ACM SIGSAM Bull., Vol.12/2, May 1978, 27-36.

AN IMPROVED ALGORITHMIC CONSTRUCTION OF GRÖBNER-BASES FOR POLYNOMIAL IDEALS

by

C. Kollreider,B. Buchberger
Johannes Kepler Universität
A-4045 Linz, Austria

Introduction

In /1/, /2/ we gave an algorithm for the construction of so called Gröbner-bases of polynomial ideals. In this paper we present some new theoretical results by which the complexity of this algorithm may drastically be reduced in many cases.

As we have pointed out in /2/ and /3/ (see also /4/, /6/ and /7/) many problems of constructive polynomial ideal theory may be solved easily once one has found Gröbner-bases for the given ideals. Therefore the efficient construction of Gröbner-bases may be considered to be a central problem in this area.

Our method for the effective construction of Gröbner-bases is based on the following

Criterion 1 (see /3/):

Let F be a finite set of polynomials.

F is a Gröbner-basis :<=>

for all $f,g \in F$: the "S-polynomial of" f and g "M-reduces" to 0 **(with respect to F).**

(For the exact definitions see /3/, Section 1).

The following algorithm for the construction of Gröbner-bases is derived from this criterion in a natural way:

Input: a finite set F of polynomials

Output: a finite set G of polynomials

such that: 1. the ideal generated by F = the ideal generated by G,

2. G is a Gröbner-basis.

Algorithm A1:

```
G: = F; B: = ∅;
while B ≠ G × G do
   begin
      (f,g): = "one of the pairs in" (G×G) - B
      h: = "a normalform of the"
           "S-polynomial of" f and g
           (with respect to G);
      if h ≠ 0 then G: = G∪{h};
      B: = B∪{(f,g)}
   end
```

For the assessment of the complexity of the algorithm the reader need not know the exact definition of the two functions "normalform of" and "S-polynomial of" (see /2/ and /3/, Section 1). It suffices to know that the construction of the normalform of the S-polynomial is the most complex statement within each cycle and, in fact, is rather clumsy. (More exactly, a suitable algorithm for the construction of a normalform for polynomial f has time complexity $O(t^2)$ where t is the order number of the highest term of f in a lexicographical ordering of the terms).

Now, the overall complexity of the algorithm is determined by the number of executions of the while-statement. If the variable G were not altered during the execution of the algorithm this number would equal $\frac{|F|.(|F|-1)}{2}$. (By the way, this is the case if G is already a Gröbner-basis).

In general however, new polynomials may be added to G. This is the reason why it is difficult to give a reasonable upper bound for the number of executions of the while-statement. (Thus, in our algorithm, while cannot be replaced by for in a straightforward manner!). Instead of trying to determine such an upper bound let us prove some theoretical results that enable us to replace the original version of the algorithm sketched above by a more sophisticated one. In many cases this new version needs considerable fewer executions of the while-statement.

The improved algorithm is based on a new Criterion 2 (see Theorem 1.5) characterizing Gröbner-bases. Criterion 2 is obtained by carefully analyzing the proof of Criterion 1. Roughly speaking, the analysis of this proof leads to the notion of "Sufficient" subsets B of $F \times F$ (see Definition 1.4) for which we can prove the following

Theorem:

B is sufficient (with respect to F),

$$\bigwedge_{(f,g)\in B} \left.\begin{array}{l}\textbf{S-polynomial of } f \textbf{ and } g \text{ is}\\ \text{M-reducible to } 0\end{array}\right\} \Longrightarrow$$

$$\Longrightarrow F \text{ is a Gröbner-basis.}$$

Furthermore, we observe that in many cases one can construct sufficient sets that have considerable fewer elements than $F \times F$. In extreme cases there are sufficient sets having |F|-1 elements. (In the worst case, however, $F \times F$ is the only sufficient set with respect to F).

The new version of the algorithm, then, is obtained by changing the termination criterion of the while-statement in the following way:

```
Algorithm A2: G: = F; B: = ∅;
              while B  is not sufficient with
                       respect to G  do
                 begin
                    (f,g): = ...
                    ...
                 end;
```

In order to work out the idea sketched above we proceed in three stages:

In Section 1, we define the notion of sufficient sets with respect to F and prove the above theorem. We also give an example of sufficient sets that may demonstrate the usefulness of this notion for reducing the complexity of the algorithm.

In Section 2, we investigate sufficient sets that do not contain proper sufficient subsets (= minimal sufficient sets). We show that, for a given set F of polynomials, all minimal sufficient sets have the same number of elements. This is a necessary prerequisite for Section 3.

In Section 3, we give an algorithm for constructing minimal sufficient sets. By the results of Section 2, we hence have a method for constructing sufficient sets with a minimal number of elements. This method then may be used as a part of Algorithm A2.

1. Sufficient sets

We assume the reader to be familiar with the basic definitions and the elementary properties of the basic notions as put together in /3/, Section 1 and 2. As we have done in /3/ we consider finite sequences of polynomials instead of finite sets. This is for technical reasons only. Furthermore we apply Convention 1.2. in /3/ on the use of variables.

The only notational change concerns the predicate Multiple: we write $s \leq_M t$ for Multiple (t,s).

1.1. Definition:

$$\text{Indexset}\ (F): = \{k \mid 1 \leq k \leq L(F),\ F_k \neq 0\}$$

$$\text{Pairset}\ (F): = \{(k,l) \mid 1 \leq k < l \leq L(F),\ F_k \neq 0,\ F_l \neq 0\}$$

$$\text{Pathset}\ (F): = \{J^l \mid l \geq 1\}$$

where J: = Indexset (F).

1.2. Convention:

In addition to Convention 1.2. in /3/ we also fix the use of the following variables:

p,q ... variables ranging over Pairset (F)

u,v,w ... variables ranging over Pathset (F)

Again, p_1, p_2, u_i denote the first, second, i-th component of pair p and path u, respectively.

1.3. Definition:

$L(u)$: = length (i.e. number of components) of the sequence u

p is connected by u: <=>

$p_1 = u_1,\ p_2 = u_l$, where $l = L(u)$.

u is contained in R: <=>

$$R \subseteq \text{Pairset}(F),$$
$$\bigwedge_{1 \leq i < L(u)} ((u_i, u_{i+1}) \in R \vee (u_{i+1}, u_i) \in R)$$

summit (u,F): = $\text{Lcm}\ (\text{Hterm}\ (F_{u_1}), \ldots, \text{Hterm}\ (F_{u_l}))$, where $l = L(u)$.

1.4. Definition:

B sufficient with respect to F: <=>

$$B \subseteq \text{Pairset}\ (F),$$
$$\bigwedge_p \bigvee_u\ (p \text{ connected by } u,\ u \text{ contained in } B,\ \text{summit}\ (u,F) \leq_M \text{summit}\ (p,F))\ .$$

1.5. Theorem:

Let B be a sufficient set with respect to F. Then the following statements are equivalent:

(G) F is a Gröbner-basis

(G8) $\bigwedge_{p \in B} \text{Spol}(F_{p_1}, F_{p_2}) > 0.$

1.6. Proof:

(G) => (G8): This is immediate from (G2) in Theorem 3.3. in /3/.

