On the fan associated to a linear code

Natalia Dück, Irene Márquez-Corbella, Edgar Martínez-Moro

On the fan associated to a linear code*

Natalia Dück, Irene Márquez-Corbella and Edgar Martínez-Moro

Abstract We will show how one can compute all reduced Gröbner bases with respect to a degree compatible ordering for code ideals - even though these binomial ideals are not toric. To this end, the correspondence of linear codes and binomial ideals will be briefly described as well as their resemblance to toric ideals. Finally, we will hint at applications of the degree compatible Gröbner fan to the code equivalence problem.

Key words: Linear code, Gröbner basis, Gröbner fan

1 Introduction

The Gröbner fan of an ideal in the commutative polynomial ring consists of polyhedral cones indexing the different leading ideals and is thus the geometric collection of all reduced Gröbner bases for this ideal. One application of the Gröbner fan is the so-called Gröbner walk which is the conversion of Gröbner bases.

With the software system TiGERS in [5] (Toric Gröbner bases Enumeration by Reverse Search) an efficient alternative for computing the Gröbner fan has been provided for the special case of toric ideals. Indeed, by identifying a reverse search

Natalia Dück
Hamburg University of Technology, Germany e-mail: natalia.dueck@tuhh.de

Irene Márquez-Corbella
INRIA Saclay- École Polytechnique, France e-mail: irene.marquez-corbella@inria.fr

Edgar Martínez-Moro
Institute of Mathematics, University of Valladolid, Spain e-mail: edgar@maf.uva.es

* First author is partially supported by a grant of the Deutscher Akademischer Austauschdienst. Second and third authors are supported by the Spanish MINECO grant MTM2012-36917-C03-03.

tree on the cones of the Gröbner fan, a memory-less combinatorial Gröbner walk can be established that furthermore, requires no cost weight vectors.

Linear codes, on the other hand, can be linked to this whole subject by associating to each linear code a binomial ideal that encodes the information about the code in the exponents. This correspondence proved to be very beneficial as it provided new approaches to several well-known problems in coding theory. Almost all applications, however, require the computation of a degree compatible Gröbner basis.

In this work, it will be shown how methods from the software system TiGERS developed by Rekha R. Thomas (see [5]) can be modified in order to compute all reduced Gröbner bases with respect to a degree compatible ordering for code ideals - even though these binomial ideals are not toric. To this end, the correspondence of linear codes and binomial ideals will be briefly described as well as their resemblance to toric ideals. Finally, we will hint at applications of the degree compatible Gröbner fan to the code equivalence problem.

2 The degree compatible Gröbner fan

In this work we shall use the notion of Gröbner basis and the ideal associated to a linear code. Due to the restriction of the space we will not define what a Gröbner basis is, the reader can find a good introductory text for example in [3]. Also for simplicity we will restrict ourselves to binary linear codes even if all the computation could be done in general (see [7] for the ideal associated to a q-ary linear code).

Let $\mathbb{K}[\mathbf{x}]$ be the polynomial ring with variables $\mathbf{x} = x_1, \ldots, x_n$ and coefficients an arbitrary field $\mathbb{K}$. We will define the ideal associated to a binary linear code $\mathscr{C}$ of length n as

$$I = I(\mathscr{C}) = \langle \{ \mathbf{x}^{\Delta \mathbf{a}} - \mathbf{x}^{\Delta \mathbf{b}} \mid \mathbf{a} - \mathbf{b} \in \mathscr{C} \} \rangle \subseteq \mathbb{K}[\mathbf{x}],$$

where the operation Δ means substitute the $\bar{0}, \bar{1}$ elements in the binary field $\mathbb{F}_2$ by the corresponding $0, 1$ in the set of integers $\mathbb{Z}$. In this extended abstract the Δ will be omitted if no confusion arises to simplify the notation.

This binomial ideal has been proved valuable for several applications and captures the combinatorial properties of the code (see [6] and the references therein). Note that for those applications $\mathbb{K}$ can be the binary field, which is the usual election, and in this case we must explicitly mark which terms are the leading terms.

