TR-0786

Removing Redundant Critical Polynomials in Construction of Boolean Gröbner Bases

by
Y. Sato, S. Menju & K. Sakai

July, 1992

ICOT
Mita Kokusai Bldg. 21F
4-28 Mita 1-Chome
(03)3456-3191 ~ 5
Telex ICOT J32964
Minato-ku Tokyo 108 Japan

Institute for New Generation Computer Technology

Removing Redundant Critical Polynomials in Construction of Boolean Gröbner Bases

YOSUKE SATO† SATOSHI MENJU† KO SAKAI‡

† *Institute for New Generation Computer Technology*
21F, Mita Kokusai Building,
4-28, Mita 1-Chome, Minato-ku, Tokyo 108, Japan

‡ *Institute of Information Sciences and Electronics,*
University of Tsukuba
1-1-1, Tennoudai, Tsukuba-Shi 305, Japan

Abstract

Detecting redundant S-polynomials raise efficiency of Buchberger's algorithm to construct Gröbner bases as was first pointed out in [Buchberger 79]. One of the most practical criteria for it is given in terms of a homogeneous basis of a module of syzygies. This criterion is also applicable in suitable forms even when coefficient domains are not fields. We show we can apply this criterion in construction of Boolean Gröbner bases introduced in [Sakai 92]. We examine its efficiency with some experimental results of our implementation.

1 Introduction

Gröbner bases introduced in [Buchberger 65] are extremely useful to decide many problems of polynomial ideals. In case a coefficient domain is not a field, however, it is not so simple to construct or even define them. There have been several researches to extend coefficient domains. One of the most important concept made by them is weak Gröbner bases. They are characterized in terms of syzygy bases. When a coefficient domain is a Noetherian ring with some computability conditions, they can be constructed by calculating syzygy bases, although this calculation is not simple. When the domain is a principal ideal integral domain, [Möller 88] presents an simple algorithm to construct weak Gröbner bases using simple syzygy bases which are very similar to Tayler bases. It is also shown how to detect redundant S-polynomials by a similar method as [Gebauer 88].

In [Sakai 92] we introduced Boolean Gröbner bases to handle ideals in Boolean polynomial rings, i.e. polynomial rings over Boolean rings. We defined special reductions which are based on the own properties of Boolean polynomial rings. Using them, Boolean Gröbner bases are defined and calculated directly similarly as Buchberger's algorithm. In this paper, it is turned out that Boolean Gröbner bases coincide with weak Gröbner bases. Hence we can characterize Boolean Gröbner bases in terms of syzygy bases. It is also shown that we can easily construct syzygy bases in Boolean polynomial rings. Using

them we present a way to detect redundant critical polynomials for calculation of Boolean Gröbner bases.

In section 2, we first give a short review of Boolean Gröbner bases, and present a result in [Möller 88] which is used in this paper. In section 3, we describe our main results. In section 4, some of our experimental results are presented.

2 Preliminaries

2.1 Boolean Gröbner bases

A **Boolean ring** B is a commutative ring with identity such that every element of B is identical, i.e.

$$a^2 = a \quad \text{for all } a \in B.$$

It has the following important property:

$$a + a = 0 \quad \text{for all } a \in B.$$

We fix such a Boolean ring and will work on a polynomial ring $B[X_1, X_2, \ldots, X_n]$. We express elements of B by lowercase letters $a, b, c, \ldots$, power products by lowercase Greek letters $\alpha, \beta, \gamma, \ldots$ (possibly with suffix).
Let $\geq$ be an admissible total order on power products, i.e. it is a total order with the following properties:

1. If $\alpha \geq \beta$, then $\alpha\gamma \geq \beta\gamma$ for any power product γ.
2. $\alpha \geq 1$, for any non-empty power product α.

