International Journal of Pure and Applied Mathematics
Volume 80 No. 3 2012, 315-329
ISSN: 1311-8080 (printed version)
url: http://www.ijpam.eu

ijpam.eu

STANDARD BASES FOR BINARY LINEAR CODES

Natalia Dück[1], Karl-Heinz Zimmermann[2 §]

[1,2]Hamburg University of Technology
21071, Hamburg, GERMANY

Abstract: Each linear code can be described by a binomial ideal given as the sum of a toric ideal and a non-prime ideal. For binary linear codes, we provide standard bases for the localizations of the code ideals.

AMS Subject Classification: 13P10, 94B05
Key Words: commutative polynomial ring, linear code, Groebner basis, local ring, standard basis

1. Introduction

Error-correcting codes are used to protect digital data against errors that occur during transmission through a communication channel [11, 19]. There are two ways to construct error-correcting codes: algebraic coding and probabilistic coding. While the construction of good codes by probabilistic methods has turned out to be difficult, R.W. Hamming has shown how easy it is to devise algebraic codes by introducing a class of binary single-error-correcting codes whose performance can easily be estimated by the computation of a parameter called Hamming distance [10].

The main objects of study in algebraic coding are codes that are linear subspaces of finite-dimensional vector spaces over a finite field. In particular, research has been mainly devoted to cyclic codes that form a class of linear codes allowing easier determination of their decoding properties and low-complexity decoders. A.B. Cooper [5] has used the polynomial description of cyclic codes in order to construct a decoder by Groebner basis computations. The "Cooper

Received: April 11, 2012

[§]Correspondence author

philosophy" was the first instance of applications to associate Groebner bases with linear codes. The application of Groebner basis computations to the study of linear codes has become an active field of research [7, 13, 17].

Recently, it has been emphasized that linear codes can be described by binomial ideals each of which given as the sum of a toric ideal and a non-prime ideal allowing to study linear codes by methods from commutative algebra and algebraic geometry [3, 16]. Lately, it has been shown that the binomial ideal associated with a linear code has a very natural Groebner basis with respect to the lexicographic order requiring that any monomial containing one of the information symbols is larger than any monomial containing only parity check symbols [15].

Originally, the method of Groebner bases has been introduced by Buchberger for the algorithmic solution of some fundamental problems in commutative algebra [4]. Today, Groebner bases provide a uniform approach to solving a wide range of problems expressed in terms of sets of multivariate polynomials such as the solvability and solving algebraic systems of equations, ideal and radial membership decision, and effective computation in residue class rings modulo polynomial ideals [1, 2, 6, 18].

In this paper, we provide standard bases for the local rings of rational functions that are regular at the points of the affine variety associated to the ideal of a binary linear code.

2. Groebner Bases

Throughout this paper, $\mathbb{K}$ denotes a field and $\mathbb{K}[\boldsymbol{X}] = \mathbb{K}[X_1, \ldots, X_n]$ the commutative polynomial ring in n indeterminates over $\mathbb{K}$. Recall that a *term* in $\mathbb{K}[\boldsymbol{X}]$ is a scalar times a monomial. The *monomials* in $\mathbb{K}[\boldsymbol{X}]$ are denoted by $\boldsymbol{X}^{\boldsymbol{u}} = X_1^{u_1} X_2^{u_2} \cdots X_n^{u_n}$ and are identified with the lattice points $\boldsymbol{u} = (u_1, \ldots, u_n) \in \mathbb{N}_0^n$, where $\mathbb{N}_0$ stands for the set of nonnegative integers. The *degree* of a monomial $\boldsymbol{X}^{\boldsymbol{u}}$ is the sum $|\boldsymbol{u}| = u_1 + \cdots + u_n$ and the degree of a polynomial f is the maximal degree of all monomials appearing in f.

A *monomial order* on $\mathbb{K}[\boldsymbol{X}]$ is any relation $\succ$ on the set of monomials $\boldsymbol{X}^{\boldsymbol{u}}$ in $\mathbb{K}[\boldsymbol{X}]$ (or equivalently, on the exponent vectors in $\mathbb{N}_0^n$) satisfying: (1) $\succ$ is a total ordering, (2) the zero vector $\boldsymbol{0}$ is the unique minimal element, and (3) $\boldsymbol{u} \succ \boldsymbol{v}$ implies $\boldsymbol{u}+\boldsymbol{w} \succ \boldsymbol{v}+\boldsymbol{w}$ for all $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in \mathbb{N}_0^n$. Familiar monomial orders are the purely lexicographic order, the degree lexicographic order, and the degree reverse lexicographic order.

Given a monomial order $\succ$, each non-zero polynomial $f \in \mathbb{K}[\boldsymbol{X}]$ has a unique *leading term*, denoted by $\mathrm{LT}_{\succ}(f)$, given by the largest involved term with respect to the monomial order. If $\mathrm{LT}_{\succ}(f) = c\boldsymbol{X}^{\boldsymbol{u}}$, where $c \in \mathbb{K} \setminus \{0\}$, then c is the *leading coefficient* of f and $\boldsymbol{X}^{\boldsymbol{u}}$ is the *leading monomial.*

Monomial orders are used in a (generalized) *division algorithm.* For this, fix a monomial order $\succ$ on $\mathbb{K}[\boldsymbol{X}]$ and let $\mathcal{F} = (f_1, \ldots, f_s)$ be an ordered sequence of polynomials in $\mathbb{K}[\boldsymbol{X}]$. Then each polynomial $f \in \mathbb{K}[\boldsymbol{X}]$ can be written as

$$f = h_1 f_1 + \ldots + h_s f_s + r, \tag{1}$$

where $h_1, \ldots, h_s, r \in \mathbb{K}[\boldsymbol{X}]$, $h_i f = 0$ or $\mathrm{LT}_{\succ}(f) \succeq \mathrm{LT}_{\succ}(h_i f_i)$, $1 \leq i \leq s$, and either $r = 0$ or r is a linear combination of monomials, none of which is divisible by any of $\mathrm{LT}_{\succ}(f_i)$, $1 \leq i \leq s$. The polynomial r is the *remainder* of f on division by $\mathcal{F}$. The key operation in the division process is the reduction of a partial dividend p ($p = f$ and $r = 0$ to start) by an element f_k (k is assumed to be minimal). If $\mathrm{LT}_{\succ}(p) = t \cdot \mathrm{LT}_{\succ}(f_k)$ for some term $t \in \mathbb{K}[\boldsymbol{X}]$, then p is replaced by $p - t \cdot f_k$.