In this paper it shall be assumed that the leading term of a binomial is the one with coefficient 1 and the non leading term has coefficient -1. Abusing the notation if $\mathbb{K}$ is the binary field, since $1 \equiv -1$, this writing of the binomials will be assumed as a formal pointer (in [5] the leading terms were underlined).

Note also that the explicit knowledge of the underlying term order is not necessary. In fact, in all the following computations only the leading term of each binomial has to be known.

In the rest of the paper we will use the following notation and concepts from [5]:

- $\mathscr{G}_\succ(I)$ is the reduced Gröbner basis for the ideal I w.r.t. the monomial order $\succ$,
- $C_\succ(I)$ is the Gröbner cone corresponding to $\mathscr{G}_\succ(I)$.
- $T_\succ(I)$ is the reverse search tree for the ideal I as constructed in [5, Definition 2.5]

Note that in [5] the *complete* Gröbner fan is considered, i.e., the whole $\mathbb{R}^n$, since the considered toric ideals are homogeneous w.r.t. a certain grading. This is not the case for our code ideal and so here the Gröbner fan is considered only in $\mathbb{R}^n_+$.

Proposition 1. *[4] Let $\succ$ be a term order and $\mathbf{v} \in C_\succ(I)$. For any $\mathbf{u} \in \mathbb{R}^n$ holds*

$$\mathrm{lt}_\mathbf{u}(I) = \mathrm{lt}_\mathbf{v}(I) \quad \Longleftrightarrow \quad \mathrm{lt}_\mathbf{u}(g) = \mathrm{lt}_\mathbf{v}(g) \quad \forall\, g \in \mathscr{G}_\succ(I),$$

where $\mathrm{lt}_\mathbf{u}$ stands for the leading (initial) term (ideal) induced by the order $\succ$ given by the weight vector $\mathbf{u}$.

Note that it is a well known fact that a reduced Gröbner basis for an ideal I w.r.t. a certain monomial order is degree compatible if and only if the corresponding Gröbner cone contains the all-one vector $\mathbf{1}$. From a coding-theory point of view, degree compatible orderings are the ones one must analyze since the weight of a vector is translated on the degree of a monomial. In this sense degree compatible orderings provide us a test set for the code and therefore a gradient descent decoding algorithm, see [1]. The following proposition characterizes when there is a unique degree compatible Gröbner basis.

Proposition 2. *Let $\mathscr{G}$ be a reduced Gröbner basis for $I(\mathscr{C})$ w.r.t. a certain degree compatible ordering $\succ$. The Gröbner basis $\mathscr{G}$ is the only reduced degree compatible Gröbner basis for $I(\mathscr{C})$ if and only if*

$$\deg(\mathbf{x}^a) > \deg(\mathbf{x}^b) \quad \textit{for all} \quad \mathbf{x}^a - \mathbf{x}^b \in \mathscr{G}. \tag{1}$$

Proof. Assume that (1) holds but there is another Gröbner basis $\mathscr{G}'$ for $I(\mathscr{C})$ w.r.t. another degree compatible order $\succ'$. Since $\succ'$ is degree compatible, $\mathrm{lt}_{\succ'}(g) = \mathrm{lt}_\succ(g)$ for all $g \in \mathscr{G}$. And by Proposition 1 we see that $\mathrm{lt}_{\succ'}(I(\mathscr{C})) = \mathrm{lt}_\succ(I(\mathscr{C}))$ and thus, $\mathscr{G} = \mathscr{G}'$.

Or equivalently, we can argue that the all-one vector is in the interior of the cone $C_\succ(I(\mathscr{C}))$ and so clearly it cannot be contained in another cone in the Gröbner fan.

In order to show the other direction assume that (1) does not hold, i.e., there is at least one binomial $\mathbf{x}^a - \mathbf{x}^b$ in $\mathscr{G}$ such that $\deg(\mathbf{x}^a) = \deg(\mathbf{x}^b)$. Then $\mathbf{1} \notin \mathrm{Int}(C_\succ(I(\mathscr{C})))$ and in particular, there must be a neighbouring cone that also contains $\mathbf{1}$ and thus corresponds to a degree compatible ordering. □

In terms of the Gröbner fan the above proposition can also be expressed as follows: A reduced Gröbner basis $\mathscr{G}$ w.r.t. a degree compatible ordering is the only degree compatible Gröbner basis if and only if the all-one vector $\mathbf{1}$ lies in the interior of the Gröbner cone of $\mathscr{G}$.

