International Journal of Pure and Applied Mathematics
Volume 84 No. 1 2013, 99-109
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: http://dx.doi.org/10.12732/ijpam.v84i1.7

COMPUTING GENERATING SETS FOR QUATERNARY CODES USING GRÖBNER BASES

Natalia Dück[1] §, Karl-Heinz Zimmermann[2]
[1,2]Hamburg University of Technology
Schwarzenbergstr. 95E, 21073 Hamburg, GERMANY

Abstract: Gröbner bases techniques can be used to compute a basis of a subspace of a finite-dimensional vector space over finite prime field given as a matrix kernel. Linear codes can be described as such subspaces and thus are an interesting area of application. Based on this, Gröbner bases techniques will be used to compute a generating set of a quaternary code given as a matrix kernel. In particular, if the quaternary code is free, the algorithm will provide a basis for the dual code.

AMS Subject Classification: 13P10, 94B60
Key Words: Gröbner basis, $\mathbb{Z}_4$-module, linear code, quaternary code, dual code

1. Introduction

During transmission through a noisy channel digital data are exposed to disturbances which can cause errors. Error-correcting codes provide means to detect and correct such errors by adding redundancy. The construction of such codes and the study of their key properties such as the number of codewords and the error-correcting capabilities are an active field of research. In particular, the link of certain families of codes to algebraic structures has enriched this field and has allowed both easier determination of their decoding properties and effi-

Received: November 28, 2012

§Correspondence author

cient decoders. In [5] the "Cooper philosophy" was born which established the first connection between linear codes and Gröbner bases.

Originating from commutative algebra Gröbner bases provide a uniform approach to solving a wide range of problems such as the solvability and solving algebraic systems of equations, ideal membership decision, and effective computation in residue class rings modulo polynomial ideals [1, 2, 6, 15]. Furthermore, they provide a powerful tool for tackling a wide range of problems in integer programming and invariant theory once these problems have been expressed in terms of sets of multivariate polynomials [4, 13, 16].

In [8] we presented an algorithm using Gröbner basis techniques to compute a basis for a finite-dimensional vector subspace over a finite prime field given as a matrix kernel. These considerations were motivated by the fact that linear codes can be described as such subspaces.

Although research is mainly devoted to the study of linear codes because of their nice structure as vector subspaces, there are certain families of non-linear codes containing more codewords than the known linear codes with the same lengths and error-correcting capabilites. These include the Nordstrom-Robinson, Kerdock, and Preparta codes [10, 12, 14]. In [9] it was shown that these codes can be easily constructed as binary images under the Gray map of linear codes over the integers modulo 4.

In this paper, we establish an algorithm using Gröbner bases techniques that provides a generating set for a $\mathbb{Z}_4$-module given as a matrix kernel. This algorithm is clearly of practical interest in conjuction with quaternary codes and particularly yields for a free quaternary code a basis for the dual code. Note that the major difference to the mentioned algorithm for computing a basis of a matrix kernel over a finite prime field is that the algorithm here requires a different lexicographic order to successfully compute a generating set.

This paper is organized as follows. The second section provides an introduction to Gröbner bases and quaternary codes. The third section contains the main results. The mentioned algorithm is presented and the link to quaternary codes is established. Finally, some examples are given.

2. Preliminaries

Throughout this paper, denote by $\mathbb{K}$ a field, by $\mathbb{Z}$ the ring of integers and by $\mathbb{N}_0$ the set of non-negative integers. Let $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ be the ring of integers modulo m and $\mathbf{e}_i$ the ith unit vector of length n in $\mathbb{Z}_m^n$, $1 \leq i \leq n$. Moreover, write the polynomial ring in n indeterminates $x_1, \ldots, x_n$ over $\mathbb{K}$ as $\mathbb{K}[\mathbf{x}] = \mathbb{K}[x_1, \ldots, x_n]$.

