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 $\Lambda$ can be described in terms of a label code $L$ and an orthogonal sublattice $\Lambda'$ such that $\Lambda/\Lambda' \cong L$ [2]. We assign binomial ideals $I_{\Lambda}$ and $I_{L}$ to an integer lattice $\Lambda$ 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 $X_{\alpha} = x_{\alpha_1}^{\alpha_1} \cdots x_{\alpha_n}^{\alpha_n}$ where $\alpha = (\alpha_1, \ldots, \alpha_n)$ is an element of $\mathbb{N}_0^n$ and $\mathbb{N}_0$ is the set of non-negative integers.

We use the notation

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

where $(\alpha^+) = \max \{a_i, 0\}$ and $\alpha^- = (-\alpha)^+ \geq 0$. Also an associated binomial ideal $I_{\Lambda}$ to $\Lambda$ is defined as

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

Let $y$ be a new variable. We identify $x_1x_2 \ldots x_ny$ with 1 by means of the equation, $x_1x_2 \ldots x_ny - 1 = 0$. In fact, we translate the relation between binomials into a quotient ring

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

The equivalence class of $x_1 \ldots x_{k-1}x_{k+1} \ldots x_ny$ 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 $B = \{b_1, \ldots, b_n\} \subseteq \mathbb{Z}^n$ be a generating set for the lattice $\Lambda$. If all coordinates in the sum of the vectors in $B \cap \mathbb{N}_0^n$ are positive, then the ideal $I_{\Lambda}$ coincides with

$$I_B := (X^{b_i^+} - X^{b_i^-} : i = 1, \ldots, n).$$
In this work, by extending the polynomial ring $K[x_1, \ldots, x_n]$ to $S$, we generalize Sturmfels’ result to any arbitrary generating set of the lattice. Theorem 1 deals with vectors of $B \cap \mathbb{N}_0^n$ with positive summation only. Without any additional condition on the basis vectors, we show that a binomial ideal associated to any generating set of $\Lambda$ is equal to its binomial ideal in the quotient ring $S$.

**Theorem 2** Let $B = \{b_1, \ldots, b_n\} \subseteq \mathbb{Z}^n$ be a generating set of an integer lattice $\Lambda$. Then the binomial ideal

$$I_B = (X^{b_i} - X^{b_i^\prime} : i = 1, \ldots, n)$$

associated with $B$ is equal to $I_\Lambda$ in the polynomial ring $S$.

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

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

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

where $L$ is a subgroup of a group code $G = \mathbb{Z}_{g_1} \times \cdots \times \mathbb{Z}_{g_n}$ and $\text{diag}(\cdot)$ 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 $\Lambda' = \mathbb{Z}^n \text{diag}(g_1, \ldots, g_n)$, respectively. Also for an integer lattice with decomposition $\Lambda = \mathbb{Z}^n C(\Lambda) + L_P(\Lambda)$ we have

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

where $I_L'$ is a binomial ideal associated to the group $L' = L_P(\Lambda)$.

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**