We say that two binary linear codes $\mathscr{C}_1$ and $\mathscr{C}_2$ are *permutation equivalent* provided there is a permutation of coordinates which sends $\mathscr{C}_1$ to $\mathscr{C}_2$. In the same fashion two binomial degree compatible Gröbner bases are *permutation equivalent* if there is a permutation of the variables that transforms one into the other. There is a close relationship between code equivalence and the equivalence of the degree compatible Gröbner bases associated to their code ideals stated as follows: If the two degree compatible Gröbner bases are permutation equivalent so are the codes, unfortunately the converse is not true, given two permutation equivalent codes not all the degree compatible Gröbner bases are permutation equivalent (only two of them should be). The reader can see [2] for a proof of this discussion.

Indeed if one has only a unique degree compatible Gröbner basis for a given code (Proposition 2) checking permutation equivalence is reduced to checking if the two unique bases are permutation equivalent using the techniques in [2]. If this is not the case one needs to compute the whole set of degree compatible Gröbner bases which we call the *degree compatible Gröbner fan*. We will tackle this task in the following section.

3 Adapting the TiGERS strategy

We can adapt the TiGERS Algorithm in [5] for computing the degree compatible Gröbner fan for $I(\mathscr{C})$ as follows: We start with a degree compatible Gröbner basis (note that this basis can be computed by the algorithm stated in [2]). By Proposition 2 we can determine whether it is the only degree compatible Gröbner basis or not. If not, we flip only those facet binomials where both terms have the same degree and recompute the Gröbner basis. Unfortunately due the lack of space these steps can not be detailed in this extended abstract but they are showed in [5]. Lemma 1 below guarantees that we will always find at least one facet binomial where both terms have the same degree. Additionally, we can employ the *reverse search tree* defined in [5] for traversing the Gröbner cones that are degree compatible.

Lemma 1. *Let $\mathscr{G}$ be the reduced Gröbner basis for $I(\mathscr{C})$ w.r.t. a degree compatible ordering. If $\mathscr{G}$ is not the only degree compatible Gröbner basis, that is $\mathbf{1} \notin \mathrm{Int}(C(I(\mathscr{C})))$, then among all the facet binomials of $\mathscr{G}$ is at least one binomial $\mathbf{x}^{\alpha} - \mathbf{x}^{\beta}$ such that $\deg(\mathbf{x}^{\alpha}) = \deg(\mathbf{x}^{\beta})$.*

Proof. Let $\mathscr{G} = \left\{\mathbf{x}^{\alpha_i} - \mathbf{x}^{\beta_i} \mid 1 \leq i \leq j+k\right\}$ and order the binomials such that $\deg(\mathbf{x}^{\alpha_i}) > \deg(\mathbf{x}^{\beta_i})$ for $1 \leq i \leq j$ and $\deg(\mathbf{x}^{\alpha_i}) = \deg(\mathbf{x}^{\beta_i})$ for $1+j \leq i \leq j+k$.

Assume that all facet binomials are such that the degree of the leading term is strictly greater than the degree of the other term. Then the cone

$$C' = \left\{\mathbf{u} \in \mathbb{R}^n_+ \mid \alpha_i \cdot \mathbf{u} \geq \beta_i \cdot \mathbf{u} \text{ for all } 1 \leq i \leq j\right\}$$

equals the Gröbner cone $C(I(\mathscr{C}))$ of the Gröbner basis $\mathscr{G}$. But then $\mathbf{1} \in \mathrm{Int}(C') = \mathrm{Int}(C(I(\mathscr{C})))$, which is a contradiction. □

Lemma 2. *Let $\mathscr{G}_{new}$ be the reduced Gröbner basis obtained from $\mathscr{G}_{old}$ by flipping the facet binomial $\mathbf{x}^{\alpha}-\mathbf{x}^{\beta}$. Any new leading terms in $\mathscr{G}_{new}$, i.e., leading terms of $\mathscr{G}_{new}$ that do not appear in $\mathscr{G}_{old}$, are divisible by $\mathbf{x}^{\alpha}$.*

