

Gröbner 基底を用いた 2元線形符号の硬/軟判定最尤復号と整数計画問題について

池上 大介*

奈良先端科学技術大学院大学 情報基礎学講座

Risa Consortium 第 10 回研究集会

2002/3/19

P. Conti と C. Traverso は Gröbner 基底を用いて整数計画問題 (図 1) を解くアルゴリズムを構成した [2] ([1, 3] に整理された形でまとめられている)。一方、発表者のグループは Conti-Traverso アルゴリズムを修正して、正整数 $q \geq 2$ を法とする整数計画問題 (図 2) を解くアルゴリズムを提案している [4]。本発表では、 q を法とする整数計画問題を、ある 0 次元イデアルの Gröbner 基底を用いて解くアルゴリズムを紹介し、計算の高速化を検討する。

また $q = 2$ の場合は、誤り訂正符号理論の復号法の一つである「任意の 2 元符号の硬/軟判定最尤復号」に応用できることがわかっている [5]。本発表の最後に、符号理論の立場から、提案復号法に適したイデアルと Gröbner 基底を考察する。

参考文献

- [1] Arjeh M. Cohen, Hans Cuypers, and Hans Sterk, editors. *Some Tapas of Computer Algebra*. Springer, 1998.
- [2] Pasqualina Conti and Carlo Traverso. Buchberger algorithm and integer programming. In H. Mattson, T. Mora, and T. Rao, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-9)*, number 539 in LNCS, pages 130–139. Springer-Verlag, October 1991.
- [3] David Cox, John Little, and Donal O’Shea. *Using Algebraic Geometry*. Springer-Verlag, 1998.
- [4] Daisuke Ikegami and Yuichi Kaji. A soft-decision MLD algorithm for linear block codes using Gröbner bases. In *The 24th Symposium on Information Theory and Its Applications (SITA 2001)*, pages 545–548, December 2001.
- [5] Daisuke Ikegami and Yuichi Kaji. Maximum likelihood decoding using gröbner bases. The 10th Risa Consortium, preprint, unpublished, March 2002.

minimize $\mathbf{w} \cdot \mathbf{u}$ subject to $A\mathbf{u} = \mathbf{b}$ where

$$\mathbf{u} \in \mathbf{Z}_{\geq 0}^n, A \in \mathbf{Z}^{m \times n}, \mathbf{b} \in \mathbf{Z}^m, \mathbf{w} \in \mathbf{R}^n.$$

図 1: 整数計画問題

minimize $\mathbf{w} \cdot \mathbf{u}$ subject to $A\mathbf{u} \equiv \mathbf{b} \pmod{q}$ where

$$\mathbf{u} \in \mathbf{Z}_q^n, A \in \mathbf{Z}_q^{m \times n}, \mathbf{b} \in \mathbf{Z}_{\geq 0}^m, \mathbf{w} \in \mathbf{R}^n, \\ \mathbf{Z}_q = \{0, 1, \dots, q-1\} \subset \mathbf{Z}_{\geq 0}.$$

図 2: q を法とした整数計画問題

*daisu-ik@is.aist-nara.ac.jp