We fix such an order throughout of the paper. The leading power product of a polynomial f and its coefficient are denoted by $lpp(f)$ and $lc(f)$ respectively.
The rest part of f is denoted by $rest(f)$. The notation $a\alpha \triangleright h$ denotes a polynomial but also indicates $lc(a\alpha \triangleright h) = a$, $lpp(a\alpha \triangleright h) = \alpha$ and $rest(a\alpha \triangleright h) = h$. A polynomial f is called a **rule** if $lc(f)rest(f) = rest(f)$.

For a rule $f = a\alpha \triangleright h$, we define a reduction $\rightarrow_f$ on polynomials. It reduces a polynomial $b\alpha\gamma + g$ such that $ab \neq 0$ as follows:

$$b\alpha\gamma + g \rightarrow_f (1 + a)b\alpha\gamma + b\gamma h + g.$$

For a set F of rules, a polynomial h is said to be **reduced** to h' by F (denoted $h \rightarrow_F h'$) if $h \rightarrow_f h'$ for some $f \in F$. The transitive reflexive closure of $\rightarrow_F$ is denoted by $\stackrel{*}{\rightarrow}_F$. For any finite set F of polynomials, the reduction $\rightarrow_F$ has a termination property, i.e. there is no infinite reduction sequence of polynomials $f_0 \rightarrow_F f_1 \rightarrow_F f_2 \cdots$.
We abuse the notation $f\downarrow_F$ to denote one of irreducible forms of a polynomial f by $\rightarrow_F$, i.e. $f \stackrel{*}{\rightarrow}_F f\downarrow_F$ and $f\downarrow_F$ is not reducible by $\rightarrow_F$.

Let I be an ideal in $B[X_1, X_2, \ldots, X_n]$. A **Boolean Gröbner basis** of I is a finite set G of rules such that

1. G generates I
2. $g+g' \in I$ if and only if there is a polynomial h such that $g \stackrel{*}{\rightarrow}_G h$ and $g' \stackrel{*}{\rightarrow}_G h$. In particular, $g \in I$ if and only if $g \stackrel{*}{\rightarrow}_G 0$.

For a pair of rules f and g, their **critical polynomial**(denoted $\mathrm{cp}(f,g)$) is the following polynomial:

$$lc(g)\frac{lpp(g)}{\mathrm{GCD}(lpp(f),lpp(g))}f \ + \ lc(f)\frac{lpp(f)}{\mathrm{GCD}(lpp(f),lpp(g))}g.$$

where $\mathrm{GCD}(lpp(f),lpp(g))$ denotes the greatest common divisor of $lpp(f)$ and $lpp(g)$. For a polynomial h, **self critical polynomial**(denoted $\mathrm{scp}(h)$) is the following polynomial:

$$(1+lc(h))h.$$

Boolean Gröbner bases are characterized as follows.

Theorem 2.1.1 A finite set G of rules is a Boolean Gröbner basis if and only if $\mathrm{cp}(f,g) \stackrel{*}{\rightarrow}_G 0$ for each pair of rules $f,g \in G$ such that $\mathrm{GCD}(lpp(f),lpp(g)) \neq 1$.

We give an algorithm to construct Boolean Gröbner bases.

Let F be a finite set of polynomials.
input $E \longleftarrow F, R \longleftarrow \emptyset$
while $E \neq \emptyset$
choose $h \in E$
if $h\downarrow_R = 0$
then
$E \longleftarrow E - \{h\}$
else let $f = h\downarrow_R$ and
$E \longleftarrow (E-\{h\}) \cup \{\mathrm{scp}(f)\} \cup \{\mathrm{cp}(lc(f)f,g) \mid g \in R, \mathrm{GCD}(lpp(f),lpp(g)) \neq 1\}$
$R \longleftarrow R \cup \{lc(f)f\}$
end-if
end-while
output R
R is a Boolean Gröbner basis of the ideal generated by F.

2.2 Weak Gröbner bases

In this section we present a result in [Möller 88], which holds for a polynomial ring over any commutative ring with identity.

