

A Variant of the Gröbner Basis Algorithm for Computing Hilbert Bases

Natalia Dück¹ and Karl-Heinz Zimmermann²

^{1,2} Hamburg University of Technology

Hamburg 21073, GERMANY

Abstract

Gröbner bases can be used for computing the Hilbert basis of a numerical submonoid. By using these techniques, we provide an algorithm that calculates a basis of a subspace of a finite-dimensional vector space over a finite prime field given as a matrix kernel.

AMS Subject Classification: 13P10, 94B05

Key Words and Phrases: Gröbner basis, integer programming, monoid, Hilbert basis, linear code

1 Introduction

Gröbner bases provide a uniform approach to tackling a wide range of problems such as the solvability and solving algebraic systems of equations, ideal and radical membership decision, and effective computation in residue class rings modulo polynomial ideals [1, 2, 6, 12].

Furthermore, Gröbner basis techniques are not only a powerful tool for the algorithmic solution of some fundamental problems in commutative algebra [4], they also provide means of solving a wide range of problems in integer programming and invariant theory once these problems have been expressed in terms of sets of multivariate polynomials [5, 10, 13]. One such problem is the computation of the Hilbert basis for a submonoid of the numerical monoid \mathbb{N}_0^n . This problem can be written in terms of polynomials and then be solved using Gröbner basis techniques [10]. Other elaborations of this method can be found in [7, 13].

In this paper we will establish an algorithm using Gröbner basis techniques that allows to calculate a basis for a subspace of a finite-dimensional vector space over a finite prime field given as a matrix kernel. This algorithm is based on the one for computing Hilbert bases proposed in [13] and is motivated by the fact that linear codes can be described as such subspaces [9, 14].

This paper is organized as follows. The first section provides an introduction to Gröbner bases, Hilbert bases and their construction for a submonoid of the numerical monoid \mathbb{N}_0^n , and linear codes. The second section contains the main theorem and a variant of the algorithm for computing a basis for a subspace of \mathbb{F}_p^n described as a matrix kernel, where p is a prime. The paper concludes with an example illustrating the algorithm and its application to linear codes.

2 Preliminaries

Throughout this paper, \mathbb{Z} denotes the ring of integers, \mathbb{N}_0 stands for the set of non-negative integers, \mathbb{K} denotes an arbitrary field, and $\mathbb{K}[\mathbf{x}] = \mathbb{K}[x_1, \dots, x_n]$ is the commutative polynomial ring in n indeterminates over \mathbb{K} .

2.1 Gröbner bases

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 $\mathbf{u} = (u_1, \dots, u_n) \in \mathbb{N}_0^n$. The *degree* of a monomial $\mathbf{x}^{\mathbf{u}}$ is the sum $|\mathbf{u}| = u_1 + \cdots + u_n$ and the degree of a polynomial f is the maximal degree of all monomials involved in f . A *term* in $\mathbb{K}[\mathbf{x}]$ is a scalar times a monomial.

Denote by $\mathbb{K}[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ the set of all polynomials given by monomials with exponents in \mathbb{Z}^n , which is called the *ring of Laurent polynomials*. Negative exponents can be overcome by introducing an additional indeterminate t . More precisely, we have

$$\mathbb{K}[x_1^{\pm 1}, \dots, x_n^{\pm 1}] \cong \mathbb{K}[x_1, \dots, x_n, t] / \langle x_1 x_2 \cdots x_n t - 1 \rangle. \quad (1)$$

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 $\text{lt}_\succ(f)$ or simply $\text{lt}(f)$, 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,

$$\langle \text{lt}(I) \rangle = \langle \text{lt}(f) \mid f \in I \rangle. \quad (2)$$

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} ; that is,

$$\langle \text{lt}(I) \rangle = \langle \text{lt}(g) \mid g \in \mathcal{G} \rangle. \quad (3)$$

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 $\text{lt}(g)$. 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 Monoids, Hilbert bases and their computation using Gröbner bases

A *monoid* is a set M together with a binary operation such that the operation is associative and M possesses an identity element. A *submonoid* of a monoid M is a subset of M that is closed under the operation and contains the identity element. For instance, the set \mathbb{N}_0^n together with component-wise addition and the zero vector forms a commutative monoid and each submonoid of it is called a *numerical monoid*.

