COMPLETE GRÖBNER BASIS ASSOCIATED TO LATTICE CODES (EXTENDED ABSTRACT)

I. ÁLVAREZ-BARRIENTOS, M. BORGES-QUINTANA, M. A. BORGES TRENARD, E. MARTÍNEZ MORO, J. A. ORNELLA RODRÍGUEZ

Decoding within a lattice is an interesting problem nowadays, closely related to the well-known Close Vector Problem (CVP). In this work, an algorithm is proposed that computes an extended complete Gröbner basis of a label code of a lattice. This basis supports all term orderings associated with a total degree compatible ordering and it provides better information about de label code of the lattice. With that extended complete Gröbner basis of the label code, it is possible, via the monomial reduction it provides, to create an algorithm that obtains all the lattice vectors that are candidates for the solution of the CVP for a given vector.

1. Introduction

A *lattice* Λ is a discrete additive subgroup of $\mathbb{R}^n$. A lattice is spanned by integer linear combinations $\Lambda = \{k_1v_1 + \ldots + k_rv_r \mid k_i \in \mathbb{Z}\}$ of a given basis $\{v_1, \ldots, v_r\}$ $(r < n)$, where r is the rank of Λ. We will call B the matrix whose rows are the elements of a given basis of the lattice, i.e. $\Lambda = \{v = xB \mid x \in \mathbb{Z}^n\}$. The determinant of Λ is given by $\det(\Lambda) = (BB^t)^{1/2}$, note that if $m = n$ then $\det(\Lambda) = |\det(B)|$.

Consider a nested sequence of vector spaces $\{0\} \subset V_0 \subset V_1 \subset \ldots \subset V_n = \mathbb{R}^n$, where $\dim(V_i) = i$ and $Vi = V_{i-1} \oplus W_i$, $1 \leq i \leq n$. If $\Lambda \subset V_n$ is an n-dimensional lattice, the *cross sections* $\Lambda_{V_i} = \Lambda \cap V_i$ and $\Lambda_{W_i} = \Lambda \cap W_i$ have a lattice structure. We will denote the projection of Λ on W_i as $P_{W_i}(\Lambda)$. Let $G_i(\Lambda) = P_{W_i}(\Lambda)/\Lambda_{W_i}$ as groups, where $1 \leq i \leq n$, a *lattice code* L in Λ is just a subgroup of $\prod_{i=1}^{n} G_i(\Lambda)$. In [1] the following result is proposed to check whether a vector in the lattice is in a code or not.

Proposition 1.1 ([1])**.** *Let $c \in G = \mathbb{Z}/g_1\mathbb{Z} \times \cdots \times \mathbb{Z}/g_n\mathbb{Z}$ the group associated to the lattice Λ and L a lattice code in G. Then $c \in L$ if and only if $cP(\Lambda){V^*}^T \in \mathbb{Z}^r$, where V^* generates Λ^* (the dual lattice of Λ), r is the number of generators of V^* and $P(\Lambda) = \operatorname{diag}(\det(P_{W_1}(\Lambda)), \ldots, \det(P_{W_n}(\Lambda)))$.*

We will call *parity check matrix* of the code to the matrix $H = P(\Lambda){V^*}^T$. Let Λ be a lattice, and $\{v_1, \ldots, v_r\}$ be a generator set for Λ, L a label code, and $C(\Lambda) = \operatorname{diag}(\det(\Lambda_{W_1}), \ldots, \det(\Lambda_{W_n}))$. In a given coordinate system, $v \in \Lambda$ can be written as $v = kC(\Lambda)+cP(\Lambda)$ for $c \in L$ and $k \in \mathbb{Z}^n$; see [3]. We define the morphism $\Phi : \Lambda \mapsto L$ assigning to $v \in \Lambda$ the codeword $c \in L$. The set $\{\Phi(v_1), \ldots, \Phi(v_r)\}$ is a generator set of L; see [3, Section 3.D, p. 828].

