数理解析研究所講究録
第 98 巻 1992 年 98-112

Gröbner Bases and Algebra Isomorphism Problem

Kiyoshi Shirayanagi (白柳 潔)
NTT Communication Science Laboratories
email: shirayan@progn.kecl.ntt.jp

1 Introduction

In this paper, we consider the isomorphism problem for finite-dimensional finitely presented algebras over a field k. In the paper [8], monomial algebras (defined by the form "monomial = 0" only), the simplest class of finitely presented algebras, have been already shown to have a very effective solution, based on the presentation uniqueness theorem. In this case, surprisingly, it turns out that the answer is independent of the ground field k. Moreover, as to non-degenerate binomial algebras (defined by the form "monomial = 0" or "binomial = 0 (*non-degenerate relations*) "), the paper [9] has provided some necessary conditions for an existence of isomorphism. These conditions were described in terms of a partially ordered set.

This paper deals with the problem for general finitely presented alge-

bras: given two finitely presented algebras A and B of the same dimension over a field k, decide whether they are isomorphic as k-algebras. In Section 2, we provide a general criterion for deciding an algebra isomorphism. In Section 3, our *non-commutative* problem is reduced to a radical membership problem in a *commutative* ring. Section 4 presents an efficient technique for computing the determinant of an isomorphism candidate. In Section 5, we can propose a Gröbner basis method for solving our problem. In particular, it is shown that the isomorphism problem in the commutative case is decidable. The method can provide a precise solution even when k is not necessarily algebraically closed. That is, if two algebras are isomorphic over an algebraic extension k' of k, then it can find k'. We present a concrete algorithm based on it and show examples. In Section 6, an application of this algorithm is described.

Throughout this paper, $k\langle X|R\rangle$ denotes the non-commutative associative algebra generated by variables in X having R as defining relations.

2 Isomorphism Criterion

Let k be a field of arbitrary characteristic and A and B finite-dimensional finitely presented algebras over k, $k\langle X_A|R_A\rangle$ and $k\langle X_B|R_B\rangle$ respectively. Take $S_A = \{t_i\}$ and $S_B = \{s_j\}$ as k-linear bases of A and B so that $t_1 = 1_A$ and $s_1 = 1_B$. If necessary, by computing (finite) non-commutative Gröbner bases of R_A and R_B, we construct S_A and S_B, using a method similar to that in the commutative case ([1], METHOD 6.6). See [6],[5], and [4] for the details of non-commutative Gröbner bases. However,

note that the main purpose of this paper is not to use non-commutative Gröbner bases here, but to use commutative Gröbner bases as discussed in Section 5.

Now assume that $\sharp S_A = \sharp S_B = n$ (i.e. $\dim A = \dim B$). Let us define a k-linear mapping $\varphi : A \to B$ by image of each generator of A as follows:

$$\varphi(x_\lambda) = \sum_{j=1}^{n} a_{j\lambda} s_j \quad a_{j\lambda} \in k \tag{1}$$

where $X_A = \{x_\lambda\}$. If φ acts on each element t_i of S_A as ring homomorphism, then $\varphi(t_i)$ is formally determined under R_B in the following manner:

$$\varphi(t_i) = \sum_{j=1}^{n} b_{ji} s_j \quad b_{ij} \in k$$

Thus we have a square matrix $M_\varphi = (b_{ji})_{1 \le i,j \le n}$ of degree n. Here we assume that $\varphi(1_A) = 1_B$. That is, $b_{11} = 1$ and $b_{j1} = 0$ for $j \neq 1$.

Let $\varphi(R_A)$ be the set of all relations applied to the respective relations in R_A by φ as ring homomorphism. Then we have:

Theorem 1 (Isomorphism Criterion) *A and B are isomorphic as k-algebras $\Longleftrightarrow$ for the above φ, both $\varphi(R_A)$ under R_B and $detM_\varphi \neq 0$ can be satisfied in the field k.*

Proof. ($\Longrightarrow$) We apply the mapping φ to an isomorphism between A and B. Then $\varphi(R_A)$ under R_B and $detM_\varphi \neq 0$ can be simultaneously satisfied in k because φ is a homomorphism from A to B and a bijective k-linear mapping.