A *Hilbert basis* of a submonoid K of \mathbb{N}_0^n is a minimal (with respect to inclusion) finite subset \mathcal{H} of K such that each element $k \in K$ can be written

as a sum $k = \sum_{h \in \mathcal{H}} c_h h$, where $c_h \in \mathbb{N}_0$. It is known that each numerical submonoid has a unique Hilbert basis [11].

Submonoids arise in various fields like integer programming. Such a problem is usually expressed in *standard form*:

$$\text{Minimize } \mathbf{c}^T \mathbf{x} \quad \text{such that } A\mathbf{x} = \mathbf{b}, \mathbf{x} \geq 0, \quad (4)$$

where $\mathbf{b} \in \mathbb{Z}^m$, $\mathbf{c} \in \mathbb{Z}^n$ and $A \in \mathbb{Z}^{m \times n}$ are given and a non-negative integer vector \mathbf{x} is to be found. The set of all integer vectors $\mathbf{x} \geq 0$ satisfying the constraint equation $A\mathbf{x} = \mathbf{b}$ is called the *feasible region*. Of interest here is the case $\mathbf{b} = \mathbf{0}$ because then the feasible region is the kernel of the matrix A , written $\ker(A)$, which is clearly a numerical submonoid. The problem is then to find a Hilbert basis of the submonoid $K = \ker(A)$ in \mathbb{N}_0^n , where $A = (a_{ij})$ is an $m \times n$ integer matrix.

Following [7] we present an algorithm that solves this problem by using Gröbner bases. This procedure can also be found in [10, 13].

The first step is to translate this problem into the realm of polynomials. To this end, we associate a variable x_i to every row of A , $1 \leq i \leq m$. Since entries of A can be negative integers, we have to consider the ring of Laurent polynomials. Furthermore, define the mapping

$$\psi : \mathbb{K}[v_1, \dots, v_n, w_1, \dots, w_n] \rightarrow \mathbb{K}[x_1^{\pm 1}, \dots, x_m^{\pm 1}][w_1, \dots, w_n] \quad (5)$$

on the variables first

$$\psi(v_j) = w_j \prod_{i=1}^m x_i^{a_{ij}} \quad \text{and} \quad \psi(w_j) = w_j, \quad 1 \leq j \leq n, \quad (6)$$

and then extend it such that it becomes a ring homomorphism. In view of the ideal

$$I_A = \left\langle w_j \prod_{i=1}^m x_i^{a_{ij}} - v_j \mid 1 \leq j \leq n \right\rangle \quad (7)$$

in $\mathbb{K}[x_1^{\pm 1}, \dots, x_m^{\pm 1}][v_1, \dots, v_n, w_1, \dots, w_n]$, we have by [3]

$$\ker(\psi) = I_A \cap \mathbb{K}[v_1, \dots, v_n, w_1, \dots, w_n]. \quad (8)$$

Using this notation and the polynomial ring in (1) instead of the ring of Laurent polynomials, we obtain the following assertion due to [13]:

Let \mathcal{G} be a Gröbner basis for I_A with respect to any monomial order for which $x_i \succ v_j$, $t \succ v_j$ and $v_j \succ w_i$ for all $1 \leq i \leq m$ and $1 \leq j \leq n$. A Hilbert basis for $K = \ker(A)$ is then given by

$$\mathcal{H} = \{\alpha \in \mathbb{N}_0^n \mid \mathbf{v}^\alpha - \mathbf{w}^\alpha \in \mathcal{G}\}. \quad (9)$$

A proof can be found in [13].

This result facilitates an algorithm for computing the Hilbert basis of a given submonoid $\ker(A)$, which is summarized by Algorithm 1.

Algorithm 1 Gröbner basis algorithm for computing a Hilbert basis.

