Binomial Ideal Associated to a Lattice and Its Label Code

Malihe Aliasgari
Amirkabir University of Technology (Iran)

Daniel Panario
Carleton University (Canada)

Mohammad-Reza Sadeghi
Amirkabir University of Technology (Iran)
ariyadokht@aut.ac.ir

Extended abstract

In coding theory the study of the binomial ideal derived from an arbitrary code is currently of great interest; see for example [5]. This is mainly because of a known relation between binomial ideals and lattices or codes. Also, studying the relation between binomial ideals associated to a lattice and its label code helps to solve the closest vector problem in lattices as well as decoding binary and non-binary codes [1, 3] and finding a label code of a lattice, as we do in this work.

Every lattice Λ can be described in terms of a label code L and an orthogonal sublattice Λ' such that $\Lambda/\Lambda' \cong L$ [2]. We assign binomial ideals I_Λ and I_L to an integer lattice Λ and its label code L, respectively. In this work, we identify the binomial ideal associated to an integer lattice and then establish the relation $I_\Lambda = I_{\Lambda'} + I_L$ between the ideal of the lattice and its label code.

In this work, we define a binomial ideal for an integer lattice and its label code slightly different from [1, 3, 4, 7].

Let $K[X] = K[x_1, \ldots, x_n]$ denote the polynomial ring, where K is an arbitrary field. Consider $\prec$ as a fixed total degree compatible term order with $x_1 \succ x_2 \succ \cdots \succ x_n$. The monomials in $K[X]$ are denoted by $X^{\mathbf{b}} = x_1^{b_1} \ldots x_n^{b_n}$ where $\mathbf{b} = (b_1, \ldots, b_n)$ is an element of $\mathbb{N}_0^n$ and $\mathbb{N}_0$ is the set of non-negative integers.

We use the notation

$$X^{\mathbf{a}} = X^{\mathbf{a}^+} - X^{\mathbf{a}^-} := \prod_{i:a_i>0} x_i^{a_i} - \prod_{j:a_j<0} x_j^{-a_j},$$

where $(\mathbf{a}^+)_i = \max\{a_i, 0\}$ and $\mathbf{a}^- = (-\mathbf{a})^+ \geq 0$. Also an *associated binomial ideal* I_Λ to Λ is defined as

$$I_\Lambda := (X^{\alpha^+} - X^{\alpha^-} : \alpha \in \Lambda).$$

Let y be a new variable. We identify $x_1 x_2 \ldots x_n y$ with 1 by means of the equation, $x_1 x_2 \ldots x_n y - 1 = 0$. In fact, we translate the relation between binomials into a quotient ring

$$S = K[x_1, \ldots, x_n, y]/(x_1 \ldots x_n y - 1).$$

The equivalence class of $x_1 \ldots x_{k-1} x_{k+1} \ldots x_n y$ is denoted by x_k^{-1}.

Sturmfels et al. [7] give the ideal of an integer lattice based on its generating set whose elements have only positive summation. This is summarized in the following theorem.

Theorem 1 *Let $\mathcal{B} = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\} \subseteq \mathbb{Z}^n$ be a generating set for the lattice Λ. If all coordinates in the sum of the vectors in $\mathcal{B} \cap \mathbb{N}_0^n$ are positive, then the ideal I_Λ coincides with*

$$I_{\mathcal{B}} := (X^{\boldsymbol{b}_i^+} - X^{\boldsymbol{b}_i^-} : i = 1, \ldots, n).$$

In this work, by extending the polynomial ring $K[x_1, \dots, x_n]$ to S, we generalize Sturmfels' result to any arbitrary generating set of the lattice. Theorem 1 deals with vectors of $\mathcal{B} \cap \mathbb{N}_0^n$ with positive summation only. Without any additional condition on the basis vectors, we show that a binomial ideal associated to any generating set of Λ is equal to its binomial ideal in the quotient ring S.

Theorem 2 *Let $\mathcal{B} = \{\boldsymbol{b}_1, \dots, \boldsymbol{b}_n\} \subseteq \mathbb{Z}^n$ be a generating set of an integer lattice Λ. Then the binomial ideal*

$$I_{\mathcal{B}} = (X^{\boldsymbol{b}_i^+} - X^{\boldsymbol{b}_i^-} : i = 1, \dots, n)$$

associated with $\mathcal{B}$ is equal to I_Λ in the polynomial ring S.

Then, we establish a relation between I_Λ and I_L for a Generalized Construction A lattices and derive the same relation for every arbitrary integer lattice.

Theorem 3 *Let Λ be an integer lattice in Generalized Construction A form which has the representation*

$$\Lambda = \mathbb{Z}^n \mathrm{diag}(g_1, \dots, g_n) + L,$$

where L is a subgroup of a group code $G = \mathbb{Z}_{g_1} \times \cdots \times \mathbb{Z}_{g_n}$ and diag(·) is a diagonal matrix. Then we have in S that

$$I_\Lambda = I_{\Lambda'} + I_L,$$

where I_L and $I_{\Lambda'}$ are binomial ideals associated to a group code L an and orthogonal sublattice $\Lambda' = \mathbb{Z}^n \mathrm{diag}(g_1, \dots, g_n)$, respectively. Also for an integer lattice with decomposition $\Lambda = \mathbb{Z}^n C(\Lambda) + LP(\Lambda)$ we have

$$I_\Lambda = I_{\Lambda'} + I_{L'},$$

where $I_{L'}$ is a binomial ideal associated to the group $L' = LP(\Lambda)$.

As an application of our work, using Theorem 3 and the result in Saleemi and Zimmerman [6], we give a method to obtain a linear label code of the lattice using its Gröbner basis.

Keywords
Lattice, label code, binomial ideal, Gröbner basis

References

[1] M. Aliasgari, M.-R. Sadeghi and D. Panario, "Gröbner bases for lattices and an algebraic decoding algorithm", *IEEE Trans. Commun.*, vol. 61, pp. 1222–1230, 2013.

[2] A. H. Banihashemi and F. R. Kschischang, "Tanner graphs for block codes and lattices: construction and complexity", *IEEE Trans. Inf. Theory*, vol. 47, pp. 822–834, 2001.

[3] M. Borges-Quintana, M.A.Borges-Trenard, P. Fitzpatrick and E. Martínez-Moro: "Gröbner bases and combinatorics for binary codes", *AAECC*, vol. 19, pp. 393-411, 2008.

[4] I. Márquez-Corbella and E. Martínez-Moro, "Algebraic structure of the minimal support codewords set of some linear codes", *Advances in Mathematics of Communications*, vol. 5, pp. 233-244, 2011.

[5] I. Márquez-Corbella and E. Martínez-Moro, "On the ideal associated to a linear code", *arXiv: math/1206.5124*, Jun. 2012.

[6] M. Saleemi and K-H. Zimmermann, "Groebner bases for linear codes over GF(4)", *International Journal of Pure and Applied Mathematics*, vol 73, pp. 435-442, 2011.

[7] B. Sturmfels, R. Weismantel, and G. Ziegler, "Gröbner bases of lattices, corner polyhedra and integer programming," *Contributions to Algebra and Geometry*, 1994.