(e_a) \longrightarrow 0.$$

Using sheaf cohomology and writing $\mathscr{I}_\Gamma$ for the sheaf of ideals corresponding to I_Γ, we can identify $\operatorname{coker}(e_a) \cong H^1(\mathscr{I}_\Gamma(a))$. Similarly, the kernel of e_a can be identified with $H^0(\mathscr{I}_\Gamma(a))$. We will write $h^0(\mathscr{I}_\Gamma(a))$ to denote the dimension of the kernel of e_a as a vector space over $\mathbb{K}$. In similar fashion, the dimension of the vector space $H^1(\mathscr{I}_\Gamma(a))$ will be denoted by $h^1(\mathscr{I}_\Gamma(a))$. The set of points Γ is said to *impose independent conditions* on polynomials of degree a if the rank of e_a is n, that is, if $\dim \operatorname{coker}(e_a) = h^1(\mathscr{I}_\Gamma(a)) = 0$.

The classical Cayley–Bacharach Theorem deals with the following situation. Suppose that $Y_1, Y_2 \subset \mathbb{P}^2$ are plane curves of degree d_1 and d_2 which intersect in a set Γ of $d_1 d_2$ distinct points. Write $\Gamma = \Gamma' \cup \Gamma''$ with Γ' and Γ'' disjoint. If $a \leqslant d_1 + d_2 - 3$ is a nonnegative integer, then the classical Cayley–Bacharach Theorem asserts that the dimension of the vector space $(I_{\Gamma'})_a/(I_\Gamma)_a$ is equal to $h^1(\mathscr{I}_{\Gamma''}(d_1 + d_2 - 3 - a))$, a measure of the failure of Γ'' to impose independent conditions in degree $d_1 + d_2 - 3 - a$. For instance, if $d_1 = d_2 = 3$, $a = 3$, and $\Gamma = \Gamma' \cup \Gamma''$, with $\deg(\Gamma') = 8$ and $\deg(\Gamma'') = 1$, then the classical Cayley–Bacharach Theorem says that $\dim(I_{\Gamma'})_a/(I_\Gamma)_a = h^1(\mathscr{I}_{\Gamma''}(0))$. Since $h^1(\mathscr{I}_{\Gamma''}(0)) = 0$, every cubic that vanishes at the 8 points in Γ' also vanishes at the point in Γ''.

To formulate the modern version of the Cayley–Bacharach Theorem, we need to use the language of schemes. For background on schemes we refer the reader to [5], and for a thorough discussion of the Cayley–Bacharach Theorem we recommend [4].

Definition 1.1 (*Residual schemes [4]*). Let Γ be a zero-dimensional scheme with coordinate ring $A(\Gamma)$. Let $\Gamma' \subset \Gamma$ be a closed subscheme and $I_{\Gamma'} \subset A(\Gamma)$ be its ideal. The subscheme of Γ *residual* to Γ' is the subscheme defined by the ideal

$$I_{\Gamma''} = Ann(I_{\Gamma'}/I_\Gamma).$$

When Γ is a complete intersection, Γ' is residual to Γ'' in Γ iff Γ'' is residual to Γ' in Γ (this need not be the case in general). We are now ready to state the version of the Cayley–Bacharach Theorem that we will use to extend the minimum distance bound.

Theorem 1.2 (*Davis–Geramita–Orecchia [2]*). *Let $\Gamma \subset \mathbb{P}^m$ be a complete intersection of hypersurfaces $X_1, X_2, \ldots, X_m$ of degrees $d_1, d_2, \ldots, d_m$ respectively, and let $\Gamma', \Gamma'' \subset \Gamma$ be closed subschemes residual to one another. Set*

$$s = \left(\sum_{i=1}^{m} d_i\right) - m - 1.$$

Then, for any $a \geqslant 0$, we have

$$h^0(\mathscr{I}_{\Gamma'}(a)) - h^0(\mathscr{I}_\Gamma(a)) = h^1(\mathscr{I}_{\Gamma''}(s - a)).$$

In [2], this theorem is proved with the assumption that the ground field is infinite. When Γ is composed of $\mathbb{F}_q$-rational points, the statement holds by interpreting the dimensions over $\overline{\mathbb{F}_q}$. If we use the monomial basis for R_a, then it is easy to see that the matrix of the evaluation map e_a: $R_a \to \overline{\mathbb{F}_q}^n$ has entries in $\mathbb{F}_q$, so the dimensions of the kernel and cokernel will be the same whether we work over the infinite field $\overline{\mathbb{F}_q}$ or the finite field $\mathbb{F}_q$.