(G8) => (G):

Sketch:

(G8) is a weaker version of (G2) in Theorem 3.3. of /3/. Nevertheless it is possible to establish the implication (G8) => (G3) refining the proof of (G2) => (G3). The crucial point of this proof is the treatment of Case IIb, line (54). What is really needed at this point is the validity of the following statement:

$$(*) \quad \bigwedge_t \bigwedge_p\ (t \ {}_M{\geq}\ \text{Hterm}(F_{p_1}),\ t \ {}_M{\geq}\ \text{Hterm}(F_{p_2}) \Rightarrow \Rightarrow \text{Spol}(F_{p_1}, F_{p_2}) > 0).$$

(*) is a trivial consequence of (G2). A careful analysis of the whole proof reveals that instead of (*) we can do with

$$(**) \quad \bigwedge_t \bigwedge_p\ [t \ {}_M{\geq}\ \text{Hterm}(F_{p_1}),\ t \ {}_M{\geq}\ \text{Hterm}(F_{p_2}) \Rightarrow \Rightarrow \bigvee_u\ (p \text{ connected by } u,\ \bigwedge_{1 \leq k < L(u)} \text{Spol}(F_{u_k}, F_{u_{k+1}}) > 0,\ \text{summit}(u,F) \leq_M t)].$$

The first two quantifiers in $(\ast\ast\ast)$ may be interchanged. Then it is easy to see that $(\ast\ast\ast)$ is a consequence of (G8) and the fact that B is sufficient.

Details:

Under the assumption that (G8) is fulfilled we shall show that all M-reductions of a given polynomial f lead to the same normalform, i.e.

$$\text{(G3)}\quad \bigwedge_{f,g,g'} (f \mathrel{\cdot\!>} \underset{\sim}{g} \text{ and } f \mathrel{\cdot\!>} \underset{\sim}{g'} \Rightarrow g = g').$$

Clearly (G3) is equivalent to

$$\text{(G3')}\quad \bigwedge_{t} \bigwedge_{f,g,g'} (\mathrm{Hterm}(f) = t \text{ and } f \mathrel{\cdot\!>} \underset{\sim}{g} \text{ and } f \mathrel{\cdot\!>} \underset{\sim}{g'} \Rightarrow g = g').$$

We prove (G3') by induction on t with respect to the lexicographical ordering $<_T$ on the set of all terms (see Def. 1.1 in /3/).

$$\boxed{t = x_1^o \dots x_n^o}$$

Let f,g,g' be such that $\mathrm{Hterm}(f) = x_1^o \dots x_n^o$, $f \mathrel{\cdot\!>} \underset{\sim}{g}$ and $f \mathrel{\cdot\!>} \underset{\sim}{g'}$.

Case 1: $\bigvee_{1 \le i \le L(F)} (\mathrm{Hterm}(F_i) = x_1^o \dots x_n^o,\ F_i \neq 0)$

In this case we have $g = 0 = g'$.

Case 2: $\neg \bigvee_{1 \le i \le L(F)} (\mathrm{Hterm}(F_i) = x_1^o \dots x_n^o,\ F_i \neq 0)$

In this case we have $g = f = g'$.

$$\boxed{t \;{}_T\!\!> x_1^o \dots x_n^o}$$

Let f,g,g' be such that $\mathrm{Hterm}(f) = t$, $f \mathrel{\cdot\!>} \underset{\sim}{g}$ and $f \mathrel{\cdot\!>} \underset{\sim}{g'}$. By J we denote the set of all indices i such that $1 \le i \le L(F)$, $F_i \neq 0$ and $\mathrm{Hterm}(F_i) \le_M t$.

We distinguish the cases $J = \emptyset$ and $J \neq \emptyset$.

Case 1: $J = \emptyset$.

From $J = \emptyset$, $f \mathrel{\cdot\!>} \underset{\sim}{g}$ and $f \mathrel{\cdot\!>} \underset{\sim}{g'}$ we easily deduce $\mathrm{Head}(g) = \mathrm{Head}(f) = \mathrm{Head}(g')$, $\mathrm{Rest}(f) \mathrel{\cdot\!>} \underset{\sim}{\mathrm{Rest}(g)}$ and $\mathrm{Rest}(f) > \underset{\sim}{\mathrm{Rest}(g')}$.

Because of $\mathrm{Hterm}(\mathrm{Rest}(f)) <_T t$ we may apply the induction hypothesis which yields $\mathrm{Rest}(g) = \mathrm{Rest}(g')$. Together with $\mathrm{Head}(g) = \mathrm{Head}(g')$ this implies $g = g'$.

Case 2: $J \neq \emptyset$.

(1) By induction hypothesis there is exactly one polynomial h_o such that $\mathrm{Rest}(f) \mathrel{\cdot\!>} \underset{\sim}{h_o}$. Given $i \in J$ let f_i and h_i be the uniquely determined polynomials with $\mathrm{Head}(f) \overset{1}{\underset{F,t,i}{\mathrel{\cdot\!>}}} f_i$ and $f_i + h_o \mathrel{\cdot\!>} \underset{\sim}{h_i}$.

(According to Def. 1.5 in /3/ the symbol $\overset{1}{\underset{F,t,i}{\mathrel{\cdot\!>}}}$ is used to denote one-step-M-reduction with respect to the polynomial F_i.) The uniqueness of f_i is clear, the uniqueness of h_i follows from the induction hypothesis and from $\mathrm{Hterm}(f_i + h_o) <_T \mathrm{Hterm}(f)$.

From $\mathrm{Rest}(f) \mathrel{\cdot\!>} h_o$ we deduce $f \mathrel{\cdot\!>} \mathrm{Head}(f) + h_o$, from $\mathrm{Head}(f) \overset{1}{\underset{F,t,i}{\mathrel{\cdot\!>}}} f_i$ we deduce

$$\mathrm{Head}(f) + h_o \overset{1}{\underset{F,t,i}{\mathrel{\cdot\!>}}} f_i + h_o.$$

Therefore we have

$f \mathrel{\cdot\!>} \mathrm{Head}(f) + h_o \mathrel{\cdot\!>} f_i + h_o \mathrel{\cdot\!>} \underset{\sim}{h_i}$ which implies $f \mathrel{\cdot\!>} \underset{\sim}{h_i}$.

(2) Under the assumption that (G8) is true we now prove that for every pair $(i,j) \in (J \times J)$ we have $h_i = h_j$. Of course we may assume $i < j$, i.e. $(i,j) \in \mathrm{Pairset}(F)$. The set B being sufficient with respect to F there exists an element $u \in \mathrm{Pathset}(F)$ such that

(i) (i,j) is connected by u,

(ii) u is contained in B,

(iii) $\mathrm{summit}\ (u,F) \le_M \mathrm{summit}((i,j),F)$.

