The shift bound for cyclic, Reed-Muller and geometric Goppa codes

Ruud Pellikaan

Appeared in *Arithmetic, Geometry and Coding Theory 4*
Luminy 1993, (R. Pellikaan, M. Perret and S.G. Vlăduţ eds.)
Walter de Gruyter & Co, Berlin 1996, 155-174
Corrected and updated version, 7 January 2013

Abstract

We give a generalization of the shift bound on the minimum distance for cyclic codes which applies to Reed-Muller and algebraic-geometric codes. The number of errors one can correct by majority coset decoding is up to half the shift bound.

1991 Mathematics Subject Classification: 94B27, 14H45.

1 Introduction

In this paper we survey various bounds on the minimum distance of cyclic and algebraic-geometric codes. For cyclic codes the BCH, Hartmann-Tzeng [12, 27], Roos [22] and the shift bound of van Lint, Wilson and van Eupen [7, 16] for the minimum distance are well known. In Section 2 we give several formulations of independent sets for the definition of the shift bound for cyclic codes. With this last reformulation we obtained, in cooperation with Shen and Tzeng [25], a generalization of the definition of independent sets

and the shift bound for arbitrary linear codes in Section 3. It appears that all these bounds give a method for finding non-singular square submatrices of a matrix of syndromes. The shift bound for Reed-Muller codes is equal to the minimum distance. In Section 4 we treat shift bounds on generalized weights. Error-correcting arrays [15, 20] are treated in Section 5. With this concept the Feng-Rao bound [11, 9] is generalized from geometric Goppa codes to arbitrary linear codes. In this setting one gets in general an improvement of the Goppa bound of algebraic-geometric codes. Although it is in many cases the true minimum distance, this is not always the case. In Section 6 we sketch how majority coset decoding of Feng-Rao [8] and Duursma [3, 4] corrects up to half the shift bound. This procedure is in the worst case not efficient. Therefore we define a restricted shift bound such that the proposed algorithm has polynomial complexity. The shift bound improves all bounds except the Roos bound. The restricted shift bound still improves the FR bound and is equal to the minimum distance of Reed-Muller codes.

A finite field is denoted by $\mathbb{F}$ and the multiplicative group of non-zero elements by $\mathbb{F}^*$. We denote a subfield of $\mathbb{F}$ by $\mathbb{F}_0$. The finite field with q elements is denoted by $\mathbb{F}_q$. We denote the coordinatewise multiplication of $\mathbf{a}$ and $\mathbf{b}$ in $\mathbb{F}^n$ by $\mathbf{a} * \mathbf{b}$, so $a_i b_i$ is the ith coordinate of $\mathbf{a} * \mathbf{b}$. With this multiplication $\mathbb{F}^n$ becomes an $\mathbb{F}$-algebra. We define $< \mathbf{a}, \mathbf{b} >= \sum a_i b_i$. The integers are denoted by $\mathbb{Z}$, the positive integers are denoted by $\mathbb{N}$ and the non-negative integers by $\mathbb{N}_0$. The integers modulo n are denoted by $\mathbb{Z}_n$. The number of elements of a finite set A we denote by $\#A$.

2 Cyclic codes and the shift bound

Fundamental for the definition of the shift bound is the notion of an independent set. In the sequel we give several equivalent definitions of this notion for cyclic codes. In Section 3 we generalize one of these definitions to a broader context which is well suited for Reed-Muller and algebraic-geometric codes.

Definition 2.1. Let $\mathbb{F}$ be a finite field. Let α be an element in $\mathbb{F}^*$ of order n. Let J be a subset of $\mathbb{Z}_n$. Define the $\mathbb{F}$-linear code $\tilde{C}(J)$ by

$$\tilde{C}(J) = \{(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}^n \mid \textstyle\sum_{k=0}^{n-1} c_k \alpha^{jk} = 0 \text{ for all } j \in J\},$$

and the $\mathbb{F}_0$-linear subfield subcode $C(J)$ by $C(J) = \tilde{C}(J) \cap \mathbb{F}_0^n$. The codes

$\tilde{C}(J)$ and $C(J)$ are *cyclic* with *defining set* J. The code $C(J \cup \{j\})$ is contained in $C(J)$ for every $j \in \mathbb{Z}_n$. Let J^* be the set of all $j \in \mathbb{Z}_n$ such that $C(J) = C(J \cup \{j\})$. Hence $J \subseteq J^*$ and $C(J) = C(J^*)$. We call J^* the *complete defining set* of $C(J)$, and we call J complete if $J = J^*$.

We give first the inductive definition of van Lint and Wilson [16] of the notion of an independent set with respect to a defining set.

Definition 2.2. Let $\mathbb{F}$ be a finite field and α a non-zero element of $\mathbb{F}$ of order n. The multiplicative subgroup of the non-zero elements of $\mathbb{F}$ generated by α we denote by $\langle\alpha\rangle$. Let R be a subset of $\langle\alpha\rangle$. A subset A of $\langle\alpha\rangle$ is called *independent* with respect to R if it can be obtained by the following rules:

(I^*.1) the empty set is independent with respect to R.

(I^*.2) if A is independent with respect to R and A is a subset of R and $b \in \langle\alpha\rangle$ is not an element of R, then $A \cup \{b\}$ is independent with respect to R.

(I^*.3) if A is independent with respect to R and $c \in \langle\alpha\rangle$, then cA is independent with respect to R, where $cA = \{ca \mid a \in A\}$.

Remark 2.3. The defining set R is complete if and only if R is invariant under the Frobenius map $\beta \mapsto \beta^{q_0}$, that is to say: if $\beta \in R$, then $\beta^{q_0} \in R$, where q_0 is the number of elements of $\mathbb{F}_0$.

We transform the multiplicative definition into an additive description as follows. Every element of $\langle\alpha\rangle$ is of the form α^i for some $i \in \mathbb{Z}_n$, since α has order n. So we can translate the definition of an independent set with respect to a subset of $\langle\alpha\rangle$ to a subset of $\mathbb{Z}_n$. Let R be a subset of $\mathbb{Z}_n$. A subset A of $\mathbb{Z}_n$ is called *independent* with respect to R if it can be obtained by the following rules:

(I^+.1) the empty set is independent with respect to R.

(I^+.2) if A is independent with respect to R and A is a subset of R and $b \in \mathbb{Z}_n$ is not an element of R, then $A \cup \{b\}$ is independent with respect to R.

(I^+.3) if A is independent with respect to R and $c \in \mathbb{Z}_n$, then $c + A$ is independent with respect to R, where $c + A = \{c + a \mid a \in A\}$.

The name "shifting" is referring to this last condition. A set A is independent with respect to R if and only if there exists a sequence of sets $A_0, A_1, \ldots, A_w$ and integers $a_i, b_i, 0 \leq i < w$ such that A_0 is the empty set and $A = A_w$ and furthermore

$$A_{i+1} = (a_i + A_i) \cup \{b_i\} \quad \text{and}$$

$$a_i + A_i \text{ is a subset of } R \text{ and } b_i \text{ is not an element of } R.$$

Then

$$A_i = \{b_{l-1} + \textstyle\sum_{j=l}^{i-1} a_j \mid l = 1, \ldots, i\},$$

and all A_i are independent with respect to R.

Let $i_1, i_2, \ldots, i_w$ and $j_1, j_2, \ldots, j_w$ be new sequences which are obtained from the sequences $a_0, \ldots, a_w$ and $b_0, \ldots, b_w$ by:

$$i_w = 0,\ i_{w-1} = a_1\ , \ldots,\ i_{w-k} = a_1 + \cdots + a_k \text{ and } j_k = b_{k-1} - i_{w-k+1}.$$

By this transformation it is easy to see that a set A is independent with respect to R if and only if there exist sequences $i_1, i_2, \ldots, i_w$ and $j_1, j_2, \ldots, j_w$ such that $A = \{i_1 + j_l \mid 1 \leq l \leq w\}$ and

$$i_k + j_l \in R \text{ for all } l + k \leq w \quad \text{and} \quad i_k + j_l \notin R \text{ for all } l + k = w + 1.$$

Notice that in this formulation we did not assume that the sets $\{i_k \mid 1 \leq k \leq w\}$, $\{j_l \mid 1 \leq l \leq w\}$ and A have size w, since this is a consequence of this definition. If for instance $i_k = i_{k'}$ for some $1 \leq k < k' \leq w$, then $i_k + i_{w+1-k'} = i_{k'} + i_{w+1-k'} \notin R$, but $i_k + i_{w+1-k'} \in R$, which is a contradiction.

The last formulation and the following definition is from van Eupen and van Lint [7, Definition 1] and is well suited for generalizations as we will see in the next section.