($\Longleftarrow$) We can naturally deem φ as a homomorphism from $k\langle X_A \rangle$ to B,

where $k\langle X_A\rangle$ is the free associative algebra generated by X_A over k. By assumption, φ is a surjective homomorphism with $R_A \subseteq \mathrm{Ker}\ \varphi$. Thus there exists a surjective homomorphism $\bar{\varphi}$: $k\langle X_A\rangle/\langle R_A\rangle \to B$ such that $\varphi = \bar{\varphi} \circ c$, where $\langle R_A\rangle$ is the two-sided ideal generated by R_A and c is the canonical mapping from $k\langle X_A\rangle$ onto $k\langle X_A\rangle/\langle R_A\rangle$. However, the assumption that $\dim A = \dim B$ implies the result since we can identify A as $k\langle X_A\rangle/\langle R_A\rangle$. ■

Example Decide whether $A = k\langle x|x^2 = x\rangle$ and $B = k\langle x|x^2 = 1\rangle$ are isomorphic. (In this case, both are *degenerate* binomial algebras, which were not treated in [9].)

Take $S_A = \{1, x\}$ and $S_B = \{1, x\}$ (using the same symbol x, if there is no confusion possible). Now, for a k-linear mapping φ from A to B, put $\varphi(x) = a + bx$, where $a, b \in k$. Thus we have

$$M_\varphi = \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}$$

$\varphi(R_A)$ is $\{\varphi(x^2) = \varphi(x)\}$. By "left hand side" $= \varphi(x)^2 = a^2 + 2abx + b^2x^2$, "right hand side" $= a + bx$, and $x^2 = 1$ in B, we have $2ab = b$ and $a^2 + b^2 = a$. Since $detM_\varphi = b$, when char $k \neq 2$, putting $a = 1/2$ and $b = \pm 1/2$, $detM_\varphi \neq 0$ can also be satisfied. Consequently,

$$\begin{cases} A \simeq B & \text{if char } k \neq 2 \\ A \not\simeq B & \text{if char } k = 2 \end{cases}$$

3 Radical Membership Problem

Let each $a_{j\lambda}$ in the expression (1) correspond one to one with a new indeterminate $x_{j\lambda}$ over k.

$$a_{j\lambda} \longrightarrow x_{j\lambda}$$

Of course, each $x_{\lambda j}$ is not in X_A or X_B. We define a commutative ring $R = k[x_{j\lambda}]$ (generated by $x_{j\lambda}$'s over k). φ is naturally extended to the k-linear mapping $\tilde{\varphi}$: $R\langle X_A|R_A\rangle \to R\langle X_B|R_B\rangle$ (coefficient ring extension). Thus

$$\tilde{\varphi}(x_\lambda) = \sum_{j=1}^{n} x_{j\lambda} s_j. \tag{2}$$

Let $M_{\tilde{\varphi}} = (y_{ji})$ denote the formal image of $M_\varphi = (b_{ji})$ by the above correspondence as ring homomorphism. Obviously, we have $detM_{\tilde{\varphi}} \in R$. Put $f(x_{j\lambda}) = detM_{\tilde{\varphi}}$.

Similarly, $\tilde{\varphi}(R_A)$ is the set of all relations applied to the respective relations in R_A by $\tilde{\varphi}$ as ring homomorphism. Now let the relations among $x_{j\lambda}$'s derived from $\tilde{\varphi}(R_A)$ using R_B be as follows:

$$\begin{cases} f_1(x_{j\lambda}) &= 0 \\ & \vdots \\ f_r(x_{j\lambda}) &= 0 \end{cases}$$

We have the polynomials $f_1(x_{j\lambda}), \cdots, f_r(x_{j\lambda})$ in R. Now put $I = (f_1, \cdots, f_r)$ (the ideal in R generated by these polynomials).

We say that $A \simeq B$ *for an extension* (k') if $k'\langle X_A|R_A\rangle \simeq k'\langle X_B|R_B\rangle$ for some algebraic extension k' of k. Then we have:

Theorem 2 (Isomorphism Test) *$A \simeq B$ for an extension $\Longleftrightarrow$ $f \notin \sqrt{I}$, where $\sqrt{I} = \{x \in R \mid \exists n \ s.t. \ x^n \in I\}$.*

Proof.

