CLOSURE RELATIONS, BUCHBERGER'S ALGORITHM, AND POLYNOMIALS IN INFINITELY MANY VARIABLES

Daniel E. Cohen

Mathematics Department, Queen Mary College, Mile End Rd, London E1 4NS

Some years ago (Cohen 1967), in the course of an investigation of varieties of metabelian groups, I showed that the polynomial ring over $\mathbb{Z}$ in infinitely many variables satisfies the ascending chain condition for a certain class of ideals. Aspects of the proof are very similar to the proof of termination in Buchberger's algorithm for a Gröbner basis (Buchberger 1983, 1984). It seems worthwhile to show how termination can be proved by these techniques.

Various generalisations of Buchberger's algorithm are also obtained. The simplest is a modification of his definition of reductions rings to include the case of fields. The proof (Buchberger 1983) that a polynomial ring over a reduction ring is a reduction ring, which generalises the earlier result about polynomials with field coefficients (Buchberger 1965, 1976), will then include this result , which his 1983 paper does not. The most interesting extension, due to a student of mine, discusses rings with operators, and includes the case of an algorithm for the special class of ideals in a polynomial ring with infinitely many variables.

1. QUASI-ORDERS

A *quasi-order* on a set Q is a reflexive transitive relation $\leqslant$. If $\leqslant$ is irreflexive, we call it a *partial order* (and the corresponding relation $<$ is a *strict partial order*). If, further, for every p and q in Q we either have $p \leqslant q$ or $q \leqslant p$ it is a *total order*. If $\leqslant$ is a quasi-order the corresponding strict partial order $<$ is defined by $p < q$ if $p \leqslant q$ but not $q \leqslant p$. The *closure* ClX of a subset X of the quasi-ordered set Q is $\{y;\ x \leqslant y$ for some $x \in X\}$.

A partial order is called *well-founded* if there is no infinite decreasing sequence $p_1 > p_2 > \ldots$; a quasi-order is well founded if its corresponding partial order is well-founded. Well-founded partial orders are often called noetherian. However, there are good algebraic reasons (see section 2) why a partial order should be called noetherian iff it is a partial well-order. Consequently we shall not use the word noetherian in connection with partial orders.

We now recall the definition of *well-quasi-order* ((Kruskal 1972) is a good general reference); for a partial order we refer to a *partial well-order* (and not to a well-partial-order). The basic results, with a different name, come from (Higman 1952) which contains the relevant proofs.

We call the quasi-ordered set Q *well-quasi-ordered* if it satisfies any of the following conditions, in which case it satisfies them all:

(i) every closed set is the closure of a finite subset;

(ii) Q satisfies the ascending chain condition on closed sets;

(iii) any collection of closed sets has a maximal member;

(iv) every infinite sequence of members of Q has an infinite subsequence;

(v) if $q_1, q_2, \ldots$ is an infinite sequence of elements of Q then there exist i and j with $i < j$ and $q_i \leqslant q_j$;
(vi) Q contains no infinite strictly descending sequence and no infinite sequence of mutually incomparable elements.

It follows immediately that any subset and any image of a quasi-well-ordered set is quasi-well-ordered, and that any extension of a quasi-well-order on a set Q to a larger quasi-order on Q will also be quasi-well-ordered. Plainly a total order is a quasi-well-order iff it is a well-order. It is also clear that if Q_1 and Q_2 are quasi-well-ordered then so is $Q_1 \times Q_2$ under the quasi-order $(p_1, p_2) \leqslant (q_1, q_2)$ iff $p_1 \leqslant q_1$ and $p_2 \leqslant q_2$.

We can apply these results to $\mathbb{N}^k$, and we can then identify $\mathbb{N}^k$ with the power products on $x_1, \ldots, x_k$, identifying $(i(1), \ldots, i(k))$ with $x_1^{i(1)} \ldots x_k^{i(k)}$. If u and v are power products then $u \leqslant v$ iff u divides v. We see that any total order extending this divisibility partial order must be a well-order. This result is also given in (Buchberger 1970) and (Dickson 1913). It is easy to construct specific examples of such total orders. That this does not depend on any properties of $\mathbb{N}$ follows from the (well-known) Lemma 1 below.