From (ii) and (G8) we obtain

$$\text{(iv)}\quad \bigwedge_{1 \le k \le L(u)} \mathrm{Spol}(F_{u_k}, F_{u_{k+1}}) \mathrel{\cdot\!>} 0.$$

On the other hand we have

$\mathrm{Hterm}(F_{u_k}) \le_M \mathrm{summit}(u,F) \le_M \mathrm{summit}((i,j),F) \le_M \mathrm{Hterm}(f)$ by (iii) and therefore

$$\text{(v)}\quad \bigwedge_{1 \le k \le L(u)} u_k \in J.$$

An easy calculation shows (see (55) in /3/,p.26)

$$\text{(vi)}\quad \bigwedge_{1 \le k \le L(u)} [(f_{u_k} + h_o) - (f_{u_{k+1}} + h_o) = - \frac{\mathrm{Hcoef}(f)}{\mathrm{Hcoef}(F_{u_k})\mathrm{Hcoef}(F_{u_{k+1}})} \cdot \frac{\mathrm{Hterm}(f)}{\mathrm{Lcm}(\mathrm{Hterm}(F_{u_k}), \mathrm{Hterm}(F_{u_{k+1}}))} \cdot \mathrm{Spol}(F_{u_k}, F_{u_{k+1}})],$$

the polynomials h_o and f_{u_k} being defined as in (1).

From (iv) and (vi) we deduce

$$\text{(vii)}\quad \bigwedge_{1 \le k < L(u)} [(f_{u_k} + h_o) - (f_{u_{k+1}} + h_o) \mathrel{\cdot\!>} 0]$$

In view of Lemma 2.4 in /3/ we therefore get

$$\text{(viii)}\quad \bigwedge_{1 \le k < L(u)} [(f_{u_k} + h_o) \overset{\mathrm{succ}}{\nabla} (f_{u_{k+1}} + h_o)].$$

Combining this with $f_{u_k} + h_o > \underset{\sim}{h_{u_k}}$, $f_{u_{k+1}} + h_o > \underset{\sim}{h_{u_{k+1}}}$, $\mathrm{Hterm}(f_{u_k} + h_o) <_T \mathrm{Hterm}(f)$ and $\mathrm{Hterm}(f_{u_{k+1}} + h_o) <_T$ $<_T \mathrm{Hterm}(f)$ we obtain by induction hypothesis

$$\text{(ix)}\quad \bigwedge_{1 \le k < L(u)} h_{u_k} = h_{u_{k+1}}.$$

Statements (i) and (ix) yield the assertion $h_i = h_j$.

(3) We complete the proof by showing that $g = h_i$ for some $i \in J$. In the same manner we could show $g' = h_j$ for some $j \in J$. By what we have proved in (2) we thus know $g = h_i = n_j = g'$.

In fact, considering the definition of M-reduction we easily see that there must be a polynomial g_o and an element $i \in J$ such that $f \rightarrow \mathrm{Head}(f)+g_o \overset{1}{\rightarrow}$ $\overset{1}{\rightarrow} f_i+g_o \rightarrow g$ where f_i is the unique polynomial with $\mathrm{Head}(f) \overset{1}{\underset{F,t,i}{\rightarrow}} f_i$. From $f \rightarrow \mathrm{Head}(f)+g_o$ we obtain $\mathrm{Rest}(f) \rightarrow g_o$. On the other hand we have $\mathrm{Rest}(f) \rightarrow \underset{\sim}{h_o}$, the polynomial h_o being defined as in (1). Applying the induction hypothesis we get $g_o \rightarrow h_o$. Let m be a natural number ≥ 0 and let $g_1,\ldots,g_m$ be polynomials such that $g_m = h_o$ and $g_{k-1} \rightarrow g_k$ for $1 \leq k \leq m$. By Lemma 2.4 in /3/ we get $f_i+g_{k-1} \overset{succ}{\nabla} f_i+g_k$ for $1 \leq k \leq m$. Together with $\mathrm{Hterm}(f) \underset{T}{\rightarrow} \mathrm{Hterm}(f_i+g_k)$ for $0 \leq k \leq m$ and $g_m = h_o$ this yields $f_i+g_o \overset{succ}{\nabla} f_i+h_o$ by induction hypothesis. Because of $f_i+g_o \rightarrow \underset{\sim}{g}$ and $f_i+h_o \rightarrow \underset{\sim}{h_i}$ we must have $g = h_i$. □

1.7. Example

Consider $F = (F_1,\ldots,F_5)$ such that

$\mathrm{Hterm}(F_1) = x^3y^2$

$\mathrm{Hterm}(F_2) = x^3yz$

$\mathrm{Hterm}(F_3) = xyz^2$

$\mathrm{Hterm}(F_4) = z^3$

$\mathrm{Hterm}(F_5) = x^3yz^3$

The following set B is sufficient with respect to F:

$B := \{(1,2),(2,3),(3,4),(2,5)\}$.

The sufficiency of B can be seen by the algorithm given in Section 3. Of course, it is also possible (but tedious) to check this by the very definition.

Note that $|B| = 4$ whereas $|\mathrm{Pairset}(F)| = 10$.

2. Minimal sufficient sets

Our next goal is the investigation of sufficient sets having as few elements as possible. It is clear that such sets are optimal for controlling the while-statement in the algorithm A2.

2.1. Definition:

B minimal sufficient with respect to F: <=>

> B is sufficient w.r.t. F and no proper subset of B is sufficient w.r.t. F.

Of course, it is not obvious from the definition that a minimal sufficient set is also "optimal" in the sense of having as few elements as possible. At first sight one could guess that minimal sufficient sets B_1 and B_2 with $|B_1| < |B_2|$ may exist. Then B_2 would not be "optimal". However we can show that all sets B that are minimal sufficient with respect to a fixed F have the same number of elements. This section is dedicated to the proof of this fact.

2.2. Definition:

Lower (p,q,F):<=> summit(p,F) $\leq_M$ summit (q,F)

Equiv (p,q,F):<=> summit(p,F) = summit(q,F)

Lowerset(p,F): = $\{q \in \mathrm{Pairset}(F) \mid \mathrm{Lower}(q,p,F)\}$

Equiset(p,F): = $\{q \in \mathrm{Pairset}(F) \mid \mathrm{Equiv}(p,q,F)\}$.

2.3. Remark:

The relation "Lower(p,q,F)" is a quasi-ordering on Pairset(F), i.e. it is reflexive and transitive.

The relation "Equiv(p,q,F)" is an equivalence relation on Pairset(F).