$A \simeq B$ for an extension k' $\Longleftrightarrow$ both $\varphi(R_A)$ under R_B and $f \neq 0$ can be satisfied in k' (by Theorem 1)

$\Longleftrightarrow$ there exist solutions of I satisfying $f \neq 0$

$\Longleftrightarrow$ $\neg$"every solution of I is a solution of $f = 0$"

$\Longleftrightarrow$ $\neg$"$f \in \sqrt{I}$ "

(by Hilbert's Nullstellensatz ([11]))

$\Longleftrightarrow$ $f \notin \sqrt{I}$

■

Corollary 1 *When k is algebraically closed, $A \simeq B \Longleftrightarrow f \notin \sqrt{I}$.*

4 Constant Elimination Technique

Before considering Gröbner basis methods, we show an efficient technique for computing the determinant $detM_{\tilde{\varphi}}$.

Theorem 3 (Determinant Property) *$detM_{\tilde{\varphi}} \in k[x_{j\lambda}; j \geq 2]$.*

Proof. First, from $\tilde{\varphi}(x_\lambda) = \sum_{j=1}^{n} x_{j\lambda} s_j$, the matrix $M_{\tilde{\varphi}}$ contains the column vectors $(x_{1\lambda}, \cdots, x_{n\lambda})$ for all λ's. Every element t_i of S_A is a k-linear combination of monomials of x_λ's in R_A. Since the image by $\tilde{\varphi}$ of a monomial of x_λ's contains products between $x_{1\mu}$ and $\sum_{j=1}^{n} x_{j\lambda} s_j$ for some μ's and λ's, the image of t_i makes a column vector containing products between $x_{1\mu}$

and $(x_{1\lambda}, \cdots, x_{n\lambda})$ for some μ's and λ's. Conversely, all $x_{1\nu}$'s appearing except in the first row vector derive from these products. Thus, by a property of determinant, we can eliminate all these products and in the new matrix, no $x_{1\nu}$'s appear except in the first row vector. Finally, since the first column vector is $(1, 0, \cdots, 0)$, the determinant can be calculated without using any entry of the first row vector. ■

By this theorem, we can propose a technique for calculating $detM_{\tilde{\varphi}}$ that we eliminate constant terms in the initial definition ((2), Section 3) of $\tilde{\varphi}$. That is,

[Constant Elimination Technique]

We assume that $\tilde{\varphi}$ is settled in the following manner:

$$\tilde{\varphi}(x_\lambda) = \sum_{j=2}^{n} x_{j\lambda} s_j. \tag{3}$$

We want to stress, however, that this assumption is only valid for computing $detM_{\tilde{\varphi}}$ and that we have to come back to (2) for developing $\tilde{\varphi}(R_A)$. In fact, there is not always an isomorphism such as (3) (see Example in Section 2).

The elimination of constant terms makes it easier to compute $\tilde{\varphi}(t_i)$ and $detM_{\tilde{\varphi}}$.

5 Gröbner Basis Method

In Section 3, we have reduced our problem into a radical ideal membership problem. So we can consider two Gröbner basis methods. One method is to compute the Gröbner basis of the radical directly and then to rewrite

the determinant modulo this basis. However, in this paper, this rewriting method will not be explained owing to limited space. See [10] for the details.

We will apply another method as follows:

[**Adjoining Method**] Introduce a new indeterminate t. Then, $A \simeq B$ for an extension $\Longleftrightarrow 1 \notin GB((I, tf-1))$ in $R[t]$.

Here $GB(J)$ denotes the (reduced) Gröbner basis of an ideal J calculated by Buchberger Algorithm ([1], ALGORITHM 6.3). This method is a well-known technique for the radical membership, based on an alternative description of Hilbert's zero point theorem. In fact, the correctness of it is shown by that "I and $f \neq 0$ in R have a solution" $\Longleftrightarrow$ "I and $tf-1$ in $R[t]$ have a solution".

We describe an algorithm based on the adjoining method.

Algorithm IT $(k; X_A, R_A; X_B, R_B)$: **Isomorphism Test**

Input: Field k; two finite presentations X_A, R_A; X_B, R_B.

Assumption: $dim A = dim B < \infty$, where $A = k\langle X_A | R_A \rangle$ and $B = k\langle X_B | R_B \rangle$.

Output: TRUE if $A \simeq B$ for an extension, otherwise FALSE.

Step 1: Find linear bases $S_A = \{t_i\}$ and $S_B = \{s_j\}$.

Step 2: Define a k-linear mapping: $\tilde{\varphi}(x_\lambda) = \sum_{j=1}^{n} x_{j\lambda} s_j$, where $X_A = \{x_\lambda\}$ and each $x_{j\lambda}$ is an indeterminate over k. Put $R = k[x_{j\lambda}]$.