Let I be an ideal in $B[X_1,\ldots,X_n]$. A finite set $G \subset I$ of polynomials is called a **weak Gröbner basis** of I if the set of head monomials of G, i.e. the set $\{lc(g)lpp(g) \mid g \in G\}$, generates the ideal which is generated by the whole set of head monomials of I, i.e. the set $\{lc(h)lpp(h) \mid h \in I\}$.

Let $M = (a_1\alpha_1, a_2\alpha_2, \ldots, a_m\alpha_m)$ be a tuple of monomials. The tuple $(h_1, h_2, \ldots, h_m)$ of polynomials such that $\sum_{i=1}^{m} a_i\alpha_i h_i = 0$ is called a **syzygy** of M. A syzygy $(h_1, h_2, \ldots, h_m)$ of M is called **homogeneous** if h_i is a monomial for each i and $lpp(h_1)\alpha_1 = lpp(h_2)\alpha_2 = \cdots = lpp(h_m)\alpha_m$. The set of all syzygies of M clearly forms a module, which is denoted by S_M.

If a polynomial f has the following representation:

$$f = \sum_{i=1}^{l} g_i f_i$$

such that $lpp(f) = \max_{i=1}^{l} lpp(g_i)lpp(f_i)$.
It is called a **weak Gröbner representation** of f in terms of $f_1, \ldots, f_l$.

Theorem 2.2.1 Let I be an ideal generated by a set $G = \{g_1, \ldots, g_m\}$ of polynomials. Let L be an arbitrary homogeneous basis of the module of syzygies S_M, where M is the set of head monomials of G, i.e. $M = \{lc(g_1)lpp(g_1), \ldots, lc(g_m)lpp(g_m)\}$.
Then the following conditions are equivalent:

(C1) G is a weak Gröbner basis of I.

(C2) For each element $(h_1, \ldots, h_m) \in L$, $\sum_{i=1}^{m} h_i g_i$ has a weak Gröbner representation in terms of G.

3 Main results

3.1 Characterization of Boolean Gröbner bases

In this section, we show that Boolean Gröbner bases are characterized in terms of syzygy bases.

We first show Boolean Gröbner bases coincide with weak Gröbner bases.

Theorem 3.1.1 Let G be a finite set of rules and I be the ideal generated by G, then G is a Boolean Gröbner basis of I if and only if G is a weak Gröbner basis of I.

proof: Suppose G is a Boolean Gröbner basis and I be the ideal generated by G. Let $G = \{a_1\alpha_1 \triangleright f_1, \ldots, a_m\alpha_m \triangleright f_m\}$. Let $a\alpha \triangleright f$ be a polynomial in I. Then, $a\alpha \triangleright f \xrightarrow{*}_G 0$ by the definition of a Boolean Gröbner basis. Hence, $a\alpha$ must be reducible by some rule $a_i\alpha_i \triangleright f_i$. Therefore $\alpha = \alpha_i\gamma$ for some power product γ. If $(1 + a_i)a = 0$, i.e. $a = aa_i$, then $a\alpha = a\gamma a_i\alpha_i$. If $(1 + a_i)a \neq 0$, then $a\alpha = a\gamma a_i\alpha_i + (1 + a_i)a\alpha$.
Since $a\alpha \triangleright f \rightarrow_{a_i\alpha_i \triangleright f_i} (1 + a_i)a\alpha \triangleright (a\gamma f_i + f)$, $(1 + a_i)a\alpha \triangleright (a\gamma f_i + f) \in I$. Hence, $(1 + a_i)a\alpha$ is again reducible by some rule $a_j\alpha_j \triangleright f_j$. Repeating the same process, we have $(1+a_k)\cdots(1 + a_j)(1 + a_i)a = 0$ at some stage since $a\alpha \triangleright f \xrightarrow{*}_G 0$. Then, we can represent $a\alpha$ as a linear combination of $a_i\alpha_i, a_j\alpha_j, \ldots, a_k\alpha_k$.