2.4. Definition:

$\mathrm{Rel}_1(p,F)$: =
= $\{(i_1,i_2) \in J \times J \mid \bigvee_u [i_1 = u_1, i_2 = u_{L(u)},$
u is contained in Lowerset(p,F)-Equivset(p,F)$]\}$
Where J: = Indexset(F)
$\mathrm{Rel}_2(p,F)$: =
= $\{(i_1,i_2) \in J \times J \mid \bigvee_u [i_1 = u_1, i_2 = u_{L(u)},$
u is contained in Lowerset(p,F)$]\}$
Where J: = Indexset(F).

2.5. Lemma:

(1) For every $p \in \mathrm{Pairset}(F)$ the relations $\mathrm{Rel}_1(p,F)$ and $\mathrm{Rel}_2(p,F)$ are equivalence relations on Indexset(F).

(2) $\mathrm{Rel}_1(p,F) \subseteq \mathrm{Rel}_2(p,F)$ for every $p \in \mathrm{Pairset}(F)$, i.e. $\mathrm{Rel}_1(p,F)$ is finer than $\mathrm{Rel}_2(p,F)$.

Proof: trivial □

2.6. Convention:

The set of all equivalence classes modulo $\mathrm{Rel}_1(p,F)$ (resp. $\mathrm{Rel}_2(p,F)$) will be denoted by $\mathrm{Part}_1(p,F)$ (resp. $\mathrm{Part}_2(p,F)$).

2.7. Definition:

$\mathrm{Rel}_3(p,F)$: =
= $\{(J_1,J_2) \in \mathrm{Part}_1(p,F) \times \mathrm{Part}_1(p,F) \mid$
$\bigvee_{i_1} \bigvee_{i_2} [i_1 \in J_1, i_2 \in J_2, (i_1,i_2) \in \mathrm{Rel}_2(p,F)]\}$.

2.8. Lemma:

For any $p \in \mathrm{Pairset}(F)$ the relation $\mathrm{Rel}_3(p,F)$ is an equivalence relation on $\mathrm{Part}_1(p,F)$.

Proof:

The reflexivity and the symmetry of $\mathrm{Rel}_3(p,F)$ are clear, the transitivity follows from $\mathrm{Rel}_1(p,F) \subseteq$ $\subseteq \mathrm{Rel}_2(p,F)$. □

2.9. Remark:

$\mathrm{Rel}_3(p,F)$ is the unique equivalence relation on $\mathrm{Part}_1(p,F)$ which is induced by $\mathrm{Rel}_2(p,F)$.

2.10. Convention:

For any $R \subseteq \mathrm{Pairset}(F)$ and every $p \in \mathrm{Pairset}(F)$ we put

$\text{Joinset}(R,p,F) :=$
$= \{(J_1,J_2) \in \text{Part}_1(p,F) \times \text{Part}_1(p,F) \mid \bigvee_q [q_1 \in J_1, c_2 \in J_2, q \in R \cap \text{Equivset}(p,F)]\}$

2.11. Convention:

Let $(u^1,\ldots,u^m)$ be an m-tupel of elements of Pathset(F). We set $l(1) := L(u^1),\ldots,l(m) := L(u^m)$ and assume

(i) $m \geq 1$,

(ii) $\bigwedge_{1 \leq k < m} u^k_{l(k)} = u^{k+1}_1$,

By $u^1 \vee \ldots \vee u^m$ we denote the unique element of Pathset(F) which is determined by

(iii) $L(u^1 \ \ldots \ u^m) = l(1)+\ldots+l(m)-m+1$,

(iv) $(u^1 \vee \ldots \vee u^m)_j = u^k_j$ whenever $j \in M_k$, the sets M_k being defined in the following way:

$M_1 := \{j \mid 1 \leq j \leq l(1)\}$,

$M_k := \{j \mid l(1)+\ldots+l(k-1)-k+2 < j \leq l(1)+\ldots+l(k)-k+1\}$ for $2 \leq k \leq m$.

We can say that the path $u^1 \vee \ldots \vee u^m$ is obtained by "pasting together" the paths $u^1,\ldots,u^m$.

2.12. Lemma:

For any $B \subseteq \text{Pairset}(F)$ the following statements are equivalent:

(a) B is sufficient with respect to F.

(b) For every $p \in \text{Pairset}(F)$ and every $(J_1,J_2) \in \text{Rel}_3(p,F)$ there exists a natural number $s \geq 1$ and a finite sequence $(\mathcal{J}_1,\ldots,\mathcal{J}_s)$ such that

(i) $\mathcal{J}_1,\ldots,\mathcal{J}_s \in \text{Part}_1(p,F)$,

(ii) $J_1 = \mathcal{J}_1$, $J_2 = \mathcal{J}_s$,

(iii) $\bigwedge_{1 \leq r < s} [(\mathcal{J}_r,\mathcal{J}_{r+1}) \in \text{Joinset}(B,p,F)$ or $(\mathcal{J}_{r+1},\mathcal{J}_r) \in \text{Joinset}(B,p,F)]$.

2.13. Proof:

(a) => (b):

We assume that B is a sufficient set with respect to F. To prove (b) we consider arbitrary but fixed elements $p \in \text{Pairset}(F)$ and $(J_1,J_2) \in \text{Rel}_3(p,F)$ and show the existence of an appropriate sequence $(\mathcal{J}_1,\ldots,\mathcal{J}_s)$.

(1) First let us choose elements $i_1 \in J_1$ and $i_2 \in J_2$ such that $(i_1,i_2) \in \text{Rel}_2(p,F)$. By the very definition of $\text{Rel}_2(p,F)$ there exists a path $u \in \text{Pathset}(F)$ of length $l \geq 1$ that is contained in Lowerset(p,F) and has the property $i_1 = u_1$, $i_2 = u_l$.

(2) Our next goal is to replace the path u by a path $v \in \text{Pathset}(F)$ of length $m \geq 1$ with $i_1 = v_1$, $i_2 = v_m$ and such that v is obtained in $B \cap \text{Lowerset}(p,F)$ (instead of being contained in Lowerset(p,F) only). To construct v we distinguish the cases $l = 1$ and $l > 1$.

$\boxed{l = 1}$ In this case we define $v := u$

$\boxed{l > 1}$ In this case we make use of the sufficiencyof B: For every j with $1 \leq j < l$ there exists a path $v^j \in \text{Pathset}(F)$ of length $m(j)$ that is contained in B and has the properties $u_j = v^j_1$, $u_{j+1} = v^j_{m(j)}$ and $\text{summit}(v^j,F) \leq_M \text{summit}((u_j,u_{j+1}),F)$.
From the last inequality and from the fact that u is contained in Lowerset(p,F) we deduce that all paths v^j are also contained in Lowerset(p,F).
Thus the path $v := v^1 \vee \ldots \vee v^{l-1}$ is contained in $B \cap \text{Lowerset}(p,F)$. Moreover we have $i_1 = u_1 = v^1_1 = v_1$ and $i_2 = u_l = v^{l-1}_{m(l-1)} = v_m$, where $m := m(1)+ \ldots +m(l-1)-l+2$ is the length of v.