Otherwise, no reduction is possible, i.e., $\mathrm{LT}_{\succ}(p)$ is not divisible by any of the $\mathrm{LT}_{\succ}(f_i)$, and the leading term of p is subtracted from p and added to the remainder.

The reduction stops when p is reduced to 0. The termination of the division process is guaranteed since in each case the leading monomial of p drops.

If I is an ideal in $\mathbb{K}[\boldsymbol{X}]$ and $\succ$ is a monomial order on $\mathbb{K}[\boldsymbol{X}]$, its *leading ideal* is the monomial ideal generated by the leading monomials of its elements,

$$\langle \mathrm{LT}_{\succ}(I) \rangle = \langle \mathrm{LT}_{\succ}(f) \mid f \in I \rangle. \tag{2}$$

The monomials that do not lie in the leading ideal of I are called the *standard monomials* of I. A finite subset $\mathcal{G}_{\succ}$ of an ideal I in $\mathbb{K}[\boldsymbol{X}]$ is a *Groebner basis* for I with respect to $\succ$ if the leading ideal of I is generated by the set of leading monomials in $\mathcal{G}_{\succ}$,

$$\langle \mathrm{LT}_{\succ}(I) \rangle = \langle \mathrm{LT}_{\succ}(g) \mid g \in \mathcal{G}_{\succ} \rangle. \tag{3}$$

If no monomial in this generating set is redundant, the Groebner basis is called *minimal.* It is called *reduced* if for any two distinct elements $g, h \in \mathcal{G}_{\succ}$, no term of h is divisible by $\mathrm{LT}_{\succ}(g)$. A reduced Groebner basis is uniquely determined provided that the generators are monic.

The remainder on division of a polynomial $f \in \mathbb{K}[\boldsymbol{X}]$ by a Groebner basis for I is a uniquely determined normal form for f modulo I. It depends only on the monomial order and not on the way the division is performed.

A Groebner basis for an ideal I in $\mathbb{K}[\boldsymbol{X}]$ and a monomial order $\succ$ on $\mathbb{K}[\boldsymbol{X}]$ can be calculated by *Buchberger's algorithm*. It starts with an arbitrary generating set for I and provides in each step new elements of I by using expressions that guarantee to cancel leading terms and thus reveal other possible leading terms. These new elements are *S-polynomials* of elements f and g (in the generating set of I) given as

$$S(f,g) = \frac{\boldsymbol{X}^{\boldsymbol{u}}}{\mathrm{LT}_{\succ}(f)} \cdot f - \frac{\boldsymbol{X}^{\boldsymbol{u}}}{\mathrm{LT}_{\succ}(g)} \cdot g, \tag{4}$$

where $\boldsymbol{X}^{\boldsymbol{u}}$ is the least common multiple of the leading monomials of f and g. *Buchberger's S-criterion* says that a set of polynomials $\mathcal{G} = \{g_1, \ldots, g_s\}$ in $\mathbb{K}[\boldsymbol{X}]$ is a Groebner basis for the ideal $I = \langle g_1, \ldots, g_s \rangle$ if and only if the remainder on division of $S(g_i, g_j)$ by $\mathcal{G}$ is 0 for all $1 \leq i < j \leq s$. For more Groebner basics the reader may consult [1, 2, 6].

3. Linear Codes and Code Ideals

Let $\mathbb{F}_p$ be the finite field with p elements. A *linear code* $\mathcal{C}$ of length n and dimension k over $\mathbb{F}_p$ is the image of a one-to-one linear mapping $\psi : \mathbb{F}_p^k \to \mathbb{F}_p^n$, i.e., $\mathcal{C} = \psi(\mathbb{F}_p^k)$, where $k \leq n$. The code $\mathcal{C}$ is an $[n,k]$ code and its elements are called *codewords*. Define the *support* of a vector $\boldsymbol{u} \in \mathbb{F}_p^n$ as the set $\mathrm{supp}(\boldsymbol{u}) = \{i \mid u_i \neq 0\}$ of non-zero coordinates. In algebraic coding, the codewords are always written as row vectors.

A *generator matrix* for an $[n,k]$ code $\mathcal{C}$ over $\mathbb{F}_p$ is a $k \times n$ matrix $\mathbf{G}$ whose rows form a basis of $\mathcal{C}$; that is, $\mathcal{C} = \{\boldsymbol{a}\mathbf{G} \mid \boldsymbol{a} \in \mathbb{F}_p^k\}$. The code $\mathcal{C}$ is in *standard form* if it has a generator matrix in reduced echelon form $\mathbf{G} = (\boldsymbol{I}_k \mid \boldsymbol{M})$, where $\boldsymbol{I}_k$ is the $k \times k$ identity matrix. Each linear code is equivalent (by a monomial transformation) to a linear code in standard form. If $\mathcal{C}$ is in standard form, the first k symbols of a codeword are the *information symbols*. These can be chosen arbitrarily and then the remaining symbols, the socalled *parity check symbols*, are determined.

Let $\mathcal{C}$ be an $[n,k]$ code over $\mathbb{F}_p$. Define the *ideal associated with* $\mathcal{C}$ as

$$I_{\mathcal{C}} = \langle \boldsymbol{X}^{c} - \boldsymbol{X}^{c'} \mid \boldsymbol{c} - \boldsymbol{c}' \in \mathcal{C} \rangle + \langle X_i^p - 1 \mid 1 \leq i \leq n \rangle, \tag{5}$$

where each word $\boldsymbol{c} \in \mathbb{F}_p^n$ is considered as an integral vector in the monomial $\boldsymbol{X}^c$ [3, 16].

The following assertion shows that in a certain way the exponents can be treated as elements of $\mathbb{F}_p$ due to the non-prime ideal $\langle X_i^p - 1 \mid 1 \leq i \leq n \rangle$.