The most interesting of Higman's results (which we shall use later) is the following:

Theorem H *Let Q be quasi-ordered. Define a relation $\leqslant$ on the finite sequences of elements of Q by $(p_1, \ldots, p_m) \leqslant (q_1, \ldots, q_n)$ iff there exist $i(1) \leqslant i(2) \leqslant \ldots \leqslant i(m)$ with $p_r \leqslant q_{i(r)}$ for all r. Then this is a quasi-order, which is a quasi-well-order if the relation $\leqslant$ on Q is a quasi-well-order.*

Lemma 1 *Any partial order on a set X can be extended to a total order on X, and any partial-well-order can be extended to a well-order.*

Proof The second part follows from the first, using previous remarks.

Suppose a and b are incomparable under the partial order $\leqslant$. Define a new relation $\leqslant'$ by $x \leqslant' y$ iff $x \leqslant y$ or $x \leqslant a$ and $b \leqslant y$. This is easily checked to be a partial order. It follows that a partial order which is not maximal cannot be a total order.

We can now apply Zorn's Lemma. It is easy to check that the hypotheses of Zorn's Lemma hold (regarding a partial order on X as a subset of $X \times X$), and so any partial order extends to a maximal partial order. //

Let W be a well-ordered set, and let Q be a quasi-ordered set with an element 0 such that $0 \leqslant q$ for all q. Let S be the set of all functions f from W to Q such that $fx = 0$ for all but finitely many x. For any f and g in S let x be as small as possible subject to $fy = gy$ for all $y > x$. Because fy and gy are 0 except for finitely many y, there is such an x; for the same reason, unless $f = g$ we do not have $fx = gx$. We now define $f \leqslant g$ to hold iff $fx \leqslant gx$. It is easy to see that this is a quasi-order, which is a partial order (a total order) if $\leqslant$ on Q is a partial order (or total order). Also, if Q has a binary operation, written additively with 0 as zero, compatible with $\leqslant$, then the same holds for S.

Lemma 2 *If $\leqslant$ on Q is well-founded then so is $\leqslant$ on F. If $\leqslant$ on Q is a quasi-well-order then so is $\leqslant$ on F.*

Proof For each $f \in F$ let $h(f)$ be the smallest x such that $fy = 0$ for all $y > x$. Let $f_1, f_2, \ldots$ be an infinite sequence. We shall show, by induction on $h(f_1)$, that if $\leqslant$ on Q is well-founded then the sequence cannot be strictly decreasing (and a similar argument will show that the sequence cannot consist of mutually incomparable elements if $\leqslant$ is a quasi-well-order).

We may assume that $h(f_1) \leqslant h(f_i)$ for all i, by induction (we use $\leqslant$ for the well-order on W as well as for the quasi-order on Q). Also, because W is well-ordered, taking a subsequence if necessary, we may assume that $h(f_i) \leqslant h(f_{i+1})$ for $i > 1$. If we have $h(f_i) < h(f_{i+1})$ for some $i \geqslant 1$ then the sequence cannot be strictly decreasing. So we may assume there is some x with $h(f_i) = x$ for all i.

If $\{f_ix\}$ is infinite then, taking a subsequence if necessary, we may assume that the elements f_ix are all distinct. In this case, the sequence $f_1, f_2, \ldots$ cannot be strictly decreasing, as that would make the sequence $f_1x, f_2x, \ldots$ strictly decreasing, contrary to hypothesis.

If $\{f_ix\}$ is finite then, taking a subsequence, we may assume that there is some q such that $f_ix = q$ for all q. Define f_i' by $f_i'y = f_iy$ for $y \neq x$ and $f_i'x = 0$. It is now easy to see that if $f_1, f_2, \ldots$ is strictly decreasing then so is $f_1', f_2', \ldots$, and this is impossible by induction.//

There are three important examples of this. This first is with W being $\{1, \ldots, k\}$ and Q being $\mathbb{N}$. We obtain the inverse lexicographic order on $\mathbb{N}^k$, and we have shown that this is a well-order. This plainly extends the component-wise partial order on $\mathbb{N}^k$. Identifying $\mathbb{N}^k$ with the power products on $x_1, \ldots, x_k$, we obtain a well-order $\leqslant$ such that $uw \leqslant vw$ if $u \leqslant v$ and such that $u \leqslant v$ if u divides v.