1. Associate the ideal I_A defined in (7) to a given $m \times n$ integer matrix A .
 2. Compute the reduced Gröbner basis \mathcal{G} for I_A with respect to a monomial order with $x_i \succ v_j$, $t \succ v_j$ and $v_j \succ w_k$ for all $1 \leq i \leq m$ and $1 \leq j, k \leq n$.
 3. Read off the elements of the shape $\mathbf{v}^\alpha - \mathbf{w}^\alpha$, $\alpha \in \mathbb{N}_0^n$, which form a Hilbert basis for $\ker(A)$.
-

2.3 Linear Codes

Let \mathbb{F} be the finite field. A *linear code* \mathcal{C} of length n and dimension k over \mathbb{F} is the image of a one-to-one linear mapping $\phi : \mathbb{F}^k \rightarrow \mathbb{F}^n$, i.e., $\mathcal{C} = \psi(\mathbb{F}^k)$, where $k \leq n$. The code \mathcal{C} is an $[n, k]$ code and its elements are called *codewords*. In algebraic coding, the codewords are always written as row vectors.

A *generator matrix* for an $[n, k]$ code \mathcal{C} is a $k \times n$ matrix G whose rows form a basis of \mathcal{C} , i.e., $\mathcal{C} = \{\mathbf{a}G \mid \mathbf{a} \in \mathbb{F}^k\}$. The code \mathcal{C} is in *standard form* if it has a generator matrix in reduced echelon form $G = (I_k \mid M)$, where 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.

For an $[n, k]$ code \mathcal{C} over \mathbb{F} , the *dual code* \mathcal{C}^\perp is given by all words $\mathbf{u} \in \mathbb{F}^n$ such that $\langle \mathbf{u}, \mathbf{c} \rangle = 0$ for each $\mathbf{c} \in \mathcal{C}$, where $\langle \cdot, \cdot \rangle$ denotes the ordinary inner product. The dual code \mathcal{C}^\perp is an $[n, n-k]$ code. If $G = (I_k \mid M)$ is a generator matrix for \mathcal{C} , then $H = (-M^T \mid I_{n-k})$ is a generator matrix for \mathcal{C}^\perp . For each word $\mathbf{c} \in \mathbb{F}^n$, $\mathbf{c} \in \mathcal{C}$ if and only if $\mathbf{c}H^T = \mathbf{0}$. The matrix H is a *parity check matrix* for \mathcal{C} [9, 14].

3 A Gröbner basis algorithm for finding a Hilbert basis of a matrix kernel

In the following, let \mathbb{F}_p denote a finite field with p elements, where p is prime. We are interested in finding the Hilbert basis of the submonoid

$$K = \ker(H_p) \cap \mathbb{F}_p^n, \quad (10)$$

where H is an $m \times n$ integer matrix and $H_p = H \otimes_{\mathbb{Z}} \mathbb{F}_p$.

In other words, we are considering the case in which the numerical monoid \mathbb{N}_0^n is replaced by the vector space \mathbb{F}_p^n over the finite prime field \mathbb{F}_p . Then the submonoid K becomes a vector space and the Hilbert basis equals an ordinary basis in the sense of linear algebra. Clearly, the uniqueness property does no longer hold. Nevertheless, the Gröbner basis algorithm for finding a Hilbert basis as described in the previous section (see Algorithm 1) can be adapted to this situation in order to find *one* vector space basis.

Since p is congruent 0 in \mathbb{F}_p , the following additional ideal will be used

$$I_p(\mathbf{x}) = \langle x_i^p - 1 \mid 1 \leq i \leq n \rangle.$$

In this way, the exponents of the monomials can be treated as vectors in \mathbb{F}_p^n .

Let $H = (h_{ij})$ be an $m \times n$ -matrix with entries in \mathbb{F}_p and define the ideals

$$J_H = \left\langle v_j - w_j \prod_{i=1}^m x_i^{h_{ij}} \mid 1 \leq j \leq n \right\rangle \quad (11)$$

and

$$I_H = J_H + I_p(\mathbf{x}) + I_p(\mathbf{v}) + I_p(\mathbf{w}). \quad (12)$$

The homomorphism ψ defined in (5) and (6) can be used to detect elements in the kernel of H . However, all entries of H can be written (modulo p) as integers in $\{0, 1, \dots, p-1\}$ and so the Laurent polynomials become ordinary polynomials. Hence, the image of ψ lies in the polynomial ring $\mathbb{K}[x_1, \dots, x_m][w_1, \dots, w_n]$. Note that each non-zero vector $\alpha \in \mathbb{F}_p^n$ can be written as

$$\alpha = (0, \dots, 0, \alpha_i, \bar{\alpha}), \quad (13)$$

where $\alpha_i \in \mathbb{F}_p \setminus \{0\}$ and $\bar{\alpha} \in \mathbb{F}_p^{n-i}$. Furthermore, put

$$\alpha' = \alpha_i \mathbf{e}_i - \alpha = (0, \dots, 0, 0, -\bar{\alpha}), \quad (14)$$

where \mathbf{e}_i is the i th unit vector.