Lemma 3.1. *For the ideal $I_{\mathcal{C}}$ defined in (5) the following holds: If a polynomial $\sum_{|\boldsymbol{e}|\le d} c\boldsymbol{X}^{\boldsymbol{e}}$ with $c \in \mathbb{F}_p$ and of total degree d is in $I_{\mathcal{C}}$, the polynomial $\sum_{|\boldsymbol{e}|\le d} c\boldsymbol{X}^{\boldsymbol{e} \bmod p}$ also lies in $I_{\mathcal{C}}$, where $\boldsymbol{e}$ mod p is to be understood as a component-wise operation.*

Proof. This assertion is a result of calculations modulo the ideal $I_p := \langle X_i^p - 1 \mid 1 \le i \le n\rangle$. For $1 \le i \le n$, we have

$$X_i^{m+p} = X_i^{m+p} - X_i^m\,(X_i^p - 1) = X_i^m \bmod I_p$$

and

$$\boldsymbol{X}^{\boldsymbol{e}} X_i^{p+m} = \boldsymbol{X}^{\boldsymbol{e}} X_i^{m+p} - \boldsymbol{X}^{\boldsymbol{e}} X_i^m\,(X_i^p - 1) = \boldsymbol{X}^{\boldsymbol{e}} X_i^m \bmod I_p$$

for any $m \in \mathbb{N}_0$. Hence, when calculating modulo I_p the components of the exponent of a monomial in $\mathbb{K}[\boldsymbol{X}]$ can be interpreted as elements of $\mathbb{F}_p$ and can likewise be replaced by their standard representative. Since $I_p \subset I_{\mathcal{C}}$ the assertion follows. ☐

Proposition 3.2. *Let $\mathcal{C}$ be an $[n,k]$ code with systematic generator matrix $\mathbf{G} = (g_{ij}) = (\boldsymbol{I}_k \mid \boldsymbol{M})$. Taking the lexicographic order $\succ$ on $\mathbb{K}[\boldsymbol{X}]$ with $X_1 \succ \ldots \succ X_n$, the code ideal $I_{\mathcal{C}}$ has the reduced Groebner basis*

$$\begin{aligned}\mathcal{G} = \{X_i - X_{k+1}^{p-g_{i,k+1}} X_{k+2}^{p-g_{i,k+2}} \cdots X_n^{p-g_{i,n}} \mid 1 \le i \le k\}& \\ \cup \{X_i^p - 1 \mid k+1 \le i \le n\}&.\end{aligned}$$

A proof can be found in [15]. By setting $\boldsymbol{m}_i = (0, \ldots, 0, p - g_{i,k+1}, p - g_{i,k+2}, \ldots, p - g_{i,n})$, $1 \le i \le k$, the above Groebner basis can be written as

$$\mathcal{G} = \{X_i - \boldsymbol{X}^{\boldsymbol{m}_i} \mid 1 \le i \le k\} \cup \{X_i^p - 1 \mid k+1 \le i \le n\}. \tag{6}$$

4. Local Rings and Standard Bases

Let $P = (p_1, \ldots, p_n)$ be a point in $\mathbb{K}^n$. Take the set of all rational functions f/g with $g(P) \ne 0$,

$$\mathcal{O}_P = \left\{ \frac{f}{g} \mid f, g \in \mathbb{K}[\boldsymbol{X}], g(P) \ne 0 \right\}.$$

Clearly, $\mathcal{O}_P$ is a subring of the field of rational functions $\mathbb{K}(\boldsymbol{X}) = \mathbb{K}(X_1, \ldots, X_n)$ containing $\mathbb{K}[\boldsymbol{X}]$. Let $\mathfrak{m}_P$ be the ideal generated by $\langle X_1 - p_1, \ldots, X_n - p_n\rangle$ in

$\mathcal{O}_P$. Then each element in $\mathcal{O}_P \setminus \mathfrak{m}_P$ is a unit in $\mathcal{O}_P$. It follows that $\mathfrak{m}_P$ is the only maximal ideal in $\mathcal{O}_P$. Thus $\mathcal{O}_P$ is a local ring in $\mathbb{K}(\boldsymbol{X})$.

Let I be a zero-dimensional ideal in $\mathbb{K}[\boldsymbol{X}]$ and let $\mathcal{V}(I) = \{P_1, \ldots, P_r\}$ be the corresponding zero set in $\mathbb{K}^n$. The *multiplicity* of a point $P \in \mathcal{V}(I)$ is the dimension of the quotient ring $\mathcal{O}_P / I\mathcal{O}_P$.

An order $>$ on the set of monomials $\boldsymbol{X}^{\boldsymbol{u}}$, $\boldsymbol{u} \in \mathbb{N}_0^n$, in $\mathbb{K}[\boldsymbol{X}]$ is called *local* if it satisfies the following: (1) $>$ is a total ordering, (2) $1 > X_i$ for all $1 \leq i \leq n$, and (3) $>$ is compatible with the multiplication of monomials. A simple example of a local order is the degree-anticompatible lexicographic order, *alex* for short, which first arranges by total degree such that lower degree terms precede higher degree terms, and which arranges monomials of the same degree lexicographically. Note that in opposition to monomial orders, local orders are not well-orderings.

Since for a given local order $>$ on the monomials in $\mathbb{K}[\boldsymbol{X}]$ every nonempty set of monomials has a maximal element under $>$, the *leading term*, $\text{LT}_>(f)$, of a non-zero polynomial $f \in \mathbb{K}[\boldsymbol{X}]$ can be defined as the largest involved term.

Each local order $>$ gives rise to a ring of fractions in the rational function field $\mathbb{K}(\boldsymbol{X})$. To see this, take the set

$$S = \{1 + g \in \mathbb{K}[\boldsymbol{X}] \mid g = 0, \text{ or } \text{LT}_>(g) < 1\}.$$

The set S is closed under multiplication, since if $\text{LT}_>(g) < 1$ and $\text{LT}_>(h) < 1$, then $(1+g)(1+h) = 1 + g + h + gh$ and $\text{LT}_>(g + h + gh) < 1$ by the definition of local order.

The localization of $\mathbb{K}[\boldsymbol{X}]$ with respect to the set S is the ring

$$\text{Loc}_>(\mathbb{K}[\boldsymbol{X}]) = S^{-1}\mathbb{K}[\boldsymbol{X}] = \left\{ \frac{f}{1+g} \mid f \in \mathbb{K}[\boldsymbol{X}], 1 + g \in S \right\}.$$

Note that S is contained in the set of units of $\mathcal{O}_{P=0}$ and so $\text{Loc}_>(\mathbb{K}[\boldsymbol{X}])$ is a subring of $\mathcal{O}_{P=0}$. However, the constants between numerator and denominator of a rational function $f/g \in \mathcal{O}_{P=0}$ can be arranged such that $f/g = f'/(1+g')$ for some $1 + g' \in S$. Hence, we have $\text{Loc}_>(\mathbb{K}[\boldsymbol{X}]) = \mathcal{O}_{P=0}$.