The second example is with W being $\mathbb{N}$ and Q being $\mathbb{N}^k$. Let $\leqslant$ be a well-order which extends the partial order on $\mathbb{N}^k$. We obtain a well-order on the set of finite sequence from $\mathbb{N}^k$. Identifying this with the set T of power products from x_{in} for $i = 1, \ldots, k$ and all n we have a well-order on T such that $uw \leqslant vw$ if $u \leqslant v$. For any order-preserving map $\alpha: \mathbb{N} \to \mathbb{N}$ and any $t \in T$, let $t\alpha$ be obtained by replacing each $x_{i,n}$ by $x_{i,n\alpha}$. The partial-well-order of Theorem H, transferred to T, becomes a partial well-order $\ll$ such that $\leqslant$ extends $\ll$ and $u \ll v$ iff there is α such that $u\alpha$ divides v.

Finally, let R be a ring with a well-founded partial order. Let T be either the set of power products of the previous example or the set of power products in $x_1, \ldots, x_k$. We see, using T as the well-ordered set, that the polynomial ring over R in the relevant variables also has a well- founded partial order. This generalises the result in (Buchberger 1983), and the analysis there was a guide to Lemma 2 (which is probably known already).

2. CLOSURE RELATIONS

A *weak algebraic closure relation* (abbreviated to *wacr*) on a set X assigns to each $A \subseteq X$ a set ClA such that (i) $A \subseteq ClA$, (ii) if $A \subseteq B$ then $ClA \subseteq ClB$, (iii) if $x \in ClA$ then $x \in ClA_0$ for some finite subset A_0 of A. If, in addition, we have $ClClA = ClA$ for all A, the relation is an *algebraice closure relation* (or *acr*). It is a *unary wacr* if any $x \in ClA$ is in Cla for some $a \in A$.

Algebraic closure relations abound. The closure already defined in a quasi-ordered set is an acr. When X is a ring we can define ClA to be the ideal generated by A (or, if preferred, the subring generated by A), and there are many similar examples. We shall need one example of a unary wacr later.

We shall prove various properties of wacrs which are well-known for acrs. The proofs will be similar to the standard ones, but some care is needed. For instance, the assumption that for every A there is a finite B with $ClA = ClB$ is not the same as saying that every A has a finite subset A_0 with $ClA = ClA_0$ for wacrs, though it is the same for an acr.

We say a wacr is *noetherian* if every A has a finite subset A_0 with $ClA = ClA_0$. When X is a ring, and ClA is the ideal generated by A, this is the same as saying that X is a noetherian ring. This explains the name, which is also used in other algebraic situations. Note, though, that for a quasi-ordered set this concept coincides with quasi-well-order.

Proposition 3 *A wacr on X is noetherian iff for every sequence $A_1 \subseteq A_2 \subseteq \ldots$ the sequence of sets ClA_n is ultimately constant.*

Proof Let A be any set, let A_0 be empty, and suppose we have defined subsets A_i of A for $i \leqslant n$ such that $A_i \subseteq A_{i+1}$. If $ClA_n \neq ClA$ take an element b of $ClA - ClA_n$. There is some finite $B_n \subseteq A$ with $b \in ClB_n$. Let $A_{n+1} = A_n \cup B_n$. Thus $ClA_n \subset ClA_{n+1}$. It follows that we must have $ClA_n = ClA$ for some n if the condition in the proposition holds, showing the wacr is noetherian.

Conversely, let $A_1 \subseteq A_2 \subseteq \ldots$. Plainly $Cl(\cup A_n) \supseteq \cup ClA_n$. Take any $a \in Cl(\cup A_n)$. Then $a \in ClF$ for some finite $F \subseteq \cup A_n$. There will be some n with $F \subseteq A_n$. Hence $Cl(\cup A_n) = \cup ClA_n$. If the wacr is noetherian we then have $\cup ClA_n = ClF$ for some finite $F \subseteq \cup A_n$. As before, there will be some n with $F \subseteq A_n$, and then $ClA_m = ClA_n$ for $m > n$, as required. //

Note that this proposition does not state that any increasing sequence of closures is ultimately constant when the wacr is noetherian. I do not know whether this holds in general, but I expect a counter-example can be constructed.