Lemma 1. *Let H be an $m \times n$ -matrix with entries in \mathbb{F}_p . For each non-zero element $\alpha \in \mathbb{F}_p^n$, we have*

$$\alpha \in \ker(H) \iff \psi(v_i^{\alpha_i} - \mathbf{v}^{\alpha'} \mathbf{w}^\alpha) = 0 \pmod{[I_p(\mathbf{x}) + I_p(\mathbf{v}) + I_p(\mathbf{w})]}.$$

Proof. All computations will be performed modulo $I_p(\mathbf{x}) + I_p(\mathbf{v}) + I_p(\mathbf{w})$. By the definition of ψ , we have

$$\begin{aligned} \psi(v_i^{\alpha_i} - \mathbf{v}^{\alpha'} \mathbf{w}^\alpha) &= w_i^{\alpha_i} \prod_{k=1}^m x_k^{h_{ki}\alpha_i} - \mathbf{w}^\alpha \cdot \mathbf{w}^{\alpha'} \prod_{i=1}^n \prod_{k=1}^m x_k^{h_{ki}\alpha'_i} \\ &= w_i^{\alpha_i} \left(\prod_{k=1}^m x_k^{h_{ki}\alpha_i} - \prod_{i=1}^n \prod_{k=1}^m x_k^{h_{ki}\alpha'_i} \right) \\ &= w_i^{\alpha_i} \left(\mathbf{x}^{H\mathbf{e}_i\alpha_i} - \mathbf{x}^{H\alpha'} \right). \end{aligned}$$

In the second equation, $\mathbf{w}^{\alpha'} \mathbf{w}^\alpha = \mathbf{w}^{\alpha'+\alpha} = \mathbf{w}^{\mathbf{e}_i\alpha_i} = w_i^{\alpha_i}$. Thus

$$\begin{aligned} \psi(v_i^{\alpha_i} - \mathbf{v}^{\alpha'} \mathbf{w}^\alpha) = 0 &\iff \mathbf{x}^{H\mathbf{e}_i\alpha_i} - \mathbf{x}^{H\alpha'} = 0 \\ &\iff H\mathbf{e}_i\alpha_i - H\alpha' = H(\mathbf{e}_i\alpha_i - \alpha') = H\alpha = 0 \\ &\iff \alpha \in \ker(H). \end{aligned}$$

□

Note that $\ker(\psi)$ is a toric ideal [3], which can be written as

$$\ker(\psi) = J_H \cap \mathbb{K}[\mathbf{v}, \mathbf{w}]. \quad (15)$$

Inspired by the assertion on Hilbert bases for numerical submonoids and based on the previous lemma, we obtain the following main result.

Theorem 2. *Let \mathcal{G} be a Gröbner basis for I_H defined as in (12) with respect to the lexicographical order with $x_1 \succ \dots \succ x_m \succ v_1 \succ \dots \succ v_n \succ w_1 \succ \dots \succ w_n$. Then a basis for $\ker(H)$ in \mathbb{F}_p^n is given by*

$$\mathcal{H} = \left\{ (0, \dots, 0, \alpha_i, \bar{\alpha}) \in \mathbb{F}_p^n \mid v_i^{\alpha_i} - \mathbf{v}^{\alpha'} \mathbf{w}^\alpha \in \mathcal{G}, \alpha' = \alpha_i \mathbf{e}_i - \alpha, \alpha_i \neq 0 \right\}.$$

Using this assertion, we can obtain an adapted version of Algorithm 1 for computing a basis for $\ker(H)$ as a subspace of \mathbb{F}_p^n (see Algorithm 2). For the proof of correctness, which comes hand in hand with the proof of Theorem 2, three facts will be required:

Algorithm 2 Gröbner basis algorithm for computing a basis for $\ker(H)$.