Step 3: Define a k-linear mapping: $\tilde{\varphi}^*(x_\lambda) = \sum_{j=2}^{n} x_{j\lambda} s_j$ and make the matrix expression $M_{\tilde{\varphi}^*}$ of $\tilde{\varphi}^*$ under S_A and S_B.

% Constant Elimination Technique

Step 4: Compute $f = detM_{\tilde{\varphi}^*}$. % $detM_{\tilde{\varphi}^*} = detM_{\tilde{\varphi}}$ by Theorem 3

Step 5: Construct the set of polynomials $\{f_1, \cdots, f_r\}$ which consists of all coefficients of $\tilde{\varphi}(R_A)$ (under the assumption that $\tilde{\varphi}$ behaves as a ring homomorphism) w.r.t. each basis in S_B, using the relation R_B. Put $I = (f_1, \cdots, f_r)$ (the ideal in R).

Step 6: Compute $G_{\tilde{I}} = GB(\tilde{I})$ for the ideal $\tilde{I} = (I, tf - 1)$ in $R[t]$, w.r.t. the purely lexicographical monomial ordering with a variable ordering such that t is the smallest.

Step 7: If $1 \in G_{\tilde{I}}$ then return FALSE otherwise return TRUE.

Remark The purely lexicographical ordering of monomials is appropriate for finding an extension field such that A and B are isomorphic over it. This is based on the well-known property that the lexicographical Gröbner basis contains a univariate polynomial in the variable with the smallest ordering. The variable ordering such that t is the smallest may be just heuristic for obtaining a univariate polynomial with minimal degree. An example will be given later.

Let us give two examples of running **IT**, assuming that k is an algebraically closed field, say C, the field of complex numbers.

Example 1 Decide whether $A = k\langle x | x^3 = x^2 - 1\rangle$ and $B = k\langle x, y | x^2 = 4x, xy = yx = 0, y^2 = 3y\rangle$ are isomorphic.

Input: C; $\{x\}, \{x^3 = x^2 - 1\}$; $\{x, y\}, \{x^2 = 4x, xy = yx = 0, y^2 = 3y\}$.

Output: TRUE.

[Trace of **IT**]

Step 1: $S_A = \{1, x, x^2\}$ and $S_B = \{1, x, y\}$.

Step 2: $\tilde{\varphi}(x) = a + bx + cy$, where a, b, c are indeterminates over k. $R = k[a, b, c]$.

Step 3: $\tilde{\varphi}^*(x) = bx + cy$, and we have $M_{\tilde{\varphi}^*} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & b & 4b^2 \\ 0 & c & 3c^2 \end{pmatrix}$.

Step 4: $f = detM_{\tilde{\varphi}^*} = bc(3c - 4b)$.

Step 5: From $\tilde{\varphi}(x^3) = \tilde{\varphi}(x^2 - 1)$, $I = (a^3 - a^2 + 1, 12ab^2 + 3a^2b + 16b^3 - 4b^2 - 2ab, 9ac^2 + 3a^2c + 9c^3 - 3c^2 - 2ca)$.

Step 6: $G_{\tilde{I}} = GB((I, tf - 1)) = \{a + 9/25c^2 + 69/200ct + 3/2c - 9/25, b - 27/100c^2 - 207/800ct - 3/8c + 1/50, c^3 - 1/9c + 23/324t, t^2 + 144/23\}$ in $k[a, b, c, t]$, w.r.t. the purely lexicographical ordering with $a > b > c > t$.

Step 7: TRUE since $1 \notin G_{\tilde{I}}$.

Example 2 (non-commutative case) What about $A = k\langle x, y | xy = x, yx = 2y\rangle$ and $B = k\langle x, y | xy = x, yx = 0, y^2 = 1\rangle$?

Input: C; $\{x, y\}, \{xy = x, yx = 2y\}$; $\{x, y\}, \{xy = x, yx = 0, y^2 = 1\}$.

Output: FALSE.

[Trace of **IT**]

Step 1: $S_A = \{1, x, y\}$ and $S_B = \{1, x, y\}$.

Step 2: $\tilde{\varphi}(x) = a + bx + cy$, $\tilde{\varphi}(y) = a' + b'x + c'y$. $R = k[a, b, c, a', b', c']$.

Step 3: $\tilde{\varphi}^*(x) = bx + cy$, $\tilde{\varphi}^*(y) = b'x + c'y$. And $M_{\tilde{\varphi}^*} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & b & b' \\ 0 & c & c' \end{pmatrix}$.

