Knuth–Bendix Procedure and Buchberger Algorithm — A Synthesis

Abdelilah Kandri-Rody
Department des Mathematiques
Faculte des Sciences
Universite Cadi Ayyad
Marrakech, Morocco

Deepak Kapur
Dept. of Computer Science
SUNY at Albany
Albany, NY 12222
USA

Franz Winkler *
Institut für Mathematik and
Research Inst. for Symbolic Comp.
J. Kepler Universität
Austria

Abstract

The Knuth–Bendix procedure for the completion of a rewrite rule system and the Buchberger algorithm for computing a Gröbner basis of a polynomial ideal are very similar in two respects: they both start with an arbitrary specification of an algebraic structure (axioms for an equational theory and a basis for a polynomial ideal, respectively) which is transformed to a very special specification of this algebraic structure (a complete rewrite rule system and a Gröbner basis of the polynomial ideal, respectively). This special specification allows to decide many problems concerning the given algebraic structure. Moreover, both algorithms achieve their goals by employing the same basic concepts: formation of critical pairs and completion.

Although the two methods are obviously related, the exact nature of this relation remains to be clarified. Based on previous work we show how the Knuth–Bendix procedure and the Buchberger algorithm can be seen as special cases of a more general completion procedure.

1. Introduction

The Buchberger algorithm BU has been introduced by B. Buchberger in 1965 [Bu 65], [Bu 85a] and it solves the following problem:

> *given a finite set F of multivarate polynomials over a field, construct a finite set F' of multivariate polynomials such that $\equiv_F = \equiv_{F'}$ and $\rightarrow_{F'}$ is Church–Rosser.*

Here, for a set F of polynomials, $\equiv_F$ is the ideal congruence modulo the ideal generated by F (i.e. $f \equiv_F g \iff f - g \in \text{ideal}(F)$) and $\rightarrow_F$ is a certain Noetherian reduction relation on polynomials induced by F [Bu 85a] with the property that $\leftrightarrow_F^*$ (the reflexive–symmetric–transitive closure of $\rightarrow_F$) is equal to $\equiv_F$. If $F' = \text{BU}(F)$, then the Church–Rosser property guarantees, that for arbitrary polynomials f, g the congruence $f \equiv_F g$ can be decided by

* Supported by the *Fonds zur Förderung der wissenschaftlichen Forschung,* Project Nr. P6763.

© 1989 ACM 0-89791-325-6/89/0007/0055 $1.50

computing normal forms of f and g modulo $\rightarrow_{F'}$ and checking for syntactic equality. A basis F' with this property is usually called a *Gröbner basis* [Bu 85a].

Such a Gröbner basis can be computed by the *Buchberger algorithm* BU in the following way:

```
$F' \leftarrow$ BU($F$);
[$F$ and $F'$ are finite sets of multivariate polynomials over a field.
$\equiv_F = \equiv_{F'}$ and $\rightarrow_{F'}$ is Church–Rosser.]
$F' \leftarrow F$;
while not all critical pairs of $F'$ are considered do
(*)  choose a critical pair $(p_1, p_2)$ of $F'$;
     reduce $(p_1, p_2)$ to normal forms $(q_1, q_2)$ modulo $\rightarrow_{F'}$;
(**) if $q_1 \neq q_2$ then $F' \leftarrow F' \cup \{q_1 - q_2\}$ endif
endwhile   ■
```

The two basic strategies of the algorithm are the formation of critical pairs in (*) and the successive completion step (**). A critical pair of F' is constructed in the following way: choose two different polynomials f, g in F'; reduce the least common multiple of the leading terms of f and g by f, getting p_1, and by g, getting p_2; then (p_1, p_2) is a critical pair of F'. Instead of reducing (p_1, p_2) to normal forms (q_1, q_2) and checking for syntactic equality, one could reduce $p_1 - p_2$ and check for equality to 0. The polynomial $p_1 - p_2$ is usually called the S-polynomial of f and g [Bu 85a]. Buchberger has shown [Bu 65], [Bu 85a] that this algorithm terminates for all inputs and computes a Gröbner basis for ideal(F).