2.1. Gröbner Basics

The *monomials* in $\mathbb{K}[\mathbf{x}]$ are denoted by $\mathbf{x}^{\mathbf{u}} = x_1^{u_1} x_2^{u_2} \cdots x_n^{u_n}$ and are identified with the lattice points $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{N}_0^n$. The *degree* of a monomial $\mathbf{x}^{\mathbf{u}}$ is the sum $|\mathbf{u}| = u_1 + \cdots + u_n$ A *term* in $\mathbb{K}[\mathbf{x}]$ is a non-zero scalar times a monomial. A *polynomial* in $\mathbb{K}[\mathbf{x}]$ is a finite sum of terms and the *degree* of a polynomial is the maximal degree of the involved monomials.

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

Given a monomial order $\succ$, each non-zero polynomial $f \in \mathbb{K}[\mathbf{x}]$ has a unique *leading term*, denoted by $\mathrm{lt}_{\succ}(f)$ or simply $\mathrm{lt}(f)$, which is given by the largest involved term. The coefficient and the monomial of the leading term are called the *leading coefficient* and the *leading monomial*, respectively.

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

$$\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}(f) \mid f \in I \rangle. \tag{1}$$

A finite subset $\mathcal{G}$ of an ideal I in $\mathbb{K}[\mathbf{x}]$ is a *Gröbner basis* for I with respect to $\succ$ if the leading ideal of I is generated by the set of leading monomials in $\mathcal{G}$; i.e.,

$$\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}(g) \mid g \in \mathcal{G} \rangle. \tag{2}$$

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

A Gröbner basis for an ideal I in $\mathbb{K}[\mathbf{x}]$ with respect to a monomial order $\succ$ on $\mathbb{K}[\mathbf{x}]$ 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 yielding eventually a Gröbner basis, which can further be transformed into a reduced one. For more about Gröbner basics the reader may consult [1, 2, 6].

2.2. Quaternary Codes

A *quaternary code* $\mathcal{C}$ of length n is a linear block code over $\mathbb{Z}_4$, or in other words, an additive subgroup of $\mathbb{Z}_4^n$.

Two quaternary codes are *permutation-equivalent* if they have the same length and differ only by a permutation of coordinates. Every quaternary code is equivalent to one having a generator matrix of the form

$$G = \begin{pmatrix} I_{k_1} & A & B \\ \mathbf{0} & 2I_{k_2} & 2C \end{pmatrix}, \tag{3}$$

where I_k denotes the $k \times k$ identity matrix, A and C are matrices over $\mathbb{Z}_2$, and B is a matrix over $\mathbb{Z}_4$. A quaternary code $\mathcal{C}$ with the above *generator matrix* G is given as $\mathcal{C} = \{(a_1, a_2)G \mid a_1 \in \mathbb{Z}_4^{k_1}, a_2 \in \mathbb{Z}_2^{k_2}\}$ and is considered as a quaternary code of *type* $4k_1 + 2k_2$. Such a code is a free $\mathbb{Z}_4$-module if and only if $k_2 = 0$.

In $\mathbb{Z}_4^n$ we concretely have the inner product $\langle a, b\rangle = \sum_{i=1}^n a_i b_i$ for $a, b \in \mathbb{Z}_4^n$, which allows to define the *dual code* $\mathcal{C}^\perp$ for a code $\mathcal{C}$ to be the subset of $\mathbb{Z}_4^n$ consisting of the vectors that are orthogonal to all codewords in $\mathcal{C}$. But as the codewords of $\mathcal{C}$ are linear combinations of the rows of any of its generating matrices G, one easily sees that the dual code equals the kernel of G. More specifically, the dual code of the code $\mathcal{C}$ generated by the matrix G in (3) has the generator matrix

$$H = \begin{pmatrix} -B^T - C^T A^T & C^T & I_{n-k_1-k_2} \\ 2A^T & 2I_{k_2} & \mathbf{0} \end{pmatrix}. \tag{4}$$

The matrix H is then called the *parity check matrix* of $\mathcal{C}$. In particular, if $\mathcal{C}$ is a free quaternary code, its dual code $\mathcal{C}^\perp$ is also free. For more on quaternary codes consult [9, 11, 17].

