JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume 15, No. 2, December 2002

GRÖBNER–SHIRSHOV BASIS AND ITS APPLICATION

Sei-Qwon Oh* and Mi-Yeon Park**

Abstract. An efficient algorithm for the multiplication in a binary finite filed using a normal basis representation of F_{2^m} is discussed and proposed for software implementation of elliptic curve cryptography. The algorithm is developed by using the storage scheme of sparse matrices.

1. Introduction

Buchberger introduced the Gröbner basis theory for commutative algebras that provides a effective solution to the reduction problem for commutative algebras [**2**]. It was generalized to associative algebras through Bergman's Diamond Lemma [**1**].

Shirshov developed the parallel theory of Gröbner bases for Lie algebras [**9**]. Shirshove's theory for Lie algebras and their universal enveloping algebras is called Gröbner-Shirshov basis theory.

In this paper, we introduce the Gröbner-Shirshov basis theory and find the Gröbner-Shirshov basis for quantum algebras.

More precisely, we introduce the Gröbner-Shirshov basis theory for a free k-algebra and we find the Gröbner-Shirshov basis for several quantum k-algebras defined by generators and relations,

$$U_q'(\mathfrak{sl}(2)), \mathcal{O}_q(M_2(k)), \mathcal{O}_q(SL_2(k))$$

Received by the editors on February 7, 2003.
2000 *Mathematics Subject Classifications*: 16S.
Key words and phrases: Elliptic Curve Cryptography, Binary finite field, Normal basis.

and McConnell-Pettit Algebra.

Throughout this paper, k will denote the ground field of characteristic zero, every vector space will be over k and every algebra will be an associative k-algebra with unity.

2. Gröbner-Shirshov Basis Theory

Let X be a set and let X^* be the free monoid of associative monomials on X. We denote the empty monomial by 1 and the *length* of a monomial u by $l(u)$. Thus we have $l(1) = 0$.

DEFINITION 2.1. [**3**, 1.1] A well-ordering $\prec$ on X^* is called a *monomial order* if $x \prec y$ implies $axb \prec ayb$ for all $a, b \in X^*$.

Fix a monomial order $\prec$ on X^*, let T_X be the free k-algebra generated by X, let I be a two sided ideal of T_X and let $T_0 = T_X/I$. The image of $p \in T_X$ in T_0 under the canonical quotient map will also be denoted by p.

Fix a subset $\mathcal{A}$ of X^* which forms a k-linear basis of T_0. Given a nonzero element $p \in T_0$, we denote by $\overline{p} \in \mathcal{A}$ the maximal monomial appearing in p under the ordering $\prec$. Thus $p = \alpha\overline{p} + \sum \beta_i w_i$ with $\alpha, \beta_i \in k, w_i \in \mathcal{A}, \alpha \neq 0$ and $w_i \prec \overline{p}$. If $\alpha = 1$, then p is said to be *monic*.

DEFINITION 2.2. [**8**, 1.2] Fix a monomial order on X^* and a subset $\mathcal{A}$ of X^* which forms a k-linear basis of $T_0 = T_X/I$. Let S be a subset of monic elements of T_0. A monomial $u \in \mathcal{A}$ is said to be *S-standard* in T_0 if $u \neq a\overline{s}b$ for any $s \in S$ and $a, b \in \mathcal{A}$. Otherwise, the monomial u is said to be *S-reducible* in T_0.

THEOREM 2.3. *Every $p \in T_0$ can be expressed as*

$$p = \sum \alpha_i a_i s_i b_i + \sum \beta_j u_j \tag{2.1}$$

where $\alpha_i, \beta_j \in k$*;* $a_i, b_i, u_j \in \mathcal{A}$*;* $s_i \in S$*;* $a_i\overline{s}_ib_i \preceq \overline{p}$*;* $u_j \preceq \overline{p}$*; and* u_j *are* S*-standard.*

Proof. It is proved by mimicking the proof of [**4**, 3.2]. □

The term $\sum \beta_j u_j$ in the expression (2.1) is called a *normal form* (or a *remainder*) of p with respect to S.

