

Gröbner bases over principal ideal rings

Ana Sălăgean* and Graham H. Norton**

* Department of Computer Science
Loughborough University
Loughborough LE11 3TU - UK

** Department of Mathematics
University of Queensland
Brisbane 4072 - Australia

Abstract

Introduction and Notation

We give an overview of our results on strong Gröbner bases over a principal ideal ring, [13, 14, 15, 16]. Our work was originally motivated by applications to coding theory, as codes over $\mathbb{Z}/4\mathbb{Z}$ and more general rings have received much attention following [6]. See Section below.

Gröbner bases, introduced by Buchberger in [3], have subsequently been generalised in numerous ways. We examine two generalisations to polynomials over a commutative ring R , namely Gröbner bases and strong Gröbner bases, as defined in [1].

As usual we consider an admissible term order on the terms in x_1, \dots, x_n and define the leading term, $\text{lt}(f)$, leading coefficient, $\text{lc}(f)$ and leading monomial, $\text{lm}(f)$ of a polynomial $f \in R[x_1, \dots, x_n]$ w.r.t. this order. We denote by $\langle G \rangle$ the ideal generated by a set G in $R[x_1, \dots, x_n]$ and by $\langle A \rangle_R$ the ideal generated by a set A in R . Reduction and strong reduction are defined as in [1]. Gröbner bases and strong Gröbner bases are defined as:

Definition 1. A finite set G of non-zero polynomials is a Gröbner basis for the ideal $I = \langle G \rangle$ iff any of the following two equivalent conditions are satisfied:

- (i) $\langle \text{lm}(G) \rangle = \langle \text{lm}(I) \rangle$,
- (ii) All polynomials in I reduce to 0 w.r.t. G .

Definition 2. A finite set G of non-zero polynomials is a strong Gröbner basis for the ideal $I = \langle G \rangle$ iff any of the following two equivalent conditions are satisfied:

- (i) For any $f \in I \setminus \{0\}$ there is a $g \in G$ such that $\text{lm}(g) \mid \text{lm}(f)$.
- (ii) All polynomials in I strongly reduce to 0 w.r.t. G .

Gröbner bases over principal ideal rings

Several authors have shown that a strong Gröbner basis exists and can be effectively constructed for any ideal of polynomials over a principal ideal domain (see the references in [2]). For an ideal of polynomials over a Noetherian ring, it was shown in [1] that a Gröbner basis always exists but a strong Gröbner basis does not always exist.

We show that any ideal of polynomials over a principal ideal ring has a strong Gröbner basis. Note that principal ideal rings lie between principal ideal domains and Noetherian rings.

We first characterise strong Gröbner bases over a principal ideal ring R . We use classical S-polynomials introduced by Buchberger, G-polynomials (see for example [2]) and a new construction which we call A-polynomial: given a polynomial g over a principal ideal ring R , an A-polynomial of g is any polynomial of the form ag where $a \in R$ is any element such that $\langle a \rangle_R$ is the annihilator ideal of $\text{lc}(g)$.

Theorem 3. ([14, Corollary 5.12]) Let R be a principal ideal ring and let $G \subset R[x_1, \dots, x_n] \setminus \{0\}$ be a finite set. Then G is a strong Gröbner basis if and only if the following three conditions are satisfied:

- (A) for any $g_1, g_2 \in G$ with $g_1 \neq g_2$, there is an S-polynomial of g_1 and g_2 which is strongly reducible to 0 w.r.t. G ,

- (B) for any $g \in G$, there is an A -polynomial of g which is strongly reducible to 0 w.r.t. G ,
 (C) for any $g_1, g_2 \in G$ with $g_1 \neq g_2$ there is a G -polynomial of g_1 and g_2 which is strongly reducible w.r.t. G .

We also show that Gröbner bases and strong Gröbner bases coincide for Artinian chain rings. A theorem similar to Theorem 3, but omitting condition (C) is valid for Artinian chain rings.

Based on the characterisation in Theorem 3, we give an algorithm for constructing strong Gröbner bases over a principal ideal ring, generalising thus Buchberger's results to a this type of ring.

We also give an alternative algorithm using a Chinese Remainder Theorem construction, [15]. We use the fact that a ring is a principal ideal ring if and only if it is isomorphic to a direct product of principal ideal domains and Artinian chain rings.

Gröbner bases over Galois rings have been studied independently in [4]. In [16, Introduction] we compare their results to ours and point out some of the advantages of our approach.