3. Gröbner Bases and Code Duality

In [8] we provided an algorithm based on Gröbner basis techniques to compute a basis of the kernel of a matrix which has entries in a finite prime field. However, the problem of computing the kernel of such a matrix changes substantially when the matrix entries are considered as entries of a residue class ring $\mathbb{Z}_m$, where m is not prime. Then $\mathbb{Z}_m$ is a commutative ring containing zero divisors and the kernel of interest is a $\mathbb{Z}_m$-module, which is finitely generated but not necessarily has a basis.

This problem is of particular interest in the setting of quaternary codes. The dual code of a quaternary code generated by a matrix G equals the kernel of G. We will show that the algorithm in [8] can be adapted in a way that it yields a generator matrix of the dual code. Beforehand, some definitions are

required. In order to account for $m \equiv 0$ in $\mathbb{Z}_m$, we need the ideal

$$I_m(\mathbf{x}) = \langle x_i^m - 1 \,|\, 1 \leq i \leq n \rangle \,. \tag{5}$$

Let $G = (g_{ij})$ be a $k \times n$-matrix with entries in $\mathbb{Z}_m$. In the polynomial ring $\mathbb{K}[x_1,\ldots,x_k,v_1,\ldots,v_n,w_1,\ldots,w_n] = \mathbb{K}[\mathbf{x},\mathbf{v},\mathbf{w}]$ define the binomial ideal

$$J_G = \left\langle v_j - w_j \prod_{i=1}^{k} x_i^{g_{ij}} \mid 1 \leq j \leq n \right\rangle, \tag{6}$$

and the ideal

$$I_G = J_G + I_m(\mathbf{x}) + I_m(\mathbf{v}) + I_m(\mathbf{w}). \tag{7}$$

Note that the subsequent considerations hold for any field $\mathbb{K}$. Furthermore, take the mapping

$$\psi : \mathbb{K}[v_1,\ldots,v_n,w_1,\ldots,w_n] \to \mathbb{K}[x_1,\ldots,x_k][w_1,\ldots,w_n], \tag{8}$$

defined on the variables as

$$\psi(v_j) = w_j \prod_{i=1}^{k} x_i^{g_{ij}} \quad \text{and} \quad \psi(w_j) = w_j, \quad 1 \leq j \leq n, \tag{9}$$

and extended linearly such that it becomes a ring homomorphism. The kernel of the corresponding matrix G can then be characterised by the kernel of the map ψ according to the following result, which is a generalization of the one in [8].

Lemma 1. *If $\alpha,\alpha',\beta,\beta' \in \mathbb{Z}_m^n$ with $\alpha' - \alpha = \beta - \beta'$ in $\mathbb{Z}_m^n$, then $\alpha' - \alpha \in \ker(G)$ if and only if*

$$\psi(\mathbf{v}^{\alpha'}\mathbf{w}^{\beta'} - \mathbf{v}^{\alpha}\mathbf{w}^{\beta}) = 0 \ mod \ (I_m(\mathbf{x}) + I_m(\mathbf{v}) + I_m(\mathbf{w}))\,. \tag{10}$$

Proof. Using $\alpha' + \beta' = \alpha + \beta$ and performing all computations modulo $I_m(\mathbf{x}) + I_m(\mathbf{v}) + I_m(\mathbf{w})$, we obtain

$$\begin{aligned} \psi\left(\mathbf{v}^{\alpha'}\mathbf{w}^{\beta'} - \mathbf{v}^{\alpha}\mathbf{w}^{\beta}\right) &= \psi\left(\mathbf{v}^{\alpha'}\right)\mathbf{w}^{\beta'} - \psi\left(\mathbf{v}^{\alpha}\right)\mathbf{w}^{\beta} \\ &= \mathbf{w}^{\alpha'}\mathbf{x}^{G\alpha'}\mathbf{w}^{\beta'} - \mathbf{w}^{\alpha}\mathbf{x}^{G\alpha}\mathbf{w}^{\beta} \\ &= \mathbf{w}^{\alpha'+\beta'}\left(\mathbf{x}^{G\alpha'} - \mathbf{x}^{G\alpha}\right). \end{aligned}$$