For the converse, suppose $G = \{a_1\alpha_1 \triangleright f_1, \ldots, a_m\alpha_m \triangleright f_m\}$ is not a Boolean Gröbner basis. Let I be the ideal generated by G. Then, there is a polynomial $f \in I$ irreducible

by G. Note that $lc(f)a_i = 0$ whenever $lpp(f) \supseteq \alpha_i$.
If $lc(f)lpp(f) = \sum_{i=1}^{m} h_i a_i \alpha_i$ for some polynomials $h_1, h_2, \ldots, h_m$. Then, there must be some i such that $lpp(f) \supseteq \alpha_i$. Hence, $lc(f)a_i = 0$. Multiplying $lc(f)$ from both sides of the above equation, we can exclude $a_i\alpha_i$. Repeating the same process, we will get $lc(f)lpp(f) = 0$ to reach contradiction. □

Lemma 3.1.2 Let F be a finite set of rules. For each polynomial g, if $g \xrightarrow{*}_F 0$, then g has a weak Gröbner representation in terms of F.

proof: Suppose a polynomial g is reduced to g' by a rule $a\alpha \triangleright f$. Then $g = b\alpha\gamma + h$ for some power product γ, polynomial h and an element b of B such that $ab \neq 0$, and $g' = (1 + a)b\alpha\gamma + b\gamma f + h$. Hence, $g = (a\alpha \triangleright f)b\gamma + g'$.
If $lpp(g) = \alpha\gamma$, then $lpp(g) = lpp(a\alpha \triangleright f)lpp(b\gamma)$ and $lpp(g) \geq lpp(g')$.
If $lpp(g) > \alpha\gamma$, then $lpp(g) = lpp(g')$. Now $g \xrightarrow{*}_F 0$ implies there is a sequence of rules $f_1, \ldots, f_k \in F$ such that $g \rightarrow_{f_1} g_1 \rightarrow_{f_2} g_2 \cdots \rightarrow_{f_k} 0$. Applying the above procedure for each step, we can get a weak Gröbner representation of f in terms of F. □

Theorem 3.1.3 Let $G = \{g_1, \ldots, g_m\}$ be a finite set of rules and L be a homogeneous basis of the module of syzygies S_M, where M is the set of head monomials of G. Then G is a Boolean Gröbner basis if and only if $\sum_{i=1}^{m} h_i g_i \xrightarrow{*}_G 0$ for each element $(h_1, \ldots, h_m) \in L$.

proof: Since $\sum_{i=1}^{m} h_i g_i$ is in the ideal generated by G, "only if" part is trivial.
Suppose $\sum_{i=1}^{m} h_i g_i \xrightarrow{*}_G 0$ for each element $(h_1, \ldots, h_m) \in L$. Then, $\sum_{i=1}^{m} h_i g_i$ has a weak Gröbner representation in terms of G by Lemma 3.1.2. Hence, G is a weak Gröbner basis of the ideal generated by G by Theorem 2.2.1. Therefore G is a Boolean Gröbner basis by Theorem 3.1.1. □

3.2 Detecting redundant critical polynomials

Let M be a tuple of monomials $(a_1\alpha_1, \ldots, a_m\alpha_m)$. For each $1 \leq i < j < k \leq m$, let

$$\alpha_{ij} = \mathrm{LCM}(\alpha_i, \alpha_j) \text{ and } \alpha_{ijk} = \mathrm{LCM}(\alpha_i, \alpha_j, \alpha_k),$$

where LCM denotes the least common multiple.
For each $1 \leq i < j \leq m$, let

$$C_{ij} = \frac{a_j\alpha_{ij}}{\alpha_i}\vec{e}_i + \frac{a_i\alpha_{ij}}{\alpha_j}\vec{e}_j \quad \text{and} \quad C_i = (1 + a_i)\vec{e}_i,$$

where $\vec{e}_i$ is a unit vector such that the i-th component is 1.