A local order $>$ on $\mathbb{K}[\boldsymbol{X}]$ can be naturally extended to $\text{Loc}_>(\mathbb{K}[\boldsymbol{X}])$. For each rational function $h = f/(1+g)$ in $\text{Loc}_>(\mathbb{K}[\boldsymbol{X}])$, define the *degree* of h as the degree of f and the *leading coefficient* and *leading monomial* of h as the leading coefficient and leading monomial of f, respectively.

Division in $\text{Loc}_>(\mathbb{K}[\boldsymbol{X}])$ can be accomplished by *Mora's division algorithm* [7]. In contrast to the (generalized) division algorithm the set of possible dividers for the reduction steps might be extended by the result of a previous reduction step. This is accomplished by using the *écart* of a polynomial, which is defined as $\operatorname{ecart}(f) = \deg f - \deg \mathrm{LT}_>(f)$ measuring how far a polynomial is away from being homogeneous [7, 9, 12]. The crucial difference is that for the reduction of a dividend p, an element f_k is chosen from the sequence of divisors $\mathcal{F}$ such that $\mathrm{LT}_>(f_k)$ divides $\mathrm{LT}_>(p)$ and $\operatorname{ecart}(f_k)$ is minimal. If $\operatorname{ecart}(f_k) > \operatorname{ecart}(p)$, then p is added to $\mathcal{F}$.

Termination is achieved either in this manner or by homogenization of the division process and introducing a monomial order which is compatible with homogenization and dehomogenization of polynomials [7, 8, 9]. In the following, we restrict our attention to ideals in $\mathrm{Loc}_>(\mathbb{K}[\boldsymbol{X}])$ that are generated by polynomials in $\mathbb{K}[\boldsymbol{X}]$. Let $>$ be a local order on $\mathbb{K}[\boldsymbol{X}]$ and let $\mathcal{F} = (f_1, \ldots, f_s)$ be an ordered sequence of non-zero polynomials in $\mathbb{K}[\boldsymbol{X}]$. Each rational function $f \in \mathrm{Loc}_>(\mathbb{K}[\boldsymbol{X}])$ can be written as

$$f = h_1 f_1 + \ldots + h_s f_s + r,$$

where $h_1, \ldots, h_s, r \in \mathrm{Loc}_>(\mathbb{K}[\boldsymbol{X}])$ such that $\mathrm{LT}_>(h_i f_i) \leq \mathrm{LT}_>(f)$ for all i with $h_i \neq 0$ and either $r = 0$ or $\mathrm{LT}_>(r) \leq \mathrm{LT}_>(f)$ and $\mathrm{LT}_>(r)$ is not divisible by $\mathrm{LT}_>(f_i)$, $1 \leq i \leq s$.

Mora's division algorithm allows to develop an analogue of Groebner bases for ideals in local rings. To see this, take a local order $>$ on $\mathrm{Loc}_>(\mathbb{K}[\boldsymbol{X}])$ and an ideal I in $\mathrm{Loc}_>(\mathbb{K}[\boldsymbol{X}])$. Define the *set of leading terms* of I, briefly $\mathrm{LT}_>(I)$, as the set of all leading terms of non-zero elements of I with respect to $>$ and the ideal of leading terms, $\langle \mathrm{LT}_>(I) \rangle$ for short, as the monomial ideal generated by the set of leading terms of I. A *standard basis* for I is a subset $\{g_1, \ldots, g_l\}$ of I such that

$$\langle \mathrm{LT}_>(I) \rangle = \langle \mathrm{LT}_>(g_1), \ldots, \mathrm{LT}_>(g_l) \rangle.$$

Standard bases are the analogues of Groebner bases for ideals in $\mathrm{Loc}_>(\mathbb{K}[\boldsymbol{X}])$ and several results carry over to the local situation. Each non-zero ideal in $\mathrm{Loc}_>(\mathbb{K}[\boldsymbol{X}])$ has a standard basis. Furthermore, the ideal membership problem for ideals generated by polynomials in a local ring is solved in the same way, i.e., for each rational function $f \in \mathrm{Loc}_>(\mathbb{K}[\boldsymbol{X}])$, the remainder upon division of f by the standard basis is zero if and only if f is in the ideal generated by the standard basis.

Standard bases for ideals generated by polynomials in local rings can be computed in the same way as Groebner bases [7]. Indeed, Buchberger's S-criterion and Buchberger's algorithm carry forward to the local situation. For this, the S-polynomials are calculated with respect to the local order and Mora's division algorithm is used for reduction. In particular, Buchberger's algorithm terminates in the local situation, since it does not require that the order used for the division procedure to be a well-ordering; it only applies the ascending chain condition to the chain of monomial ideals generated by the leading terms in the division process [6].

Standard bases can be used to compute the dimension of $\mathrm{Loc}_>(\mathbb{K}[\boldsymbol{X}])/I$ when this number is finite. For this, let $>$ be a local order on $\mathrm{Loc}_>(\mathbb{K}[\boldsymbol{X}])$ and let I be an ideal in $\mathrm{Loc}_>(\mathbb{K}[\boldsymbol{X}])$. A monomial $\boldsymbol{X}^{\boldsymbol{u}}$ in $\mathbb{K}[\boldsymbol{X}]$ is *standard* if $\boldsymbol{X}^{\boldsymbol{u}}$ is not contained in $\langle \mathrm{LT}_>(I)\rangle$. If there are only finitely many standard monomials, then

$$\dim \mathrm{Loc}_>(\mathbb{K}[\boldsymbol{X}])/I = \dim \mathrm{Loc}_>(\mathbb{K}[\boldsymbol{X}])/\langle \mathrm{LT}_>(I)\rangle.$$

For more basics on standard bases the reader may consult [7].