Step 4: $f = detM_{\tilde{\varphi}^*} = bc' - b'c$.

Step 5: $I = (aa' + cc' - a, ab' + ba' + bc' - b, ac' + ca' - c, aa' + cc' - 2a', ab' + ba' + cb' - 2b', ac' + ca' - 2c')$.

Step 6: $G_{\tilde{I}} = GB((I, tf - 1)) = \{1\}$ in $k[a, b, c, a', b', c't]$, w.r.t. the purely lexicographical ordering with $a > a' > b > b' > c > c' > t$.

Step 7: FALSE since $1 \in G_{\tilde{I}}$.

Furthermore, when k is not algebraically closed, if two algebras are isomorphic over an algebraic extension k' of k, then we can find k' by simply inspecting $G_{\tilde{I}}$ (in **Step 6** of **IT**). In Example 1, when k is $\mathbb{Q}$, the field of rational numbers, $t^2 + 144/23$ has no solution in k. This implies that $A \not\simeq B$ over $\mathbb{Q}$, since if a, b, c (a solution of I) $\in \mathbb{Q}$, then $f \in \mathbb{Q}$ and hence $t = f^{-1} \in \mathbb{Q}$. From $G_{\tilde{I}}$, we can obtain the result that:

$$\mathbb{Q}(\sqrt{-23}, \alpha)\langle x | x^3 = x^2 - 1\rangle \simeq \mathbb{Q}(\sqrt{-23}, \alpha)\langle x, y | x^2 = 4x, xy = yx = 0, y^2 = 3y\rangle,$$

where α is a root of $x^3 - 1/9x + \sqrt{-23}/27 = 0$.

Finally, let us note the decidability of the isomorphism problem.

Theorem 4 (Decidability) *It is decidable whether two given finite-dimensional commutative finitely presented algebras are isomorphic for an extension.*

Proof. The dimension of an underlying linear space is computable by Gröbner basis method ([1], METHOD 6.6). If the dimensions of the two algebras are not equal, return FALSE. Otherwise employ **IT**. All we need to check therein is **Step 1**, i.e., to find the linear bases, but it is also possible by the same method (METHOD 6.6). ■

Remark In the non-commutative case, if finite (non-commutative) Gröbner

bases are given for two given relations, it is decidable because the linear bases and dimensions are computable by a method similar to METHOD 6.6.

6 Application

Here we want to claim the possibility of an application of **IT** to the factorization or irreducibility modulo a polynomial ideal. It would be interesting if we focus on the commutative case.

Given a polynomial ideal $\mathfrak{a}$ and a polynomial f in $k[x_1, \cdots, x_n]$. Consider two problems:

(a)Factorize f modulo $\mathfrak{a}$ over k.

(b)Decide the irreducibility of f modulo $\mathfrak{a}$ over k.

If there are an isomorphism φ and a quotient algebra $k[t_1, \cdots, t_m]/\mathfrak{b}$ such that $\varphi : k[x_1, \cdots, x_n]/\mathfrak{a} \simeq k[t_1, \cdots, t_m]/\mathfrak{b}$, then the factorization and irreducibility are preserved under φ: that is,

(1)if $f = f_1 \cdots f_r \bmod \mathfrak{a}$, then $\varphi(f) = \varphi(f_1) \cdots \varphi(f_r) \bmod \mathfrak{b}$ (and vice versa); and

(2)f is irreducible mod $\mathfrak{a}$ iff $\varphi(f)$ is irreducible mod $\mathfrak{b}$.

Therefore, as a candidate of the algebra $k[t_1, \cdots, t_m]/\mathfrak{b}$, a "simpler" form than the initial algebra $k[x_1, \cdots, x_n]/\mathfrak{a}$, will be appropriate; at least, it will be desirable if we can make m as small as possible, compared with n. Clearly the situation that $m = 1$ would be the best.

One strategy for solving the above problems is as follows:

[Variable Reduction by Isomorphism]

(1)Find an isomorphism φ and a quotient algebra $k[t_1, \cdots, t_m]/\mathfrak{B}$ such that $\varphi : k[x_1, \cdots, x_n]/\mathfrak{A} \simeq k[t_1, \cdots, t_m]/\mathfrak{B}$ and $m < n$, by **IT**

(2)Put $h(t_1, \cdots, t_m) := \varphi(f(x_1, \cdots, x_n))$.