Definition 2.4. For a subset R of $\mathbb{Z}_n$, let $n(R)$ be the maximal size of a set which is independent with respect to R. Define the *shift* bound for a subset J of $\mathbb{Z}_n$ as follows:

$$\delta_{SHIFT}(J) = \min\{n(R) \mid J \subseteq R \subseteq \mathbb{Z}_n \text{ and } R^* = R \neq \mathbb{Z}_n\}.$$

Theorem 2.5 *The minimum distance of $C(J)$ is at least $\delta_{SHIFT}(J)$.*

Proof. See the proof of Theorem 1 in [7] or Theorem 3.7 in the next section. □

Definition 2.6. The *Bose-RayChaudhuri-Hocquenghem* bound [17]. For a subset J of $\mathbb{Z}_n$, let $\delta_{BCH}(J)$ be the largest $\delta \leq n$ such that $i+1, \ldots, i+\delta-1 \in J$ for some i.

Definition 2.7. The *Hartmann-Tzeng* bound [12]. For a subset J of $\mathbb{Z}_n$, let $\delta_{HT}(J)$ be the largest number $\delta + s$, such that there exist i, a and s with the property that $\mathrm{GCD}(a, n) < \delta$ and $\{i + j + ka \mid 1 \leq j < \delta,\ 0 \leq k \leq s\} \subseteq J$.

Proposition 2.8 *The following inequalities hold:*

$$\delta_{SHIFT}(J) \geq \delta_{HT}(J) \geq \delta_{BCH}(J).$$

Proof. The last inequality is obvious. Let J be a subset of $\mathbb{Z}_n$ which contains $\{i + j + ka \mid 1 \leq j < \delta,\ 0 \leq k \leq s\}$. Suppose R is a complete defining set which contains J and is not equal to $\mathbb{Z}_n$. Then there exists a $\delta' \geq \delta$ such that $i + j \in R$ for all $1 \leq j < \delta'$ and $i + \delta' \notin R$. The set $\{i + j + ka \mid 1 \leq j < \delta, k \in \mathbb{Z}_n\}$ is equal to $\mathbb{Z}_n$, since $\mathrm{GCD}(a, n) < \delta$. So there exist $s' \geq s$ and j' such that $i + j + ka \in R$ for all $1 \leq j < \delta$ and $0 \leq k \leq s'$, and $1 \leq j' < \delta$ and $i + j' + (s' + 1)a \notin R$. Let $w = \delta + s'$. Let $i_k = (k-1)a$ for all $1 \leq k \leq s' + 1$, and $i_k = \delta' - \delta - s' - 1 + k$ for all k such that $s' + 2 \leq k \leq \delta + s'$. Let $j_l = i + l$ for all $1 \leq l \leq \delta - 1$, and let $j_l = i + j' + (l - \delta + 1)a$ for all l such that $\delta \leq l \leq \delta + s'$. Then one easily checks that $i_k + j_l \in R$ for all $k + l \leq w$, and $i_k + j_{w-k+1} = i + j' + (s' + 1)a \notin R$ for all $1 \leq k \leq s' + 1$, and $i_k + j_{w-k+1} = i + \delta' \notin R$ for all $s' + 2 \leq k \leq \delta + s'$. So we have a set which is independent with respect to R and has size $w = \delta + s' \geq \delta + s$. Hence $n(R) \geq \delta + s$ for all complete defining sets R which contain J and are not equal to $\mathbb{Z}_n$. Therefore $\delta_{SHIFT}(J) \geq \delta_{HT}(J)$. □

Example 2.9. It is easy to make examples of defining sets J such that $\delta_{BCH}(J) < \delta_{HT}(J)$. In the following example we show that the shift bound is strictly greater than the HT bound and is still not equal to the minimum distance. The binary Golay code of length 23 can be defined as the cyclic code with defining set R_1 which is the cyclotomic coset of 1, that is to say 1, 2, 3,

4, 6, 8, 9, 12, 13, 16, 18 are the elements of R_1, see [16, Example 7], where $\mathbb{F} = \mathbb{F}_{2048}$, $\mathbb{F}_0 = \mathbb{F}_2$ and α an element of $\mathbb{F}$ of order 23. Then $\delta_{BCH}(R) = \delta_{HT}(R) = 5$. Let $(a_0, \ldots, a_5) = (1, -1, -3, 7, 4, 13)$ and $(b_0, \ldots, b_5) = (5, 5, 5, 14, 5, 5)$. Then $A_0 = \emptyset$, $A_1 = \{5\}$, $A_2 = \{4, 5\}$, $A_3 = \{1, 2, 5\}$, $A_4 = \{8, 9, 12, 14\}$, $A_5 = \{12, 13, 16, 18, 5\}$, $A_6 = \{2, 3, 6, 8, 18, 5\}$ are independent sets with respect to R_1. The corresponding sequences (i_k) and (j_l) are $(i_1, \ldots, i_6) = (-3, 7, 3, -4, -1, 0)$ and $(j_1, \ldots, j_6) = (5, 6, 9, 11, -2, 8)$. So R_1 has an independent set of size 6, in fact this is the maximal size of an independent set of R_1, so $n(R_1) = 6$. Let $R_0 = \{0\}$, and $R_5 = \{5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\}$. The sets R_0, R_1, R_5 and their unions have the property that $R = R^*$, that is to say they are complete, and these are the only ones. Let $R_{0,1} = R_0 \cup R_1$, then $R_{0,1}$ has an independent set of size 7, since A_6 is independent with respect to R_1 and also with respect to $R_{0,1}$, and $-2 + A_6 = \{0, 1, 4, 6, 16, 3\}$ is a subset of $R_{0,1}$ and $5 \notin R_{0,1}$, so $A_7 = \{0, 1, 4, 6, 16, 3, 5\}$ is independent with respect to $R_{0,1}$. Furthermore $R_{1,5} = R_1 \cup R_5$ contains a sequence of 22 consecutive elements, so $n(R_{1,5}) = 23$. Therefore $\delta_{SHIFT}(R_1) = 6$. But the minimum distance of the binary Golay code is 7, since otherwise there would be a word $\mathbf{c} \in C(R_1)$ of weight 6, so $\mathbf{c} \in C(R_{0,1})$, but $\delta_{SHIFT}(R_{0,1}) = 7$, which is a contradiction.

Remark 2.10. In many cases of binary codes of length at most 62 the shift bound is equal to the minimum distance, see [16]. In about 95% of all ternary codes of length at most 40 the shift bound is equal to the minimum distance, see [7].

Example 2.11. It is necessary to take the minimum of all $n(R)$ in the definition of the shift bound. It does not suffice to take $n(J^*)$ as the following example shows. Let $\mathbb{F}$ be a finite field of odd characteristic. Let α be a non-zero element of $\mathbb{F}$ of even order $n \geq 6$. Let $J = \{2, 4, \ldots, n-2\}$ and $R = \{0, 2, 4, \ldots, n-2\}$. Then J and R are complete and $n(J) = 3$, since $\{2, 0, 1\}$ is independent with respect to J, but $n(R) = 2$. In particular, take $n = 6$, $q = 7$ and $\alpha = 3$ as generator of the cyclic group $\mathbb{F}_7^*$. Consider the cyclic code of length 6 over $\mathbb{F}_7$ with generator polynomial $g(X) = X^3 - 1 = (X-1)(X-2)(X-4)$. Then C has defining set $\{0, 2, 4\}$, since $\alpha^0 = 1$, $\alpha^2 = 2$ and $\alpha^4 = 4$. The code C has minimum distance 2.

Definition 2.12. Let b and n be positive integers such that $GCD(b, n) = 1$. If $B = \{i_1 b, i_2 b, \ldots, i_t b\}$, where $0 \leq i_1 < \cdots < i_t < n$, then we denote by

$\bar{B}$ the set $\{ib \mid i_1 \leq i \leq i_t\}$. The *Roos* bound [16, 22] of a defining set J, which we denote by $\delta_R(J)$, is the largest number $\#B + d_A - 1$ such that there exist defining sets A and $B = \{i_1 b, i_2 b, \ldots, i_t b\}$, where $0 \leq i_1 < \cdots < i_t < n$, with the property that $A + B \subseteq J$, and $\tilde{C}(A)$ has minimum distance d_A and $\#\bar{B} \leq \#B + d_A - 2$.

Example 2.13. Let $n = 26$, $\mathbb{F} = \mathbb{F}_{27}$, and $\mathbb{F}_0 = \mathbb{F}_3$. Let 0, 13, 14, 16, 17, 22, 23 and 25 be the elements of J, see [7, Example 26.7]. Let $A = \{13, 14\}$ and $B = \{0, 3, 9, 12\}$. Then $d_A = 3$ and $\bar{B} = \{0, 3, 6, 9, 12\}$, so $\#\bar{B} = 5 \leq 4+3-2$. Moreover J contains $A+B$. Hence $\delta_R(J) = 4+3-1 = 6$, but $\delta_{SHIFT}(J) = 5$.

Remark 2.14. It follows directly from the definitions that the Roos bound is a generalization of the HT bound, so $\delta_R \geq \delta_{HT}$. The above example shows that sometimes $\delta_R(J) > \delta_{SHIFT}(J)$. In section 6 we will see a general method to decode up to half the shift bound. A general algorithm which decodes up to half the Roos bound is not known, but it is still possible to decode in many cases up to half the Roos bound with error-correcting pairs, see [4, 6, 19]. It is possible to generalize the Roos bound to general linear codes, see [5, 21].