Proposition 4 *Suppose a wacr has the property that $Cl(A_1 \cup A_2) = ClA_2$ whenever $ClA_1 \subseteq ClA_2$. Then the following are equivalent: (i) the wacr is noetherian, (ii) the ascending chain condition holds for closures, (iii) any set of closures has a maximal member.*

Proof The equivalence of (ii) and (iii) is standard, and (ii) implies (i) by the previous proposition. Suppose we have an increasing sequence ClA_n of closures. Let $B_n = A_1 \cup \ldots \cup A_n$. Our hypothesis on the wacr lets us show, by induction, that $ClB_n = ClA_n$. *Since* $B_n \subseteq B_{n+1}$, the previous proposition tells us that the sequence of closures is ultimately constant if the wacr is noetherian. //

Lemma 5 *$Cl(A_1 \cup A_2) = ClA_2$ whenever $ClA_1 \subseteq ClA_2$ if Cl is either an acr or a unary wacr.*

Proof If $ClA_1 \subseteq ClA_2$ then $A_1 \cup A_2 \subseteq ClA_2$, and so $ClA_2 \subseteq Cl(A_1 \cup A_2) \subseteq ClClA_2$. The result follows for an acr.

The result holds for a unary acr because we then have $Cl(A_1 \cup A_2) = ClA_1 \cup ClA_2$ for all A_1 and A_2.//

The next result is a stronger version of Proposition 1 of (Cohen 1967). Let Cl be a wacr on a set X, and let $\leqslant$ be a quasi-order on a set Q. Define Cl^* on $X \times Q$ as follows. We define (x,q) to be in Cl^*S iff there are $(x_i, q_i) \in S$ for $i = 1,\dots,n$ (some n) such that $q_i \leqslant q$ for all i and $x \in Cl(x_1,\dots,x_n)$. Then Cl^* is easily seen to be a wacr, which is an acr if Cl is, and is unary if Cl is.

Theorem 6 *If Cl is noetherian and $\leqslant$ is a quasi-well-order then Cl^* is noetherian.*

Proof Let $C = Cl^*S$. Define $C(q)$ to be $\{x:\ (x,p) \in C$ for some $p \leqslant q\}$ and $S(q)$ to be $\{x:\ (x,p) \in S$ for some $p \leqslant q\}$. It is easy to check that $S(p) \subseteq S(q)$ for $p \leqslant q$, and that $C(q) = ClS(q)$ for all q.

Write $p \ll q$ if $p \leqslant q$ and $C(p) = C(q)$. We show that $\ll$ is a quasi-well-order. So take any infinite sequence $q_1, q_2, \dots$. Since $\leqslant$ is a quasi-well- order, we may assume that $q_i \leqslant q_{i+1}$ for all i, taking a subsequence if necessary. Since Cl is noetherian, the remarks already made, together with Proposition 3, show that there is some n such that $C(q_n) = C(q_{n+1})$. Hence $q_n \ll q_{n+1}$, which shows that $\ll$ is a quasi-well-order.

It then follows that there are finitely many elements $q_1,\dots,q_n$ such that for every q there is some i with $q_i \ll q$. Since Cl is noetherian, we can find for each i finitely many elements x_{ij} in $S(q_i)$ for $j = 1,\dots,m_i$ such that $C(q_i) = Cl\{x_{ij};\ j = 1,\dots,m_i\}$. We can then, by definition, find p_{ij} such that $p_{ij} \leqslant q_i$ and $(x_{ij}, p_{ij}) \in S$. Take any $(x,q) \in C$. Our choice of the elements q_i ensures that there is some i with $q_i \leqslant q$ and $C(q) = C(q_i)$. Hence $x \in Cl\{x_{ij};\ j = 1,\dots,m_i\}$. It follows at once that $C = Cl^*\{(x_{ij}, p_{ij});$ all $i,j\}$, as needed.//

3. REDUCTION RINGS

Buchberger (1983, 1984) defines a *reduction ring*. He shows that a version of his earlier algorithm (Buchberger 1965, 1976) applies in any reduction ring, and that the polynomial ring (in any finite number of variables) over a reduction ring is a reduction ring. The results and proofs are modelled on his work for the ring of polynomials over a field, and this ring is a reduction ring. However, this result cannot be obtained directly from the result about polynomials over a reduction ring, since a field is not usually a reduction ring. We begin by showing how to cure this anomaly. For all notations, and parallel results, see (Buchberger 1983, 1984).