2. Review of $\mathbb{P}^2$ result

Let $\Gamma \subset \mathbb{P}^2$ be a reduced complete intersection of two curves of degrees d_1, d_2 defined over $\mathbb{F}_q$. Theorem 4.4 of [8] tells us that if $d_i \geqslant 3$ and $\max\{d_i - 2\} \leqslant a \leqslant d_1 + d_2 - 3$, then the evaluation code $C(\Gamma)_a$ has minimum distance $d \geqslant d_1 + d_2 - a - 1$. The proof in [8] uses Serre duality to compute the dimension of a certain cohomology group, which is why the hypothesis $a \geqslant \max\{d_i - 2\}$ is needed; also useful is the following lemma (2.6 of [8]):

Lemma 2.1. *Let Γ be a finite set of points in $\mathbb{P}^m$, with $|\Gamma| = deg\ \Gamma$. Then for $j \geqslant |\Gamma| - 1$, $h^1(\mathcal{I}_\Gamma(j)) = 0$.*

What Hansen actually shows in the proof of Theorem 4.4 in [8] is that if $\Gamma \subseteq \mathbb{P}^2$ is a (d_1,d_2) complete intersection, and $\Gamma' \subset \Gamma$ satisfies

$$|\Gamma'| \geqslant d_1d_2 - d_1 - d_2 + a + 4,$$

then the projection map $\pi : C(\Gamma)_a \to C(\Gamma')_a$, obtained by deleting the components of the codewords of $C(\Gamma)_a$ corresponding to the points in Γ'', is injective. We warm up by using the Cayley–Bacharach Theorem to give a slight improvement.

Lemma 2.2. *If $\Gamma' \subset \Gamma$ satisfies*

$$|\Gamma'| \geqslant d_1d_2 - d_1 - d_2 + a + 2,$$

then the projection map $\pi : C(\Gamma)_a \to C(\Gamma')_a$, obtained by deleting the components of the codewords of $C(\Gamma)_a$ corresponding to the points in Γ'', is injective.

Proof. Since Γ is reduced, $|\Gamma| = d_1d_2$. Let $s = d_1 + d_2 - 3$ and let Γ' be any subset of the points of Γ such that $|\Gamma'| \geqslant d_1d_2 - s + a - 1$. Then letting $\Gamma'' = \Gamma \backslash \Gamma'$ be the subscheme residual to Γ', we have

$$|\Gamma''| \leqslant d_1d_2 - (d_1d_2 - s + a - 1) = s - a + 1.$$

Since $s - a \geqslant |\Gamma''| - 1$, Lemma 2.1 tells us that Γ'' imposes independent conditions in degree $s - a$, so $h^1(\mathcal{I}_{\Gamma''}(s - a)) = 0$. On the other hand, Γ' and Γ'' are closed subschemes of Γ residual to one another, so by Theorem 1.2 we know that for any $a \geqslant 0$,

$$h^0(\mathcal{I}_{\Gamma'}(a)) - h^0(\mathcal{I}_\Gamma(a)) = h^1(\mathcal{I}_{\Gamma''}(s - a)).$$

The right-hand side is zero, so $h^0(\mathcal{I}_{\Gamma'}(a)) = h^0(\mathcal{I}_\Gamma(a))$. In other words, $H^0(\mathcal{I}_{\Gamma'}(a)) \simeq H^0(\mathcal{I}_\Gamma(a))$, that is, $(I_{\Gamma'})_a = (I_\Gamma)_a$. Hence the projection map $C(\Gamma)_a \xrightarrow{\pi} C(\Gamma')_a$ is injective.