DEFINITION 2.4. [**8**, 1.2] Let p and q be monic elements of T_0.
(a) If there exist a and b in $\mathcal{A}$ such that $\overline{p}a = b\overline{q} = w$ with $l(\overline{p}) > l(b)$, then the *composition of intersection* is defined to be $(p,q)_w = pa - bq$.
(b) If there exist a and b in $\mathcal{A}$ such that $a \neq 1, a\overline{p}b = \overline{q} = w$, then the *composition of inclusion* is defined to be $(p,q)_w = apb - q$.

EXAMPLE 2.5. Let $X = \{x_1, x_2, x_3, x_4\}$.

If $p = x_1^2x_3 - x_2x_4$ and $q = x_3^2x_2 + x_1$, then we have a composition of intersection:

$$\begin{aligned}(p,q)_{x_1^2x_3^2x_2} &= (x_1^2x_3 - x_2x_4)x_3x_2 - x_1^2(x_3^2x_2 + x_1)\\ &= x_1^2x_3^2x_2 - x_2x_4x_3x_2 - x_1^2x_3^2x_2 - x_1^3\\ &= -x_2x_4x_3x_2 - x_1^3.\end{aligned}$$

Fix a subset $\mathcal{A}$ of X^* which forms a k-linear basis of $T_0 = T_X/I$. Let S be a subset of monic elements of T_0 and let J be the two sided ideal of T_0 generated by S.

Let $p, q \in T_0$ and $w \in X^*$. We define a congruence relation on T_0 as follows: $p \equiv q \mod(J; w)$ if and only if $p - q = \sum \alpha_i a_i s_i b_i$, where $\alpha_i \in k; a_i, b_i \in \mathcal{A}; s_i \in S$; $a_i\overline{s}_ib_i \prec w$.

DEFINITION 2.6. [**8**, 1.3] A subset S of monic elements in T_0 is said to be *closed under composition* in T_0 if $(p,q)_w \equiv 0 \mod(J; w)$ for all $p, q \in S, w \in \mathcal{A}$, whenever the composition $(p,q)_w$ is defined.

THEOREM 2.7. [**8**, 1.5] *Fix a subset $\mathcal{A}$ of X^* which forms a k-linear basis of $T_0 = T_X/I$. Let S be a subset of monic elements of T_0 and let J be the two sided ideal of T_0 generated by S. Then the following are equivalent:*

(i) *S is closed under composition in T_0.*
(ii) *The subset of $\mathcal{A}$ consisting of S-standard monomials in T_0 forms a k-linear basis of the algebra T_0/J.*

DEFINITION 2.8. [**4**, 2.5] A subset S of monic elements of T_0 is called a *Gröbner-Shirshov basis* if the subset of $\mathcal{A}$ consisting of S-standard monomials in T_0 forms a k-linear basis of the algebra T_0/J. In this case, we say that S is a Gröbner-Shirshov basis for the algebra T_0/J defined by S.

3. Poincaré-Birkhoff-Witt Theorem for Quantum Algebras

3.1. Algebra $U_q'(\mathfrak{sl}(2))$

DEFINITION 3.1. [**5**, VI.1.1] We define $U_q = U_q(\mathfrak{sl}(2))$ as the algebra generated by the four variables E, F, K, K^{-1} with the relations

$$KK^{-1} = K^{-1}K = 1,$$

$$KEK^{-1} = q^2E,$$

$$KFK^{-1} = q^{-2}F,$$

and

$$[E, F] = \frac{K - K^{-1}}{q - q^{-1}}.$$

A Hopf algebra $U_q = U_q(\mathfrak{sl}(2))$ is an one-parameter deformation of the enveloping algebra of the Lie algebra $\mathfrak{sl}(2)$. When the parameter q is not a root of unity, the algebra U_q has properties parrel to those of the enveloping algebra of $\mathfrak{sl}(2)$.

Proposition 3.2. [**5**, VI.1.4] *The algebra U_q is Noetherian and has no zero divisors. The set $\{E^iF^jK^l\}_{\ i,j\in\mathbb{N};\ l\in\mathbb{Z}}$ is a basis of U_q.*

One expects to recover $U = U(\mathfrak{sl}(2))$ from U_q by setting $q = 1$. This is impossible with Definition 3.1. So, we first have to give another presentation for U_q.