1. Associate the ideal I_H defined as in (12) to a given $m \times n$ -matrix H over \mathbb{F}_p .
 2. Compute the reduced Gröbner basis \mathcal{G} for I_H with respect to the lexicographical order with $x_1 \succ \dots \succ x_m \succ v_1 \succ \dots \succ v_n \succ w_1 \succ \dots \succ w_n$.
 3. Read off the elements of the form $v_i^{\alpha_i} - \mathbf{v}^{\alpha'} \mathbf{w}^\alpha$ with $\alpha' = \alpha_i \mathbf{e}_i - \alpha$ and $\alpha_i \neq 0$, which give a basis for $\ker(H)$.
-

1. The reduced Gröbner basis of a binomial ideal consists of binomials [8].
2. The ideal J_H contains no monomials.
3. The ideal J_H is prime and I_H resembles a prime ideal in the following sense: If $f, g \in k[\mathbf{x}, \mathbf{v}, \mathbf{w}]$ are polynomials such that each variable x_i involved in fg has an exponent of at most $p - 1$, i.e., the exponents of the monomials are written as elements in \mathbb{F}_p^n , then $fg \in I_H$ implies either $f \in I_H$ or $g \in I_H$.

The following proof is an adapted version of the one in [13]. Note that all subsequently performed calculations will be either in \mathbb{F}_p or modulo the ideal $I_p(\mathbf{x}) + I_p(\mathbf{v}) + I_p(\mathbf{w})$.

Proof. We need to show that the obtained set \mathcal{H} is a minimal spanning set. Assume that this is not the case. Then there must be a non-zero element $\beta \in \ker(H)$ that cannot be written as a linear combination of elements in \mathcal{H} . Choose an element β such that the monomial \mathbf{x}^β is minimal with respect to the chosen monomial order. Write $\beta = (0, \dots, 0, \beta_i, \bar{\beta})$, where $\beta_i \neq 0$ and $\bar{\beta} \in \mathbb{F}_p^{n-i}$. By Lemma 1, (15), and $\ker(\psi) \subset J_H$, we obtain

$$f = v_i^{\beta_i} - \mathbf{v}^{\beta'} \mathbf{w}^{\bar{\beta}} \in J_H.$$

Thus f can be reduced to zero on division by \mathcal{G} , since $J_H \subset I_H$. Hence by the definition of Gröbner bases, there must be a polynomial $g \in \mathcal{G}$ with $\text{lt}(g) = v_i^{\gamma_i}$ and $1 \leq \gamma_i \leq \beta_i$. Put $\delta = \beta_i - \gamma_i$. In view of the chosen elimination order and the fact that \mathcal{G} consists of binomials, it follows that g is of the form

$$g = v_i^{\gamma_i} - \mathbf{v}^{\gamma'} \mathbf{w}^\eta,$$

for some $\gamma' = (0, \dots, 0, -\bar{\gamma})$, where $\bar{\gamma} \in \mathbb{F}_p^{n-i}$, and $\eta \in \mathbb{F}_p^n$. But by Lemma 1, the Gröbner basis element g will vanish under ψ and so

$$\eta = \gamma_i \mathbf{e}_i + \gamma' =: \gamma.$$

Then we have

$$\begin{aligned} f - v_i^\delta \cdot g &= v_i^{\beta_i} - \mathbf{v}^{\beta'} \mathbf{w}^\beta - v_i^{\delta+\gamma_i} + v_i^\delta \mathbf{v}^{\gamma'} \mathbf{w}^\gamma \\ &= v_i^\delta \mathbf{v}^{\gamma'} \mathbf{w}^\gamma - \mathbf{v}^{\beta'} \mathbf{w}^\beta \\ &= \mathbf{v}^{(0 \dots 0 \delta - \bar{\gamma})} \mathbf{w}^{(0 \dots 0 \gamma_i \bar{\gamma})} - \mathbf{v}^{(0 \dots 0 0 - \bar{\beta})} \mathbf{w}^{(0 \dots 0 \beta_i \bar{\beta})} \\ &= \mathbf{v}^{(0 \dots 0 0 - \bar{\gamma})} \mathbf{w}^{(0 \dots 0 \gamma_i \bar{\gamma})} \left(v_i^\delta - \mathbf{v}^{(0 \dots 0 0 - \bar{\beta} + \bar{\gamma})} \mathbf{w}^{(0 \dots 0 \delta \bar{\beta} - \bar{\gamma})} \right) \\ &= \mathbf{v}^{\gamma'} \mathbf{w}^\gamma \left(v_i^\delta - \mathbf{v}^{-\beta' + \gamma'} \mathbf{w}^{\beta' - \gamma' + \delta \mathbf{e}_i} \right). \end{aligned}$$