(3) Now in the last step of the proof we shall construct an appropriate sequence $(\mathcal{J}_1,\ldots,\mathcal{J}_s)$.
Since v is contained in Lowerset(p,F) there is a unique finite sequence $(k(1),\ldots,k(s))$ of natural numbers such that

(iv) $s \geq 1$,

(v) $1 \leq k(1) < k(2) < \ldots < k(s-1) < k(s) = m$

where $m = L(v)$,

(vi) $\bigwedge_{1 \leq r < s} [(v_{k(r)},v_{k(r)+1}) \in \text{Equivset}(p,F)$ or $(v_{k(r)+1},v_{k(r)}) \in \text{Equivset}(p,F)]$

(vii) $\bigwedge_{1 \leq k < m} [k \notin \{k(1),\ldots,k(s)\} \Rightarrow$ $(v_k,v_{k+1}) \in \text{Lowerset}(p,F)-\text{Equivset}(p,F)$ or $(v_{k+1},v_k) \in \text{Lowerset}(p,F)-\text{Equivset}(p,F)]$.

For every r with $1 \leq r \leq s$ let $\mathcal{J}_r$ be the equivalence class of $v_{k(r)}$ modulo the equivalence relation $\text{Rel}_1(p,F)$. We show that $(\mathcal{J}_1,\ldots,\mathcal{J}_s)$ has the desired properties (i) - (iii).

ad (i): trivial

ad(ii): From (vii) be deduce $(v_1,v_{k(1)}) \in \text{Rel}_1(p,F)$. With respect to $v_1 = i_1 \in J_1$ and $v_{k(1)} \in \mathcal{J}_1$ this implies $J_1 = \mathcal{J}_1$.
The proof of $J_2 = \mathcal{J}_s$ is trivial because $i_2 \in J_2$, $v_{k(s)} \in \mathcal{J}_s$ and $i_2 = v_m = v_{k(s)}$.

ad (iii): Using (vii) again we get

(viii) $\bigwedge_{1 \leq r < s} (v_{k(r)+1},v_{k(r+1)}) \in \text{Rel}_1(p,F)$ and

therefore

(ix) $\bigwedge_{1 \leq r < s} v_{k(r)+1} \in \mathcal{J}_{r+1}$.

On the other hand we have

(x) $\bigwedge_{1 \leq r < s} [(v_{k(r)},v_{k(r)+1}) \in B$ or $(v_{k(r)+1},v_{k(r)}) \in B]$

since v is contained in B.

From (ix), (vi) and (x) we can derive (iii).

(b) => (a):

Let B be a subset of Pairset(F) that fulfills condition (b). We snall prove the sufficiency of B with respect to F.

First of all let us define

$c(p) := |\mathrm{Lowerset}(p,F)|$

for every $p \in \mathrm{Pairset}(F)$.

Then the following statements are equivalent:

(*) B is sufficient with respect to F.

$$(**)\ \bigwedge_{k\geq 0}\ \bigwedge_{p}\ [c(p) = k \implies \bigvee_{u} (\text{ p is connected by u, u is contained in B, } \mathrm{summit}(u,F) \leq_M \mathrm{summit}(p,F))].$$

The validity of (**) will be shown by induction on k.

To do this let $k\geq 0$ and $p \in \mathrm{Pairset}(F)$ be such that $c(p) = k$. Under the induction hypothesis

$$(***)\ \bigwedge_{q}\ c(q) < k \implies \bigvee_{w} (\text{ q is connected by w, w is contained in B, } \mathrm{summit}(w,F) \leq_M \mathrm{summit}(q,F))]$$

we show the existence of a path $u \in$ Pathset(F) that connects p, is contained in B and has the property $\mathrm{summit}(u,F) \leq_M \mathrm{summit}(p,F)$.

By J_1 and J_2 we denote the equivalence classes of p_1 and p_2 with respect to $\mathrm{Rel}_1(p,F)$. Clearly we have $(J_1,J_2) \in \mathrm{Rel}_3(p,F)$. Since B satisfies condition (b) by assumption, there exists a finite sequence $(J_1,\ldots,J_s)$ of length $s\geq 1$ that has the properties (i), (ii) and (iii). From these properties we can derive the existence of a path $v \in \mathrm{Pathset}(F)$ such that

(xi) $L(v) = 2s$,

(xii) $p_1 = v_1,\ p_2 = v_{2s}$,

(xiii) $\bigwedge_{1\leq r\leq s} v_{2r-1},\ v_{2r} \in J_r$,

(xiv) $\bigwedge_{1\leq r<s} [(v_{2r},\ v_{2r+1}) \in B \cap \mathrm{Equivset}(p,F)$ or $(v_{2r+1},\ v_{2r}) \in B \cap \mathrm{Equivset}(p,F)]$.

The assertions (i) and (xiii) yield

(xv) $\bigwedge_{1\leq r\leq s} (v_{2r-1},\ v_{2r}) \in \mathrm{Rel}_1(p,F)$.

Consequently, for every r with $1\leq r\leq s$ there must be a path $v^r \in \mathrm{Pathset}(F)$ of length $m(r)\geq 1$ such that

(xvi) $v_{2r-1} = v^r_1,\ v_{2r} = v^r_{m(r)}$,

(xvii) v^r is contained in Lowerset(p,F) - - Equivset(p,F).

From (xvii) we easily deduce that for every r with $1\leq r\leq s$ and every j with $1\leq j<m(r)$ the inequality $c(v^r_j,\ v^r_{j+1}) < c(p)$ (in case of $v^r_j < v^r_{j+1}$) resp. $c(v^r_{j+1},\ v^r_j) < c(p)$ (in case of $v^r_{j+1} < v^r_j$) holds.

Applying the induction hypothesis we can conclude that for $1\leq r\leq s$ and $1\leq j<m(r)$ there always exists a path $u^{r,j} \in \mathrm{Pathset}(F)$ of length $l(r,j)\geq 2$ such that

(xviii) $v^r_j = u^{r,j}_1,\ v^r_{j+1} = u^{r,j}_{l(r,j)}$,

(xix) $u^{r,j}$ is contained in B,

(xx) $\mathrm{summit}(u^{r,j},\ F) \leq_M \mathrm{summit}((v^r_j,\ v^r_{j+1}),\ F)$.

For every r with $1\leq r\leq s$ we define the path $u^r \in$ Pathset(F) of length $l(r)\geq m(r)$ as follows:

$\boxed{m(r) = 1}$ $\quad u^r := v^r$

$\boxed{m(r) > 1}$ $\quad u^r := u^{r,1} \vee \ldots \vee u^{r,m(r)-1}$.

Observing (xvi) - (xx) we get

(xxi) $\bigwedge_{1\leq r\leq s} u^r_1 = v_{2r-1},\ u^r_{l(r)} = v_{2r}$,

(xxii) $\bigwedge_{1\leq r\leq s} u^r$ is contained in B,

(xxiii) $\bigwedge_{1\leq r\leq s} \mathrm{summit}(u^r,\ F) \leq_M \mathrm{summit}(p,F)$.