2. Ideals associated with group codes

Let us assume that we have a group $G = \mathbb{Z}/g_1\mathbb{Z} \times \cdots \times \mathbb{Z}/g_n\mathbb{Z}$ and L a lattice code over G. We will develop our computations over the ring of polynomials

$\mathbb{K}[x_1, x_2, \ldots, x_n]$ where $\mathbb{K}$ is a field (note that any field will do since all the relevant information is given by the exponents of the monomials, thus usually $\mathbb{K} = \mathbb{F}_2$). We will introduce a setting that provides a general insight of those in [4, 5] given for binary codes and for linear codes in general; in [6] for codes over $\mathbb{Z}_m$; and in [1] for label codes of lattices.

Depending on the context, we will consider an element as a integer or as an element in the group G. For instance, in the monomial $x^{\mathbf{a}} = x_1^{a_1} x_1^{a_2} \cdots x_1^{a_n}$, $\mathbf{a}$ is a vector in $\mathbb{Z}^n_{\geq 0}$, while in $\mathbf{a} \in G$ each component a_i is the corresponding element in G_i. For $\mathbf{a} \in G$, $x^{\mathbf{a}}$ is the monomial such that the exponent of each variable is the corresponding a_i as an integer number, $0 \leq a_i \leq g_i - 1$. This abuse of notation can be solved introducing two cross characteristic functions as in [6], but we will avoid it to get a clearer notation. The support of $\mathbf{a}$ is $\mathrm{supp}(\mathbf{a}) = \{i \in 1, \ldots, n \mid a_i \neq 0\}$, in this case we say also that $x_i \in \mathit{supp}(x^{\mathbf{a}})$. There are three ways of associating an ideal with a code L.

$$I_{\equiv_L} = \langle \{x^{\mathbf{a}} - x^{\mathbf{b}} \mid \mathbf{a}, \mathbf{b} \in \mathbb{Z}^n_{\geq 0},\, \mathbf{a} - \mathbf{b} \in L\} \rangle \subseteq \mathbb{F}_2[x_1, x_2, \ldots, x_n]. \tag{1}$$

$$I_{L_1} = \langle \{x^{\mathbf{a}} - 1 \mid \mathbf{a} \in L\} \cup \{x_i^{g_i} - 1 \mid i = 1, \ldots, n\} \rangle \subseteq \mathbb{F}_2[x_1, x_2, \ldots, x_n]. \tag{2}$$

And if $L = \langle \{\mathbf{a}_1, \ldots, \mathbf{a}_k\} \rangle$,

$$I_{L_2} = \langle \{x^{\mathbf{a}_i} - 1 \mid i = 1, \ldots, n\} \cup \{x_i^{g_i} - 1 \mid i = 1, \ldots, n\} \rangle \subseteq \mathbb{F}_2[x_1, x_2, \ldots, x_n]. \tag{3}$$

The first one is a natural way of introducing a binomial ideal associated with L using the equivalence relation that determines L in G. The definition of an ideal associated with a linear code [5] is using $I_{\equiv_L}$ [1]; this was later seen in [6] for codes over $\mathbb{Z}_m$. On the other hand, I_{L_2} is used in [4] and [6] where is shown that is the same ideal as $I_{\equiv_L}$. In [1] I_{L_1} is used to define the ideal associated with a lattice by means of the label code of the lattice.

Proposition 2.1 ([2]). *Let $G = \mathbb{Z}_{g_1} \times \cdots \times \mathbb{Z}_{g_n}$ and L a subgroup of G. Then, the three ideals given above coincide.*

2.1. **Möller's algorithm for lattices.** We associate a Möller's like algorithm to lattices using an additive monoid structure for the lattice, for a detailed description see [5]. The main objects of it will be the following. Let $[X]$ denote the set of monomials in the variables $x_1, x_2, \ldots, x_n$, the injective linear morphism $\xi : [X] \mapsto \mathbb{R}^n$ associates to each monomial a vector in $\mathbb{R}^n$ as follows:

