Gröbner Bases and Linear Codes over Prime Fields

Natalia Dück, Karl-Heinz Zimmermann
Hamburg University of Technology (Germany)

natalia.dueck@tuhh.de

Abstract

In this short paper, a link between Gröbner bases and linear codes over prime fields will be established by associating to each linear code the so-called code ideal which is a binomial ideal given as the sum of toric ideal and a non-prime ideal.

An algorithm using Gröbner basis techniques will be presented that computes a basis for a subspace of a finite-dimensional vector space over a finite prime field given as a matrix kernel which is an adaptation of the Gröbner basis based method used to calculate the Hilbert basis of a numerical submonoid. Furthermore, results concerning the universal Gröbner basis of the code ideals will be given. In particular, it will be shown that for binary codes the universal Gröbner basis consists of all binomials associated to codewords whose Hamming weight satisfies the Singleton bound and a particular rank condition. This will give rise to a new class of binary linear codes called Singleton codes.

Keywords

Linear code, Gröbner basis, universal Gröbner basis, binomial ideal, toric ideal

1 Introduction

Digital data are exposed to errors when transmitted through a noisy channel. But as receiving correct data is indispensable in many applications, error-correcting codes are employed to tackle this problem. By adding redundancy to the messages, errors can be detected and corrected. Since the late 1940's the study of such codes is an ongoing and important task.

Gröbner bases, on the other hand, are a powerful tool that has originated from commutative algebra providing a uniform approach to grasp a wide range of problems such as solving algebraic systems of equations, ideal membership, and effective computation in residue class rings modulo polynomial ideals [1, 2]. Additionally, Gröbner basis techniques also provide means of solving problems in integer programming and invariant theory.

Both disciplines can be linked by associating a linear code over a prime field with a binomial ideal given as the sum of a toric ideal and a non-prime ideal called code ideal. In this way, several concepts from the rich theory of toric ideals can be translated into the setting of code ideals. This idea stems from [4] and has already proven its value in the binary case as it allows for determining the error-corrrecting capabilities of a binary linear code.

In this short paper, some connections between Gröbner bases and linear codes over prime fields will be established. As a first application we will give an algorithm using Gröbner basis techniques which computes a basis for a subspace of a finite-dimensional vector space over a finite prime field given as a matrix kernel [5]. In fact, this algorithm is an adaptation of the Gröbner basis based method used to calculate the Hilbert basis of a numerical submonoid [10]. This is of particular interest in the context of linear codes over prime fields. Using this method a generator matrix for such a code can be computed that is described by its parity check matrix.

The second part is devoted to the universal Gröbner basis of the code ideal. Gröbner bases are an essential tool for utilizing ideals in computer algebra systems. But as Gröbner bases vary with the monomial order and distinct applications require different monomial orders, it is advantageous to know the universal Gröbner basis, i.e., a finite generating set of the ideal which is a Gröbner basis for all monomial orders. For toric ideals this problem has been solved and an algorithm for computing the universal Gröbner basis has been provided [9]. For the code ideal, however, this problem remains unsolved. To this end several concepts used in connection with toric ideals will be adapted. In particular, it will be shown that for binary linear codes the universal Gröbner basis can be completely described by a linear algebraic rank condition.

2 Computing Matrix Kernel oder so

Let $\mathcal{A}$ be an $m \times n$ matrix with entries in $\mathbb{Z}$ and denote by $\Lambda(\mathcal{A})$ its Lawrence lifting. For any $u \in \mathbb{Z}$ write $u^+ = \max\{u, 0\}$ and $u^- = \max\{-u, 0\}$ and for any vector $v \in \mathbb{Z}^n$ define v^+ and v^- componentwise. Clearly, $v = v^+ - v^-$, where $v^+, v^- \in \mathbb{N}_0^n$ have disjoint support.

It is well-known that the toric ideal $I(\mathcal{A})$ associated to the matrix $\mathcal{A}$ is generated by pure binomials $\mathbf{x}^{v^+} - \mathbf{x}^{v^-}$, where $v^+ - v^-$ belongs to $\ker_{\mathbb{Z}}(\mathcal{A})$, and that there is a bijection between pure binomials in $I(\mathcal{A})$ and $I(\Lambda(\mathcal{A}))$ by mapping $\mathbf{x}^u - \mathbf{x}^v$ to $\mathbf{x}^u\mathbf{y}^v - \mathbf{x}^v\mathbf{y}^u$. It follows that if $u \in \ker_{\mathbb{Z}}(\mathcal{A}) \cap \mathbb{N}_0$, then the binomial $\mathbf{x}^u - \mathbf{y}^u$ belongs to $I(\Lambda(\mathcal{A}))$ [3, 8, 9]. This gives the foundation for an algorithm computing the Hilbert basis of the submonoid $\ker_{\mathbb{Z}}(\mathcal{A}) \cap \mathbb{N}_0$ using Gröbner bases [10].