Proof. Any new leading terms arise from the Gröbner basis computation of the quasi-monomial ideal

$$T := \left\{\mathbf{x}^{\beta}-\mathbf{x}^{\alpha}\right\} \cup T', \quad T' := \left\{\mathbf{x}^{\alpha_i} \mid \mathbf{x}^{\alpha_i}-\mathbf{x}^{\beta_i} \in \mathscr{G}_{old}\right\}$$

that consists of the designated flipping binomial with changed leading term and all the other leading terms in $\mathscr{G}_{old}$. To be more precise, a new leading term arises from an S-polynomial of the form

$$S\left(\mathbf{x}^{\beta}-\mathbf{x}^{\alpha}, \mathbf{x}^{\alpha_i}\right) = \mathbf{x}^{\gamma}\mathbf{x}^{\alpha}, \quad \text{where } \mathbf{x}^{\gamma} = \operatorname{lcm}(\mathbf{x}^{\beta}, \mathbf{x}^{\alpha_i})/\mathbf{x}^{\beta},$$

which is not being reduced to zero by the elements in T. When computing a Gröbner basis, then this S-polynomial is either reduced to zero or its remainder on division by the set T is added to the Gröbner basis of T. We distinguish the following situations:

1. Neither $\mathbf{x}^{\beta}$ nor any monomial in T' divides $\mathbf{x}^{\gamma}\mathbf{x}^{\alpha}$: The monomial $\mathbf{x}^{\gamma}\mathbf{x}^{\alpha}$ cannot be further reduced and thus is being attached to the Gröbner basis of T.
2. A monomial in T' divides $\mathbf{x}^{\gamma}\mathbf{x}^{\alpha}$: The monomial $\mathbf{x}^{\gamma}\mathbf{x}^{\alpha}$ is being reduced to zero and thus, this S-polynomial results in no new term.
3. The monomial $\mathbf{x}^{\beta}$ divides $\mathbf{x}^{\gamma}\mathbf{x}^{\alpha}$: Since $\mathbf{x}^{\alpha}$ and $\mathbf{x}^{\beta}$ have disjoint support (see [1]), $\mathbf{x}^{\beta}$ has to divide $\mathbf{x}^{\gamma}$, the monomial $\mathbf{x}^{\gamma}\mathbf{x}^{\alpha}$ is reduced to

$$\mathbf{x}^{\gamma}\mathbf{x}^{\alpha} - \mathbf{x}^{\alpha}\frac{\mathbf{x}^{\gamma}}{\mathbf{x}^{\beta}}\left(\mathbf{x}^{\beta}-\mathbf{x}^{\alpha}\right) = \frac{\mathbf{x}^{\gamma}}{\mathbf{x}^{\beta}}\left(\mathbf{x}^{\alpha}\right)^2.$$

So, whenever the S-polynomial cannot be reduced to zero, we obtain a monomial which is divisible by $\mathbf{x}^{\alpha}$. □

Proposition 3. *$T_{\succ}(I(\mathscr{C}))$ is an acyclic directed graph with a unique sink that we will call the reverse search tree.*

Proof. We prove that $T_{\succ}(I(\mathscr{C}))$ is a tree by showing that there is no cycle in this construction. We show this by contradiction. For the other claims see the proof of [5, Theorem 2.6].