- let e_i be the ith coordinate vector of G, that is, $e_{ii} = 1_{\mathbb{Z}_{g_i}}$ and $e_{ij} = 0$ if $i \neq j$;
- $\xi(x_i) = \mathrm{frac}(e_i P(\Lambda) V^{*T})$, that is, $\xi(x_i) = \mathrm{frac}(e_i H)$, where $\mathrm{frac}(\cdot)$ represents the fractional part between 0 and 1 of the real number;
- $\xi(\prod_{i=1}^n x_i^{m_i}) = \mathrm{frac}(\sum_{i=1}^n (m_i \bmod g_i)\xi(x_i))$, that is, $\xi(\prod_{i=1}^n x_i^{m_i}) = \mathrm{frac}((\sum_{i=1}^n m_i\, e_i)H)$;
- let $\psi : [X] \mapsto G$ be an morphism of monoids such that $\psi(x_i) = e_i$ and extending the morphism of monoids naturally $\psi(u) = \psi(\prod_{i=1}^n x_i^{m_i}) = \sum_{i=1}^n m_i\, e_i$; we note that the relation between ξ and ψ is given by $\xi(u) := \psi(u)H$.

[1] To consider the non binary case in this definition, the linear code $\mathcal{C}$ has to be interpreted over $\mathbb{F}_q^n$, with $q = p^m$ and p a prime number, as the isomorphic monoid structure of the corresponding code over $\mathbb{F}_p^{mn}$.

The equivalence relation R_L that determines the code L over G, can be translated to $[X]$, given $x^{\mathbf{a}}, x^{\mathbf{b}} \in [X]$, $x^{\mathbf{a}} \equiv_L x^{\mathbf{b}}$ if and only if $(\psi(x^{\mathbf{a}}), \psi(x^{\mathbf{b}})) \in R_L$, that by Proposition 1.1 happens if and only if $(\psi(x^{\mathbf{a}}) - \psi(x^{\mathbf{b}}))H \in \mathbb{Z}^n$, that is if the fractional parts of $\psi(x^{\mathbf{a}})$ and $\psi(x^{\mathbf{a}})$ are equal.

By Proposition 2.1, we have that the ideal I_{L_1} associated to the lattice as in [1] is the ideal $I_{\equiv_L}$ which is related to the application of Möller's algorithm. From now on, we denote this ideal by I_L.

2.2. **Decoding.** Let $\prec$ be a total degree compatible ordering on $[X]$. Given $\mathbf{a} = (a_1, \ldots, a_n)$ in a group code G, we define the G-norm of $\mathbf{a}$ as $\|\mathbf{a}\|_G = a_1 + \ldots + a_n \in \mathbb{R}$ (see [1]).

Lemma 2.2. *Let $\mathbf{a}, \mathbf{c} \in G$ and $\mathbf{c} \prec \mathbf{a}$. If $\mathbf{a}$ is the nearest codeword to $\mathbf{c}$ w.r.t. $\prec$, then $\mathbf{a}$ is the closest codeword to $\mathbf{c}$ w.r.t. the G-norm.*

Let φ be a morphims relating a monomial and a group element in G, $\varphi : X \to G$ where $x^{\mathbf{a}} \mapsto (a_1 \bmod g_1, \ldots, a_n \bmod g_n)$.

Theorem 2.3. *Let L be a code over the group G, and G_L a Gröbner basis of L w.r.t. $\prec$. Let $\mathbf{a} \in G$ be an arbitrary vector and $x^{\mathbf{a}}$ its associated monomial, and $\mathbf{e} = \varphi(Can(x^{\mathbf{a}}, G_L))$. Then $\mathbf{c} = \mathbf{a} - \mathbf{e}$ is the closest codeword in L to $\mathbf{a}$ w.r.t. $\|.\|_G$.*

This result generalize those in [5, 4] in the context of group codes. On the othere hand, those vectors $\mathbf{a} \in G$ with smallest weight w.r.t. $\|.\|_G$ in a coset of G/L (coset leaders) are in correspondence with those monomials of smaller degree $x^{\mathbf{a}}$ w.r.t. $\equiv_L$.

3. Complete Gröbner basis

A *complete Gröbner basis* (GbC) w.r.t. $\prec$ associated to L, is a Gröbner basis for L such that if we change the order of the indeterminates it is still a a Gröbner basis for L w.r.t. $\prec$, in other words, a GbC is a Gröbner basis for any permutation of the variables keeping the same underlying ordering $\prec$. The *complete reduced Gröbner basis* (GbCr) is the union of all the reduced Gröbner basis associated to L w.r.t. all the possible orderings on the indeterminates (note that indeed it is a GbC also). It is clear that a binomial is in the GbCr if and only if it belongs to a reduced Gröbner basis for some ordering on the indeterminates.