(3)For (a): investigate the irreducibility of h modulo $\mathfrak{B}$.

For (b): factorize h modulo $\mathfrak{B}$, say $h = h_1 \cdots h_r$. Then $f = (\varphi^{-1}h_1) \cdots (\varphi^{-1}h_r)$ modulo $\mathfrak{A}$.

Remark: In a quotient algebra, a linear polynomial may not necessarily be irreducible. For instance, $x+3 = (x^2+1)(-x^2+2) \bmod (x^3 - x^2 + 1)$.

Example: Given $\mathfrak{A} = (x^2 - 4x, y^2 - 3y, xy)$ in $\mathbb{C}[x, y]$ and $f = 7x^3 + 6xy^2 - 9y^2 - 109x + 29y$. Then is f irreducible mod $\mathfrak{A}$?

First of all, consider the quotient algebra $A = \mathbb{C}[x, y]/\mathfrak{A}$. In A, $f = 3x + 2y$. By Example 1 in Section 5, we have $\psi = \varphi^{-1} : A \simeq B = \mathbb{C}[z]/(z^3 - z^2 + 1)$, where $\varphi = \begin{pmatrix} 1 & a & a^2 \\ 0 & b & 2ab + 4b^2 \\ 0 & c & 2ac + 3c^2 \end{pmatrix}$ and a, b, and c are a solution of $(I, tbc(3c - 4b) - 1)$. It follows that $\psi(f) = 1/D\{(-12b^2c + 9bc^2 - 2a^2c - 6ac^2) + (4ac + 6c^2)z - 2cz^2\}$, where $D = det\varphi = -4b^2c + 3bc^2$. Since we can easily show that $c \neq 0$, $\psi(f)$ is reducible in B. Thus f is reducible mod $\mathfrak{A}$.

As the example shows, if the image in the algebra with one variable is not linear over an algebraically closed field, then it is immediate that the given initial polynomial is reducible.

There may be other applications of **IT** (e.g. solving of algebraic equations), which will deserve some further detailed study.

7 Conclusion

We have proposed a Gröbner basis method for solving the isomorphism problem for finitely presented algebras. As a result, we have obtained the decidability in the commutative case. We hope that the isomorphism test can be applied to the factorization or irreducibility modulo a polynomial ideal.

We used REDUCE 3.3 on NEC PC-98 (BUG, Sapporo Japan) for calculating Gröbner bases.

References

[1] Buchberger, B., Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory, *Chapter 6 in Multidimensional Systems Theory (N. K. Bose ed.), D. Reidel Publishing Company* (1985), 184-232.

[2] Gianni, P., Trager B., and Zacharias G., Gröbner Bases and Primary Decomposition of Polynomial Ideals, *J. Symbolic Computation* **6** (1988), 149-168.

[3] Glass, A. M. W., The Word and Isomorphism Problems in Universal Algebra, *Proc. Universal Algebra and Lattice Theory, L. N. Math.* **1149** (1984), 123-128.

[4] Kandri-Rody, A. and Weispfenning, V., Non-commutative Gröbner Bases in Algebras of Solvable Type, *J. Symbolic Computation* **9** (1990), 1-26.

[5] Le Chenadec, P., Canonical Forms in Finitely Presented Algebras, *Research Notes in Theoretical Computer Science, Pitman*, (1986).

[6] Mora, T., Groebner bases for non-commutative polynomial rings, *Proc. AAECC3, L. N. Comp. Sci.* **229** (1986), 353-362.

[7] Seidenberg, A., Constructions in algebra, *Trans. Am. Math. Soc.* **197** (1974), 273-313.

[8] Shirayanagi, K., A Classification of Finite-dimensional Monomial Algebras, *Effective Methods in Algebraic Geometry (T. Mora and C. Traverso eds.), Progress in Mathematics* **94**, *Birkhäuser* (1991), 469-482.

[9] Shirayanagi, K., On the Isomorphism Problem for Finite-dimensional Binomial Algebras, *Proc. International Symposium on Symbolic and Algebraic Computation (ISSAC-90)* (1990), 106-111.

[10] Shirayanagi, K., Decision of Algebra Isomorphisms Using Gröbner Bases, *Proc. Riken Symposium (91.3.8)*, (1991), 10-16.

[11] Zariski, O. and Samuel, P., Commutative Algebra Vol. II, *Van Nostrand*, (1960).