Proposition 3.3. [**5**, VI.2.1] *The algebra U_q is isomorphic to the algebra U'_q generated by the five variables K, K^{-1}, L, E, F and the relations*

$$KK^{-1} = K^{-1}K = 1,$$

$$KEK^{-1} = q^2E,$$

$$KFK^{-1} = q^{-2}F,$$

$$[E, F] = L,$$

$$(q - q^{-1})L = K - K^{-1},$$

$$[L, E] = q(EK + K^{-1}E),$$

$$[L, F] = -q^{-1}(FK + K^{-1}F).$$

Observe that, contrary to U_q, the algebra U'_q is defined for all values of the parameter q, in particular for $q = 1$.

Theorem 3.4. *The algebra U'_q has a k-linear basis*

$$\mathfrak{B} = \{K^lE^mF^n \mid l = 0, \pm1, \pm2, \cdots; m, n = 0, 1, 2, \cdots\}.$$

Proof. Let T_0 be the free k-algebra generated by K, K^{-1}, L, E and F.

We give an ordering $<$ on the set of generators of T_0 by

$$K < K^{-1} < L < E < F.$$

The degree of a monomial $u = u_1 \cdots u_l \in T_0$, where $u_j = K, u_j = K^{-1}$,
$u_j = L, u_j = E$, or $u_j = F$, is defined by $\deg(u) = l$.

We now give a well-ordering $\prec$ on the set of all monomials in T_0 as follows:

For monomials $u = u_1 \cdots u_l$ and $v = v_1 \cdots v_m$, we denote $u \prec v$ if one of the following conditions holds:

(i) $\deg(u) < \deg(v)$

(ii) $\deg(u) = \deg(v)$ (hence $l = m$), $u_1 = v_1, \cdots, u_r = v_r$ and $u_{r+1} < v_{r+1}$ for some r.

Note that the ordering $\prec$ is a monomial order.[**8**]

We shall replace K^{-1} by K' for convenience. So, the given relations can be expressed as follows :

$$K'K - KK' = 0 \tag{3.1}$$

$$EK - q^{-2}KE = 0 \tag{3.2}$$

$$FK - q^{2}KF = 0 \tag{3.3}$$

$$FE - EF + L = 0 \tag{3.4}$$

$$L - \frac{1}{q - q^{-1}}(K - K') = 0 \tag{3.5}$$

$$KEL - KLE + qKEK + qE = 0 \tag{3.6}$$

$$KFL - KLF - q^{-1}KFK - q^{-1}F = 0. \tag{3.7}$$

Let S be the subset of monic elements of T_0 consisting of (3.1), (3.2), (3.3), (3.4), (3.5), (3.6) and (3.7), and let J be the two sided ideal of T_0 generated by S. By Theorem 2.10, it is enough to show that the generators of J are closed under composition in T_0. There are only nine possible compositions among the generators of J:

$$
\begin{aligned}
&(K'K-KK', \quad KEL-KLE+qKEK+qE)_{K'KEL}\\
&(K'K-KK', \quad KFL-KLF-q^{-1}KFK-q^{-1}F)_{K'KFL}\\
&(FE-EF+L, \quad EK-q^{-2}KE)_{FEK}\\
&(EK-q^{-2}KE, \quad KEL-KLE+qKEK+qE)_{EKEL}\\
&(EK-q^{-2}KE, \quad KFL-KLF-q^{-1}KFK-q^{-1}F)_{EKFL}\\
&(FK-q^{2}KF, \quad KEL-KLE+qKEK+qE)_{FKEL}\\
&(FK-q^{2}KF, \quad KFL-KLF-q^{-1}KFK-q^{-1}F)_{FKFL}\\
&(KEL-KLE+qKEK+qE, \quad L-\frac{1}{q-q^{-1}}(K-K'))_{KEL}\\
&(KFL-KLF-q^{-1}KFK-q^{-1}F, \quad L-\frac{1}{q-q^{-1}}(K-K'))_{KFL}.
\end{aligned}
$$

For the each case, S is closed under composition in T_0. Thus, the set

$$\{K^i(K^{-1})^jE^mF^n \mid i\cdot j=0; i,j,m,n=0,1,2,\cdots\}$$

is a basis of $T_0/J=U_q'$, and so S is a Gröbner-Shirshov basis for the algebra U_q'. □