The same basic strategies have been used independently by D.E. Knuth and P.B. Bendix [KB 67] in the context of an equational theory T over an algebra T of first-order terms. The Knuth–Bendix procedure solves the following problem:

> *given a finite set E of equations between first-order terms, construct a finite set E' of equations such that $\equiv_E = \equiv_{E'}$ and $\rightarrow_{E'}$ is Church–Rosser and Noetherian.*

Here, for a set E of first-order equations [HO 80], $\equiv_E$ is the equational theory generated by E, i.e. the set of all equations $s = t$ which can be derived from E, $E \vdash s = t$ [BL 83]. $\rightarrow_E$ is the reduction relation on terms induced by E viewed as a system of rewrite rules with $\equiv_E = \leftrightarrow^*_E$. Again, the Church–Rosser property guarantees that $s \equiv_E t$ can be decided by reducing s and t to normal forms modulo $\rightarrow_{E'}$ and checking for syntactic equality. A finite set of equations E, viewed as a system of rewrite rules, such that $\rightarrow_E$ is Church–Rosser and Noetherian is called a *canonical* rewrite rule system.

The *Knuth-Bendix procedure* KB attempts to compute a canonical rewrite rule system in the following way:

```
$E' \leftarrow$ KB($E$);
[$E$ and $E'$ are finite sets of equations of first-order terms which can be viewed
as Noetherian rewrite rule systems.
$\equiv_E = \equiv_{E'}$ and $\rightarrow_{E'}$ is Church–Rosser.]
$E' \leftarrow E$;
while not all critical pairs of $E'$ are considered do
```

```
        choose a critical pair $(c_1, c_2)$ of $E'$;
        reduce $(c_1, c_2)$ to normal forms $(d_1, d_2)$ modulo $\rightarrow_{E'}$;
        if $d_1 \neq d_2$ then
            if $\rightarrow_{E' \cup \{d_1 = d_2\}}$ is Noetherian then $E' \leftarrow E' \cup \{d_1 = d_2\}$
            elsif $\rightarrow_{E' \cup \{d_2 = d_1\}}$ is Noetherian then $E' \leftarrow E' \cup \{d_2 = d_1\}$
            else exit with failure
        endif
    endwhile ■
```

For the notion of a critical pair we refer to [BL 83]. We say that an equation $s = t$ can be viewed as a rewrite rule $s \rightarrow t$ if every variable occurring in t also occurs in s. A set of equations $E = \{s_1 = t_1, \ldots, s_n = t_n\}$ can be viewed as a rewrite rule system $\{s_1 \rightarrow t_1, \ldots, s_n \rightarrow t_n\}$ if every equation $s_i = t_i$ in it can be viewed as a rewrite rule $s_i \rightarrow t_i$. In contrast to the Buchberger algorithm there are situations in which the Knuth–Bendix procedure may terminate with **failure** or run forever.

Certain types of equations cannot be handled by the Knuth–Bendix procedure: a commutativity axiom immediately destroys the Noetherianity of the reduction, and an associativity axiom together with other equations can cause the procedure to run indefinitely. Peterson and Stickel [PS 81] have proposed to keep such equations in an equational theory T (the equations in T are not viewed as rewrite rules) and do all the computations in KB modulo this equational theory T, i.e. not terms t in T are reduced but equivalence classes $[t]_T$ in $\mathrm{T}_{/T}$. This approach works whenever a complete unification algorithm modulo this theory T exists. For technical reasons the equational theory E has to be modified so that it becomes T–compatible. For theories T consisting of commutativity and associativity axioms this is a straightforward process.