Moreover, the map is injective for *all ways* of splitting Γ as a union of Γ' and Γ'' with the same cardinality as above. □

We claim that the result $d \geqslant s-a+2$ on the minimum distance now follows. To see this, consider the case $|\Gamma'| = d_1d_2 - s + a - 1$ and $|\Gamma''| = s - a + 1$. Let $0 \neq f \in R_a$. If f is nonzero at $s - a + 2$ or more points in Γ', then we are done, so we assume that f is only nonzero at t points in Γ' with

$$1 \leqslant t \leqslant s - a + 1.$$

It suffices to see that f must be nonzero at $\geqslant s - a + 2 - t$ points in Γ''. If not, then f is nonzero at $\leqslant s - a + 1 - t$ points in Γ'', so f vanishes at $\geqslant |\Gamma''| - (s - a + 1 - t) = t$ points of Γ''. Then we can subdivide Γ into two new 0-cycles $\overline{\Gamma}'$ and $\overline{\Gamma}''$ by exchanging t points from Γ'' where f vanishes with t points from Γ' where f is nonzero. We obtain a new decomposition $\Gamma = \overline{\Gamma}' \cup \overline{\Gamma}''$ such that f vanishes at all the points in $\overline{\Gamma}'$. From the previous proof, we know that $C(\Gamma)_a \xrightarrow{\pi} C(\overline{\Gamma}')_a$is injective, so f must vanish on all of Γ. It follows that $d \geqslant s - a + 2$. If $|\Gamma'| > d_1d_2 - s + a - 1$, then we can apply the same argument to any subset of Γ' of size $d_1d_2 - s + a - 1$ to obtain the bound.

3. Main theorem

We are now ready to prove the main result of this paper: Hansen's bound generalizes to reduced complete intersections in $\mathbb{P}^m$. This can be proved along the lines just sketched for the $\mathbb{P}^2$ case. However, the proof is shorter if we utilize the criteria of [7] (Proposition 6 and Theorem 8). In the language of this paper, the result is:

Proposition 3.1. *Let Γ be a subset of points in $\mathbb{P}^m$, and let $C(\Gamma)_a$ be the evaluation code defined in Section* 1. *For $i \geqslant 1$, $d(C(\Gamma)_a) \geqslant deg(\Gamma) - i + 1$ iff $h^0(\mathscr{I}_\Gamma(a)) = h^0(\mathscr{I}_{\Gamma'}(a))$ for all $\Gamma' \subset \Gamma$ with $|\Gamma'| = i$. Furthermore, $C(\Gamma)_a$ is an MDS code iff $h^0(\mathscr{I}_\Gamma(a)) = h^0(\mathscr{I}_{\Gamma'}(a))$ for all $\Gamma' \subset \Gamma$ such that $|\Gamma'| = |\Gamma| - h^1(\mathscr{I}_\Gamma(a))$.*

Combining the Cayley–Bacharach Theorem, Proposition 3.1 and Lemma 2.1 yields our main result:

Theorem 3.2. *Let $\Gamma \subset \mathbb{P}^m$ be a reduced complete intersection of hypersurfaces of degrees $d_1, d_2, \ldots, d_m$, and let $s = (\sum_{i=1}^m d_i) - m - 1$ as in Theorem* 1.2. *If $1 \leqslant a \leqslant s$, then the evaluation code $C(\Gamma)_a$ has minimum distance $d \geqslant (\sum_{i=1}^m d_i) - a - (m-1) = s - a + 2$.*

Proof. Put $\deg(\Gamma) - i + 1 = s - a + 2$, so that $i = \deg(\Gamma) - (s - a + 1)$. Applying Proposition 3.1, we see that the theorem is true iff $h^0(\mathscr{I}_{\Gamma'}(a)) - h^0(\mathscr{I}_\Gamma(a)) = 0$ for all subsets Γ' with $\deg(\Gamma') = \deg(\Gamma) - (s - a + 1)$. The modern Cayley–Bacharach Theorem tells us that

$$h^0(\mathscr{I}_{\Gamma'}(a)) - h^0(\mathscr{I}_\Gamma(a)) = h^1(\mathscr{I}_{\Gamma''}(s - a)).$$

But for any subset $\Gamma'' \subset \Gamma$ of $s + 1 - a$ points, Lemma 2.1 implies that $h^1(\mathscr{I}_{\Gamma''}(s - a)) = 0$. □