3.2. Algebra $\mathcal{O}_q(M_2(k))$ and $\mathcal{O}_q(SL_2(k))$

THEOREM 3.5. [**7**] *Let $0\neq q\in k$. The coordinate ring of quantum 2×2-matrices, denoted by $\mathcal{O}_q(M_2(k))$, is the k-algebra generated by $a,b,c,d,$ subject to the relations*

$$ab=q^2ba, \quad ac=q^2ca,$$

$$bc=cb, \qquad bd=q^2db,$$

$$cd=q^2dc,$$

$$ad - da = (q^2 - q^{-2})bc.$$

Assume that q is not a root of unity. Then the algebra $\mathcal{O}_q(M_2(k))$ has a k-linear basis

$$\mathfrak{B} = \{a^i b^j c^m d^n \mid \ i,\ j,\ m,\ n = 0, 1, 2, \cdots\}.$$

Proof. Let T_0 be the free k-algebra generated by a, b, c and d.

We give an ordering $<$ on the set of generators of T_0 by

$$a < b < c < d.$$

The degree of a monomial $u = u_1 \cdots u_l \in T_0$, where $u_j = a, u_j = b, u_j = c$ or $u_j = d$, is defined by $\deg(u) = l$.

We now give a well-ordering $\prec$ on the set of all monomials in T_0 as Theorem 3.4.

The given relations can be expressed as follows:

$$ba - q^{-2}ab = 0, \quad ca - q^{-2}ac = 0 \tag{3. 8}$$

$$cb - bc = 0, \quad db - q^{-2}bd = 0 \tag{3. 9}$$

$$dc - q^{-2}cd = 0 \tag{3.10}$$

$$da - ad + q^2 bc - q^{-2}bc = 0. \tag{3.11}$$

Let S be the subset of monic elements of T_0 consisting of (3.8), (3.9), (3.10), and (3.11), and let J be the two sided ideal of T_0 generated by S.

By Theorem 2.10, it is enough to show that the generators of J are closed under composition T_0. There are only four possible compositions among the generators of J:

$(cb - bc, \ \ ba - q^{-2}ab)_{cba}$, $\qquad (db - q^{-2}bd, \ \ ba - q^{-2}ab)_{dba}$

$(dc - q^{-2}cd, \ \ ca - q^{-2}ac)_{dca}$, $\qquad (dc - q^{-2}cd, \ \ cb - bc)_{dcb}$.

Thus, the set $\mathfrak{B} = \{a^i b^j c^m d^n \mid \ i,\ j,\ m,\ n = 0, 1, 2, \cdots\}$ is a basis of $T_0/J = \mathcal{O}_q(M_2(k))$, and so S is a Gröbner-Shirshov basis for the algebra $\mathcal{O}_q(M_2(k))$. □

The element of $\mathcal{O}_q(M_2(k))$

$$det_q = ad - q^2 bc \tag{3.12}$$

is called the *quantum determinant*.

DEFINITION 3.6. Let J' be the two sided ideal of $\mathcal{O}_q(M_2(k))$ generated by $ad - q^2bc - 1$. Then we can define the algebra

$$\mathcal{O}_q(SL_2(k)) = \mathcal{O}_q(M_2(k))/J'.$$

COROLLARY 3.7. *The algebra $\mathcal{O}_q(SL_2(k))$ has a k-linear basis*

$$\mathfrak{B}' = \{a^i b^j c^m d^n \mid \ j \cdot m = 0; i, j, m, n = 0, 1, 2, \cdots\}.$$

Proof. Let S' be the relation $ad - q^2bc - 1$ and let J' be the two sided ideal of $\mathcal{O}_q(M_2(k))$ generated by S'.

By Theorem 2.10, it is enough to show that the generator of J' is closed under composition in $\mathcal{O}_q(M_2(k))$. Thus, the set

$$\mathfrak{B}' = \{a^i b^j c^m d^n \mid \ j \cdot m = 0; i, j, m, n = 0, 1, 2, \cdots\}$$

is a basis of $\mathcal{O}_q(SL_2(k))$, and so S' is a Gröbner-Shirshov basis for the algebra $\mathcal{O}_q(M_2(k))/J' = \mathcal{O}_q(SL_2(k))$. □

3.3. McConnell-Pettit Algebra

EXAMPLE 3.8. (McConnell-Pettit Algebra) [**6**] Let $\overline{q} = (q_{ij})$ be a matrix with nonzero entries in k such that $q_{ii} = 1$ and $q_{ij} = q_{ji}^{-1}$. Let

$\mathcal{O}_q(k^n)$ be the k-algebra generated by $x_1, x_2, \cdots, x_n$ subject to the relations

$$x_i x_j - q_{ij} x_j x_i \qquad \text{for all } i > j. \tag{3.13}$$

Then $\mathcal{O}_q(k^n)$ has a k-linear basis $\mathfrak{B} = \{x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \mid i_j = 0, 1, 2, \cdots\}$.