3 A generalization of the shift bound

One way to get a bound on the weight of a codeword $\mathbf{c} = (c_0, \ldots, c_{n-1})$ is obtained by looking for a maximal non-singular square submatrix of the matrix of syndromes $(S_{i,j})$. For cyclic codes we get in this way a matrix, with entries $S_{i,j} = \sum c_k \alpha^{k(i+j)}$, which is constant along back-diagonals. For Reed-Muller and algebraic-geometric codes this is not the case anymore. So instead of looking at an independent set which is a subset of $\mathbb{Z}_n$ we give a definition of an independent set which is a subset of $\mathbb{N}^2$, and we think of it as a set of indices of entries of a matrix of syndromes.

In a discussion with B.-Z. Shen we came to the following generalization of independent sets and the shift bound, see also Shen and Tzeng [25] and Augot, Charpin and Sendrier [1] on *generalized Newton identities*.

Definition 3.1. Let $N = \mathbb{N}$ or $N = \{1, \ldots, n\}$ for some $n \in \mathbb{N}$. Let R be a subset of N^2. A subset A of N^2 is called *independent* with respect to R if there exist sequences $i_1, i_2, \ldots, i_w$ and $j_1, j_2, \ldots, j_w$ such that $A =$

$\{(i_1, j_l) \mid 1 \leq l \leq w\}$ and

$$(i_k, j_l) \in R \text{ for all } k + l \leq w \quad \text{and} \quad (i_k, j_l) \notin R \text{ for all } k + l = w + 1.$$

Let $\mathbb{F}$ be a finite field and $\mathbb{F}_0$ a subfield of $\mathbb{F}$. Consider $\mathbb{F}^n$ with the multiplication $*$ as an $\mathbb{F}$-algebra. Let K be an $\mathbb{F}$-algebra. Let $\varphi : K \to \mathbb{F}^n$ be a morphism of $\mathbb{F}$-algebras. Let $(f_i \mid i \in N)$ and $(g_j \mid j \in N)$ be two sequences in K such that $\{\varphi(f_i g_j) \mid i, j \in N\}$ generates $\mathbb{F}^n$ as a vector space.

We have now the following generalization of a theorem of van Lint and Wilson [16, Theorem 11].

Lemma 3.2 *Let $\mathbf{y} \in \mathbb{F}_0^n$. Let $R = \{(i, j) \in N^2 \mid \ < \mathbf{y}, \varphi(f_i g_j) >= 0\}$. If A is independent with respect to R, then $wt(\mathbf{y}) \geq \#A$.*

Proof. The *syndrome* of a word $\mathbf{y} \in \mathbb{F}_0^n$ with respect to f_i and g_j is defined by

$$S_{i,j}(\mathbf{y}) =< \mathbf{y}, \varphi(f_i g_j) > .$$

Let $S(\mathbf{y})$ be the matrix with entries $S_{i,j}(\mathbf{y})$. Suppose A is independent with respect to R and has w elements, then there exist sequences $i_1, \ldots, i_w$ and $j_1, \ldots, j_w$ such that $A = \{(i_1, j_1), (i_1, j_2), \ldots, (i_1, j_w)\}$ and $(i_k, j_l) \in R$ for all $k + l \leq w$ and $(i_k, j_l) \notin R$ for all $k + l = w + 1$. Consider the $(w \times w)$ matrix M with entries $M_{k,l} = S_{i_k, j_l}(\mathbf{y})$. By the assumptions we have that M is a matrix such that $M_{k,l} = 0$ for all $k + l \leq w$ and $M_{k,l} \neq 0$ for all $k + l = w + 1$, that is to say with zeros above the back-diagonal and non-zeros on the back-diagonal, so M has rank w. Moreover M is a submatrix of the matrix $S(\mathbf{y})$ which can be written as a product:

$$S(\mathbf{y}) = Y D(\mathbf{y}) X,$$

where Y is the matrix with the $\varphi(f_i)$ as row vectors, $D(\mathbf{y})$ is the diagonal matrix with the entries of $\mathbf{y}$ on the diagonal and zeros outside this diagonal, and X is the matrix with the $\varphi(g_j)^T$ as column vectors. Hence

$$\#A = w = \text{rank}(M) \leq \text{rank}(S(\mathbf{y})) \leq \text{rank}(D(\mathbf{y})) = wt(\mathbf{y}).$$

This proves the lemma. □

Definition 3.3. Let J be a subset of N^2. Define the $\mathbb{F}$-linear code $\tilde{C}(J)$ by

$$\tilde{C}(J) = \{\mathbf{y} \in \mathbb{F}^n \mid \ < \mathbf{y}, \varphi(f_i g_j) >= 0 \ \text{ for all } \ (i, j) \in J\},$$

and the $\mathbb{F}_0$-linear subfield subcode $C(J)$ by $C(J) = \tilde{C}(J) \cap \mathbb{F}_0^n$. The code $C(J \cup \{(i,j)\})$ is contained in $C(J)$ for every $(i,j) \in N^2$. Let J^* be the set of all $(i,j) \in N^2$ such that $C(J) = C(J \cup \{(i,j)\})$. Hence $J \subseteq J^*$ and $C(J) = C(J^*)$. We call J a *defining set* for the code $C(J)$, and J^* the *complete defining set* of this code. We call a defining set J complete if $J = J^*$. For a subset R of N^2, let $n(R)$ be the maximal size of a set which is independent with respect to R. Define the *shift* bound for a subset J of N^2 as follows:

$$\delta_{SHIFT}(J) = \min\{n(R) \mid J \subseteq R \subseteq N^2 \text{ and } R^* = R \neq N^2\}.$$

Remark 3.4. The number of subsets R of N^2 such that $R = R^*$ is finite, since the number of subspaces of the given vector space $\mathbb{F}_0^n$ is finite.

Lemma 3.5 *Let J be a complete defining set. If $\mathbf{y} \in C(J)$ and $\mathbf{y} \notin C(I)$ for all complete defining sets I which contain J and are not equal to J, then $wt(\mathbf{y}) \geq n(J)$.*

Proof. Let $\mathbf{y} \in C(J)$ and $\mathbf{y} \notin C(I)$ for all I such that $J \subseteq I = I^* \neq J$. Define

$$R = \{(i,j) \mid < \mathbf{y}, \varphi(f_i g_j) >= 0\}.$$

We always have that $R \subseteq R^*$ and $C(R) = C(R^*)$. Now $\mathbf{y} \in C(R)$, so $\mathbf{y} \in C(R^*)$. If $(i,j) \in R^*$, then $< \mathbf{y}, \varphi(f_i g_j) >= 0$, so $(i,j) \in R$. Hence R is a complete defining set. Clearly $J \subseteq R$, since $\mathbf{y} \in C(J)$. If $J \neq R$, then $\mathbf{y} \in C(I)$ and $J \subseteq I = I^* \neq J$ for $I = R$, which is a contradiction. Hence $J = R$, and $wt(\mathbf{y}) \geq n(J)$, by Lemma 3.2. This proves the lemma. □

The following theorem generalizes Theorem 1 of van Eupen and van Lint [7].

Theorem 3.6 *The minimum distance of $C(J)$ is at least $\delta_{SHIFT}(J)$.*

Proof. Let $\mathbf{y}$ be a non-zero codeword of $C(J)$. Let R be equal to $\{(i,j) \mid < \mathbf{y}, \varphi(f_i g_j) >= 0\}$. Then $R \neq N^2$, since $\mathbf{y}$ is not zero and $\{\varphi(f_i g_j) \mid i,j \in N\}$ generates $\mathbb{F}^n$. The theorem now follows from Lemma 3.5 and the definition of the shift bound. □

Remark 3.7. The computation of the shift bound is quite involved, and is done by the use of a computer. It makes sense if one classifies codes with

respect to the minimum distance, since in order to get $\delta_{SHIFT}(J)$ one gets at the same time the $\delta_{SHIFT}(R)$ for all $J \subseteq R$.