Assume that there is a cycle in the reverse search tree, say $\mathscr{G}_1 \longrightarrow \mathscr{G}_2 \longrightarrow \ldots \longrightarrow \mathscr{G}_{\ell} \longrightarrow \mathscr{G}_1$, where $\mathscr{G}_{i+1}$ is obtained from $\mathscr{G}_i$ by flipping along $\mathbf{x}^{\alpha_i}-\mathbf{x}^{\beta_i}$. Then $\mathscr{G}_i$ contains this binomial with leading term $\mathbf{x}^{\alpha_i}$ and $\mathscr{G}_{i+1}$ with leading term $\mathbf{x}^{\beta_i}$. Inspecting the cycle we see that the binomial $\mathbf{x}^{\alpha_1}-\mathbf{x}^{\beta_1}$ lies in $\mathscr{G}_1$ with leading term $\mathbf{x}^{\alpha_1}$ and appears in $\mathscr{G}_2$ with leading term $\mathbf{x}^{\beta_1}$. Then no binomial in $\mathscr{G}_2$ has the leading term $\mathbf{x}^{\alpha_1}$. However, as we arrive at $\mathscr{G}_1$ after ℓ flipping steps, we conclude that $\mathbf{x}^{\alpha_1}-\mathbf{x}^{\beta_1}$ must be inserted at some successive flipping step. Assume that this happens in the i_1th flipping process, $1 < i_1 \leq \ell$. Then by Lem. 2, $\mathbf{x}^{\alpha_1}$ is divisible by $\mathbf{x}^{\alpha_{i_1}}$. And since $\mathscr{G}_1$ is a Gröbner basis this implies that $\mathbf{x}^{\alpha_{i_1}}$ cannot be the leading term of any element in

$\mathscr{G}_1$; it must have been inserted as a new leading term during some preceding flipping step, say $i_2 < i_1$. By the same argument the monomial $\mathbf{x}^{\alpha_{i_1}}$ is divisible by $\mathbf{x}^{\alpha_{i_2}}$ and then $\mathbf{x}^{\alpha_{i_2}}$ cannot appear as the leading term of any element in $\mathscr{G}_1$. Continuing this process we get a decreasing sequence of indices $i_1 > i_2 > i_3 > \dots$ which eventually must terminate, say after k steps, i.e., $i_k = 1$. Then $\mathbf{x}^{\alpha_{i_k}} = \mathbf{x}^{\alpha_1}$ and from the divisibility relations $\mathbf{x}^{\alpha_{i_k}} \mid \mathbf{x}^{\alpha_{i_{k-1}}} \mid \dots \mid \mathbf{x}^{\alpha_{i_2}} \mid \mathbf{x}^{\alpha_{i_1}} \mid \mathbf{x}^{\alpha_1}$ we actually obtain equality of all leading terms of the flipping binomials. However, this is a contradiction. □

The following proposition states the discussion at the end of Section 2.

Proposition 4. *Two linear codes $\mathscr{C}_1$ and $\mathscr{C}_2$ are permutation-equivalent if and only if they have the same degree compatible Gröbner fan structure, i.e., there is permutation $\sigma \in S_n$ such that $\sigma(Gfan(\mathscr{C}_1)) = Gfan(\mathscr{C}_2)$, where $\sigma(Gfan(\mathscr{C}_1))$ means permuting the variables in each of the degree compatible Gröbner basis within the fan.*

Example 1. Consider two binary $[6,3]$ codes $\mathscr{C}_1$ and $\mathscr{C}_2$ with respective parity check matrices

$$H_1 = \begin{pmatrix} 1&1&0&0&0&0 \\ 0&0&1&1&0&0 \\ 0&0&0&0&1&1 \end{pmatrix}, H_2 = \begin{pmatrix} 1&1&1&1&1&1 \\ 0&0&0&1&0&1 \\ 0&1&0&1&0&0 \end{pmatrix}$$

In [2, Example 2 and 5] it is shown that these codes are not permutation-equivalent. Here, we show how the degree compatible Gröbner fans of both codes can be employed to show their non-equivalence. The degree compatible Gröbner fan for $\mathscr{C}_1$ consists of 8 Gröbner basis which are all of cardinality 6 (see Ex. 2). The Gröbner basis for $\mathscr{C}_2$ w.r.t. the grevlex basis is given by

$$\{x_3 - x_5, x_1 - x_5, x_4x_5 - x_2x_6, x_2x_5 - x_4x_6, x_2x_4 - x_5x_6\} \cup \{x_i^2 - 1 \mid i = 2,4,5,6\}$$

and consists of 9 elements. Thus, we can already conclude that these two codes cannot be permutation-equivalent.

Example 2. The reverse search tree $T_{\succ}(I(\mathscr{C}))$ for the binary $[6,3]$ code $\mathscr{C}_1$ from the previous example with $\succ$ being pure lex is given in Fig. 1.