Let R be a ring with a partial order and a set M of multipliers, and let $P = \{p \in M;\ p$ has an inverse in M and, for every $a,b \in R$, $pa < pb$ iff $a < b\}$. Then $1 \in P$, and P may consist only of 1.

It is easy to check that if $p \in P$ and a is a non-trivial common reducible for c_1 and c_2 then pa is also a non-trivial common reducible for c_1 and c_2. Further, if a is a minimal non-trivial common reducible for c_1 and c_2 then so is pa. Hence the termination condition (T2) cannot hold if P is infinite.

On the other hand, suppose we have a set C, a minimal non-trivial common reducible a for some c_1 and c_2 in C, and a corresponding critical pair b_1 and b_2 such that $b_1 \leftrightarrow_C^*(<a)\ b_2$. Then pb_1 and pb_2 are a critical pair for pa, and $pb_1 \leftrightarrow_C^*(<a)\ pb_2$. Define the P-class of a to be $\{b;\ b = pa$ for some $p \in P\}$ (notice that this relation between a and b is obviously an equivalence). We have just shown that if the hypotheses of Buchberger's Main Theorem hold for some a then they also hold for all members of the P-class of a. This means that in Buchberger's algorithm all that is really relevant is the P-classes of elements, not the elements themselves.

We define a *modified reduction ring* to be a ring R with a well-founded partial order and a set of multipliers M satisfying Buchberger's axioms (M0)-(M5), (A1)-(A5), and (T1), and with his axion (T2) replaced by (T2') *for every c_1 and c_2 there are only finitely many P-classes of minimal non-trivial common reducibles for c_1 and c_2.* We need his effectiveness conditions, except that the condition about non-trivial common reducibles is replaced by the condition that *we can effectively find for every c_1 and c_2 a finite set $I(c_1,c_2)$ consisitng of minimal non-trivial common irreducibles for c_1 and c_2 which contains at least one element from each P-class of minimal non-trivial common irreducibles.*

Observe that any field is a modified reduction ring, if we define $a < b$ to hold iff $a = 0$ and $b \neq 0$. Also the proof that the polynomial ring over a modifed reduction ring is a modified reduction ring is as before.

The earlier remarks lead to the following algorithm to obtain from a finite set C a finite set D such that $\leftrightarrow_C^* = \leftrightarrow_D^*$ and $\rightarrow_D$ has the Church-Rosser property:

$D: = C$
$B: = \{ (\{c_1, c_2\}, a);\ c_1, c_2 \in C$ and $a \in I(c_1, c_2)\}$

<u>while</u> B is not empty <u>do</u>

$(\{c_1, c_2\}, a): =$ one triple from B
$B : = B - \{ (\{c_1, c_2\}, a) \}$
$(b_1, b_2) : =$ two elements such that a reduces to b_i with respect to c_i for $i=1,2$
$(b_1, b_2) : = (S_D(b_1), S_D(b_2))$

<u>if</u> $b_1 \neq b_2$ <u>do</u>

$c: = b_1 - b_2$
$B: = B \cup \{ (\{c, c'\}, a);\ c' \in D,\ a \in I(c, c')\}$
$D: = D \cup \{c\}$.

The partial correctness of the algorithm is proved using the following inductive assumption for the while-loop.

$\equiv_C = \equiv_D$.
if $(\{c_1, c_2\}, a) \in B$ then $c_1, c_2 \in D$ and $a \in I(c_1, c_2)$.
if $c_1, c_2 \in D$ and a is a minimal non-trivial common reducible for c_1 and c_2 then either a has a critical pair b_1, b_2 such that $b_1 \leftrightarrow_D^*(<a)\ b_2$ or there is a' in the P-class of a with $(\{c_1, c_2\}, a') \in D$.
The details are a very slight change from the previous details.

The messiest part of Buchberger's argument is the proof that (T1) for R implies (T1) for the polynomial ring. We now show how this follows from Theorem 6 of the previous section.

For any subset S of R let Red$S$ be $\{0\} \cup \{r;\ r \to_S\}$. Then Red is easily seen to be a unary wacr, and condition (T1) implies that Red is noetherian.

Let T be the set of power products, with $u \ll v$ iff u divides v; we know $\ll$ is a partial-well-ordering. By Theorem 6 and the discussion before it, we know that there is an induced noetherian unary wacr Red* on $R \times T$. The other results of section 2 show that $R \times T$ has ascending chain condition on sets of the form Red*S.