Example 3.8. *Reed-Solomon* and *cyclic* codes. Let $\mathbb{F}$ be a finite field. Let $K = \mathbb{F}[X]$ be the ring of polynomials in one variable and coefficients in $\mathbb{F}$; this is an $\mathbb{F}$-algebra by the ordinary multiplication of polynomials. Let $\alpha_1, \ldots, \alpha_n$ be n distinct elements of $\mathbb{F}$. Let $\varphi : K \to \mathbb{F}^n$ be the evaluation map which is defined by $\varphi(f) = (f(\alpha_1), \ldots, f(\alpha_n))$ for $f \in K$, then φ is a morphism of $\mathbb{F}$-algebras. Let $f_i = g_i = X^{i-1}$, then $f_i g_j = f_{i+j-1} = X^{i+j-1}$. Then

$$C(J) = \{(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_0^n \mid \sum_{k=0}^{n-1} c_k \alpha_k^{i+j-1} = 0 \text{ for all } (i,j) \in J\},$$

If in particular $\{i + j - 1 \mid (i,j) \in J\} = \{0, 1, \ldots, k-1\}$ and $\mathbb{F} = \mathbb{F}_0$, then $C(J)$ is the dual of a Reed-Solomon code. Let J be a subset of N^2 and let J^+ be the subset of $\mathbb{Z}_n$ defined by $J^+ = \{i + j - 1 + n\mathbb{Z} \mid (i,j) \in J\}$. If $\alpha_i = \alpha^i$, for some non-zero $\alpha \in \mathbb{F}$ of order n, then $C(J)$ is a cyclic code with defining set J^+. For cyclic codes we have defined in Definition 2.1 for a subset J of $\mathbb{Z}_n$,

$$C(J) = \{(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_0^n \mid \sum_{k=0}^{n-1} c_k \alpha^{kj} = 0 \text{ for all } j \in J\},$$

by abuse of notation. This ambiguity is justified, since $C(J) = C(J^+)$ and $(J^*)^+ = (J^+)^*$ and $n(J) = n(J^+)$ and $\delta_{SHIFT}(J) = \delta_{SHIFT}(J^+)$ for all $J \subseteq N^2$.

Example 3.9. *Generalized Reed-Muller* codes. Let $\mathbb{F} = \mathbb{F}_0 = \mathbb{F}_q$. Let K be the ring $\mathbb{F}[X_1, \ldots, X_m]$ of polynomials in m variables with coefficients in $\mathbb{F}$. We abbreviate the notation for the monomial $X_1^{\varepsilon_1} \cdots X_m^{\varepsilon_m}$ by X^ε, where $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_m)$. The degree of a polynomial f is denoted by $\deg(f)$. Define a total order on the monomials by the *total degree lexicographic order*, that is to say $X^\varepsilon < X^\varphi$ if and only if $\deg(X^\varepsilon) < \deg(X^\varphi)$, or $\deg(X^\varepsilon) = \deg(X^\varphi)$ and there exists a k such that $1 \leq k \leq m$ and $\varepsilon_k < \varphi_k$ and $\varepsilon_l = \varphi_l$ for all $1 \leq l < k$. Hence

$$1 < X_m < \cdots < X_1 < X_m^2 < X_m X_{m-1} < X_{m-1}^2 < X_m X_{m-2} < X_{m-1} X_{m-2} < \cdots$$

Let f_i be the ith element in this sequence and let $g_i = f_i$. Let $n = q^m$ and $P_1, \ldots, P_n$ be an enumeration of all elements of $\mathbb{F}_q^m$. Let $\varphi : K \to \mathbb{F}^n$ be

the evaluation map defined by $\varphi(f) = (f(P_1), \ldots, f(P_n))$. The Generalized Reed-Muller code of order r and length q^m is defined by

$$\mathcal{RM}_q(r,m) = \{\varphi(f) \mid f \in K \text{ and } \deg(f) \leq r\}.$$

The dual of $\mathcal{RM}_q(r,m)$ is equal to $\mathcal{RM}_q(m(q-1)-r-1,m)$. Write $r+1 = \rho(q-1)+\mu$ with $\rho, \mu \in \mathbb{N}_0$ such that $\mu < q-1$. Then the minimum distance of the dual of $\mathcal{RM}_q(r,m)$ is equal to $(\mu+1)q^\rho$, see [2, 13, 29] and also [16]. Remark that $\varphi(f) = \varphi(f^q)$. Denote the reduction modulo $q-1$ of a positive integer ε by ε', that is to say $\varepsilon = \varphi(q-1)+\varepsilon'$ where $\varepsilon', \varphi \in \mathbb{N}_0$ and $0 < \varepsilon' < q$. If $\varepsilon = 0$, then $\varepsilon' = 0$. We denote $\sum \varepsilon_i'$ by $\mathrm{rdeg}(X^\varepsilon)$ for a monomial X^ε, and call it the *reduced degree*. We call a monomial X^ε *reduced* if $\varepsilon_i < q$ for all i. Let $R(r,m) = \{(i,j) \mid \mathrm{rdeg}(f_i f_j) \leq r\}$. Then $R(r,m)$ is a complete defining set for the dual of the Reed-Muller code $\mathcal{RM}_q(r,m)$, so $C(R(r,m)) = \mathcal{RM}_q(m(q-1)-r-1,m)$. We will show that the shift bound for $R(r,m)$ also gives $(\mu+1)q^\rho$. Let R be a complete defining set which contains $R(r,m)$ and is not equal to $\mathbb{N}^2$. Then there exists an $s \geq r$ such that $R(s,m) \subseteq R$ and $R(s+1,m)$ is not a subset of R. Let f_j be the smallest monomial of degree $s+1$ such that $(1,j) \notin R$. Hence $(k,l) \in R$ in case $f_k f_l < f_j$. The monomial $f_j = X^\varepsilon$ is reduced. The number of all monomials X^φ such that $0 \leq \varphi_i \leq \varepsilon_i$ for all i is equal to $w = \prod(\varepsilon_i+1)$, and let $f_{i_1}, \ldots, f_{i_w}$ with $i_1 < \cdots < i_w$, be an enumeration of these monomials in increasing order with respect to the total order on the monomials. So $f_{i_1} = 1$ and $f_{i_w} = X^\varepsilon$. If $X^\varphi < X^\psi$ and $0 \leq \varphi_i \leq \varepsilon_i$ and $0 \leq \psi_i \leq \varepsilon_i$ for all i, then $X^{\varepsilon-\psi} < X^{\varepsilon-\varphi}$. Hence the sequence $f_{i_1}, \ldots, f_{i_w}$ is transformed into the sequence $f_{i_w}, \ldots, f_{i_1}$ under the operation $X^\varphi \mapsto X^{\varepsilon-\varphi}$, so $f_{i_k} f_{i_l} = X^\varepsilon$ for all $k+l = w+1$. Furthermore if $k+l \leq w$, then there exists a k' such that $k < k'$ and $k'+l = w+1$, so $f_{i_k} f_{i_l} < f_{i_{k'}} f_{i_l} = X^\varepsilon$. Let $j_l = i_l$. Therefore $(i_k, j_l) \in R$ for all $k+l \leq w$ and $(i_k, j_l) \notin R$ for all $k+l = w+1$. Hence we have a set of size w which is independent with respect to R. Now $w = \prod(\varepsilon_i+1)$ and $\sum \varepsilon_i = s+1 \geq r+1$. Write $s+1 = \sigma(q-1)+\nu$. We leave it as an exercise in the calculus of functions in several variables to show that the function $F(\varepsilon_1, \ldots, \varepsilon_m) = \prod(\varepsilon_i+1)$ on the domain defined by the constraints $0 \leq \varepsilon_i < q$ for all i and $\sum \varepsilon_i = s+1$, has as a minimum $(\nu+1)q^\sigma$, which is at least $(\mu+1)q^\rho$. If in particular $s = r$ and $\varepsilon_i = (q-1)$ for all $1 \leq i \leq \rho$, and $\varepsilon_{\rho+1} = \mu$ and $\varepsilon_i = 0$ for all $i > \rho+1$, then $w = (\mu+1)q^\rho$. Therefore $\delta_{SHIFT}(R(r,m)) = (\mu+1)q^\rho$. Remark that the independent sets we have found have the property that $f_{i_k} f_{j_{w-k+1}}$ is equal to a fixed f_j for all k.

4 Shift bound for generalized weights

In order to compute the shift bound of the code $C(J)$ with defining set J we have to compute the maximum size $n(R)$ of a set A which is independent with respect to R, for all complete defining sets R which contain J. Wei [28] has defined the notion of generalized weights of a linear code which is a generalization of the minimum distance. A simple observation leads to a bound for the r^{th} generalized weight of $C(J)$ without any extra costs.

Definition 4.1. The *support* $\mathrm{supp}(C)$ of a code C is defined by

$$\mathrm{supp}(C) = \{i \mid c_i \neq 0 \ \text{ for some } \ \mathbf{c} \in C\}.$$

The r^{th} *generalized weight* $d_r(C)$ of a linear code C is defined by

$$d_r(C) = \min\{\#\mathrm{supp}(D) \mid \ D \ \text{ is a linear subcode of } \ C \ \text{ and } \ \dim(D) = r \ \}.$$

Lemma 4.2 *If $C_2 \subseteq C_1$ and C_2 has codimension s in C_1, then $d_{r+s}(C_1) \geq d_r(C_2)$.*

Proof. Let D_1 be a linear subcode of C_1 of dimension $r+s$ such that $\#\mathrm{supp}(D_1) = d_{r+s}(C_1)$. The dimension of the intersection of D_1 with C_2, which we denote by D_2, is at least r, since C_2 has codimension s in C_1. So $\#\mathrm{supp}(D_2) \geq d_r(C_2)$. The support of D_2 is contained in the support of D_1. Hence $d_{r+s}(C_1) \geq d_r(C_2)$. This proves the lemma. □

Definition 4.3. Let J and R be defining sets such that $J \subseteq R$. The *height* of R above J is by definition the largest $t \in \mathbb{N}_0$ such that there is a sequence $R_0, \ldots, R_t$ of $t+1$ distinct complete defining sets such that $J^* = R_0$ and $R^* = R_t$ and $R_i \subseteq R_{i+1}$ for all $i < t$. We denote the height of R above J by $h(R, J)$.