And the Gröbner bases are (the flipping binomials are underlined)

$$\begin{aligned}
\mathscr{G}_1 &= \{x_1 - x_2, x_3 - x_4, x_5 - x_6, x_2^2 - 1, x_4^2 - 1, x_6^2 - 1\} \\
\mathscr{G}_2 &= \{x_1 - x_2, \underline{x_4 - x_3}, x_5 - x_6, x_2^2 - 1, x_3^2 - 1, x_6^2 - 1\} \\
\mathscr{G}_3 &= \{\underline{x_2 - x_1}, x_4 - x_3, x_5 - x_6, x_1^2 - 1, x_3^2 - 1, x_6^2 - 1\} \\
\mathscr{G}_4 &= \{x_1 - x_2, x_3 - x_4, \underline{x_6 - x_5}, x_2^2 - 1, x_4^2 - 1, x_5^2 - 1\} \\
\mathscr{G}_5 &= \{x_1 - x_2, \underline{x_4 - x_3}, x_6 - x_5, x_2^2 - 1, x_3^2 - 1, x_5^2 - 1\} \\
\mathscr{G}_6 &= \{\underline{x_2 - x_1}, x_4 - x_3, x_6 - x_5, x_1^2 - 1, x_3^2 - 1, x_5^2 - 1\} \\
\mathscr{G}_7 &= \{\underline{x_2 - x_1}, x_3 - x_4, x_6 - x_5, x_1^2 - 1, x_4^2 - 1, x_5^2 - 1\} \\
\mathscr{G}_8 &= \{\underline{x_2 - x_1}, x_3 - x_4, x_5 - x_6, x_1^2 - 1, x_4^2 - 1, x_6^2 - 1\}.
\end{aligned}$$

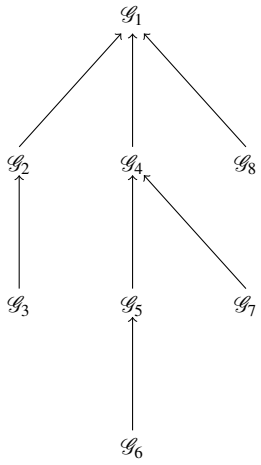

Fig. 1 The reverse search tree for $\mathscr{C}_1$

Conclusions

We have shown how the computation of the degree compatible Gröbner fan of a code is useful for determining the code equivalence problem. Anyway one can not forget that this is an NP-problem and therefore the Gröbner basis computation comprises a hard step. Further research in the topic points toward analyzing heuristic techniques for eliminating the need of transverse the whole fan or at least for trying to deduce the answer from partial information about the initial Gröbner basis.

References

1. Borges-Quintana, M., Borges-Trenard, M.A., Fitzpatrick, P., Martínez-Moro, E.: Gröbner bases and combinatorics for binary codes. Appl. Algebra Engrg. Comm. Comput. **19**(5), 393–411 (2008)
2. Borges-Quintana, M., Borges-Trenard, M.A., Martínez-Moro, E.: On a Gröbner bases structure associated to linear codes. J. Discrete Math. Sci. Cryptogr. **10**(2), 151–191 (2007)
3. Cox, D., Little, J., O'Shea, D.: Ideals, varieties, and algorithms: An introduction to computational algebraic geometry and commutative algebra. Undergraduate Texts in Mathematics. Springer-Verlag, New York, second edn. (1997)
4. Fukuda, K., Jensen, A.N., Thomas, R.R.: Computing Gröbner fans. Math. Comp. **76**(260), 2189–2212 (electronic) (2007)
5. Huber, B., Thomas, R.R.: Computing Gröbner fans of toric ideals. Experiment. Math. **9**(3), 321–331 (2000)
6. Márquez-Corbella, I., Martínez-Moro, E.: Algebraic structure of the minimal support codewords set of some linear codes. Adv. Math. Commun. **5**(2), 233–244 (2011)
7. Márquez-Corbella, I., Martínez-Moro, E., Suárez Canedo, E.: On the ideal associated to any linear code. Adv. Math. Commun. **-**(-), Submitted (2014)