We have a unary wacr on the polynomial ring, which we also denote by Red. We want to show the ascending chain condition holds for sets of the form Red$S$. Buchberger proves a property (RED), which says, in the current notation, that a non-zero polynomial ϕ is in Red$S$ iff there is a monomial ct occurring in ϕ such that $(c,t) \in$ Red*S^*, where S^* is the set opf those (a,u) for which au is the leading monomial of a member of S. The ascending chain condition for Red follows at once from the ascending chain condition for Red*.

Now let R be any noetherian ring, and let S be the polynomial ring $R(x_{in};\ i = 1,\dots,k,$ all $n)$. Plainly S does not satisfy the ascending chain condition on ideals. But we are able to recover the ascending chain condition if we restrict attention to a special class of ideals.

Let α be any order-preserving map from $\mathbb{N}$ to $\mathbb{N}$. Then α induces an endomorphism of S, which we still call α, by sending $x_{i,n}$ to $x_{i,n\alpha}$. We call an ideal I *special* if $I\alpha \subseteq I$ for all α. The following theorem is a slight strengthening of the result in (Cohen 1967).

Theorem 7 *Let R and S be as above. Then S has ascending chain condition on special ideals.*

Proof For any subset A of S there is a smallest special ideal containing A. We call this the special ideal generated by A. If we assign to each A the special ideal it generates we obtain an algebraic closure relation. We have to show this acr is noetherian. We also have an acr on R assigning to each subset the ideal it generates, and we are given that this acr is noetherian.

Let T be the set of all power products of the x_{in}. In section 1 we obtained a well-ordering $\leqslant$ and a partial-well-ordering $\ll$ on T. The well-ordering lets us refer to leading monomials of members of S. The noetherian acr on R and the partial-well-ordering $\ll$ provide, by Theorem 6, a noetherian acr on $R \times T$.

Let I be a special ideal, and let $I^* \subseteq R \times T$ be $\{(c,t);\ c = 0$ or ct is the leading monomial of a member of $I\}$. We show that I^* is closed. Take any $(c,t) \in CI I^*$. Then there are $(c_r, t_r) \in I^*$ for $r = 1,\dots,m$ for some m such that $t_r \ll t$ for all r and $c = \sum a_r c_r$ for some $a_r \in R$. Since $t_r \ll t$ there are maps α_r and power products u_r such that $t = t_r \alpha_r u_r$, and, by definition of I^*, there are $f_r \in I$ such that $c_r t_r$ is the leading monomial of f_r. Then $\sum a_r u_r (f_r \alpha_r)$ is a polynomial in I with leading monomial ct. Hence $(c,t) \in I^*$, as required.

Since I^* is closed, and the closure operation is noetherian, I^* is the closure of a finite subset. This subset consists of the leading monomials of a finite subset of I. Let J be the special ideal generated by this finite subset of I. By the same argument as in the previous paragraph, for any $f \in I$ there is some $g \in J$ with the same leading monomial as f. Then $f - g \in I$ and $f - g$ has smaller leading power product than f. Inductively, $f - g \in J$. Hence $f \in J$, so $I = J$.//

Now let M be the free $R[x_{in}, x_{in}^{-1}]$-module with basis u_{pn}, for $p = 1,\ldots,r$ and all n. Each α produces an R-module endomorphism of M sending $x_{i,n}$ to $x_{i,n\alpha}$ and $u_{p,n}$ to $u_{p,n\alpha}$. We call a submodule special if it is mapped into itself by every α. Then M has ascending chain condition on special submodules.

The easiest proof of this is to make M a ring by requiring $u_{pm}u_{qn}$ to be 0 for all p, q, m, n. Then M is the quotient of the ring $R[x_{in}, y_{in}, u_{pn}]$ by the special ideal generated by $\{x_{in}y_{in} - 1, u_{i1}u_{j1}, u_{i1}u_{j2}\}$, and the result follows from the previous theorem.

This result was used to show that all metabelian varieites of groups are finitely based. In view of the similarity of the techniques used here and in Buchberger's algorithm, it is natural to ask if the algorithm can be generalised to give a Gröbner-type basis for special ideals. In addition to its interest for its own sake, such a result might be useful in studying specific metabelian varieties.