Remark 4.4. If $\mathbb{F} = \mathbb{F}_0$, and J and R are defining sets such that $J \subseteq R$, then $C(R)$ has codimension $h(R, J)$ in $C(J)$.

Definition 4.5. Define for an $r \in N$

$$\delta_{r,SHIFT}(J) = \max\{\delta_{SHIFT}(R) \mid J \subseteq R \subseteq N^2 \text{ and } R \neq N^2 \text{ and } h(R, J) = r-1\}.$$

Theorem 4.6 *If* $\mathbb{F} = \mathbb{F}_0$*, then*

$$d_r(C(J)) \geq \delta_{r,SHIFT}(J).$$

Proof. This follows directly from the Definitions, Lemma 4.2 and Remark 4.4. □

Example 4.7. The higher weights of Reed-Muller codes are not very well explained by the shift bound. Take for instance the first order Reed-Muller code $\mathcal{RM}_q(1, m)$. The sequence of generalized weights is equal to

$$q^m - q^{m-1}, q^m - q^{m-2}, \ldots, q^m - q, q^m - 1, q^m,$$

whereas every subcode of $\mathcal{RM}_q(1, m)$, which is not zero and not equal to $\mathcal{RM}_q(0, m)$, has minimum distance $q^m - q^{m-1}$. We will see in the following section that the shift bound explains the higher weights of algebraic-geometric codes very well.

5 Shift bound for algebraic-geometric codes and error-correcting arrays

The following definition is from [15, 20].

Definition 5.1. Consider $\mathbb{F}^n$ with the multiplication $*$ as an $\mathbb{F}$-algebra. Let K be an $\mathbb{F}$-algebra. Let $\varphi : K \to \mathbb{F}^n$ be a morphism of $\mathbb{F}$-algebras. Let $\mathcal{C} = (C_r)_{r \in \mathbb{N}_0}$ be a sequence of linear codes in $\mathbb{F}_0^n$. An *array* for the sequence of codes $\mathcal{C}$ is a triple $(\mathcal{U}, \mathcal{V}, \mathcal{W})$ of sequences of sub spaces of K enumerated by $\mathcal{U} = (U_i)_{i \in \mathbb{N}_0}$, $\mathcal{V} = (V_j)_{j \in \mathbb{N}_0}$ and $\mathcal{W} = (W_r)_{r \in \mathbb{N}_0}$, such that

$$C_r = \{\mathbf{y} \in \mathbb{F}_0^n \mid \ < \mathbf{y}, \varphi(h) >= 0 \ \text{ for all } \ h \in W_r\}$$

and the following holds:

(*A*.1) $\dim(U_i) = i$, $\dim(V_j) = j$ and $\dim(W_r) = r$ for all $i, j, r \in \mathbb{N}_0$.

(*A*.2) $U_i \subseteq U_{i+1}$, $V_j \subseteq V_{j+1}$ and $W_r \subseteq W_{r+1}$ for all $i, j, r \in \mathbb{N}_0$.

$(A.3)$ For all $i, j \in \mathbb{N}_0$ there exists an $r \in \mathbb{N}_0$ such that $U_i V_j \subseteq W_r$, where $U_i V_j$ is the set of products fg in K of elements $f \in U_i$ and $g \in V_j$. For every $i, j \in \mathbb{N}_0$, we define $r(i, j)$ to be the smallest index $r \in \mathbb{N}_0$ such that $U_i V_j \subseteq W_r$.

$(A.4)$ If $f \in U_i \setminus U_{i-1}$ and $g \in V_j \setminus V_{j-1}$ and $r = r(i, j)$, then $fg \in W_r \setminus W_{r-1}$, for all $i, j \in \mathbb{N}$.

$(A.5)$ $r(i-1, j) < r(i, j)$ and $r(i, j-1) < r(i, j)$, for all $i, j \in \mathbb{N}$.

We denote the intersection of all $C_r, r \in \mathbb{N}$ by C_∞. We say that the array is an *error-correcting array* if moreover:

$(A.6)$ $C_\infty = 0$.

Remark 5.2. For the sequel we choose elements $f_i \in U_i \setminus U_{i-1}$, and $g_j \in V_j \setminus V_{j-1}$, and $h_r \in W_r \setminus W_{r-1}$. From Conditions $(A.1)$ and $(A.2)$ it follows that these elements exist and that $f_1, \ldots, f_i$ is a basis of U_i, and $g_1, \ldots, g_j$ is a basis of V_j, and $h_1, \ldots, h_r$ is a basis of W_r. Either Condition $(A.4)$ or $(A.5)$ is superfluous, [15]. Condition $(A.6)$ implies that $\{\varphi(f_i g_j) \mid i, j \in \mathbb{N}\}$ generates $\mathbb{F}^n$.

Definition 5.3. Define the following set

$$N_r = \{(i, j) \in \mathbb{N}^2 \mid r(i, j) = r + 1\}.$$

Let n_r be the number of elements of N_r. Define

$$\delta_{FR}(r) = \min\{n_s \mid r \leq s \in \mathbb{N}\} \cup \{d(C_\infty)\}.$$

The minimum distance of the zero code is by definition ∞. We call $\delta_{FR}(r)$ the *Feng-Rao designed minimum distance* of the code C_r of the array of codes.

Theorem 5.4 *For an array for a sequence of codes we have that the minimum distance of C_r is at least $\delta_{FR}(r)$. If moreover $\mathbb{F} = \mathbb{F}_0$, then the s^{th} generalized weight of C_r is at least $\delta_{FR}(r + s - 1)$.*

Proof. See [11, 9, 15, 20].

Example 5.5. *Geometric Goppa* or *algebraic-geometric* codes. Let $\mathbb{F}$ be a finite field and let $\mathbb{F}_0 = \mathbb{F}$. Let $\mathcal{X}$ be an algebraic curve over $\mathbb{F}$ of genus g with at least $n+1$ distinct rational points P and $P_1, \ldots, P_n$ over $\mathbb{F}$. Let K be the $\mathbb{F}$-algebra of rational functions on $\mathcal{X}$ which have only poles at P. Define the map $\varphi : K \to \mathbb{F}^n$ by $\varphi(f) = (f(P_1), \ldots, f(P_n))$ for $f \in K$, then φ is a morphism of $\mathbb{F}$-algebras. The function $o : K \to \mathbb{N}_0$ is defined by: $o(f)$ is the pole order of f at P. Then o is a degree function on K. Let (μ_i) be the non-gap sequence at P, that is to say it is the increasing sequence of numbers such that there exists a rational function f_i which has only a pole of order μ_i at P. Let $U_i = V_i = W_i$ be the vector space of rational functions which have only poles at P of order at most μ_i. Then $N_r = \{(i,j) \in \mathbb{N}^2 \mid \mu_i + \mu_j = \mu_{r+1}\}$ and $n_r \geq r+1-g$ if $r \geq g$, and equality holds in case $r > 3g-2$. See [15, 20] for more properties of the FR bound in terms of the semigroup of non-gaps at P. The *Goppa* bound of C_r is defined by $r+1-g$ for $r \geq g$ and denoted by $\delta_\Gamma(r)$. It is shown in [11, 9, 15] that the FR bound improves the Goppa bound for algebraic-geometric codes. Furthermore we gave several properties for the FR bound in terms of the semigroup of non-gaps, see [14, 15]. Majority coset decoding decodes up to half the FR bound. We will generalize this decoding algorithm for the shift bound in Section 6.

Example 5.6. *Hermitian* codes. It follows from the work of Yang, Kumar and Stichtenoth [30] that the s^{th} generalized weights of the code C_r on the Hermitian curve is equal to $\delta_{FR}(r+s-1)$, see also Munuera [18].

Finally we compare the FR bound with the shift bound.

Definition 5.7. Define the set $J_r = \{(i,j) \in \mathbb{N}^2 \mid r(i,j) \leq r\}$ for an error-correcting array and consider the following two conditions:

$(A.7)$ For every $r \in \mathbb{N}$ there exist $i, j \in \mathbb{N}_0$ such that $r(i,j) = r$.

$(A.8)$ W_r is generated as a vector space by $\{f_i g_j \mid r(i,j) \leq r\}$ for all $r \in \mathbb{N}_0$.

Remark 5.8. The Conditions $(A.7)$ and $(A.8)$ are equivalent for an error-correcting array.