Thus we have

$$\begin{aligned} \psi\left(\mathbf{v}^{\alpha'}\mathbf{w}^{\beta'} - \mathbf{v}^{\alpha}\mathbf{w}^{\beta}\right) = 0 \quad &\iff \quad \mathbf{x}^{G\alpha'} - \mathbf{x}^{G\alpha} = 0 \\ &\iff \quad G\alpha' = G\alpha \\ &\iff \quad G(\alpha' - \alpha) = 0. \end{aligned}$$

□

Note that according to [3, Prop. 1.4], the kernel of ψ can be written as

$$\ker(\psi) = J_G \cap \mathbb{K}[\mathbf{v}, \mathbf{w}]. \tag{11}$$

Consider the problem of computing a generator matrix for the dual code of a given quaternary code $\mathcal{C}$, which is expressed by a generator matrix G as in (3). We start with the case of $k_2 = 0$ in which the code as well as its dual are free modules and their respective generator matrices have the shape

$$G = \begin{pmatrix} I_k & B \end{pmatrix} \quad \text{and} \quad H = \begin{pmatrix} -B^T & I_{n-k} \end{pmatrix}, \tag{12}$$

where $k = k_1$. The following result provides the basis for Alg. 1.

Proposition 2. *Let $G \in \mathbb{Z}_4^{k\times n}$ be a block matrix of the form $\begin{pmatrix} I_k & B \end{pmatrix}$ and let $\mathcal{G}$ be a minimal Gröbner basis for the ideal I_G associated with G w.r.t. the lexicographic order given as*

$$x_1 \succ \ldots \succ x_k \succ v_n \succ v_{n-1} \succ \ldots \succ v_1 \succ w_1 \succ \ldots \succ w_n.$$

Then a basis for the kernel of G is given by the $(n-k)$-set

$$\begin{aligned} \mathcal{H} = \{\alpha \in \mathbb{Z}_4^n \mid v_i^{\alpha_i} - \mathbf{v}^{\alpha'}\mathbf{w}^{\alpha} \in \mathcal{G},\ \mathrm{lt}(v_i^{\alpha_i} - \mathbf{v}^{\alpha'}\mathbf{w}^{\alpha}) = v_i^{\alpha_i}, \\ \alpha = \alpha_i\mathbf{e}_i - \alpha',\ k+1 \le i \le n\}. \end{aligned} \tag{13}$$

Moreover, if $\mathcal{G}$ is a reduced Gröbner basis for I_G, then the elements of the set $\mathcal{H}$ are exactly the row vectors of the matrix $H = \begin{pmatrix} -B^T & I_{n-k} \end{pmatrix}$.

Proof. In [8] it has been shown that a set of the shape

$$\begin{aligned} \mathcal{H}' = \left\{\alpha \in \mathbb{Z}_p^n \mid v_i^{\alpha_i} - \mathbf{v}^{\alpha'}\mathbf{w}^{\alpha} \in \mathcal{G}',\ \mathrm{lt}(v_i^{\alpha_i} - \mathbf{v}^{\alpha'}\mathbf{w}^{\alpha}) = v_i^{\alpha_i}, \right. \\ \left. \alpha = \alpha_i\mathbf{e}_i - \alpha' \text{ for some } 1 \le i \le n\right\} \end{aligned} \tag{14}$$

is a generating set for the kernel of an arbitrary matrix G over $\mathbb{Z}_p$ regardless of whether p is prime or not, and where $\mathcal{G}'$ is the reduced Gröbner basis for the ideal I_G associated to G w.r.t. the lexicographic order defined as

$$x_1 \succ \ldots \succ x_k \succ v_1 \succ \ldots \succ v_n \succ w_1 \succ \ldots \succ w_n.$$

Note that this result differs from the assertion to be proved in two respects. First, by the chosen lexicographic order, i.e., $v_n \succ \ldots \succ v_1$ instead of $v_1 \succ \ldots \succ v_n$, and second that due to the form of G, the elements in the set (13) have a more concrete form.