In the following, let $\mathbb{F}_p$ denote a finite field with p elements, where p is a prime. We will provide an adaptation of the above mentionend Hilbert basis algorithm for finding a basis of the subspace

$$\ker(H) := \ker(H_p) \subset \mathbb{F}_p^n, \tag{1}$$

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

In order to account for $p = 0$ in $\mathbb{F}_p$, the following 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

$$J_H = \left\langle v_j - w_j \prod_{i=1}^m x_i^{h_{ij}} \mid 1 \leq j \leq n \right\rangle \tag{2}$$

and

$$I_H = J_H + I_p(\mathbf{x}) + I_p(\mathbf{v}) + I_p(\mathbf{w}). \tag{3}$$

Furthermore, define the mapping $\psi : \mathbb{K}[v_1, \ldots, v_n, w_1, \ldots, w_n] \to \mathbb{K}[x_1, \ldots, x_m, w_1, \ldots, w_n]$ on the variables first

$$\psi(v_j) = w_j \prod_{i=1}^m x_i^{h_{ij}} \quad \text{and} \quad \psi(w_j) = w_j, \quad 1 \leq j \leq n, \tag{4}$$

and then extend it such that it becomes a ring homomorphism. Obviously, $\ker(\psi) = J_H \cap \mathbb{K}[\mathbf{v}, \mathbf{w}]$. This homomorphism can be used to detect elements in the kernel of H.

Lemma 2.1. *If $\alpha, \alpha', \beta, \beta' \in \mathbb{F}_p^n$ with $\alpha' - \alpha = \beta - \beta'$ in $\mathbb{F}_p^n$, then $\alpha' - \alpha \in \ker(H)$ if and only if*

$$\psi(\mathbf{v}^{\alpha'}\mathbf{w}^{\beta'} - \mathbf{v}^{\alpha}\mathbf{w}^{\beta}) = 0 \mod (I_p(\mathbf{x}) + I_p(\mathbf{v}) + I_p(\mathbf{w})) . \tag{5}$$

Indeed, this result also holds when the field $\mathbb{F}_p$ is replaced by $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$, where m is an arbitrary positive integer [6].

Note that each nonzero vector $\alpha \in \mathbb{F}_p^n$ can be written as $\alpha = (0, \ldots, 0, \alpha_i, \bar{\alpha})$, where $\alpha_i \in \mathbb{F}_p \setminus \{0\}$ and $\bar{\alpha} \in \mathbb{F}_p^{n-i}$. Put $\alpha' = \alpha_i \mathbf{e}_i - \alpha = (0, \ldots, 0, 0, -\bar{\alpha})$, where $\mathbf{e}_i$ is the ith unit vector.

Theorem 2.2. *Let $\mathcal{G}$ be a Gröbner basis for I_H w.r.t. the lexicographical order with $x_1 \succ \ldots \succ x_m \succ v_1 \succ \ldots \succ v_n \succ w_1 \succ \ldots \succ w_n$. Then a basis for $\ker(H)$ in $\mathbb{F}_p^n$ is given by*

$$\mathcal{H} = \left\{ (0, \ldots, 0, \alpha_i, \bar{\alpha}) \in \mathbb{F}_p^n \mid v_i^{\alpha_i} - \mathbf{v}^{\alpha'}\mathbf{w}^{\alpha} \in \mathcal{G},\ \alpha' = \alpha_i \mathbf{e}_i - \alpha,\ \alpha_i \neq 0,\ 1 \leq i \leq n \right\}. \tag{6}$$

This result provides an algorithm for computing a basis of the matrix kernel over a finite prime field. Moreover, if this algorithm is applied to $\mathbb{Z}_m$ where m is not prime, it yields a module basis when $\ker(H)$ is a free $\mathbb{Z}_m$-module and a generating set in row reduced echelon form when it is not free.

There are several differences between this adaptation and the original method. First, Hilbert bases for submonoids are unique as opposed to bases for vector spaces. Thus in the first case, the unique Hilbert basis is computed. In the second case, however, a specific vector space basis is calculated, namely the one which is in reduced row echelon form with respect to the first m

columns. Indeed, changing the lexicographic order $x_1 \succ \ldots \succ x_m$ to $x_{i_1} \succ \ldots \succ x_{i_m}$ yields a basis in reduced row echelon form with respect to the columns $i_1, i_2, \ldots, i_m$.