5. Standard Bases for Binary Linear Codes

Let $\mathcal{C}$ be a binary $[n,k]$ code. The code ideal $I_{\mathcal{C}}$ has a single zero $(1,\ldots,1)$ in the affine space over $\mathbb{F}_2$ (and over any field extension of $\mathbb{F}_2$) [14]. Rather than localizing at the maximal ideal $\langle X_1-1,\ldots,X_n-1\rangle$, we change coordinates to translate the point to the origin and conduct the computations there. The corresponding ideal is denoted by $I'_{\mathcal{C}}$.

In the following, for each set $J\subseteq\{1,\ldots,n\}$ let $\boldsymbol{X}_J=\prod_{j\in J}X_j$. In particular, $\boldsymbol{X}_\emptyset=1$.

Proposition 5.1. *In view of the negative degree (reverse) lexicographic order $>$ on $\mathbb{F}_2[\boldsymbol{X}]$, the ideal $I=I'_{\mathcal{C}}\mathrm{Loc}_>(\mathbb{F}_2[\boldsymbol{X}])$ in $\mathrm{Loc}_>(\mathbb{F}_2[\boldsymbol{X}])$ has the standard basis*

$$\mathcal{S}=\left\{X_i-\sum_{\substack{J\subseteq\mathrm{supp}(\boldsymbol{m}_i)\\ J\neq\emptyset}}\boldsymbol{X}_J \mid 1\le i\le k\right\}\cup\left\{X_i^2\mid k+1\le i\le n\right\}. \tag{7}$$

Set $g_i=X_i-\sum_{\substack{J\subseteq\mathrm{supp}(m_i)\\ J\neq\emptyset}}\boldsymbol{X}_J$ for $1\le i\le k$ and $g_i=X_i^2$ for $k+1\le i\le n$. Before proving this result we will make use of the following assertion.

Lemma 5.2. *The translated code $I'_{\mathcal{C}}$ can be written as*

$$I'_{\mathcal{C}}=\left\langle (X_i+1)+\prod_{j\in\mathrm{supp}(\boldsymbol{m}_i)}(X_j+1)\mid 1\le i\le k\right\rangle + \left\langle (X_i+1)^2+1\mid k+1\le i\le n\right\rangle.$$

Proof. In view of Proposition 3.2, the ideal $I_{\mathcal{C}}$ defined in (5) has the reduced Groebner basis (6) with respect to the lexicographic order on $\mathbb{K}[\boldsymbol{X}]$. This is an ideal basis of $I_{\mathcal{C}}$ in $\mathbb{K}[\boldsymbol{X}]$ for any order. But $\mathbb{K}[\boldsymbol{X}] \subset \mathrm{Loc}_{>}(\mathbb{K}[\boldsymbol{X}])$ and so this assertion immediately extends to $I_{\mathcal{C}}$ as an ideal in $\mathrm{Loc}_{>}(\mathbb{K}[\boldsymbol{X}])$. Thus by taking $p = 2$, the claim for the translated ideal follows. $\square$

We can now prove Proposition 5.1.

Proof. First, we show that the polynomials in $\mathcal{S}$ generate $I'_{\mathcal{C}}$. Cleary, we have $\mathcal{S} \subseteq I'_{\mathcal{C}}$ because $(X_i+1)^2+1 = X_i^2+1+1 = X_i^2$ for $k+1 \leq i \leq n$, and

$$(X_i+1) + \prod_{j \in \mathrm{supp}(\boldsymbol{m}_i)} (X_j+1) = X_i + 1 + \sum_{J \subseteq \mathrm{supp}(\boldsymbol{m}_i)} \boldsymbol{X}_J = X_i + \sum_{\substack{J \subseteq \mathrm{supp}(\boldsymbol{m}_i) \\ J \neq \emptyset}} \boldsymbol{X}_J$$

for $1 \leq i \leq k$. By Lemma 5.2, $\mathcal{S}$ is a generating set for $I'_{\mathcal{C}}$.

Second, we prove that $\mathcal{S}$ is a standard basis using Buchberger's criterion. For this, we consider three cases:

1. Let $k+1 \leq i < j \leq n$. Then $S(X_i^2, X_j^2) = X_j^2 X_i^2 - X_i^2 X_j^2 = 0$.

2. Let $1 \leq i \leq k$ and $k+1 \leq m \leq n$. Then

$$S(X_i - \sum_{\substack{J \subseteq \mathrm{supp}(\boldsymbol{m}_i) \\ J \neq \emptyset}} \boldsymbol{X}_J, X_m^2) = X_m^2 \sum_{\substack{J \subseteq \mathrm{supp}(\boldsymbol{m}_i) \\ J \neq \emptyset}} \boldsymbol{X}_J. \tag{8}$$

   Since J is a subset of $\{k+1, \ldots, n\}$, each term on the right-hand side cannot be divided by any g_j, $1 \leq j \leq k$. Furthermore, in every term of $\sum \boldsymbol{X}_J$ each variable appears with exponent of at most 1. Thus all terms are divisible only by g_m. It follows that the expression (8) is divided by $\mathcal{S}$ according to Mora's algorithm in such a way that in each step a reduction by $g_m = X_m^2$ is carried out leading to a zero remainder. Note that because of $\mathrm{ecart}(g_m) = 0$ no polynomial is added to the set of possible divisors during the division process.

3. Let $1 \leq i < j \leq k$. Then by Lemma 5.3, the S-polynomial

$$S(X_i - \sum_{\substack{J \subseteq \mathrm{supp}(\boldsymbol{m}_i) \\ J \neq \emptyset}} \boldsymbol{X}_J, X_j - \sum_{\substack{K \subseteq \mathrm{supp}(\boldsymbol{m}_j) \\ K \neq \emptyset}} \boldsymbol{X}_K)$$

   reduces to zero.

$\square$

In the following, we use a variant of Mora's division algorithm in which the set of divisors will not be increased during the division process. Note that if a polynomial is reduced to zero by this variant of Mora's algorithm, it will also be reduced to zero by Mora's original algorithm.

Lemma 5.3. *In view of the negative degree lexicographic order, the S-polynomial*

$$S(X_i - \sum_{\substack{J\subseteq \mathrm{supp}(\boldsymbol{m}_i)\\ J\neq\emptyset}} \boldsymbol{X}_J, X_j - \sum_{\substack{K\subseteq \mathrm{supp}(\boldsymbol{m}_j)\\ K\neq\emptyset}} \boldsymbol{X}_K)$$

is reduced to zero by $\mathcal{S}$ in $\left(2^{|\mathrm{supp}(\boldsymbol{m}_i)|}-1\right)+\left(2^{|\mathrm{supp}(\boldsymbol{m}_j)|}-1\right)$ steps.