Minimal univariate Gröbner bases

We now turn our attention to univariate polynomials. Minimal Gröbner bases for univariate polynomials over a principal ideal domain have been characterised by Lazard, [8]. We generalise this result, characterising a minimal strong Gröbner basis over a principal ideal ring R :

Theorem 4. ([16, Theorem 5.4]) *A finite set $G \subset R[x] \setminus \{0\}$ is a minimal strong Gröbner basis if and only if there are $r \in R$, r not a zero-divisor, $s \geq 0$, $r_i \in R$ and $g_i \in R[x]$ for $i = 0, \dots, s$ such that:*

$$G = \{r_0 g_0, \dots, r_s g_s\}$$

and

- (i) $\langle r_i \rangle_R \supset \langle r_{i+1} \rangle_R$ with strict inclusion, for $i = 0, \dots, s-1$;
- (ii) $\text{lc}(g_i) = r$ for $i = 0, \dots, s$;
- (iii) $\deg(g_i) > \deg(g_{i+1})$ for $i = 0, \dots, s-1$ and
- (iv) $r_{i+1} g_i \in \langle r_{i+1} g_{i+1}, \dots, r_s g_s \rangle$ for $i = 0, \dots, s-1$.

For the particular case of Artinian chain rings, the minimal strong Gröbner bases in the theorem above coincide with the generator sets described in [9, 5, 12].

Applications to Coding Theory

Recall that cyclic codes of length n over a ring R are ideals in $R[x]/\langle x^n - 1 \rangle$. The structure of cyclic codes over $\mathbb{Z}/p^a\mathbb{Z}$ is described in [5] for the case where the length of the code is not divisible by p . Namely it is shown that any code is of the form $\langle f_0, p f_1, \dots, p^{a-1} f_{a-1} \rangle$, with $f_{i+1} | f_i$ and $f_0 | x^n - 1$. This result can be generalised to Artinian chain rings, see [12]. Using Theorem 4 these results can be generalised to principal ideal rings and the restriction on the length of the code can be removed. The so-called repeated-root cyclic codes are therefore also covered. More details are given in [16, 17].

Another application of Gröbner bases over Galois rings appears in [4], where a Gröbner basis is computed in order to decode alternant codes. Alternatively one can decode these codes using the Berlekamp-Massey algorithm, which has quadratic complexity and has been generalised to Galois rings in [10, 7, 11].

References :

References

- [1] W. Adams and P. Loustaunau. *An Introduction to Gröbner bases*, volume 3 of *Graduate Studies in Mathematics*. American Mathematical Society, 1994.
- [2] T. Becker and V. Weispfenning. *Gröbner Bases*. Springer, 1993.
- [3] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. PhD thesis, University of Innsbruck, Austria, 1965.

- [4] E. Byrne and P. Fitzpatrick. Gröbner bases over Galois rings with an application to decoding alternant codes. *J. Symbolic Computation*, 31:565–584, 2001.
- [5] A. R. Calderbank and N. J. A. Sloane. Modular and p -adic codes. *Designs, Codes and Cryptography*, 6:21–35, 1995.
- [6] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé. The \mathbb{Z}_4 linearity of Kerdock, Preparata, Goethals and related codes. *IEEE Trans. Inform. Theory*, 40:301–319, 1994.
- [7] J. C. Interlando, R. Palazzo, and M. Elia. On the decoding of Reed-Solomon and BCH codes over integer residue rings. *IEEE Trans. Inform. Theory*, 43(3):1013–1021, 1997.
- [8] D. Lazard. Ideal bases and primary decomposition: Case of two variables. *J. Symb. Comp.*, 1:261–270, 1985.
- [9] A.A. Nechaev. Linear recurrence sequences over commutative rings. *Discrete Math. Appl.*, 2(6):659–683, 1992.
- [10] G. H. Norton. On minimal realization over a finite chain ring. *Designs, Codes and Cryptography*, 16:161–178, 1999.
- [11] G.H. Norton and A. Sălăgean. On the key equation over a commutative ring. *Designs, Codes and Cryptography*, 20:125–141, 2000.
- [12] G.H. Norton and A. Sălăgean. On the structure of linear and cyclic codes over finite chain rings. *Applicable algebra in engineering, communication and computing*, 10:489–506, 2000.
- [13] G.H. Norton and A. Sălăgean. Strong Gröbner bases and cyclic codes over a finite-chain ring. In *Proceedings of the Workshop on Coding and Cryptography, Paris*, Electronic Notes in Discrete Mathematics, pages 391–401, 2001. <http://www.elsevier.nl:80/inca/publications/store/5/0/5/6/0/9/>.
- [14] G.H. Norton and A. Sălăgean. Strong Gröbner bases for polynomials over a principal ideal ring. *Bull. of the Australian Mathematical Soc.*, 64:505–528, 2001.
- [15] G.H. Norton and A. Sălăgean. Gröbner bases and products of coefficient rings. *Bull. of the Australian Mathematical Soc.*, 65:145–152, 2002.
- [16] G.H. Norton and A. Sălăgean. Cyclic codes and minimal strong Gröbner bases over a principal ideal ring. *Finite Fields and Their Applications*, 9:237–249, 2003.
- [17] A. Sălăgean. Repeated-root cyclic and negacyclic codes over a finite chain ring. *Discrete Applied Mathematics*, 2004. to appear.