Second, in the algorithm for computing the Hilbert basis the set $\mathcal{H}$ is constructed by selecting binomials of the form $\mathbf{v}^\alpha - \mathbf{w}^\alpha$ from the Gröbner basis which is justified by the fact that every pure binomial in the ideal $I(\Lambda(\mathcal{A}))$ has the shape $\mathbf{v}^\alpha \mathbf{w}^\beta - \mathbf{v}^\beta \mathbf{w}^\alpha$. However, adding the ideals $I_p(\mathbf{x}), I_p(\mathbf{v})$ and $I_p(\mathbf{w})$ produces an ideal which also contains pure binomials $\mathbf{v}^\alpha \mathbf{w}^\beta - \mathbf{v}^{\alpha'} \mathbf{w}^{\beta'}$ with $\alpha - \alpha' = \beta' - \beta$ but possibly $\alpha \neq \beta'$ and $\alpha' \neq \beta$ in $\mathbb{F}_p^n$.

Finally, the proposed method is rather unefficient when compared to other known methods from linear algebra since computation of Gröbner bases can be rather costly. Nevertheless it is of interest from the theoretical point of view because it demonstrates the extension to the finite module case.

3 Universal Gröbner Basis for the Code Ideal

For an $[n, k]$ code $\mathcal{C}$ over a prime field $\mathbb{F}_p$ define the associated *code ideal* to be

$$I_\mathcal{C} = \left\langle \mathbf{x}^c - \mathbf{x}^{c'} \mid c - c' \in \mathcal{C} \right\rangle + I_p(\mathbf{x}) \subset \mathbb{K}[x_1, \ldots, x_n], \tag{7}$$

where $\mathbb{K}$ is an arbitrary field. As in the previous section $I_p(\mathbf{x})$ allows to view the exponents of the monomials as vectors in $\mathbb{F}_p^n$. This ideal can be based on a toric ideal as follows,

$$I_\mathcal{C} = I_A + I_p(\mathbf{x}), \tag{8}$$

where A in an integral $n - k \times n$ matrix such that $H = A \otimes_\mathbb{Z} \mathbb{F}_p$ is a parity check matrix for $\mathcal{C}$. This shows that $I_\mathcal{C}$ is given as the sum of a toric ideal and a non-prime ideal.

Clearly, the ideal $I_\mathcal{C}$ is generated by pure binomials $\mathbf{x}^c - \mathbf{x}^{c'}$ with $c - c' \in \mathcal{C}$. Thus, in what follows binomials will always be considered to be pure. A binomial $\mathbf{x}^c - \mathbf{x}^{c'}$ in $I_\mathcal{C}$ is said to be associated to the codeword $c - c'$, but unlike for a toric ideal, there is more than one binomial associated to a codeword since the decomposition $c = c^+ - c^-$ is not unique. This is one of the main reasons why results concering toric ideals cannot be translated one-to-one to this setting.

In [9] the author has introduced several concepts in the context of toric ideals which will be utilized in the following. Because of the mentionend subtleties, however, several of these concepts need to be adapted.

A binomial $\mathbf{x}^c - \mathbf{x}^{c'}$ in $I_\mathcal{C}$ is called *primitive* if there is no other binomial $\mathbf{x}^u - \mathbf{x}^{u'}$ in $I_\mathcal{C}$ such that $\mathbf{x}^u$ divides $\mathbf{x}^c$ and $\mathbf{x}^{u'}$ divides $\mathbf{x}^{c'}$. If $\mathcal{C}$ is a binary code then we additionally require $c' \neq \mathbf{0}$. The *Graver basis* for $\mathcal{C}$ consists of all primitive binomials lying in the corresponding code ideal and is denoted by $\mathrm{Gr}_\mathcal{C}$.

A binomal $\mathbf{x}^c - \mathbf{c}^{c'}$ in $I_\mathcal{C}$ is called a *circuit* if it is a primitive binomial and its support is minimal with respect to inclusion. Denote by $\mathrm{C}_\mathcal{C}$ the set of all circuits of the ideal $I_\mathcal{C}$. Finally, denote the universal Gröbner basis by $\mathcal{U}_\mathcal{C}$.

The binary and non-binary case differ substantially. In the binary case, being a circuit is a property which only depends on the codeword associated to the binomial. To be more precise, the binomial $\mathbf{x}^c - \mathbf{x}^{c'}$ is a circuit if and only if the associated codeword $c - c'$ has minimal support w.r.t. inclusion. In other words, if one expansion $c = c^+ - c^-$ yields a circuit, then every expansion of c is a circuit and the same is true for being primitive. In the non-binary situation, however, this is not true as is illustrated next.