In [8] even more has been shown, namely that the set (14) is a basis. However, this can only be guaranteed when p is prime because then $\mathbb{Z}_p$ is a field and the rows of a triangular matrix over a field are linearly independent. But in the module $\mathbb{Z}_4^n$, a set of vectors forming a triangular matrix can still be linearly dependent; e.g., when it contains a vector having only 0's and 2's as entries. Thus from the result in [8] it can be only deduced that the set (13) is a generating set.

It remains to show that the set $\mathcal{H}'$ (with $p = 4$) is linearly independent and has the described form in $\mathcal{H}$. For this, let $\mathcal{H}' = \{\alpha^{(1)}, \ldots, \alpha^{(s)}\}$, where $\alpha^{(i)} = (\alpha_1^{(i)}, \ldots, \alpha_{j_i}^{(i)}, 0, \ldots, 0)$ with rightmost nonzero entry $\alpha_{j_i}^{(i)}$ corresponds to the binomial $g_i = v_{j_i}^{\alpha_{j_i}^{(i)}} - \mathbf{v}^{\alpha^{(i)'}}\mathbf{w}^{\alpha^{(i)}}$ in $\mathcal{G}$, where $\alpha^{(i)'} = \alpha^{(i)} - \alpha_{j_i}^{(i)}\mathbf{e}_{j_i}$. One can assume that $j_1 < j_2 < \cdots < j_s$; these indices must be pairwise distinct since $\mathcal{G}$ is a minimal Gröbner basis.

Claim that $\alpha_{j_i}^{(i)} = 1$. Indeed, $GH^T = \mathbf{0}$ implies that every row of H lies in the kernel of G. Write the ith row of H as $\mathbf{h}_i = \mathbf{e}_{i+k} - (\mathbf{b}_i, 0, \ldots, 0)$, where $\mathbf{b}_i$ denotes the ith row of B^T. Then by Lemma 1, for each $1 \leq i \leq n-k$,

$$v_{i+k} - \mathbf{v}^{(\mathbf{b}_i,0,\ldots,0)}\mathbf{w}^{\mathbf{h}_i} \in \ker(\psi) \subseteq J_G \subseteq I_G,$$

where $\alpha' = \mathbf{e}_{i+k}$, $\alpha = (\mathbf{b}_i, 0, \ldots, 0)$, $\beta = \alpha' - \alpha$ and $\beta' = 0$ according to Lemma 1. Thus $v_{i+k} \in \langle \mathrm{lt}(I_G) \rangle$ and this proves the claim. Then the rightmost nonzero entries of the vectors in $\mathcal{H}'$ are all 1 and have pairwise distinct positions and so are linearly independent. But the rank of a free module is well-defined and so $s = n - k$ and $(j_1, j_2, \ldots, j_{n-k}) = (k+1, k+2, \ldots, n)$. This yields the shape as given in (13).

If $\mathcal{G}$ is reduced, we can conclude that for $1 \leq i \leq n-k$,

$$g_i = v_{i+k} - v_1^{\alpha_1^{(i)}} v_2^{\alpha_2^{(i)}} \cdots v_k^{\alpha_k^{(i)}} \mathbf{w}^{\alpha^{(i)}}, \tag{15}$$

i.e. the non-leading term of g_i contains only $v_1, v_2, \ldots, v_k$. In other words, if we arrange the elements of $\mathcal{H}$ as row vectors in a matrix, it will have the structure $\begin{pmatrix} A & I_{n-k} \end{pmatrix}$ for some matrix A of size $(n-k) \times k$. Comparing this with the already known generator matrix $\begin{pmatrix} -B^T & I_{n-k} \end{pmatrix}$ shows that $A = -B^T$. □

The above result provides a proof of correctness for Alg. 1. The major difference between this algorithm and the one presented in [8] lies in the chosen

monomial order. In the previous paper, the lexicographical order with $v_1 \succ \ldots \succ v_n$ gave rise to a generator matrix of the kernel in upper triangular form. Such a parity check matrix may not exist in the current setting. However, a generator matrix for the kernel exists such that the upper-right block is an identity matrix as given in (12). This motivates the choice of a lexicographic order with $v_n \succ v_{n-1} \succ \ldots \succ v_1$.