Suppose $(A.7)$ holds. Condition $(A.8)$ is now shown by induction on r. $W_0 = 0$ is generated by the empty set. Now assume that W_{r-1} is generated as a vector space by $\{f_i g_j \mid r(i,j) \leq r-1\}$. There exist $i, j \in \mathbb{N}_0$ such

that $r(i,j) = r$, so $f_i g_j \in W_r \setminus W_{r-1}$. Furthermore $\dim(W_r) = \dim(W_{r-1}) + 1$, so $W_r = \langle f_i g_j \rangle + W_{r-1}$. Hence W_r is generated as a vector space by $\{f_i g_j \mid r(i,j) \leq r\}$.

Suppose $(A.8)$ holds. If $r(i,j) \leq r$ implies $r(i,j) < r$ for all i,j, then $W_{r-1} \subseteq W_r$, and $\{f_i g_j \mid r(i,j) \leq r\}$ is a subset of W_{r-1} and W_r is generated as a vector space by $\{f_i g_j \mid r(i,j) \leq r\}$, so $W_r = W_{r-1}$. But $\dim(W_r) = \dim(W_{r-1}) + 1$, which gives a contradiction. Hence there exists a pair (i,j) such that $r(i,j) = r$, so $(A.7)$ holds.

Lemma 5.9 *For an error-correcting array of codes such that moreover Condition* $(A.8)$ *holds we have that:*

$$C_r = C(J_r)$$

Proof. The inclusion $C_r \subseteq C(J_r)$ holds always, since if $\mathbf{y} \in C_r$ and $r(i,j) \leq r$, then $f_i g_j \in W_r$, so $< \mathbf{y}, \varphi(f_i g_j) >= 0$. If moreover W_r is generated as a vector space by $\{f_i g_j \mid r(i,j) \leq r\}$, then $C_r = C(J_r)$. Because, if $\mathbf{y} \in C(J_r)$, then $< \mathbf{y}, \varphi(f_i g_j) >= 0$, for all $(i,j) \in J_r$. We assumed that W_r is generated by $\{f_i g_j \mid (i,j) \in J_r\}$, so $< \mathbf{y}, \varphi(h) >= 0$ for all $h \in W_r$, hence $\mathbf{y} \in C_r$. This proves the lemma. □

Proposition 5.10 *For an error-correcting array of codes such that moreover Condition* $(A.8)$ *holds we have that:*

$$\delta_{SHIFT}(J_r) \geq \delta_{FR}(r).$$

Proof. Let R be a subset of $\mathbb{N}^2$ which contains J_r and such that $R^* = R \neq \mathbb{N}^2$. Let $s \in \mathbb{N}$ be the greatest number such that $J_s \subseteq R$. Such an s exists, since $J_r \subseteq R$ and $R \neq \mathbb{N}^2$. Hence $(i,j) \in R$ if $r(i,j) \leq s$, and there exists a pair (k,l) such that $r(k,l) = s+1$ and $(k,l) \notin R$. So there exists a $\mathbf{c} \in C(R)$ such that $< \mathbf{c}, \varphi(f_k g_l) >\neq 0$, since $R = R^*$. Suppose there exists a pair $(u,v) \in R$ such that $r(u,v) = s+1$ and $< \mathbf{c}, \varphi(f_u g_v) >= 0$. Then $\langle f_u g_v \rangle + W_s = W_{s+1}$ and $< \mathbf{y}, \varphi(h) >= 0$ for all $h \in W_s$ and $\mathbf{y} \in C(R)$, since W_s is generated as a vector space by $\{f_i g_j \mid (i,j) \in J_s\}$ and $J_s \subseteq R$. So $< \mathbf{y}, \varphi(h) >= 0$ for all $h \in W_{s+1}$ and $\mathbf{y} \in C(R)$. This gives a contradiction, since $f_k g_l \in W_{s+1}$, $\mathbf{c} \in C(R)$ and $< \mathbf{c}, \varphi(f_k g_l) >\neq 0$. Hence $(i,j) \in R$ for all (i,j) such that $r(i,j) \leq s$ and $(u,v) \notin R$ for all (u,v) such that $r(u,v) = s+1$. Let $N_s = \{(i_k, j_{w-k+1}) \mid 1 \leq k \leq w\}$ such that $j_1 < \cdots < j_w$

and $w = n_s$. Then $r(i_k, j_l) < r(i_k, j_k) = s + 1$, by Condition $(A.5)$, so $(i_k, j_l) \in J_s \subseteq R$ for all $k + l \leq w$ and $(i_k, j_l) \notin R$ for all $k + l = w + 1$. Let $A = \{(i_1, i_l) \mid 1 \leq l \leq w\}$, then A is independent with respect to R and has size n_s. So $\delta_{FR}(r) \leq n_s \leq n(R)$. Hence $\delta_{FR}(r)$ is a lower bound for all complete defining sets which contain J_r and are not equal to $\mathbb{N}^2$. Therefore $\delta_{FR}(r) \leq \delta_{SHIFT}(J_r)$. □

Example 5.11. Consider the hyperelliptic curve with equation $Y^2 = F(X)$, where $F(X)$ has odd degree m and has no square divisors. It is shown in [15, Remark 7.5] that $\delta_{FR}(r) = 2$ for all $r \leq (m + 1)/2$. If the n distinct points $P_i = (x_i, y_i), 1 \leq i \leq n$ are chosen in such a way that $x_i = x_j$ for some $i < j$, then the minimum distance is equal to 2. If the x_i are mutually distinct, then C_r is a Reed-Solomon code of dimension $n - r$, so C_r has parameters $[n, n - r, r + 1]$. This follows also from the shift bound. Let $f_i = X^{i-1}$ for $1 \leq i \leq (m + 1)/2$, $f_i = X^j Y$ for $i = (m + 3)/2 + 2j$, and $f_i = X^{i-1+j}$ for $i = (m + 1)/2 + 2j$ and $0 < j$. Let $i_k = j_k$ be the positive integer such that $f_{i_k} = X^{k-1}$. Then $f_{i_k} f_{j_l} = X^{k+l-1}$. The set $\{\varphi(X^i) \mid i \in \mathbb{N}_0\}$ generates $\mathbb{F}^n$, since the x_i are mutually distinct. Let R be a complete defining set which contains J_r and is not equal to $\mathbb{N}^2$, for some $r \leq (m + 1)/2$. Then there exists a $w > r$ such that $(i_k, j_l) \in R$ for all $k + l \leq w$ and $(i_k, j_l) \notin R$ for all $k + l = w + 1$. Hence $n(R) \geq w > r$ and $\delta_{SHIFT}(J_r) = r + 1$.

6 Decoding up to half the shift bound

With *majority coset decoding* one decodes up to half the FR designed minimum distance, see [3, 4, 8, 15, 20]. We have seen in Section 5 that the shift bound improves the FR bound. In this section we will sketch how majority coset decoding can be generalized and decodes up to half the shift bound. This algorithm is not polynomial, therefore we define a restricted shift bound and show that the complexity of the algorithm for the restricted case is at most $\mathcal{O}(n^3)$.

Suppose R_1 is a complete defining set for $C_1 = C(R_1)$. Let $\mathbf{y}_1$ be a received word with error $\mathbf{e}$ with respect to C_1 with at most $\lfloor (\delta_{SHIFT}(R_1) - 1)/2 \rfloor$ errors, so $\mathbf{y}_1 = \mathbf{c}_1 + \mathbf{e}$ for some $\mathbf{c}_1 \in C_1$ and $wt(\mathbf{e}) \leq (n(R_1) - 1)/2$. Let A be an independent set with respect to R_1 of size $w = n(R_1)$, that is to say there exist $i_1, \ldots, i_w$ and $j_1, \ldots, j_w$ such that $(i_k, j_l) \in R_1$ if $k + l \leq w$, and

$(i_k, j_k) \notin R_1$ if $k + l = w + 1$.

Define

$$S_{i,j}(\mathbf{y}) = < \mathbf{y}, \varphi(f_i g_j) > .$$

We denote $S_{i,j}(\mathbf{e})$ by $S_{i,j}$. Now $S_{i,j}(\mathbf{y}_1) = S_{i,j}$ for all $(i,j) \in R_1$. So we have a $(w \times w)$-matrix M with entries $M_{k,l} = S_{i_k,j_l}$ of syndromes and these are known for all $k + l \leq w$.

First we introduce some definitions, see [3, 4, 8, 11, 9, 15, 20]. Let $M(u,v)$ be the $(u \times v)$-matrix with entries $M_{i,j}, 1 \leq i \leq u, 1 \leq j \leq v$. Consider the following two conditions:

$(D.1)$ $\text{rank}(M(u-1, v-1)) = \text{rank}(M(u-1, v)) = \text{rank}(M(u, v-1))$

$(D.2)$ $\text{rank}(M(u-1, v-1)) = \text{rank}(M(u, v))$

Clearly Condition $(D.2)$ implies $(D.1)$; conversely if Condition $(D.1)$ holds, then there exists a unique value for $M_{u,v}$ such that Condition $(D.2)$ holds, we denote this value by $M'_{u,v}$. We call (u,v) a *discrepancy* if Condition $(D.1)$ holds and Condition $(D.2)$ does not hold. Remark that Condition $(D.1)$ holds for (u,v) if and only if Condition $(D.2)$ holds for all $(i,v), 1 \leq i < u$ and all $(u,j), 1 \leq j < v$. Hence in every row there is at most one discrepancy and the same holds for every column. The number of discrepancies of M is equal to the rank of M.