Results of this kind have been proved recently by a student of mine, Phillip Emmott, in his thesis. The simplest of Emmott's results is a localisation of Buchberger's results. This, for instance, covers those ordinary ideals in $R[x_{in}]$ which are finitely generated. Precisely, he defines a *local reduction ring* to consist of a ring R with multipliers M and a partial ordering $<$ together with a family of subrings R_i such that:
(i) each R_i is a reduction ring with multipliers $M \cap R_i$ and order $<$,
(ii) every finite subset of R is contained in some R_i, (iii) if $a \to_c b$ in R and a and c are in some R_i then b is in R_i and there is m in $M \cap R_i$ with $b = a - mc$, (iv) if c_1 and c_2 are in some R_i and r is a minimal non-trivial common reducible for c_1 and c_2 then r is in R_i. We also require Buchberger's effectiveness conditions to hold in R. Then (as can be seen easily; the conditions can be varied slightly) he proves

Theorem 8 *In any local reduction ring Buchberger's algorithm terminates and gives a Gröbner basis.*

Another result looks at a monoid X and the corresponding monoid ring $R[X]$. He obtain conditions on X which make $R[X]$ a reduction ring when R is a reduction ring. To save space this result is not stated; it follows at once from Theorem 9 by requiring the operators to consist only of the identity.

His most interesting result defines an operator reduction ring. He is able to show that a Buchberger-type algorithm holds in these rings. Also if X is an operator monoid satisfying suitable conditions, then $R[X]$ is an operator reduction ring if R is. All his results can be stated for modified operator reduction rings also, and even for modified local operator reduction rings. The proofs of the current results for modified reduction rings were influenced by his work.

In particular, his results apply to our rings $R[x_{in}]$ when R is a reduction ring. This example motivates some of the technicalities in his definition. Essentially, he remarks that when we look at critical pairs corresponding to

f and g we also need to consider the critical pairs corresponding to the infinitely many $f\alpha$ and $g\beta$ for all α and β. But it is not difficult to show that, given f and g, there are finitely many pairs (α_j, β_j) such that for any α and β there is some j and some γ such that $f\alpha = f\alpha_j\gamma$ and $\zeta b = g\beta_j\gamma$. So we only need to look at the finitely many pairs $f\alpha_j$ and $g\beta_j$.

Definition Let R be a ring with multipliers M and a partial well-ordering $<$, and let Ω be a monoid of operators on R which preserve $<$ and M. Then (R,Ω) is an *operator reduction ring* if R satisfies Buchberger's conditions (M0) – (M5), (A1) – (A5), and (T2) (but not (T1)), and Ω is such that (i) a is a minimal non-trivial common reducible for c_1 and c_2 iff $a\omega$ is a minimal non-trivial common reducible for $c_1\omega$ and $c_2\omega$, and any minimal non-trivial common reducible for $c_1\omega$ and $c_2\omega$ is $a\omega$ for some a, (ii) there is no increasing sequence of sets $\mathrm{Red}(F_j\Omega)$, (iii) for any c_1 and c_2 we can effectively find a finite set Ω_0 such that for any ω_1 and ω_2 there are ω_1' and ω_2' in Ω_0 and ω^* in Ω such that $c_i\omega_i = c_i\omega_i'\omega^*$ for $i = 1, 2$, and R satisfies the effectiveness conditions of the next paragraph. We call R a *strong reduction ring-with-operators* if (iii) is replaced by the stronger condition
(iv) for any c_{ij} in R with $i = 1,\ldots,n$ and $j = 1,\ldots,m_i$ we can effectively find a finite subset Ω_0 of Ω such that for any ω_i in Ω for $i = 1,\ldots,n$ there exist ω_i' in Ω_0 and ω^* in Ω with $c_{ij}\omega_i = c_{ij}\omega_i'\omega^*$.

We plainly require the operations in R, the multiplication in Ω, and the action of Ω on R to be effective. We also need, given a minimal non-trivial common reducible with respect to c_1 and c_2 to be able to reduce it effectively. Finally, for any finite subset D, we need to be able to compute the simplifier $S_{D\Omega}$ effectively. We can replace these conditions by stronger but more straightforward ones.