To complete the proof we set $w^r := (v_{2r},\ v_{2r+1})$ whenever $1\leq r<s$ and
$u := u^1 \vee w^1 \vee u^2 \vee w^2 \vee u^3 \vee \ldots \vee u^{s-1} \vee w^{s-1} \vee u^s$.
With respect to (xii), (xiv), (xxi), (xxii) and (xxiii) we finally obtain

(xxiv) p is contained by u,

(xxv) u is contained in B,

(xxvi) $\mathrm{summit}(u,F) \leq_M \mathrm{summit}(p,F)$. □

Next we shall give a more convenient formulation of the foregoing lemma and a useful characterization of minimal sufficient sets. In order to do this let us introduce some new notations and a new concept.

2.14. Convention:

(1) For every p let K_p be the canonical map from Indexset(F) onto $\mathrm{Part}_1(p,F)$.

(2) The set of all equivalence classes modulo $\mathrm{Rel}_3(p,F)$ will be denoted by $\mathrm{Part}_3(p,F)$.

2.15. Definition:

Let A be an arbitrary set.

C connecting with respect to A :<=>

$C \subseteq A\times A$,

for every $(a_1,a_2)\in A\times A$ there exists a natural number $m\geq 1$ and a finite sequence $(b_1,\dots,b_m)$ such that

(i) $a_1 = b_1$, $a_2 = b_m$,

(ii) $\bigwedge_{1\leq k<m} [(b_k,b_{k+1})\in C$ or $(b_{k+1},b_k)\in C]$.

C minimal connecting with respect to A :<=>

C connecting with respect to A and no proper subset of C is connecting with respect to A.

Now Lemma 2.12. may be re-formulated as follows:

2.16. Lemma:

For any $B\subseteq \mathrm{Pairset}(F)$ the following statements are equivalent:

(a) B is sufficient with respect to F.

(b) $\bigwedge_{p} \bigwedge_{M\in \mathrm{Part}_3(p,F)}$ $(\mathrm{Joinset}(B,p,F)\cap(M\times M)$ is connecting w.r.t. M).

Proof: obvious □

In a similar manner minimal sufficient sets may be characterized:

2.17. Lemma:

For any $B\subseteq \mathrm{Pairset}(F)$ the following statements are equivalent:

(a) B is minimal sufficient with respect to F.

(b) B fulfills the following conditions:

(i) $\bigwedge_{p} \bigwedge_{M\in \mathrm{Part}_3(p,F)}$ $(\mathrm{Joinset}(B,p,F)\cap(M\times M)$ is minimal connecting w.r.t. M)

(ii) $\bigwedge_{p}$ $|B\cap \mathrm{Equivset}(p,F)| = |\mathrm{Joinset}(B,p,F)|$.

2.18. Proof:

(a) => (b):

Assume that B is minimal sufficient with respect to F. Then B satisfies (i) and (ii) as we shall prove just now.

ad (i): Let p and $M\in \mathrm{Part}_3(p,F)$ be given. By Lemma 2.16. $\mathrm{Joinset}(B,p,F)\cap(M\times M)$ is connecting with respect to M. Let us suppose that this set is not minimal connecting. Then we can find an element $q\in B$ such that $(K_p(q_1), K_p(q_2)) \in \mathrm{Joinset}(B,p,F)\cap(M\times M)$ and $[\mathrm{Joinset}(B,p,F)\cap(M\times M)] - \{(K_p(q_1), K_p(q_2))\}$ is also connecting with respect to M. We contend that $B' := B - \{q\}$ is sufficient with respect to F. In view of Lemma 2.16. the sufficiency of B' is equivalent to

(iii) $\bigwedge_{r\in \mathrm{Pairset}(F)} \bigwedge_{N\in \mathrm{Part}_3(r,F)}$ $[\mathrm{Joinset}(B',r,F)\cap(N\times N)$ is connecting with respect to N].

To prove (iii) let $r\in \mathrm{Pairset}(F)$ and $N\in \mathrm{Part}_3(r,F)$ be arbitrary.

Case 1: Equiv(p,r,F)

In this case we have

(iv) $\mathrm{Part}_i(r,F) = \mathrm{Part}_i(p,F)$ for $i = 1,2,3$

(v) $\mathrm{Joinset}(B',r,F) = \mathrm{Joinset}(B',p,F)$.

Case 1a: N = M

From (v) we deduce $\mathrm{Joinset}(B',r,F)\cap(M\times M) = \mathrm{Joinset}(B',p,F)\cap(M\times M)$.
On the other hand $\mathrm{Joinset}(B',p,F)\cap(M\times M) \supseteq [\mathrm{Joinset}(B,p,F)\cap(M\times M)] - \{(K_p(q_1), K_p(q_2))\}$ and the last of these sets is connecting with respect to M by assumption.

Case 1b: N ≠ M

Because of (v) we have $\mathrm{Joinset}(B',r,F)\cap(N\times N) = \mathrm{Joinset}(B',p,F)\cap(N\times N)$, because of $N \neq M$ we have $\mathrm{Joinset}(B',p,F)\cap(N\times N) = \mathrm{Joinset}(B,p,F)\cap(N\times N)$. This yields the assertion.

Case 2: not Equiv(p,r,F)

In this case we have $\mathrm{Joinset}(B',r,F) = \mathrm{Joinset}(B,r,F)$ and there is nothing to prove.

Assertion (iii) being shown we see that $B' = B - \{q\}$ is sufficient with respect to F. Because B is minimal sufficient by assumption we must have $B' = B$. But this is a contradiction to $q\in B$.

ad (ii): For every $p\in \mathrm{Pairset}(F)$ the map $q \mapsto (K_p(q_1), K_p(q_2))$ from $B\cap \mathrm{Equivset}(p,F)$ to $\mathrm{Joinset}(B,p,F)$ is surjective. Let p be such that the corresponding map is not injective. Then there exist different elements $q, q'\in B\cap \mathrm{Equivset}(p,F)$ such that $(K_p(q_1), K_p(q_2)) = (K_p(q_1'), K_p(q_2'))$. We shall prove that $B - \{q'\}$ is sufficient with respect to F thereby constructing a contradiction to the minimality of B.

It is easy to see that all we have to show is the following statement:

(vi) $\bigvee_{u}$ (q' is connected by u, u is contained in $B - \{q'\}$, $\mathrm{summit}(u,F) \leq_M \mathrm{summit}(q',F)$).

However, the proof of (vi) is rather simple:

Because of $K_p(q_1) = K_p(q_1')$ and $K_p(q_2) = K_p(q_2')$ we have $(q_1, q_1')\in \mathrm{Rel}_1(p,F)$ and $(q_2, q_2')\in \mathrm{Rel}_1(p,F)$. By the very definition of $\mathrm{Rel}_1(p,F)$ there exist paths v^1, $v^2 \in$ Pathset(F) of length m(1) and m(2) respectively such that

(vi.i) $q_1' = v_1^1$, $r_1 = v_{m(1)}^1$, $q_2 = v_1^2$, $q_2' = v_{m(2)}^2$,

(viii) v^1, v^2 are contained in Lowerset(p,F) - Equivset(p,F).