We call a pair (u,v) a *candidate* if $u + v = w + 1$ and Condition $(D.1)$ holds. A candidate is called *true* or *correct* if Condition $(D.2)$ holds, and *false* or *incorrect* otherwise. We know the candidates but we do not know which candidates are true nor false. We first prove that the number of true candidates, which we will denote by T, is strictly greater than the number of false candidates, which we will denote by F. We have seen already in the proof of Lemma 3.2 that the rank of M is at most $wt(\mathbf{e})$. Denote the number of *known* discrepancies, that is discrepancies at entries (u,v) such that $u + v \leq w$, by K. The other discrepancies are called *unknown*. Clearly we have that all false candidates are unknown discrepancies. Hence

$$K + F \leq \text{the number of all discrepancies} = \text{rank}(M) \leq wt(\mathbf{e}).$$

Every known discrepancy (i, j) gives rise to exactly two non-candidates $(i, w-i+1)$ and $(w-j+1, j)$ on the back-diagonal $u+v = w+1$. Furthermore for every pair (u, v) such that $u+v = w+1$ which is not a candidate, there exists a known discrepancy in the same row or column, possibly in both. Hence the number of pairs (u, v) on the back-diagonal $u+v = w+1$, which are not candidates, is at most $2K$. For every candidate, true or false, there exists no known discrepancy in the same row nor column. M is a square matrix of size $w = n(R_1)$. Hence

$$n(R_1) \leq T + F + 2K.$$

If we combine the two inequalities above and use that $2wt(\mathbf{e}) < n(R_1)$, then we get

$$n(R_1) \leq T + F + 2K \leq T + F + (2wt(\mathbf{e}) - 2F) < T - F + n(R_1).$$

Therefore

$$F < T,$$

that is the number of true candidates is greater than the number of false candidates.

Let $R_2 = (R_1 \cup \{(i_k, j_{w-k+1}) \mid 1 \leq k \leq w\})^*$ be the complete defining set for $C_2 = C(R_2)$. We want to find a word $\mathbf{y}_2$ which has the same coset as $\mathbf{e}$ with respect to C_2, so $\mathbf{y}_2 = \mathbf{c}_2 + \mathbf{e}$ for some $\mathbf{c}_2 \in C_2$ and $\mathbf{y}_2 = \mathbf{y}_1 + \mathbf{c}$ for some $\mathbf{c} \in C_1$.

Lemma 6.1 *The set of equations:*

$$S_{i,j}(\mathbf{x}) = S_{i,j} - S_{i,j}(\mathbf{y}_1) \quad \textit{for all} \quad (i, j) \in R_2$$

has the coset $\mathbf{c} + C_2$ *as the unique solution in* C_1/C_2.

Proof. We leave this as an exercise for the reader, see [3, 4]. □

Furthermore $S_{i,j}(\mathbf{x}) = 0$ for all $(i, j) \in R_1$ if and only if $\mathbf{x}$ is an element of C_1, and $M_{k,w-k+1} = M'_{k,w-k+1}$ if and only if $(k, w-k+1)$ is a true candidate.

Assume for simplicity that $R_2 = (R_1 \cup \{(i_1, j_w)\})^*$, then R_2 is equal to $(R_1 \cup \{(i_k, j_{w-k+1})\})^*$ for all k, and the equation $S_{i_k,j_{w-k+1}}(\mathbf{x}) = M'_{k,w-k+1} - S_{i_k,j_{w-k+1}}(\mathbf{y}_1)$ has a unique coset $\mathbf{x} + C_2$ in C_1/C_2 as a solution for all true

candidates $(k, w-k+1)$. In this case we compute for all candidates this unique coset. If there is not such a coset, then we know that the candidate was false. Choose the coset which appears most often, by a majority vote. We know that this majority vote gives the true candidates, since $T > F$. In this way we find a $\mathbf{y}_2$ and the unknown syndromes $S_{i_k, j_{w-k+1}}$ for all k. By continuing in this way we find a finite sequence $R_1, \ldots, R_t, R_{t+1}$ of complete defining sets and a sequence of pairs $(u_1, v_1), \ldots, (u_t, v_t)$ such that $R_{i+1} = (R_i \cup \{(u_i, v_i)\})^*$ and $R_{t+1} = N^2$. For the corresponding decreasing sequence of codes $C_i = C(R_i)$ we will find words $\mathbf{y}_i$ such that $\mathbf{y}_i = \mathbf{c}_i + \mathbf{e}$ for some $\mathbf{c}_i \in C_i$. So we end with $\mathbf{y}_{t+1} = \mathbf{e}$, since $C_{t+1} = 0$.

In general we do not have $R_2 = (R_1 \cup \{(i_1, j_w)\})^*$ and we have to look at all $R_{2,k} = (R_1 \cup \{(i_k, j_{w-k+1})\})^*$. So instead of an increasing chain we get a partial order of complete defining sets. We apply the majority voting on these defining sets, combined with a depth first search in this partial order.

Hence we have sketched the proof of the following theorem:

Theorem 6.2 *A combination of majority voting and depth first search gives a decoding algorithm which corrects at least* $(\delta_{SHIFT}(J) - 1)/2$ *errors with respect to the code* $C(J)$.

The depth first search might give in the worst case that we have to search the whole partial order of all possible larger complete defining sets, hence our algorithm will have exponential complexity as a function of the code length. In case of the restricted shift bound we have $(i_k, j_{w-k+1}) \in (R \cup \{(i_1, j_w)\})^*$ for all k, by the following definition.

Definition 6.3. Let R be a complete defining set and let $r \in N^2$ and $r \notin R$. Let $n(R, r)$ be the greatest number w such that there exist sequences $i_1, i_2, \ldots, i_w$ and $j_1, j_2, \ldots, j_w$ such that

$(i_k, j_l) \in R$ for all $k+l \leq w$, and $(i_k, j_l) \in (R \cup \{r\})^* \backslash R$ for all $k+l = w+1$.

Lemma 6.4 *Let* $\mathbf{y} \in \mathbb{F}_0^n$. *Let* $R = \{(i,j) \in N^2 \mid < \mathbf{y}, \varphi(f_i g_j) >= 0\}$. *If* $r \in N^2$ *and* $r \notin R$, *then* $wt(\mathbf{y}) \geq n(R, r)$.

Proof. The proof is the same as the proof of Lemma 3.2. □

Lemma 6.5 *Let R be a subset of N^2. Let $r \in N^2$ and $r \notin R$.*

$$\text{If } \mathbf{y} \in C(R) \text{ and } \mathbf{y} \notin C(R \cup \{r\}), \quad \text{then } wt(\mathbf{y}) \geq n(R, r).$$

Proof. The proof is the same as the proof of Lemma 3.5. □

Definition 6.6. We call a finite sequence $\mathcal{R} = (R_1, \ldots, R_t, R_{t+1})$ of complete defining sets with the property that there exists a sequence of pairs $r_1, \ldots, r_t \in N^2$ such that $R_{i+1} = (R_i \cup \{r_i\})^*$ and $R_1 = J^*$ and $R_{t+1} = N^2$ a *restricted chain* starting at J. For such a restricted chain $\mathcal{R} = (R_1, \ldots, R_t, R_{t+1})$ we define

$$\delta_{RES}(\mathcal{R}) = \min\{n(R_i, r_i) \mid 1 \leq i \leq t\}.$$

Define the *restricted shift* bound for a subset J of N^2 as follows:

$$\delta_{RES}(J) = \max\{\delta_{RES}(\mathcal{R}) \mid \mathcal{R} \text{ is a restricted chain starting at } J\}.$$

Theorem 6.7 *The minimum distance of $C(J)$ is at least $\delta_{RES}(J)$.*

Proof. This follows directly from Lemma 6.5 and the Definitions. □

Theorem 6.8 *Majority coset decoding corrects at least $(\delta_{RES}(J) - 1)/2$ errors with respect to the code $C(J)$ and its complexity is at most $\mathcal{O}(n^3)$.*

Proof. This is shown at the beginning of this section. The complexity of all computations is not greater than solving systems of linear equations. □

For fast decoding algorithms we refer to [11, 23, 24].