Proof. Let T_0 be the free k-algebra generated by $x_1, x_2, \cdots, x_n$.

We give an ordering $<$ on the set of generators of T_0 by

$$x_1 < x_2 < x_3 < \cdots < x_n.$$

The degree of a monomial $u = u_1 \cdots u_l \in T_0$, where $u_j = x_k$ for some k
$(k = 1, 2, \cdots n)$, is defined by $\deg(u) = l$.

We now give a well-ordering $\prec$ on the set of all monomials in T_0 as Theorem 3.4.

Let S be the subset of monic elements of T_0 consisting of (3.13), and let J be the two sided ideal of T_0 generated by S. By Theorem 2.10, it is enough to show that the generators of J are closed under composition in T_0. There is only one possible composition among the generators of J:$(x_i x_j - q_{ij} x_j x_i, \ \ x_j x_k - q_{jk} x_k x_j)_{x_i x_j x_k}$ $(i > j > k)$.

$$\begin{aligned}
(x_i x_j - q_{ij} x_j x_i, \ \ & x_j x_k - q_{jk} x_k x_j)_{x_i x_j x_k} \\
&= x_i x_j x_k - q_{ij} x_j x_i x_k - x_i x_j x_k + q_{jk} x_i x_k x_j \\
&= -q_{ij} x_j x_i x_k + q_{jk} x_i x_k x_j \\
&\equiv -q_{ij} x_j (q_{ik} x_k x_i) + q_{jk} (q_{ik} x_k x_i) x_j \\
&= -q_{ij} q_{ik} x_j x_k x_i + q_{jk} q_{ik} x_k x_i x_j \\
&\equiv -q_{ij} q_{ik} (q_{jk} x_k x_j) x_i + q_{jk} q_{ik} x_k (q_{ij} x_j x_i) \\
&= -q_{ij} q_{ik} q_{jk} x_k x_j x_i + q_{jk} q_{ik} q_{ij} x_k x_j x_i \\
&\equiv 0 \mod (J; x_i x_j x_k).
\end{aligned}$$

□

References

1. G.M.Bergman, *The diamond lemma for ring theory*, Adv. Math. **29** (1978), 178-218.
2. B.Buchberger, *An algorithm for finding a basis for the residue class ring of a zero-dimensional ideal*, Ph.D. Thesis, University of Innsbruck (1965).
3. Seok-Jin Kang and Kyu-Hwan Lee, *Gröbner-Shirshov bases for irreducible $\mathfrak{sl}_{n+1}$-modules*, J. Algebra **232** (2000), 1-20.
4. Seok-Jin Kang and Kyu-Hwan Lee, *Gröbner-Shirshov bases for representation theory*, J. Korean Math. Soc. **37** (2000), 55-72.
5. Christian Kassel, *Quantum Groups*, Springer-Verlag, 1995.
6. J.C.McConnell and J.J.Pettit, *Crossed products and multiplicative analogues of Weyl algebras*, J. London Math. Soc. **(2) 38** (1988), 47-55.
7. Sei-Qwon Oh, *Symplectic ideals of Poisson algebras and the Poisson structure associated to quantum matrices*, Comm. Algebra **27** (1999), 2163–2180.
8. Sei-Qwon Oh, Chun-Gil Park and Yong-Yeon Shin, *A Poincaré-Birkhoff-Witt theorem for Poisson enveloping algebras*, Comm. Algebra (To appear).
9. A.I.Shirshov, *Some algorithmic problems for Lie algebras*, Siberian Math. J. **3** (1962), 292-296.

*

Sei-Qwon Oh
Department of Mathematics
Chungnam National University
Taejon 305-764, Korea

E-mail: sqoh@math.cnu.ac.kr

**

Mi-Yeon Park
Department of Mathematics
Chungnam National University
Taejon 305-764, Korea