Ther GbCr is given by all the binomials of the form $\mathbf{w} - \mathbf{w}'$ such that $\mathbf{w}'$ is the canonical form of $\mathbf{w}$. Constructing such a set has a great computational cost since not all the coset leaders are a canonical form for an ordering in the variables. In this section we will construct a GbC with similar properties to a GbCr by substituting the role of the canonical forms by the coset leaders. Let *CL(L)* the *set of coset leaders* w.r.t. $\|.\|_G$, where L is a lattice code.

Lemma 3.1. *Let $\mathbf{y} \in CL(L)$, if $\mathbf{y}' \in G$ and $y'_i = y_i$ for each $i \in \operatorname{supp}(\mathbf{y}')$, then $\mathbf{y}'$is also in $CL(L)$.*

Let $\mathbf{w} = x^{\mathbf{a}} \in [X]$, we say that it is an irredundant term if for each $i \in \operatorname{supp}(\mathbf{a})$ such that $\mathbf{w} = x^{\mathbf{b}} x_i$ then $\mathbf{b} \in CL(L)$. We will denote by $IT(L)$ the set of all irredundant terms. In other words,

$$x^{\mathbf{a}} \in IT(L) \Leftrightarrow (x^{\mathbf{a}} = x^{\mathbf{b}} x_i \Rightarrow \mathbf{b} \in CL(L)\ \forall x_i \in \operatorname{supp}(x^{\mathbf{a}})).$$

We will call *extended complete rduced Gröbner basis* (GbECr) to a GbC defined as follows

$$GbECr = \{x^{\mathbf{a}} - x^{\mathbf{b}} \mid x^{\mathbf{a}} \in IT(L), b \in CL(\mathbf{a}), \mathbf{a} \neq \mathbf{b}\}.$$

The following algorithm computes a GbECr.

Algorithm 1. Algorithm for computing GbECr
Input $\prec$ an ordering n, H for a given lattice code L.
Output $GC(I, \prec)$ GbECr of L.

$G \leftarrow \emptyset$, $List \leftarrow \{1\}$, $r \leftarrow 0$
while $List \neq \emptyset$ **do**
  $w \leftarrow NextTerm[List]$
  if if $w \in IT(L)$ **then**
    $c \leftarrow False$,
    $v' \leftarrow \xi(w)$,
    $(\Lambda, j) \leftarrow Member[v_0, v_1, ..., v_r]$,
    if $\Lambda = True$ **then**
      if $(deg(w_{j1}) \neq 0)$ and $(deg(w) = deg(w_{j1}))$ **then**
        $List \leftarrow InsertNext[w, List]$,
        $N_j \leftarrow N_j \cup \{w\}$,
        $c \leftarrow True$,
      end if
      for $i = 1$ to $Length[N_j]$ **do**
        $G \leftarrow G \cup \{w - w_{ji}\}$,
        if $c = True$ **then**
          $G \leftarrow G \cup \{w_{ji} - w\}$,
        end if
      end for
    else
      $r \leftarrow r + 1$,
      $v_r \leftarrow v'$,
      $w_{r1} \leftarrow w$, $N_r \leftarrow \{w_{r1}\}$,
      $List \leftarrow InsertNext[w_{r1}, List]$,
    end if
  end if
end while
Return G

where **InsertNext[w,List]** inserts the product $x\mathbf{w}$ for each $x \in \{x_1, \ldots, x_n\}$ in *List*, a list always ordered in increasing ordering w.r.t. $\prec$. The output of the instruction **Member**$[v_0, v_1, \ldots, v_r]$ has as first component TRUE if v_0 is in the syndrome list $(v_1, ..., v_r)$ or FALSE, in the other case. Its second component is the position of the syndrome when it is in the list. **N** is the list where we keep the coset leaders meanwhile they are found. **List** is a list where the multiples of the coset leaders are kept in increasing order w.r.t. $\prec$, i.e. the irredundant terms.