Corollary 3.3. *An evaluation code $C(\Gamma)_a$ obtained from a reduced complete intersection Γ is MDS iff*

$$h^1(\mathscr{I}_{\Gamma''}(s-a)) = 0 \text{ for all } \Gamma'' \text{ such that } |\Gamma''| = h^1(\mathscr{I}_\Gamma(a)).$$

Proof. By Proposition 3.1, $C(\Gamma)_a$ is an MDS code iff $h^0(\mathscr{I}_\Gamma(a)) = h^0(\mathscr{I}_{\Gamma'}(a))$ for all $\Gamma' \subset \Gamma$ such that $|\Gamma'| = |\Gamma| - h^1(\mathscr{I}_\Gamma(a))$. By the Cayley–Bacharach Theorem, $h^0(\mathscr{I}_\Gamma(a)) = h^0(\mathscr{I}_{\Gamma'}(a))$ for all subsets Γ' of cardinality i iff $h^1(\mathscr{I}_{\Gamma-\Gamma'}(s-a)) = 0$ for all subsets Γ' of cardinality i. Hence, $C(\Gamma)_a$ is MDS iff $h^1(\mathscr{I}_{\Gamma''}(s-a)) = 0$ for all subsets Γ'' with $|\Gamma''| = |\Gamma| - (|\Gamma| - h^1(\mathscr{I}_\Gamma(a)))$. □

Write σ_Γ for the largest i such that $h^1(\mathscr{I}_\Gamma(i)) \neq 0$. A zero-dimensional scheme Γ' such that $h^0(\mathscr{I}_\Gamma(\sigma_\Gamma)) = h^0(\mathscr{I}_{\Gamma'}(\sigma_\Gamma))$ for all $\Gamma' \subset \Gamma$, $|\Gamma'| = |\Gamma| - 1$ is called a *Cayley–Bacharach* scheme. In [7], Hansen showed that if Γ is a Cayley–Bacharach scheme, then $C(\Gamma)_{\sigma_\Gamma}$ is an MDS code. Of course, a complete intersection is a Cayley–Bacharach scheme, with $s = \sigma_\Gamma$, so the complete intersection codes $C(\Gamma)_s$ are MDS. Are there other complete intersection codes which are MDS? We know that $h^1(\mathscr{I}_{\Gamma''}(s-a)) = 0$ if $s - a \geqslant |\Gamma''| - 1$; so we see that a sufficient condition for the MDS property is

$$s - a \geqslant h^1(\mathscr{I}_\Gamma(a)) - 1.$$

Lemma 3.4. *If Γ is a complete intersection, then*

$$h^1(\mathscr{I}_\Gamma(a)) = |\Gamma| - h^1(\mathscr{I}_\Gamma(s-a)).$$

Proof. From the four term exact sequence of Section 1.2, it follows that $h^1(\mathscr{I}_\Gamma(a)) = |\Gamma| - \dim_{\mathbb{K}}(R/I_\Gamma)_a$. Thus, it suffices to show

$$\dim_{\mathbb{K}}(R/I_\Gamma)_a + \dim_{\mathbb{K}}(R/I_\Gamma)_{s-a} = |\Gamma|.$$

Let $L \in R_1$ be a nonzero divisor on R/I_Γ (such an L exists since R/I_Γ is Cohen-Macaulay). We pass to the Artinian reduction $R/(I_\Gamma + \langle L\rangle)$. It is easy to see that

$$\sum_{i=0}^{s+1} \dim_{\mathbb{K}}(R/(I_\Gamma + \langle L\rangle))_i = |\Gamma|.$$

Since L is not a zero divisor, there is an exact sequence

$$0 \longrightarrow (R/I_\Gamma)(-1) \xrightarrow{\cdot L} R/I_\Gamma \longrightarrow R/(I_\Gamma + \langle L\rangle) \longrightarrow 0.$$

From the exact sequence, it follows that

$$\dim_{\mathbb{K}}(R/I_\Gamma)_a = \sum_{i=0}^{a} \dim_{\mathbb{K}}(R/(I_\Gamma + \langle L\rangle)_i).$$