If we can compute $S_{D\Omega}$ then we can tell whether or not an element is reducible with respect to $D\Omega$, since a is irreducible iff $a = S_{D\Omega}a$. Conversely, suppose we can tell whether or not an element is reducible with respect to $D\Omega$. Then we can compute $S_{D\Omega}$ if we can effectively find a reduction of any element reducible with respect to $D\Omega$ (by iterating this reduction until we find an irreducible element). If the set M of multipliers and the relation $<$ are both effectively decidable (which is a very reasonable condition) then we can reduce (with respect to $D\Omega$ or to a single element c) any reducible element a simply by looking systematically at all elements $a - m(d\omega)$ until we find one which is $< a$; this remark is useful even for ordinary reduction rings. We can tell whether or not an element is reducible with respect to $D\Omega$ provided that we can tell for any a and c whether or not a is reducible with respect to c and that we can also effectively find, for any element a and finite set D a finite subset Ω_1 of Ω such that a is reducible with respect to $D\Omega$ iff it is reducible with respect to $D\Omega_1$. This condition also is freqeuntly satisfied.

Let X be a monoid with left cancellation, and let E be a monoid of one-one operators on X. Let $\leqslant$ be a well-ordering on X such that, for any u,v, and w, $w < wv$ and $uw < vw$ if $u < v$ and with $\leqslant$ preserved by E. We say u divides v, written $u|v$, if $v = uw$ for some w, and we write $u \ll v$ if $ue|v$ for some e in E. We require $\ll$ to be a partial well-ordering such that $u \leqslant v$ if $u \ll v$. We require least common right multiples to exist in X, and we require them to be preserved by E; here w_0 is the l.c.m. of u and v if $u|w_0$ and $v|w_0$ and $w_0|w$ whenever $u|w$ and $v|w$. Finally we require condition (iv) above to hold for X and E.

We also require various effectiveness conditions. Multiplication in X and in E

and the action of E on X and the formation of least common multiples must be effective, and the relation $\leqslant$ must be effectively decidable. The relation $\ll$ must also be effectively decidable. This last holds if $|$ is effectively decidable and we can effectively find for any u and v a finite subset E_1 of E such that $u \ll v$ iff $ue_1 | v$ for some e_1 in E_1.

Theorem 9 *If X is as above and R is a strong operator reduction ring then the ring $R[X]$ with operators $\Omega \times E$ is a strong operator reduction ring.*

Theorem 10 *Let R be an operator reduction ring. Then a modified Buchberger algorithm applies to give a Gröbner-type basis for operator ideals.*

The relevant modification is straightforward. We begin with D: $=C$ and B: $=\{((c_1\omega_1, c_2\omega_2), a)$; c_1, c_2 in D, ω_1, ω_2 in Ω_0, and a a minimal non-trivial common reducible for $c_1\omega_1$ and $c_2\omega_2\}$, and each time we update D by adding a new element c we must also update B by adding all $((c\omega, c'\omega'), a)$ with c' in the original D, ω and ω' in Ω_0 for c and c', and a a minimal non-trivial common reducible.

References

Buchberger B (1965) Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem null-dimensionalen Polynomideal. Ph. D. thesis, University of Innsbruck, Austria.

Buchberger B (1970) Ein algorithmisches Kriterium für die Lösbarkeit eines algebraisches Gleichunssystems. Aequationes Mathematicae 4: 374 - 383.

Buchberger B (1976) A theoretical basis for the reduction of polynomials to canonical form. ACM SIGSAM Bull. 10/3: 19 - 29.

Buchberger B (1983) A critical-pair completion algorithm in reduction rings. Technical report CAMP 83-21.0. Math. Institute, University of Linz, Austria

Buchberger B (1984) A critical-pair completion algorithm for finitely generated ideals in rings. In: Börger E et al. (eds) Logic and machines: decison problems and complexity. Lecture Notes in Computer Science 171. Springer, Berlin Heidelberg New York

Cohen DE (1967) On the laws of a metabelian variety. Journal of Algebra 5: 267 - 273.

Dickson L. (1913) Finiteness of the odd perfect and primitive abundant numbers with *n* distinct prime factors. American J. Math. 35: 413 - 422.

Emmott P (1987) Ph. D. thesis, Queen Mary College, London University.

Higman G (1952) Ordering by divisibility in abstract algebras. Proc London Math. Soc. (3) 2: 326 - 336.

Kruskal JB (1972) The theory of well-quasi-ordering: a frequently discovered concept. J. Combinatorial Theory A 13: 297 - 305.