Algorithm 1 Gröbner basis algorithm for computing a basis for the dual code of a quaternary code

1. For a given generator matrix $G \in \mathbb{Z}_4^{k\times n}$ of the form (12) of a quaternary code $\mathcal{C}$ associate the ideal I_G defined as in (6)-(7).
2. Compute the minimal (or reduced) Gröbner basis $\mathcal{G}$ for I_G w.r.t. the lexicographic order given by $x_1 \succ \ldots \succ x_k \succ v_n \succ v_{n-1} \succ \ldots \succ v_1 \succ w_1 \succ \ldots \succ w_n$.
3. Read off the elements of the form $v_i^{\alpha_i} - \mathbf{v}^{\alpha'}\mathbf{w}^{\alpha}$ with $\alpha' = \alpha_i \mathbf{e}_i - \alpha$, $\alpha_i \neq 0$ and leading term $v_i^{\alpha_i}$, which give a basis for $\ker(G)$.

After considering the case of free modules, we turn to the general situation.

Proposition 3. *Let $G \in \mathbb{Z}_4^{k\times n}$ be a block matrix of the form (3) and let $H \in \mathbb{Z}_4^{n-k_1\times n}$ be the corresponding parity check matrix given by (4). Let $\mathbf{h}_j$, $1 \leq j \leq n-k_1$, denote the jth row of the matrix H. Applying Alg. 1 to the matrix G yields a parity check matrix H' of the same size as H, whose rows are*

$$\mathbf{h}'_j = \mathbf{h}_j + \sum_{i=1}^{k_2} a_{ji}\mathbf{h}_{n-k_1-k_2+i}, \quad 1 \leq j \leq n-k_1-k_2, \tag{16}$$

$$\mathbf{h}'_j = \mathbf{h}_j, \quad n-k_1-k_2+1 \leq j \leq n-k_1, \tag{17}$$

for some $a_{ij} \in \mathbb{Z}_2$.

Proof. Using the same arguments as in the proof of Prop. 2, we conclude that the resulting matrix whose row vectors generate the kernel of G has the block form

$$\begin{pmatrix} \tilde{A} & \tilde{B} & I_{n-k} \\ \tilde{C} & 2I_{k_2} & \mathbf{0} \end{pmatrix}.$$

By comparing this block matrix with the one in (4), it follows that $\tilde{C} = 2A^T$ and so the equations in (17) will hold. But then also the equations in (16) will be valid since arbitrary multiples of the last k_2 rows of H can be added to the first $n - k_1 - k_2$ rows without changing the row space. □

Finally, we will present two examples. Note that the computations of the Gröbner bases have been carried out with the computer algebra system `Singular` [7].

Example 1. Consider the free quaternary code $\mathcal{C}_1$ of type $4k_1$, $k_1 = 4$, with generator matrix

$$G = \begin{pmatrix} I_4 & B \end{pmatrix}, \quad B = \begin{pmatrix} 3 & 3 & 0 \\ 1 & 0 & 1 \\ 2 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}. \tag{18}$$

Using (12), the dual code is generated by the matrix

$$H = \begin{pmatrix} 1 & 3 & 2 & 3 & 1 & 0 & 0 \\ 1 & 0 & 0 & 3 & 0 & 1 & 0 \\ 0 & 3 & 0 & 3 & 0 & 0 & 1 \end{pmatrix}. \tag{19}$$

Applying Alg. 1 to the matrix G yields the polynomials

$$v_5 - v_1^3 v_2 v_3^2 v_4 w_1 w_2^3 w_3^2 w_4^3 w_5,\ v_6 - v_1^3 v_4 w_1 w_4^3 w_6,\ v_7 - v_2 v_4 w_2^3 w_4^3 w_7,$$

which (in matrix form) exactly correspond to the rows of the matrix H.