Example 1. *Consider the linear code $\mathcal{C}$ over $\mathbb{F}_7$ generated by $G = \begin{pmatrix} 1 & 0 & 4 \\ 0 & 1 & 1 \end{pmatrix}$ and the corresponding code ideal $I_\mathcal{C}$ in $\mathbb{Q}[a, b, c]$. The codeword $(2, 6, 0)$ has minimal support. Expanding $(2, 6, 0) = (2, 0, 0) - (0, 1, 0)$ gives the circuit $a^2 - b$. However, writing $(2, 6, 0) = (0, 6, 0) - (5, 0, 0)$ yields the binomial $b^6 - a^5$ which is not even primitive because $b^2 - a^4$ also belongs to $I_\mathcal{C}$.*

Proposition 3.1. *For a linear code $\mathcal{C}$ over $\mathbb{F}_p$, $\mathrm{C}_\mathcal{C} \subseteq \mathcal{U}_\mathcal{C} \subseteq \mathrm{Gr}_\mathcal{C}$.*

Note that the same inclusions are obtained for toric ideals [9]. For non-binary linear codes, these inclusions can be strict. For binary linear codes, however, all three sets coincide.

Theorem 3.2. *For a binary linear code $\mathcal{C}$ the set of circuits $\mathrm{C}_\mathcal{C}$ equals the Graver basis $\mathrm{Gr}_\mathcal{C}$.*

For a binary $[n,k]$ code $\mathcal{C}$ one can even further describe all primitive binomials in the code ideal $I_{\mathcal{C}}$. If $\mathbf{x}^c - \mathbf{x}^{c'}$ is primitive, then $\mathrm{wt}(c-c') \leq n-k+1$ and for any generator matrix G of the code $\mathcal{C}$ the submatrix $G_{\underline{n}\setminus \mathrm{supp}(c-c')}$ has rank $k-1$. And the converse is also true, i.e., if c is a codeword of Hamming weight less than or equal to $n-k+1$ and such that $G_{\underline{n}\setminus \mathrm{supp}(c)}$ has rank $k-1$, then any binomial associated to c is primitive.

Theorem 3.3. *Let $\mathcal{C}$ be a binary $[n,k]$ code. The universal Gröbner basis for the corresponding code ideal $I_{\mathcal{C}}$ is given by the set*

$$\begin{aligned}\mathcal{U}_{\mathcal{C}} = &\left\{\mathbf{x}^c - \mathbf{x}^{c'} \mid c-c' \in \mathcal{C}, wt(c-c') \leq n-k+1, rk\left(G_{\underline{n}\setminus supp(c-c')}\right) = k-1\right\}\\ &\cup \left\{x_i^2 - 1 \mid 1 \leq i \leq n\right\}.\end{aligned}$$

In other words, the universal Gröbner basis for the code ideal consists of all binomials which correspond to codewords that satisfy the Singleton bound and a particular rank condition.

This result gives rise to a new class of binary linear codes whose codewords which fulfill the Singleton bound also satisfy the rank condition. A binary linear code $\mathcal{C}$ is called a *Singleton code* if each non-zero codeword c with Hamming weight $\leq n-k+1$ has the property that the submatrix $G_{\underline{n}\setminus \mathrm{supp}(c)}$ has rank $k-1$ for any generator matrix G for $\mathcal{C}$.

Singleton codes are the parity check codes, the MDS codes, the binary Golay code and its parity check extension, the Simplex codes, and the first order Reed-Muller codes and their duals. On the other hand, not all Hamming codes are Singleton.

References

[1] W. Adams and P. Loustaunau, ”An Introduction to Gröbner Bases”, American Mathematical Society, 1994

[2] D. Cox, J. Little and D. O’Shea, ”Using Algebraic Geometry”, Springer, 1998

[3] A. Bigatti and L. Robbiano, ”Toric Ideals”, Mathematica Contemporanea, vol. 21, p. 1-25, 2001

[4] M. Borges-Quintana, M.A. Borges-Trenard, P. Fitzpatrick and E. Martinez-Moro, ”Gröbner bases and combinatorics for binary codes”, AAECC, vol. 19 (5), p. 393-411, 2008

[5] N. Dück and K.-H. Zimmermann, ”A variant of the Gröbner basis algorithm for computing Hilbert bases”, IJPAM, vol. 81 (1), p. 145-155, 2012

[6] N. Dück and K.-H. Zimmermann, ”Computing generating sets for quaternary codes using Gröbner bases”, IJPAM, vol. 84 (1), p. 99-109, 2013

[7] N. Dück and K.-H. Zimmermann, ”Universal Gröbner bases for binary linear codes”, IJPAM, to appear

[8] M. Kreuzer and L. Robbiano, ”Computational Commutative Algebra 2”, Springer, 2005

[9] B. Sturmfels, ”Gröbner Bases and Convex Polytopes”, American Mathematical Society, 1996

[10] B. Sturmfels, ”Algorithms in Invariant Theory”, Springer, 2008