Proposition 6.9

$$\delta_{RES}(J) \leq \delta_{SHIFT}(J).$$

Proof. Let $\mathcal{R} = (R_1, \ldots, R_t, R_{t+1})$ be a sequence of complete defining sets which is a restricted chain starting at J such that $\delta_{RES}(J) = \delta_{RES}(\mathcal{R})$. Then there exists a sequence of pairs $r_1, \ldots, r_t \in N^2$ such that $R_{i+1} = (R_i \cup \{r_i\})^*$ and $R_1 = J^*$ and $R_{t+1} = N^2$. Let R be a complete defining set which contains J and is not equal to N^2. So R contains R_1 and is not equal to R_{t+1}. Let i be the smallest index such that R contains R_i and does not contain R_{i+1}. Then $r_i \notin R$ and $n(R) \geq n(R_i, r_i)$. Hence $n(R) \geq \delta_{RES}(\mathcal{R}) = \delta_{RES}(J)$ for all

complete defining sets R which contain J and are not equal to N^2. Therefore $\delta_{RES}(J) \leq \delta_{SHIFT}(J)$. This proves the proposition. □

Remark 6.10. We have seen in Example 3.9 that the independent sets for the Generalized Reed-Muller codes have the property that the function associated with (i_k, j_{w-k+1}) is the same for all k, hence

$$\delta_{RES}(R(r,m)) = \delta_{SHIFT}(R(r,m)) = (\mu+1)q^{\rho},$$

where $r+1 = \rho(q-1)+\mu$ for $\mu < q-1$.

Remark 6.11. The same proof of Proposition 5.10 will give $\delta_{RES}(J_r) \geq \delta_{FR}(r)$.

Remark 6.12. We construct an example with the HT bound such that the restricted shift bound is strictly smaller than the shift bound. Take $J = \{1,2,4,5\}$, $a = 3$ and $s = 1$. If n is not divisible by 3, then $\delta_{SHIFT}(J) \geq \delta_{HT}(J) = 4$. If $n = 8$, then $\delta_{RES}(J) = 4$, since we can make an independent set with the following diagram.

	2	1	5	0
0	2	1	5	0
3	5	4	0	
7	1	0		
6	0			

If $n \geq 10$, then $\delta_{RES}(J) = 3$, as one sees by inspecting all possibilities.
Let $n = 10, \mathbb{F} = \mathbb{F}_0 = \mathbb{F}_{11}$ and $J = \{1,2,4,5\}$. Then $\delta_{SHIFT}(J) > \delta_{RES}(J)$.

Classes For the independent sets for the HT bound we get for the pairs (i_k, j_l) on the back-diagonal $k+l = w+1$, two districts $1 \leq k \leq s'+1$ and $s'+2 \leq k \leq \delta+s'$ where $i_k + j_{w-k+1}$ is constant, see the proof of Proposition 2.8. We perform a majority vote in both districts, and the true candidates have a majority in at least one of the two districts, since the number of true candidates has the majority in the union of both districts. Suppose the number of true candidates is T_1 and T_2 in the first and second district, respectively, and the number of false candidates is F_1 and F_2 in the first and second district, respectively. If $T_1 \geq F_1$ and $F_2 \geq T_2$, then $T_1 - F_1 > F_2 - T_2$, since $T_1 + T_2 = T > F = F_1 + F_2$. So if we take the district and the candidate

which has the largest majority, then we get a true candidate. Therefore we still can decode up to half the HT bound with complexity $\mathcal{O}(n^3)$.
See Theorem 3 of [10] on the Majority Principle for Two Conjugate Syndrome. See also Algorithm 2 (Majority Voting Scheme) of [26] that covers the cases $w = 1$ and $w = 2$, where w is the number of districts.

Acknowledgement I want to thank I.M. Duursma, M. van Eupen, G.-L. Feng and B.-Z. Shen for numerous discussions I had with them on several topics discussed in this paper.

Update

1. (31 October 1997) I want to thank G. Schiffels for several remarks. In particular the example in Remark 6.12 was not correct.
2. (7 January 2013) References are updated.

References

[1] Augot, D., P. Charpin, N. Sendrier, Studying the locator polynomials of minimum weight codewords of BCH codes. IEEE Trans. Inform. Theory **38** (1992), 960-973.

[2] Delsarte, P., J.-M. Goethals, F.J. MacWilliams, On generalized Reed-Muller codes and their relatives. Information and Control **16** (1970), 403-422.

[3] Duursma, I.M., Majority coset decoding. IEEE Trans. Inform. Theory **39** (1993), 1067-1070.

[4] Duursma, I.M., Decoding codes from curves and cyclic codes. PhD Thesis, Eindhoven Un. Techn., Sept. 1993.

[5] Duursma, I.M., A symmetric Roos bound for general linear codes. Preprint 1994.

[6] Duursma, I.M., R. Kötter, Error-locating pairs for cyclic codes. IEEE Trans. Inform. Theory **40** (1994), 1108-1121.

[7] van Eupen, M., J.H. van Lint, On the minimum distance of ternary cyclic codes. IEEE Trans. Inform. Theory **39** (1993), 409-422.

[8] Feng, G.-L., T.R.N. Rao, Decoding of algebraic geometric codes up to the designed minimum distance. IEEE Trans. Inform. Theory **39** (1993), 37-46.

[9] Feng, G.-L., T.R.N. Rao, A simple approach for construction of algebraic-geometric codes from affine plane curves. IEEE Trans. Inform. Theory **40** (1994), 1003-1012.

[10] Feng, G.-L., K.K. Tzeng, A new procedure for decoding cyclic and BCH codes up to the actual minimum distance. IEEE Trans. Inform. Theory **40** (1994), 1364-1374.

[11] Feng, G.-L., V.K. Wei, T.R.N. Rao, K.K Tzeng, Simplified understanding and efficient decoding of a class of algebraic-geometric codes. IEEE Trans. Inform. Theory **40** (1994), 981-1002.

[12] Hartmann, C.R.P., K.K. Tzeng, Generalizations of the BCH bound. Inform. and Control **20** (1972), 489-498.

[13] Kasami, T. , S. Lin, W.W. Peterson, New generalizations of Reed-Muller codes, Part I: Primitive codes. IEEE Trans. Inform. Theory **14** (1968), 189-199.

[14] Kirfel, C., On the Clifford defect of special curves. These proceedings.

[15] Kirfel, C., R. Pellikaan, On the minimum distance of codes in an array coming from telescopic semigroups. IEEE Trans. Inform. Theory **41** (1995), 1720-1732.

[16] van Lint, J.H., R.M. Wilson, On the minimum distance of cyclic codes. IEEE Trans. Inform. Theory **32** (1986), 23-40.

[17] Macwilliams, F.J., N.J.A. Sloane, The theory of error-correcting codes. North-Holland Math. Library **16**, North-Holland, Amsterdam 1977.

[18] Munuera, C., On the generalized Hamming weigths of geometric Goppa codes. IEEE Trans. Inform. Theory **40** (1994), 2092-2099.

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

[20] Pellikaan, R., On the efficient decoding of algebraic-geometric codes. Eurocode 92, edited by P.Camion, P. Charpin and S. Harari, Udine, CISM Courses and Lectures **339**, Springer-Verlag, Wien-New York 1993, 231-253.

[21] Pellikaan, R., On the existence of error-correcting pairs. Journal of Statistical Planning and Inference **51** (1996), 229-242.

[22] Roos, C., A new lower bound for the minimum distance of a cyclic code. IEEE Trans. Inform. Theory **29** (1983), 330-332.

[23] Sakata, S., J. Justesen, Y. Madelung, H. Elbrønd Jensen, T. Høholdt, Fast decoding of algebraic-geometric codes up to the designed minimum distance. IEEE Trans. Inform. Theory **41** (1995), 1672-1677.

[24] Sakata, S., H. Elbrønd Jensen, T. Høholdt, Generalized Berlekamp-Massey decoding of algebraic geometric codes up to half the Feng-Rao bound. Proceedings 1994 IEEE ISIT, Trondheim, Norway July 1994.

[25] Shen, B.-Z., K.K. Tzeng, Generation of matrices for determining minimum distance and decoding of algebraic-geometric codes. IEEE Trans. Inform. Theory **41** (1995), 1703-1708.

[26] Shen, B.-Z., K. K. Tzeng, A code decomposition approach for decoding cyclic and algebraic-geometric codes. International Symposium on Information Theory and Its Applications, Sydney, Australia Nov. 20-25, 1994; IEEE Trans. Inform. Theory **41** (1995), 1969-1987.

[27] Tzeng, K.K., C.R.P. Hartmann, On the minimum distance of certain reversible cyclic codes. IEEE Trans. Inform. Theory **16** (1970), 644-646.

[28] Wei, V.K., Generalized Hamming weigths for linear codes. IEEE Trans. Inform. Theory **37** (1991), 1412-1418.

[29] Weldon Jr., E.J., New generalizations of the Reed-Muller codes, Part II: Nonprimitive codes. IEEE Trans. Inform. Theory **14** (1968), 199-205.

[30] Yang, K., P.V. Kumar, H. Stichtenoth, On the weight hierarchy of geometric Goppa codes. IEEE Trans. Inform. Theory **40** (1994), 913-920.