Proof. Notice that the considered S-polynomial can be written as

$$\begin{aligned}
S(X_i - \sum \boldsymbol{X}_J, X_j - \sum \boldsymbol{X}_K) &= X_j \sum_{\substack{J\subseteq \mathrm{supp}(\boldsymbol{m}_i)\\ J\neq\emptyset}} \boldsymbol{X}_J + X_i \sum_{\substack{K\subseteq \mathrm{supp}(\boldsymbol{m}_j)\\ K\neq\emptyset}} \boldsymbol{X}_K \\
&= \underbrace{\left(X_j + \sum_{\substack{K\subseteq \mathrm{supp}(\boldsymbol{m}_j)\\ K\neq\emptyset}} \boldsymbol{X}_K\right)}_{=g_j} \sum_{\substack{J\subseteq \mathrm{supp}(\boldsymbol{m}_i)\\ J\neq\emptyset}} \boldsymbol{X}_J \\
&\quad + \underbrace{\left(X_i + \sum_{\substack{J\subseteq \mathrm{supp}(\boldsymbol{m}_i)\\ J\neq\emptyset}} \boldsymbol{X}_J\right)}_{=g_i} \sum_{\substack{K\subseteq \mathrm{supp}(\boldsymbol{m}_j)\\ K\neq\emptyset}} \boldsymbol{X}_K. \qquad (9)
\end{aligned}$$

Assume that $i < j$ and apply the above variant of Mora's division algorithm. Initialize

$$h_0 = X_j \sum_{\substack{J\subseteq \mathrm{supp}(\boldsymbol{m}_i)\\ J\neq\emptyset}} \boldsymbol{X}_J + X_i \sum_{\substack{K\subseteq \mathrm{supp}(\boldsymbol{m}_j)\\ K\neq\emptyset}} \boldsymbol{X}_K. \qquad (10)$$

Set $\mathrm{supp}(\boldsymbol{m}_i) = \{i_1, i_2, \ldots, i_{|\mathrm{supp}(\boldsymbol{m}_i)|}\}$, where $i_1 < i_2 < \cdots < i_{|\mathrm{supp}(\boldsymbol{m}_i)|}$, and $\mathrm{supp}(\boldsymbol{m}_j) = \{j_1, \ldots, j_{|\mathrm{supp}(\boldsymbol{m}_j)|}\}$, where $j_1 < \cdots < j_{|\mathrm{supp}(\boldsymbol{m}_j)|}$. Rewriting (10) into

$$h_0 = X_j \left(\sum_{s=1}^{|\mathrm{supp}(\boldsymbol{m}_i)|} \sum_{\substack{J\subseteq \mathrm{supp}(\boldsymbol{m}_i)\\ |J|=s}} \boldsymbol{X}_J\right) + X_i \left(\sum_{s=1}^{|\mathrm{supp}(\boldsymbol{m}_j)|} \sum_{\substack{K\subseteq \mathrm{supp}(\boldsymbol{m}_j)\\ |K|=s}} \boldsymbol{X}_K\right)$$

shows that the first $|\mathrm{supp}(\boldsymbol{m}_j)|$ leading terms are

$$X_i \boldsymbol{X}_{\{j_1\}}, X_i \boldsymbol{X}_{\{j_2\}}, \ldots, X_i \boldsymbol{X}_{\{j_{|\mathrm{supp}(\boldsymbol{m}_j)|}\}}.$$

So, in step ℓ, $1 \le \ell \le |\mathrm{supp}(\boldsymbol{m}_j)|$, the polynomial $h_{\ell-1}$ is reduced by g_i, i.e., the polynomial $\boldsymbol{X}_{\{j_\ell\}} g_i$ is added to $h_{\ell-1}$. Besides, the preceding reduction step cannot have produced another term which is greater than $X_i \boldsymbol{X}_{\{j_\ell\}}$ because all terms in $\boldsymbol{X}_{\{j_{\ell-1}\}} g_i$ except its leading term $X_i \boldsymbol{X}_{\{j_{\ell-1}\}}$, which cancels out, have total degree ≥ 2 and consist only of indeterminates smaller than X_i. Analogously, in step ℓ, $|\mathrm{supp}(\boldsymbol{m}_j)| + 1 \le \ell \le |\mathrm{supp}(\boldsymbol{m}_j)| + |\mathrm{supp}(\boldsymbol{m}_i)|$, the polynomial $h_{\ell-1}$ is reduced by g_j. So after $a_1 = |\mathrm{supp}(\boldsymbol{m}_j)| + |\mathrm{supp}(\boldsymbol{m}_i)|$ steps, we have

$$\begin{aligned} h_{a_1} &= X_j \left(\sum_{s=1}^{|\mathrm{supp}(\boldsymbol{m}_i)|} \sum_{\substack{J \subseteq \mathrm{supp}(\boldsymbol{m}_i) \\ |J|=s}} \boldsymbol{X}_J \right) + X_i \left(\sum_{s=1}^{|\mathrm{supp}(\boldsymbol{m}_j)|} \sum_{\substack{K \subseteq \mathrm{supp}(\boldsymbol{m}_j) \\ |K|=s}} \boldsymbol{X}_K \right) \\ &\quad + \sum_{j_\ell \in \mathrm{supp}(\boldsymbol{m}_j)} \mathbf{X}_{\{j_\ell\}} g_i + \sum_{i_\ell \in \mathrm{supp}(\boldsymbol{m}_i)} \boldsymbol{X}_{\{i_\ell\}} g_j \\ &= X_j \left(\sum_{s=2}^{|\mathrm{supp}(\boldsymbol{m}_i)|} \sum_{\substack{J \subseteq \mathrm{supp}(\boldsymbol{m}_i) \\ |J|=s}} \boldsymbol{X}_J \right) + X_i \left(\sum_{s=2}^{|\mathrm{supp}(\boldsymbol{m}_j)|} \sum_{\substack{K \subseteq \mathrm{supp}(\boldsymbol{m}_j) \\ |K|=s}} \boldsymbol{X}_K \right) \\ &\quad + \left(\sum_{j_\ell \in \mathrm{supp}(\boldsymbol{m}_j)} \boldsymbol{X}_{\{j_\ell\}} \sum_{\substack{J \subseteq \mathrm{supp}(\boldsymbol{m}_i) \\ J \ne \emptyset}} \boldsymbol{X}_J \right) \\ &\quad + \left(\sum_{i_\ell \in \mathrm{supp}(\boldsymbol{m}_i)} \boldsymbol{X}_{\{i_\ell\}} \sum_{\substack{K \subseteq \mathrm{supp}(\boldsymbol{m}_j) \\ K \ne \emptyset}} \boldsymbol{X}_K \right). \end{aligned}$$