Theorem 3.2.1 The sets $L = \{C_{ij} \mid 1 \leq i < j \leq m\} \cup \{C_i \mid 1 \leq i \leq m\}$ forms a homogeneous basis of S_M.

proof: Clearly C_{ij} and C_i are homogeneous syzygies of M.
Since a set of all homogeneous syzygies of M forms a basis of S_M, it suffices to show that every homogeneous syzygy of M can be represented as a linear combination of L. Let $(b_1\beta_1, \ldots, b_m\beta_m)$ be a homogeneous syzygy of M. Then, $b_1a_1 + \cdots + b_ma_m = 0$ and

$\beta_1\alpha_1 = \cdots = \beta_m\alpha_m$(call this γ).
Note first that $b_i\beta_i\vec{e}_i = b_ia_i\beta_i\vec{e}_i + b_i(1+a_i)\beta_i\vec{e}_i = b_ia_i\beta_i\vec{e}_i + b_i\beta_iC_i$ for each i.
Hence, $(b_1\beta_1, \ldots, b_m\beta_m)$
$= (b_1a_1\beta_1, \ldots, b_ma_m\beta_m) + \sum_{i=1}^m b_i\beta_iC_i$
$= ((b_1a_1 + \cdots + b_ma_m)\beta_1, b_2a_2\beta_2, \ldots, b_ma_m\beta_m) + b_2a_2\beta_1\vec{e}_1 + \cdots + b_ma_m\beta_1\vec{e}_1 + \sum_{i=1}^m b_i\beta_iC_i$
$= (0, b_2a_2\beta_2, \ldots, b_ma_m\beta_m) + b_2a_2\beta_1\vec{e}_1 + \cdots + b_ma_m\beta_1\vec{e}_1 + \sum_{i=1}^m b_i\beta_iC_i$
$= (0, b_2a_2\beta_2 + b_2a_1\beta_2, \ldots, b_ma_m\beta_m + b_ma_1\beta_m) + \sum_{i=2}^m (b_ia_i\beta_1\vec{e}_1 + b_ia_1\beta_i\vec{e}_i) + \sum_{i=1}^m b_i\beta_iC_i$
$= (0, b_2(a_2+a_1)\beta_2, \ldots, b_m(a_m+a_1)\beta_m) + \sum_{i=2}^m b_i(a_i(\gamma/\alpha_1)\vec{e}_1 + a_1(\gamma/\alpha_i)\vec{e}_i) + \sum_{i=1}^m b_i\beta_iC_i$
$= (0, b_2(a_2+a_1)\beta_2, \ldots, b_m(a_m+a_1)\beta_m) + \sum_{i=2}^m b_i(\gamma/\alpha_{1i})C_{1i} + \sum_{i=1}^m b_i\beta_iC_i$
Hence, $(0, b_2(a_2+a_1)\beta_2, \ldots, b_m(a_m+a_1)\beta_m)$ is also a homogeneous syzygy of M. Therefore we can apply the same procedure. Repeating this, we will finally be able to express $(b_1\beta_1, \ldots, b_m\beta_m)$ as a linear combination of L. □

Lemma 3.2.2 If $\alpha_k \subseteq \alpha_{ij}$ and $a_ka_ia_j = a_ia_j$, then C_{ij} can be represented as a linear combination of C_{ik}, C_{jk}, C_i and C_j.

proof: We first note the following equation which is easily checked by a simple calculation.

$$a_k\frac{\alpha_{ijk}}{\alpha_{ij}}C_{ij} + a_j\frac{\alpha_{ijk}}{\alpha_{ij}}C_{ik} + a_i\frac{\alpha_{ijk}}{\alpha_{jk}}C_{jk} = 0$$