Similarly, we have

$$\dim_{\mathbb{K}}(R/I_\Gamma)_{s-a} = \sum_{i=0}^{s-a} \dim_{\mathbb{K}}(R/(I_\Gamma + \langle L\rangle)_i).$$

Now, since Γ is a complete intersection, the Hilbert function of the Artinian reduction is symmetric. So

$$\sum_{i=0}^{s-a} \dim_{\mathbb{K}}(R/(I_\Gamma + \langle L\rangle)_i) = \sum_{i=a+1}^{s+1} \dim_{\mathbb{K}}(R/(I_\Gamma + \langle L\rangle)_i),$$

yielding the result. □

Thus, a sufficient condition for the MDS property is that $s - a + 1 \geqslant \deg(\Gamma) - h^1(\mathscr{I}_\Gamma(s-a)) = \dim_{\mathbb{K}}(R/I_\Gamma)_{s-a}$. If Γ is a set of collinear points, then $\dim_{\mathbb{K}}(R/I_\Gamma)_m = \min\{m+1, |\Gamma|\}$, so a set of collinear points always gives an MDS code.

4. Examples

We now give several examples to illustrate our results. First, we quickly review the notation from the previous sections. We consider codes $C(\Gamma)_a$ constructed by evaluating the homogeneous polynomials of degree a at the points of a complete intersection $\Gamma = X_1 \cap \cdots \cap X_m$, where X_i has degree d_i. As in Theorem 3.2, we write $s = (\sum_{i=1}^m d_i) - m - 1$. Then the result of that theorem says that if $1 \leqslant a \leqslant s$, then the minimum distance d of the evaluation code satisfies $d \geqslant s - a + 2$.

Example 4.1. Let x_j, $0 \leqslant j \leqslant m$ be the homogeneous coordinates on $\mathbb{P}^m$, and let $X_1, \ldots, X_{m-1}$ be the hyperplanes $X_j = V(x_j)$ for $1 \leqslant j \leqslant m-1$. Let X_m be the hypersurface $V(x_m^q - x_0^{q-1}x_m)$. Then the intersection of the X_i is a complete intersection Γ, consisting of the set of affine $\mathbb{F}_q$-rational points (i.e. points with $x_0 \neq 0$) on the line $L = X_1 \cap \cdots \cap X_{m-1}$. The evaluation codes in this case are just the usual extended Reed–Solomon codes, and Theorem 3.2 yields the following. We have $s = m - 1 + q - m - 1 = q - 2$. If $a \leqslant s$, then we get that the minimum distance satisfies

$$d \geqslant q - 2 - a + 2 = q - a = n - k + 1,$$

since the block length n is q, and the dimension k is $a + 1$. Thus we have recovered the well-known fact that the extended Reed–Solomon codes are MDS codes.

Example 4.2. Second, consider the usual Reed–Muller evaluation codes as in Example 4.5 of [8], where the case $m = 2$ is studied. The set of all affine $\mathbb{F}_q$-rational points in $\mathbb{A}^m$ is the projective complete intersection

$$\Gamma = V(x_j^q - x_0^{q-1}x_j : j = 1, \ldots, m).$$

Hence we have $s = mq - m - 1 = m(q-1) - 1$. Our Theorem 3.2 implies that for the $C(\Gamma)_a$ code with $a \leqslant s$, the minimum distance is bounded below by

$$d \geqslant s - a + 2 = m(q-1) - a + 1.$$

We note that this example shows the type of bound we are considering here is likely to be of interest in general only when a is relatively large compared to s. For instance, it is

known that if $a=\alpha(q-1)+\beta$, where $0\leqslant\beta\leqslant q-2$, then the exact minimum distance of the Reed–Muller code is $d=(q-\beta)q^{m-1-\alpha}$ (see [1], Corollary 5.5.4, for instance). If $\alpha<m-1$, then our lower bound will be considerably smaller than the actual minimum distance. On the other hand, if, for example, $a=(m-1)(q-1)$, so $\alpha=m-1$ and $\beta=0$, the actual minimum distance is $d=q$, while our bound also gives $d\geqslant m(q-1)+1-(m-1)(q-1)=q$.