But all terms of the last two parts in the sum with total degree of 2 cancel out, leaving

$$h_{a_1} = X_j \left(\sum_{s=2}^{|\mathrm{supp}(\boldsymbol{m}_i)|} \sum_{\substack{J \subseteq \mathrm{supp}(\boldsymbol{m}_i) \\ |J|=s}} \boldsymbol{X}_J \right) + X_i \left(\sum_{s=2}^{|\mathrm{supp}(\boldsymbol{m}_j)|} \sum_{\substack{K \subseteq \mathrm{supp}(\boldsymbol{m}_j) \\ |K|=s}} \mathbf{X}_K \right) \tag{11}$$

$$+\left(\sum_{j_\ell\in\operatorname{supp}(\boldsymbol{m}_j)}\boldsymbol{X}_{\{j_\ell\}}\sum_{\substack{J\subseteq\operatorname{supp}(\boldsymbol{m}_i)\\|J|\geq 2}}\boldsymbol{X}_J\right)$$
$$+\left(\sum_{i_\ell\in\operatorname{supp}(\boldsymbol{m}_i)}\boldsymbol{X}_{\{i_\ell\}}\sum_{\substack{K\subseteq\operatorname{supp}(\boldsymbol{m}_j)\\|K|\geq 2}}\boldsymbol{X}_K\right). \tag{12}$$

Obviously, the second part of h_{a_1} given by (12) consists of monomials whose total degree is greater than three involving only indeterminates greater than X_k. Thus all terms in the first part of h_{a_1} defined by (11) with total degree of three are greater than all terms in (12). Hence, the next $\binom{|\operatorname{supp}(\boldsymbol{m}_j)|}{2}$ leading terms of h_{a_1} are

$$X_i\boldsymbol{X}_{\{j_1,j_2\}},X_i\boldsymbol{X}_{\{j_1,j_3\}},\ldots,X_i\boldsymbol{X}_{\{j_1,j_{|\operatorname{supp}(\boldsymbol{m}_j)|}\}},X_i\boldsymbol{X}_{\{j_2,j_3\}},\ldots,X_i\boldsymbol{X}_{\{j_2,j_{|\operatorname{supp}(\boldsymbol{m}_j)|}\}},$$
$$X_i\boldsymbol{X}_{\{j_3,j_4\}},X_i\boldsymbol{X}_{\{j_3,j_5\}},\ldots,X_i\boldsymbol{X}_{\{j_{|\operatorname{supp}(\boldsymbol{m}_j)|-1},j_{|\operatorname{supp}(\boldsymbol{m}_j)|}\}}. \tag{13}$$

As before, the generator g_i is used in the reduction steps. If the current leading term is $X_i\boldsymbol{X}_{\{j_r,j_s\}}$, the polynomial $\boldsymbol{X}_{\{j_r,j_s\}}g_i$ is subtracted producing new terms that are greater than the terms in the list (13). To continue in this fashion, set $|\operatorname{supp}(\boldsymbol{m})|=\max\{|\operatorname{supp}(\boldsymbol{m}_i)|,|\operatorname{supp}(\boldsymbol{m}_j)|\}$ and $\bar\ell=\min\{|\operatorname{supp}(\boldsymbol{m}_i)|,|\operatorname{supp}(\boldsymbol{m}_j)|\}$, and put

$$a_\ell = \begin{cases}\sum_{s=1}^{\ell}\binom{|\operatorname{supp}(\boldsymbol{m}_j)|}{s}+\sum_{s=1}^{\ell}\binom{|\operatorname{supp}(\boldsymbol{m}_i)|}{s}, & \text{if } \ell\leq\bar\ell,\\ a_{\bar\ell}+\sum_{s=\bar\ell+1}^{|\operatorname{supp}(\boldsymbol{m})|}\binom{|\operatorname{supp}(\boldsymbol{m})|}{s}, & \text{if } \ell>\bar\ell.\end{cases}$$

Then after a_ℓ steps all polynomials of the form $\boldsymbol{X}_Kg_i$ and $\boldsymbol{X}_Jg_j$ with $|K|\leq\ell$ and $|J|\leq\ell$ have been added to h_0 during the reduction steps, i.e.,

$$h_{a_\ell}=X_j\left(\sum_{s=1}^{|\operatorname{supp}(\boldsymbol{m}_i)|}\sum_{\substack{J\subseteq\operatorname{supp}(\boldsymbol{m}_i)\\|J|=s}}\boldsymbol{X}_J\right)+X_i\left(\sum_{s=1}^{|\operatorname{supp}(\boldsymbol{m}_j)|}\sum_{\substack{K\subseteq\operatorname{supp}(\boldsymbol{m}_j)\\|K|=s}}\boldsymbol{X}_K\right)$$
$$+\sum_{\substack{K\subseteq\operatorname{supp}(\boldsymbol{m}_j)\\|K|\leq\ell}}\boldsymbol{X}_Kg_i+\sum_{\substack{J\subseteq\operatorname{supp}(\boldsymbol{m}_i)\\|J|\leq\ell}}\boldsymbol{X}_Jg_j$$
$$=X_j\left(\sum_{s=\ell+1}^{|\operatorname{supp}(\boldsymbol{m}_i)|}\sum_{\substack{J\subseteq\operatorname{supp}(\boldsymbol{m}_i)\\|J|=s}}\boldsymbol{X}_J\right)+X_i\left(\sum_{s=\ell+1}^{|\operatorname{supp}(\boldsymbol{m}_j)|}\sum_{\substack{K\subseteq\operatorname{supp}(\boldsymbol{m}_j)\\|K|=s}}\boldsymbol{X}_K\right)$$

$$+ \sum_{\substack{K\subseteq \mathrm{supp}(\boldsymbol{m}_j)\\ |K|\leq \ell}} \boldsymbol{X}_K \sum_{|J|>\ell} \boldsymbol{X}_J + \sum_{\substack{J\subseteq \mathrm{supp}(\boldsymbol{m}_i)\\ |J|\leq \ell}} \boldsymbol{X}_J \sum_{|K|>\ell} \boldsymbol{X}_K.$$