Applying the previous stated facts 2 and 3 yields

$$v_i^\delta - \mathbf{v}^{-\beta' + \gamma'} \mathbf{w}^{\beta' - \gamma' + \delta \mathbf{e}_i} \in J_H.$$

Thus by Lemma 1, $\beta' - \gamma' + \delta \mathbf{e}_i \in \ker(H)$. But by the choice of g , $\delta < \beta_i$ and so $\mathbf{x}^{\beta' - \gamma' + \delta \mathbf{e}_i} \prec \mathbf{x}^\beta$. Hence by the selection of β , $\beta' - \gamma' + \delta \mathbf{e}_i$ can be written as a linear combination of elements in \mathcal{H} . The same holds for γ , since it lies in \mathcal{H} due to the choice of the corresponding Gröbner basis element g . But then

$$\beta = \beta' + \beta_i \mathbf{e}_i = \beta' + (\delta + \gamma_i) \mathbf{e}_i + \gamma' - \gamma' = (\beta' - \gamma' + \delta \mathbf{e}_i) + \gamma,$$

and so β can also be written as such a linear combination contradicting the choice of β and hence proving the assertion. \square

We conclude by giving an example illustrating applications to linear codes.

Example 1. Consider the [11, 6] ternary Golay code [9, 14] with the generator matrix $G = (I_6 \mid M)$, where

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 2 & 1 \\ 1 & 0 & 1 & 2 & 2 \\ 2 & 1 & 0 & 1 & 2 \\ 2 & 2 & 1 & 0 & 1 \\ 1 & 2 & 2 & 1 & 0 \end{pmatrix}.$$

Then a parity check matrix is

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

Applying Algorithm 2 for computing a basis of $\ker(H)$ yields the following polynomials belonging to the reduced Gröbner basis

$$\begin{aligned} v_6 &- v_7^2 v_8 v_9 v_{10}^2 w_6 w_7 w_8^2 w_9^2 w_{10}, \\ v_5 &- v_7 v_8 v_9^2 v_{11}^2 w_5 w_7^2 w_8^2 w_9 w_{11}, \\ v_4 &- v_7 v_8^2 v_{10}^2 v_{11} w_4 w_7^2 w_8 w_{10} w_{11}^2, \\ v_3 &- v_7^2 v_9^2 v_{10} v_{11} w_3 w_7 w_9 w_{10}^2 w_{11}^2, \\ v_2 &- v_8^2 v_9 v_{10} v_{11}^2 w_2 w_8 w_9^2 w_{10}^2 w_{11}, \\ v_1 &- v_7^2 v_8^2 v_9^2 v_{10}^2 v_{11}^2 w_1 w_7 w_8 w_9 w_{10} w_{11}. \end{aligned}$$

The Hilbert basis taken from these polynomials corresponds to the row vectors of the matrix G .

References

- [1] W. Adams and P. Loustanaunau. *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] A.M. Bigatti and L. Robbiano. Toric ideals. *Mathematica Contemporanea*, 21:1–25, 2001.
- [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] Pasqualina Conti and Carlo Traverso. Buchberger algorithm and integer programming. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 539 of *Lecture Notes in Computer Science*, pages 130–139. Springer Berlin / Heidelberg, 1991.

- [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] D. Eisenbud and B. Sturmfels. Binomial ideals. *Duke Mathematical Journal*, 84(1):1–45, 1996.
- [9] F.J. MacWilliams and N.J.A Sloane. *Error Correcting Codes*. North Holland, New York, 1977.
- [10] L. Pottier. Minimal solutions of linear diophantine systems: bounds and algorithms. In *RTA*, pages 162–173, 1991.
- [11] R. P. Stanley. *Enumerative Combinatorics*. Cambridge University Press, 1997.
- [12] B. Sturmfels. *Groebner Bases and Convex Polytopes*. American Mathematical Society, 1996.
- [13] B. Sturmfels. *Algorithms in Invariant Theory*. Springer, Wien, 2008.
- [14] J.H. van Lint. *Introduction to Coding Theory*. Springer, Berlin, 1999.