Due to the lack of space we can not show the proof of the correctness, but the following can be proven

Proposition 3.2. *(1) Let $x^{\mathbf{a}} \in [X]$ be a monomial. Then $\mathbf{a} \in CL(L)$ if and only if $x^{\mathbf{a}} \in List$ and $x^{\mathbf{a}} \in N$.*
(2) The algorithm computes the GbECr w.r.t. $\prec$ for the given lattice code L.

Remark 3.3 (On decoding)**.** *In Theorem 2.3 we find an element c such that $\|a-c\|_G$ is minimal. Thus reducing $x^{-\mathbf{a}}$ w.r.t. G_L, we have the following. If $\mathbf{e}' = \varphi(Can(X^{-\mathbf{a}}, G_L))$, then $\mathbf{c}' = -\mathbf{a} - \mathbf{e}'$ is a codeword in L and $\mathbf{c}_0 = -\mathbf{c}'$. Moreover, $\mathbf{c}_0$ is the nearest codeword in L to a and hence $\|\mathbf{c}_0 - \mathbf{a}\|_G$ is minimal. This is implemented in the following algorithm similar to the one in [1] but now we use a GbECr. It can be proven that it returns different optimal solutions w.r.t. the l_1-norm and therefore we can say that they are the candidates v such that $\|v-u\|_{l_1}$ is minimal for al given vector u.*

Algorithm 2. Nearest point in a Lattice
Input $u = (u_1, \ldots, u_n), C(\Delta), P(\Delta), G_L$, GbECr
Output $v = (v_1, \ldots, v_n)$

```
for i = 1, ..., rank(Δ) do
    k_i ← ⌊u_i/Δ_{W_i}⌋, R_i ← Remainder(u_i, |Δ_{W_i}|), r_i ← R_i/|P_{W_i}|, z_i ← ⌈r_i⌋,
end for
e ← φ(Red(X^z, G_L)),
if ‖e‖_G = 0 then c ← z,
else if ‖e‖_G = 1 then c ← z − e
else
    e' ← φ(Red(X^{-z}, G_L)), c_0 = z + e',
    if ‖e‖_G < ‖e'‖_G then c ← z − e
    else
        if ‖e‖_G = ‖e'‖_G then
            if d_l1(z, c) ≤ d_l1(z, c_0) then c ← z − e
            else c ← c_0
            end if
        else c ← c_0
        end if
    end if
end if
for i = 1, ..., rank(Δ) do
    v_i ← k_i|Δ_{W_i}| + c_i|P_{W_i}|
end for
```

Return $v = (v_1, \ldots, v_n)$

References

[1] Malihe Aliasgari, Mohammad-Reza Sadeghi, and Daniel Panario. Grobner bases for lattices and an algebraic decoding algorithm. *IEEE Transactions on Communications*, 61(4):1222–1230, 2013.

[2] Ismara Álvarez Barrientos, Mijail Borges-Quintana, Miguel Angel Borges-Trenard, and Daniel Panario. Computing Gröbner bases associated with lattices. *Adv. Math. Commun.*, 10(4):851–860, 2016.

[3] Amir H. Banihashemi and Frank R. Kschischang. Tanner graphs for group block codes and lattices: construction and complexity. *IEEE Trans. Inform. Theory*, 47(2):822–834, 2001.

[4] M. Borges-Quintana, M. A. Borges-Trenard, P. Fitzpatrick, and E. Martínez-Moro. Gröbner bases and combinatorics for binary codes. *Appl. Algebra Engrg. Comm. Comput.*, 19(5):393–411, 2008.

[5] M. Borges-Quintana, M. A. Borges-Trenard, and E. Martínez-Moro. On a Gröbner bases structure associated to linear codes. *J. Discrete Math. Sci. Cryptogr.*, 10(2):151–191, 2007.

[6] Irene Márquez-Corbella and Edgar Martínez-Moro. Algebraic structure of the minimal support codewords set of some linear codes. *Adv. Math. Commun.*, 5(2):233–244, 2011.