In this way, we arrive at

$$\begin{aligned} h_{s_{total}} &= h_0 + \sum_{s=1}^{|\mathrm{supp}(\boldsymbol{m}_j)|} \sum_{\substack{K\subseteq \mathrm{supp}(\boldsymbol{m}_j)\\ |K|=s}} \boldsymbol{X}_K g_i + \sum_{s=1}^{|\mathrm{supp}(\boldsymbol{m}_i)|} \sum_{\substack{J\subseteq \mathrm{supp}(\boldsymbol{m}_i)\\ |J|=s}} \boldsymbol{X}_J g_j \\ &= h_0 + \sum_{\substack{K\subseteq \mathrm{supp}(\boldsymbol{m}_j),\\ K\neq\emptyset}} \mathbf{X}_K g_i + \sum_{\substack{J\subseteq \mathrm{supp}(\boldsymbol{m}_i),\\ J\neq\emptyset}} \mathbf{X}_J g_j, \end{aligned} \tag{14}$$

where s_{total} denotes the total number of steps. Comparing (9) with (14) yields $h_{s_{total}} = h_0 + h_0 = 0$. Moreover, the total number of steps is

$$\begin{aligned} s_{total} = &\sum_{s=1}^{|\mathrm{supp}(\boldsymbol{m}_i)|} \binom{|\mathrm{supp}(\boldsymbol{m}_i)|}{s} + \sum_{s=1}^{|\mathrm{supp}(\boldsymbol{m}_j)|} \binom{|\mathrm{supp}(\boldsymbol{m}_j)|}{s} \\ &= \left(2^{|\mathrm{supp}(\boldsymbol{m}_i)|} - 1\right) + \left(2^{|\mathrm{supp}(\boldsymbol{m}_j)|} - 1\right). \end{aligned}$$

□

So far we have only considered binary linear codes. The situation is somewhat different when the underlying field $\mathbb{K}$ has characteristic $\neq 2$. If $\mathrm{char}(\mathbb{K}) = 0$, then the standard basis is $\mathcal{S} = \{X_1, \ldots, X_k, X_{k+1}, \ldots, X_n\}$ since $X_i \in I = I'_{\mathcal{C}}\mathrm{Loc}_>(\mathbb{F}_2[\boldsymbol{X}])$ for all $i = 1, \ldots, n$. This follows from the fact that $(X_i - p_i)^p - 1$ lies in I and can be written as a product of X_i and a unit in $\mathrm{Loc}_>(\mathbb{F}_2[\boldsymbol{X}])$, where the p_i denote the coordinates of the point translated to the origin.

Example 5.4. The binary [7,4] Hamming code $\mathcal{C}$ has the generator matrix

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

In terms of the negative degree lexicographic order on $\mathbb{F}_2[\boldsymbol{X}]$, the ideal $I = I'_{\mathcal{C}}\mathrm{Loc}_>(\mathbb{F}_2[\mathbf{X}])$ has the standard basis

$$\begin{array}{ll} X_5^2, & X_1 - X_5X_6X_7 - X_5X_6 - X_5X_7 - X_6X_7 - X_5 - X_6 - X_7, \\ X_6^2, & X_2 - X_5X_6 - X_5 - X_6, \\ X_7^2, & X_3 - X_5X_7 - X_5 - X_7, \\ & X_4 - X_6X_7 - X_6 - X_7. \end{array}$$

◇

References

[1] W. Adams and P. Loustaunau, *An Introduction to Groebner Bases*, American Mathematical Society (1994).

[2] T. Becker and V. Weispfenning, *Groebner Bases – A Computational Approach to Commutative Algebra*, Springer (1998).

[3] M. Borges-Quintana, M. Borges-Trenard, P. Fitzpatrick, and E. Martinez-Moro, Groebner bases and combinatorics for binary codes, *AAECC*, 19(5):393–411 (2008).

[4] B. Buchberger, *An Algorithm for Finding the Bases Elements of the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal*, PhD thesis, University of Innsbruck (1965).

[5] A. Cooper, Towards a new method of decoding algebraic codes using groebner bases, *Transactions 10th Army Conf. Appl. Math. Comp.*, 93:293–297, (1992).

[6] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms*, Springer (1996).

[7] D. Cox, J. Little, and D. O'Shea, *Using Algebraic Geometry*, Springer (1998).

[8] H.-G. Graebe, Algorithms in local algebra, *Journal of Symbolic Computation*, 19:545–557 (1995).

[9] G.-M. Greuel and G. Pfister, *A Singular Introduction to Commutative Algebra*, Springer, Berlin (2002).

[10] R. W. Hamming, Error detecting and error correcting codes, *The Bell System Technical Journal*, 29:147–160 (1950).

[11] F. MacWilliams and N. Sloane, *Error Correcting Codes*, North Holland, New York (1977).

[12] T. Mora, G. Pfister, and C. Traverso, An introduction to the tangent cone algorithm, *Advances in Computing Research*, 6:199–270 (1992).

[13] M. Sala, T. Mora, L. Perret, S. Sakata, and C. Traverso, *Groebner Bases, Coding, and Cryptography*, Springer, Berlin (2009).

[14] M. Saleemi and K.-H. Zimmermann, Syzygies and free resolutions of linear codes, *International Electronic Journal of Pure and Applied Mathematics*.

[15] M. Saleemi and K.-H. Zimmermann, Groebner bases for linear codes, *International Journal of Pure and Applied Mathematics*, 62:481–491 (2010).

[16] M. Saleemi and K.-H. Zimmermann, Linear codes as binomial ideals, *International Journal of Pure and Applied Mathematics*, 61:147–156 (2010).

[17] M. Saleemi and K.-H. Zimmermann, Groebner bases for a class of ideals in commutative polynomial rings, *International Journal of Pure and Applied Mathematics* (2011).

[18] B. Sturmfels, *Groebner Bases and Convex Polytopes*, American Mathematical Society (1996).

[19] J. van Lint, *Introduction to Coding Theory*, Springer, Berlin (1999).