Example 2. Take the quaternary code $\mathcal{C}_2$ of type $4k_1 + 2k_2$ with $k_1 = 2$ and $k_2 = 2$, generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 3 & 2 & 1 \\ 0 & 1 & 0 & 1 & 2 & 0 & 1 \\ 0 & 0 & 2 & 0 & 2 & 2 & 0 \\ 0 & 0 & 0 & 2 & 2 & 0 & 2 \end{pmatrix}$$

and parity check matrix

$$H = \begin{pmatrix} \mathbf{h}_1 \\ \mathbf{h}_2 \\ \mathbf{h}_3 \\ \mathbf{h}_4 \\ \mathbf{h}_5 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 & 0 & 1 & 0 \\ 2 & 2 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 2 & 2 & 0 & 2 & 0 & 0 & 0 \end{pmatrix}.$$

Applying Alg. 1 yields a reduced Gröbner basis that contains the binomials

$$v_3^2 - w_3^2, \quad v_4^2 - v_1^2 v_2^2 w_1^2 w_2^2 w_4^2, \quad v_5 - v_1^2 v_2 v_3 v_4 w_1^2 w_2^3 w_3^3 w_4^3 w_5,$$
$$v_6 - v_1^2 v_3 w_1^2 w_3^3 w_6, \quad v_7 - v_4 w_4^3 w_7,$$

which are written in matrix form as

$$H' = \begin{pmatrix} 2 & 3 & 3 & 3 & 1 & 0 & 0 \\ 2 & 0 & 3 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 2 & 2 & 0 & 2 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} \mathbf{h}_1 + \mathbf{h}_4 + \mathbf{h}_5 \\ \mathbf{h}_2 + \mathbf{h}_4 \\ \mathbf{h}_3 + \mathbf{h}_5 \\ \mathbf{h}_4 \\ \mathbf{h}_5 \end{pmatrix}.$$

References

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

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

[3] A.M. Bigatti, L. Robbiano, Toric ideals, *Mathematica Contemporanea*, **21** (2001), 1-25.

[4] Pasqualina Conti, Carlo Traverso, Buchberger algorithm and integer programming, In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, Volume 539 of *Lecture Notes in Computer Science*, 130-139; Springer, Berlin-Heidelberg, 1991.

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

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

[7] G.-M. Pfister; H. Schönemann Decker, W. Greuel, SINGULAR 3-1-5 — A computer algebra system for polynomial computations, 2012, http://www.singular.uni-kl.de.

[8] N. Dück, K.-H. Zimmermann, A variant of the gröbner basis algorithm for computing hilbert bases, *International Journal of Pure and Applied Mathematics*, **81** (2012), 145-155.

[9] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Sole, The $\mathbb{Z}_4$-linearity of kerdock, preparata, goethals, and related codes, *IEEE Trans. Inform. Theory*, **40** (1994), 301-319.

[10] A.M. Kerdock, A class of low-rate nonlinear binary codes, *Information and Control*, **20** (1972), 182-187.

[11] R. Leppert, M. Saleemi, K.-H. Zimmermann, Groebner bases for quaternary codes, *International Journal of Pure and Applied Mathematics*, **71** (2011), 595-608.

[12] A.W. Nordstrom, J.P. Robinson, An optimal nonlinar code, *Information and Control*, **11** (1967), 613-616.

[13] L. Pottier, Minimal solutions of linear diophantine sytems: Bounds and algorithms, In: *RTA*, (1991), 162-173.

[14] F.P. Preparata, A class of optimum nonlinear double-error-correcting codes, *Information and Control*, **13** (1968), 378-400.

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

[16] B. Sturmfels, *Algorithms in Invariant Theory*, Springer, Wien, 2008.

[17] J.H. van Lint, *Introduction to Coding Theory*, Springer, Berlin, 1999.