Example 4.3. For our final example, we consider codes related to Hermitian codes. The evaluation geometric Goppa codes over $\mathbb{F}_{q^2}$ are defined using the Hermitian curves $X_q=V(x_1^{q+1}-x_2^q x_0-x_2 x_0^q)\subset\mathbb{P}^2$, and the divisors $G=uQ$, where $Q=[0,0,1]$ is the unique point at infinity on X_q. There are precisely q^3 affine $\mathbb{F}_{q^2}$-rational points on X_q. However the Γ consisting of all of them is not a projective complete intersection. To construct codes for which our main results apply, we let

$$F(x_0,x_1,x_2)=\prod_{\{\alpha\in\mathbb{F}_{q^2}:\alpha^q+\alpha\neq 0\}}(x_2-\alpha x_0).$$

Then $\Gamma=X_q\cap V(F)$ consists of the q^3-q $\mathbb{F}_{q^2}$-rational points on X_q with $x_1\neq 0$ (all in the affine part of the plane). In a very precise sense (see [9]), the evaluation codes $C(\Gamma)_a$ are related to the usual Hermitian codes constructed using the divisor D consisting of all $\mathbb{F}_{q^2}$-rational points in the same way that Reed–Solomon codes are related to the extended Reed–Solomon codes.

As in the Reed–Muller case, our bound only gives sharp results when the degree a is large relative to s. Since the equations defining Γ have degrees $d_1=q+1$ and $d_2=q^2-q$, we have $s=q^2-2$. For example, with $a=q^2-q$, our Theorem 3.2 yields $d\geqslant s+2-a=q$. By way of comparison, the usual Hermitian evaluation code constructed using $L(uQ)$ for $u=a(q+1)=q^3-q$ (the maximum pole order at Q of the functions corresponding to the elements of R_a) also has $d=q^3-(q^3-q)=q$ by [10], Proposition VII.4.3. Note that our code has block length $n=q^3-q$ rather than q^3, and the dimension is also one less than the dimension of the corresponding usual Hermitian code because the polynomial F has degree $a=q^2-q$.

There is an extension of the notion of a residual scheme from the case when Γ is a complete intersection to the case when Γ is arithmetically Gorenstein. It seems reasonable to expect that similar methods would yield bounds on the minimum distance in this case; we hope to study this question in a future paper. We note that in [6], Eisenbud and Popescu use the (local) Gorenstein property to give a proof of Goppa duality.

Acknowledgements

This collaboration began while the authors were members of MSRI. We also thank the Institute for Scientific Computation at Texas A&M for providing logistical support. Gold is partially supported by an NSF-VIGRE postdoctoral fellowship. Schenck is partially supported by NSF grant 03-11142, NSA grant 904-03-1-0006 and ATP grant 010366-0103.

References

[1] E.F. Assmus, J.D. Key, Designs and Their Codes, Cambridge University Press, Cambridge, 1992.
[2] E. Davis, A. Geramita, F. Orecchia, Gorenstein algebras and the Cayley–Bacharach Theorem, Proc. Amer. Math. Soc. 93 (1985) 593–597.
[3] I. Duursma, C. Rentería, H. Tapia-Recillas, Reed–Muller codes on complete intersections, Appl. Algebra Eng. Comm. 11 (2001) 455–462.
[4] D. Eisenbud, M. Green, J. Harris, Cayley–Bacharach Theorems and conjectures, Bull. Amer. Math. Soc. (N.S.) 33 (3) (1996) 295–324.
[5] D. Eisenbud, J. Harris, The Geometry of Schemes, Springer, New York, 2000.
[6] D. Eisenbud, S. Popescu, The projective geometry of the Gale transform, J. Algebra 230 (2000) 127–173.
[7] J. Hansen, Points in uniform position and maximum distance separable codes, in: Zero-Dimensional Schemes (Ravello, 1992), de Gruyter, Berlin, 1994, pp. 205–211.
[8] J. Hansen, Linkage and codes on complete intersections, Appl. Algebra Eng. Comm. Comput. 14 (2003) 175–185.
[9] J. Little, K. Saints, C. Heegard, On the structure of Hermitian codes, J. Pure Appl. Algebra 121 (1997) 293–314.
[10] H. Stichtenoth, Algebraic Function Fields and Codes, Springer, Berlin, Heidelberg, New York, 1993.