Since $\alpha_k \subseteq \alpha_{ij}$ implies $\alpha_{ijk} = \alpha_{ij}$, a_kC_{ij} is written as a linear combination of C_{ik} and C_{jk}.
Note that $(1+a_k)C_{ij} = (1+a_k)a_j(\alpha_{ij}/\alpha_i)\vec{e}_i + (1+a_k)a_i(\alpha_{ij}/\alpha_j)\vec{e}_j$.
Since $a_ia_j + a_ka_ia_j = 0$,
$(1+a_k)a_j = a_j + a_ka_j = a_j + a_ka_j + a_ia_j + a_ka_ia_j = (1+a_k)a_j(1+a_i)$.
Similarly $(1+a_k)a_i = (1+a_k)a_i(1+a_j)$.
Therefore $(1+a_k)C_{ij} = (1+a_k)a_j(1+a_i)(\alpha_{ij}/\alpha_i)\vec{e}_i + (1+a_k)a_i(1+a_j)(\alpha_{ij}/\alpha_j)\vec{e}_j = (1+a_k)a_j(\alpha_{ij}/\alpha_i)C_i + (1+a_k)a_i(\alpha_{ij}/\alpha_j)C_j$. Hence we can represent C_{ij} as a linear combination of C_{ik}, C_{jk}, C_i and C_j. □

This lemma is generalized as follows.

Corollary 3.2.3 If $\alpha_{n_k} \subseteq \alpha_{ij}$ for each $k = 1, \ldots, l$ and $(a_{n_1} \vee a_{n_2} \cdots \vee a_{n_l})a_ia_j = a_ia_j$, then C_{ij} can be represented as a linear combination of $C_{in_1}, C_{in_2}, \ldots, C_{in_l}$ and $C_{jn_1}, C_{jn_2}, \ldots, C_{jn_l}$ and C_i, C_j.
Where the symbol $\vee$ denotes the sum of Boolean algebra, i.e. $a \vee b = a + b + ab$ for each element $a, b \in B$.

proof: We can show that each of $a_{n_1}C_{ij}, \ldots, a_{n_l}C_{ij}$ and $(1 + a_{n_1} \vee a_{n_2} \vee \cdots \vee a_{n_l})C_{ij}$ is represented as a linear combination of $C_{in_1}, C_{in_2}, \ldots, C_{in_l}$ and $C_{jn_1}, C_{jn_2}, \ldots, C_{jn_l}$ and C_i, C_j similarly as in the proof of the lemma. Note that we can express $a_{n_1} \vee a_{n_2} \vee \cdots \vee a_{n_l}$ as $b_1a_{n_1} + b_2a_{n_2} + \cdots + b_la_{n_l}$ by some elements $b_1, b_2, \ldots, b_l$ of B. Hence, $C_{ij} = (1 + a_{n_1} \vee a_{n_2} \vee \cdots \vee a_{n_l})C_{ij} + b_1a_{n_1}C_{ij} + \cdots + b_la_{n_l}C_{ij}$. □

Using this Corollary, we can improve the algorithm by removing redundant critical polynomials as follows.

Let F be a finite set of polynomials.

input $E \longleftarrow F, R \longleftarrow \emptyset$
  while $E \neq \emptyset$
    choose $h \in E$
      if $h\downarrow_R = 0$
        then
        $E \longleftarrow E - \{h\}$
        else let $f = h\downarrow_R$ **and**
        $E \longleftarrow (E - \{h\}) \cup \{\mathrm{scp}(f)\} \cup \{\mathrm{cp}(lc(f)f, g) | \, g \in R, \neg\mathrm{Red}(f, g, R)\}$
        $R \longleftarrow R \cup \{lc(f)f\}$
      end-if
  end-while
output R

R is a Boolean Gröbner basis of the ideal generated by F.