Since B is sufficient the paths v^1, v^2 may be replaced by some paths u^1, $u^2 \in$ Pathset(F) having the following properties:

(ix) $q_1' = u_1^1$, $q_1 = u_{l(1)}^1$, $q_2 = u_1^2$, $q_2' = u_{l(2)}^2$

where $l(1) := L(u^1)$, $l(2) := L(u^2)$,

(x) u^1 and u^2 are contained in B$\cap$(Lowerset(p,F) - Equivset(p,F)).

The paths u^1 and u^2 are constructed in the usual manner (cf. proof of Lemma 2.12.).

From (x) and Equiv(p, q', F) we derive

(xi) u^1, u^2 are contained in B - {q'}.

Now we set $u := u^1 \vee q \vee u^2$. Because of (ix), (x), (xi), $q \neq q'$ and Equiv(p, q', F) the path u connects q', is contained in B - {q'} and has the property summit(u,F) $\leq_M$ summit(q',F).

(b) $\Rightarrow$ (a):

Assume that B fulfills (i) and (ii).

From (i) and Lemma 2.16. we obtain that B is sufficient with respect to F. In order to show that B is minimal sufficient we choose an element $p \in B$ and prove that B' := B - {p} is not sufficient.

Observing (ii) and the fact that $q \longmapsto (K_p(q_1), K_p(q_2))$ is a surjective map from B'$\cap$ Equivset(p,F) to Joinset(B',p,F) we get

|Joinset(B',p,F)| ≤ |B'$\cap$ Equivset(p,F)| < < |B$\cap$Equivset(p,F)| = |Joinset(B,p,F)|.

Therefore Joinset(B',p,F) is a proper subset of Joinset(B,p,F).

On the other hand Joinset(B',p,F) (resp. Joinset(B,p,F)) is the union of all the sets Joinset(B',p,F)$\cap$(M×M) (resp. Joinset(B,p,F)$\cap$(M×M)) where $M \in \mathrm{Part}_3(p,F)$.

Combining these results we conclude that there must be an element $M_0 \in \mathrm{Part}_3(p,F)$ such that Joinset(B',p,F)$\cap(M_0 \times M_0)$ is a proper subset of the minimal connecting set Joinset(B,p,F)$\cap$ $(M_0 \times M_0)$. Consequently Joinset(B',p,F)$\cap(M_0 \times M_0)$ is not connecting with respect to M_0 and B' is not sufficient with respect to F. □

The following graph-theoretical lemma is well-known and will be stated here without proof.

2.19. Lemma:

Let A be a finite nonempty set and let C be connecting with respect to A. Then the following statements are equivalent:

(a) C is minimal connecting w.r.t. A,

(b) |C| = |A| - 1. □

Now we are able to prove the main result of this section.

2.20 Theorem:

B_1, B_2 minimal sufficient w.r.t. F $\Rightarrow$

$\Rightarrow$ $|B_1| = |B_2|$.

2.21. Proof:

Let P be a set of representatives modulo the equivalence relation "Equiv(p,q,F)" on Pairset(F) and suppose that B_1 and B_2 are minimal sufficient with respect to F. Then for i = 1,2 we have

(i) $B_i = \dot{\bigcup}\{B_i \cap \mathrm{Equivset}(p,F) \mid p \in P\}$

($\dot{\bigcup}$ denotes the disjoint union).

From (i) and Lemma 2.17. we obtain

$$\text{(ii)}\quad |B_i| = \sum_{p \in P} |B_i \cap \mathrm{Equivset}(p,F)| =$$

$$= \sum_{p \in P} |\mathrm{Joinset}(B_i,p,F)|.$$

On the other hand the assertion

$$\text{(iii)}\quad \bigwedge_{p \in P} \mathrm{Joinset}(B_i,p,F) =$$

$$= \dot{\bigcup}\{\mathrm{Joinset}(B_i,p,F) \cap (M \times M) \mid M \in \mathrm{Part}_3(p,F)\}$$

holds.

Using Lemma 2.17. and Lemma 2.19. we thus obtain

$$\text{(iv)}\quad \bigwedge_{p \in P} |\mathrm{Joinset}(B_i,p,F)| =$$

$$= \sum_{M \in \mathrm{Part}_3(p,F)} |\mathrm{Joinset}(B_i,p,F) \cap (M \times M)| =$$

$$= \sum_{M \in \mathrm{Part}_3(p,F)} (|M| - 1).$$

Combining (ii) and (iv) we get for i = 1,2

$$\text{(v)}\quad |B_i| = \sum_{p \in P} \sum_{M \in \mathrm{Part}_3(p,F)} (|M| - 1).$$

Since the number on the right side of (v) is independent of B_i the theorem is proved. □

3. An algorithm for the construction of minimal sufficient sets

By Theorem 2.20 we know that minimal sufficient sets are "optimal" for controlling the while - statement in the algorithm A2. Therefore we focus our attention to the development of an algorithm to construct minimal sufficient sets.

Throughout this section let m := |Pairset(F)|.

3.1. Theorem:

(a) If $e : \{1,\dots,m\} \longrightarrow \mathrm{Pairset}(F)$ is bijective then algorithm A3 below yields a sufficient set B.

(b) If in addition e has the property

$$(*) \quad \bigwedge_{1\le k,l\le m} [\mathrm{summit}(e(k),F) <_M <_M \mathrm{summit}(e(l),F) \Rightarrow k < l]$$

then algorithm A3 below yields a minimal sufficient set B.

Algorithm A3:

```
B := $\emptyset$;
for k := 1 step 1 until m do
    if $\neg A(k)$ then B := B $\cup \{e(k)\}$;
where
A(k) $:\Leftrightarrow \bigvee_u$ [e(k) connected by u,
                u contained in
                Lowerset(e(k),F)$\cap$B]
```

3.2. Proof:

For every k with $0\le k\le m$ let B(k) be the unique set obtained by the k-th execution of the for-statement in algorithm A3. We must show that B(m) is sufficient w.r.t. F (resp. minimal sufficient w.r.t. F) provided e is bijective (resp. e is bijective and has property (*)).

(1) Suppose that e is bijective and let p be arbitrary but fixed. There is exactly one l such that $1\le l\le m$ and $p = e(l)$.

In order to prove the existence of a path u with the properties

(i) p is connected by u,

(ii) u is contained in B(m),

(iii) $\mathrm{summit}(u,F) \le_M \mathrm{summit}(p,F)$

we distinguish two cases:

Case 1: A(l) is true

In this case there exists a path u which connects p and is contained in Lowerset(p,F)$\cap$B(l-1). Clearly u has the properties (i) - (iii).