A criterion to detect redundant critical polynomials is given by $\mathrm{Red}(f, g, R)$, which holds if $\mathrm{GCD}(lpp(f), lpp(g)) = 1$ or there are rules $h_1, \ldots h_l \in R$ distinct from $lc(f)f$ and g such that $(lc(h_1) \vee \cdots \vee lc(h_l))lc(f)lc(g) = lc(f)lc(g)$ and $lpp(h_i) \subseteq \mathrm{LCM}(lpp(f), lpp(g))$ for each $i = 1, \ldots, l$.

4 Experimental data

We give some experimental data from our implementation[Sato 91] to examine effectiveness of our criterion to detect redundant critical polynomials.

The following equations express a constraint over sets.

```
S1/\ ~{a1,a8}/\(({a5,a6}/\S2)\/(S3/\S4))=(S5/\S6)\/(S2/\S4/\S7)\/S8
S4/\S5/\{a3,a4,a7}=0
S5/\S8/\ ~{a5,a9}=0
S2/\ ~{a10}=S4\/S8
S2/\ ~{a11}=S7\/S10\/S9
S3/\S9/\ ~{a1,a2}=0
S3/\S10/\ ~{a11,a12}=0
S11/\ ~{a13}=S12\/S7
S7/\S12/\ ~{a1,a14}=0
{a4}/\S6={a4}
{a1}/\S12={a1}
S1\/S10\/{a1,a2}=((S11\/(S13/\ ~{a1,a10}))/\{a2,a4})\/S10
((S1\/S2\/S11)/\{a1,a2})\/S6=S10\/S12\/(S7/\ ~{a3})\/S2
S2\/S3\/S5\/{a4}=S1\/({a1,a2}/\(S3\/S10\/{a3,a4,a7}))
```

The symbols `a1,a2,a3,...` are constant symbols of elements. The symbols `S1,S2,S3,...` are variables, and their domain is a family of all the finite or co-finite subsets of `{a1,a2,a3, ...}`. The symbols `/\`, `\/` and `~` are intersection, union and complement respectively. The symbol `0` denotes an empty set.

The set of all finite or co-finite subsets of {a1,a2,a3,...} forms a Boolean algebra(call B). Hence, each equation is translated to an equation of a polynomial ring B[S1,S2,S3,...]. We implemented a solver which calculate Boolean Gröbner bases in this polynomial ring.

In the following table, we give some data of the calculations of Boolean Gröbner bases. Each constraint #1 - #7 is given as a conjunction of equations similarly as the above example. The numbers in each column are the number of elements, variables, actually created critical polynomials, removed critical polynomials by our criterion and created self critical polynomials.

	#1	#2	#3	#4	#5	#6	#7
elements	4	6	9	14	18	23	7
variables	13	13	12	13	13	13	17
created cp's	1058	1192	1234	886	1006	1021	6027
removed cp's	1272	1371	1921	1165	1332	1400	18532
created sp's	163	207	195	181	198	207	460

References

[Buchberger 65] Buchberger, B. (1965). Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal.*PhD thesis, Universität Innsbruck.*

[Buchberger 79] Buchberger, B. (1979). A criterion for detecting unnecessary reductions in the construction of Gröbner bases. *EUROSAM 79. Springer Lec. Notes Comp. Sci.* **72**, 3-21.

[Gebauer 88] Gebauer, R., Möller, H.M. (1988). On an installation of Buchberger's algorithm. *J.Symbol.Comput.* **6**, 275-286.

[Möller 88] Möller, H.M. (1988). On the Construction of Gröbner Bases Using Syzygies *J.Symbol.Comput.* **6**, 345-359.

[Sato 91] Sato, Y., Sakai, K., Menju, S. (1991). Solving Constraints over Sets by Boolean Gröbner Bases. *Proceeding of The Logic Programming Conference '91* 73-79.

[Sakai 92] Sakai, K., Sato, Y., Menju, S. (1992). Boolean Gröbner bases. *ICOT Technical Report*. also submitted for publication.