Case 2: A(l) is false

In this case we have $p\in B(m)$. Setting u := p the path u satisfies (i) - (iii).

(2) Suppose that e is bijective and has property (*). In view of (1) it is only necessary to show that no proper subset of B(m) is sufficient w.r.t. F. This can be done by an indirect proof as follows:

Let C be a sufficient proper subset of B(m). From B(m) - C we choose an element $p = e(l)$ where l is uniquely determined by p. Since C is sufficient by assumption there exists a path u of length r such that

(i) e(l) is connected by u,

(ii) u is contained in C,

(iii) $\mathrm{summit}(u,F) \le_M \mathrm{summit}(e(l),F)$.

From (iii) we obtain

(iv) u is contained in Lowerset(e(l),F).

But we also have

(v) u is contained in B(l-1)

as we shall prove just now.

For every i with $1\le i<r$ there is exactly one number k_i such that $1\le k_i\le m$ and $(u_i, u_{i+1}) = e(k_i)$ or $(u_{i+1},u_i) = e(k_i)$. We prove assertion (v) by showing $k_i<l$ for $1\le i<r$.

Suppose there is an index i with $k_i\ge l$ and let j be such that $k_j = \max(k_1,\dots,k_{r-1})$. Then we also have $k_j\ge l$. From $k_j\ge l$, (iii) and (*) we get

(vi) Equiv(e(l), e(k_j), F),

from (iii) and (vi) we obtain

$$(\mathrm{vii}) \quad \bigwedge_{1\le i<r} \mathrm{Lower}(e(k_i), e(k_j), F).$$

Of course we may assume that the pairs (u_i, u_{i+1}) are mutually distinct. Then the numbers k_i with $1\le i<r$ are also distinct and we get

$$(\mathrm{viii}) \quad \bigwedge_{1\le i<r} (i \neq j \Rightarrow k_i < k_j).$$

Last we have

(ix) $l < k_j$

since $l \le k_j$, $e(k_j)\in C$ and $e(l)\notin C$.

Now let us define a path $v\in\mathrm{Pathset}(F)$ in the following way:

$$v := \begin{cases} (u_j, u_{j-1},\dots,u_2, u_1, u_r, u_{r-1},\dots \\ \quad \dots,u_{j+2}, u_{j+1}) \text{ if } e(k_j) = (u_j, u_{j+1}), \\ (u_{j+1}, u_{j+2},\dots,u_{r-1}, u_r, u_1, u_2,\dots \\ \quad \dots,u_{j-1}, u_j) \text{ if } e(k_j) = (u_{j+1}, u_j). \end{cases}$$

The path v has the following properties:

(x) $e(k_j)$ is connected by v,

(xi) v is contained in Lowerset($e(k_j)$, F),

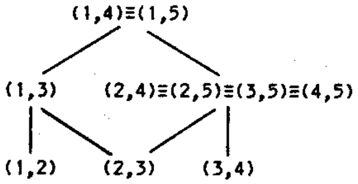
(xii) v is contained in B(k_j-1).

The proof of (x) is trivial, (xi) follows from (vi) and (vii), (xii) follows from (viii) and (ix). Thus condition $A(k_j)$ is fulfilled and we must have $e(k_j)\notin B(m)$. But in view of $C\subseteq B(m)$ this is a contradiction to (ii). Therefore we have $k_i < l$ for $1\le i<r$ and assertion (v) is proved.

Noting(i), (iv) and (v) we see that A(l) is satisfied. Consequently we must have $e(l) \notin B(m)$. This, however, contradicts the assumption $e(l) \in B(m)$. □

3.3. Example:

We resume Example 1.7. First we establish the quasi - ordering "Lower(p,q,F)":



Here "(i,j)≡(k,l)" means "Equiv((i,j), (k,l), F)".

Next we define a bijective function e from {1,...,10} to Pairset(F) in the following way:

$$\begin{aligned} e(1) &= (1,2)\\ e(2) &= (2,3)\\ e(3) &= (3,4)\\ e(4) &= (1,3)\\ e(5) &= (2,4)\\ e(6) &= (2,5)\\ e(7) &= (3,5)\\ e(8) &= (4,5)\\ e(9) &= (1,4)\\ e(10) &= (1,5). \end{aligned}$$

It is easy to see that e satisfies condition (*) in Theorem 3.1. Applying algorithm A3 we successively obtain the following values for k and B:

k	B
1	{(1,2)}
2	{(1,2), (2,3)}
3	{(1,2), (2,3), (3,4)}
4	{(1,2), (2,3), (3,4)}
5	{(1,2), (2,3), (3,4)}
6	{(1,2), (2,3), (3,4), (2,5)}
7	{(1,2), (2,3), (3,4), (2,5)}
8	{(1,2), (2,3), (3,4), (2,5)}
9	{(1,2), (2,3), (3,4), (2,5)}
10	{(1,2), (2,3), (3,4), (2,5)}

3.4. Remark:

In a practical implementation of algorithm A3 condition A(k) should be programmed by using Warshall's algorithm for constructing the transitive closure of the set $\mathrm{Lowerset}(e(k),F) \cap B$.

Conclusion

In order to reduce the complexity of the basic algorithm for the construction of Gröbner-bases we must try to derive theoretical results of the following type:

If $E \subseteq F \times F$ and E has a certain property with respect to F, then

$$\bigwedge_{(f,g)\in E} \mathrm{Spol}(f,g) \underset{F}{>} 0 \implies F \text{ is Gröbner-basis.}$$

In this paper we derived one such result by defining and investigating the property "sufficient with respect to F".

We have not investigated properties that might involve the stepwise growing of the set G. This seems to be a promising direction for future research: intuitively, the more polynomials have been already added to the basis by the execution of line 6 of algorithm A2, the less polynomials may probably appear by the execution of line 5 of the algorithm.

Also the Criteria S.1. and S.2. in /2/ may be considered to be of the above type.

Another type of simplification may be found in /5/.

Referrences

/1/ Bruno Buchberger, Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal,
Dissertation, Universität Innsbruck, 1965

/2/ Bruno Buchberger, Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems,
Aequationes mathematicae, Vol.4/3, S.374-383, 1970

/3/ Bruno Buchberger, A Teoretical Basis for the Reduction of Polynomials to Canonical Forms,
ACM SIGSAM Bulletin <u>39</u>, August 1976, 19-29

/4/ Markus Lauer, Kanonische Repräsentanten für die Restklassen nach einem Polynomideal,
Diplomarbeit, Universität Kaiserslautern, 1976

/5/ Stuart C. Schaller, On Algebraic Simplification and Polynomial Ideal Theory, A Research Proposal,
July 1976

/6/ Wolfgang Trinks, Über B. Buchbergers Verfahren, Systeme algebraischer Gleichungen zu lösen,
Internal Report, Institut für Mathematik,
Universität Karlsruhe

/7/ David A. Spear, A constructive Approach to Commutative Ring Theory,
Proceed of the MACSYMA User's Conference 1977,
M.I.T.