The striking similarity between the Buchberger algorithm and the Knuth–Bendix procedure have been observed in [Lo 81], [BL 83], [Bu 85b]. Le Chenandec [Le 86] gives a completion algorithm for commutative polynomials over rings generated by a finite set G of generators. His method does not apply to the case where the base coefficients belong to a field, since fields cannot be described equationally.

The following approach towards a unified procedure has been tried by Llopis de Trias [Ll 83]: describe $K[x_1, \ldots, x_n]$ by the reduction system R_0 consisting of the nine rewrite rules

$$\begin{array}{ll}
x + 0 \rightarrow x & x + (-x) \rightarrow 0 \\
-0 \rightarrow 0 & -(-x) \rightarrow x \\
-(x + y) \rightarrow (-x) + (-y) & x \cdot 1 \rightarrow x \\
x \cdot 0 \rightarrow 0 & x \cdot (-y) \rightarrow -(x \cdot y) \\
x \cdot (y + z) \rightarrow x \cdot y + x \cdot z &
\end{array}$$

and the equational theory

$$\begin{aligned}
T = \{x + y = y + x, \quad (x + y) + z = x + (y + z), \\
x \cdot y = y \cdot x, \quad (x \cdot y) \cdot z = x \cdot (y \cdot z)\}.
\end{aligned}$$

Le Chenandec [Le 86] demonstrates that R_0 is a confluent rewrite system with respect to the equational theory T. The underlying term structure T contains constants for the elements of K and constants $X_1, \ldots, X_n$ for the indeterminates and the function symbols $+$

and $\cdot$. To the rewrite system R_0 one adds rules for each of the polynomials in the ideal basis F, thus creating the new rewrite system R. R has to be made T–compatible by adding variable enlargements $s^e \to t^e$ for the rewrite rules $s \to t$, as described in [PS 81]. Finally one applies the completion procedure to R and T, thus constructing a rewrite system R' which generates the same equivalence relation as R and which is confluent modulo T.

This approach, however, neglects the following problem. Suppose we are given the ideal basis

$$F = \{xy^2 - 2xy - 2,\ x^2y - x - y,\ xy + y^2 - 4x - 2y\} \subseteq \mathbb{Q}[x, y].$$

Then the initial rewrite system would be

$$\begin{aligned} R = R_0 \cup R_0^e \cup \{&(1)XY^2 \to 2XY + 2,\\ &(2)X^2Y \to X + Y,\\ &(3)XY \to -Y^2 + 4X + 2Y\}\\ \cup\{&(1^e)XY^2x \to 2XYx + 2x,\\ &(2^e)X^2Yy \to Xy + Yy,\\ &(3^e)XYz \to -Y^2z + 4Xz + 2Yz\}. \end{aligned}$$

Because of the associativity and commutativity of $+$ and $\cdot$ we may omit the parentheses in the polynomials. During the execution of the completion procedure the following reductions have to be considered:

$$\begin{tikzcd}
& {[X^2Y^2]_T} \arrow[dl, "(1^e)"] \arrow[dr, "(2^e)"] & \\
{[2X^2Y + 2X]_T} \arrow[d, "(2)"] & & {[XY + Y^2]_T} \arrow[d, "(3)"'] \\
{[2X + 2Y + 2X]_T} \arrow[d, equal] & & {[-Y^2 + 4X + 2Y + Y^2]_T} \arrow[d, equal] \\
{[2X + 2X + 2Y]_T} & & {[-Y^2 + Y^2 + 4X + 2Y]_T}
\end{tikzcd}$$

In order to recognize the results as equal, it would be necessary to "add the coefficients of like powers", i.e. to apply the distributivity rule in the opposite direction. Clearly this cannot be done without destroying the termination property of the rewrite system.

There are two possible directions in which one could look for a solution of this problem. First one could try to add the distributivity rule to the equational theory T. This would entail the need for an associative–commutative–distributive unification algorithm. Raulefs et al. [Ra 79], however, list this unification problem as undecidable.

The second way is to separate the polynomial reduction from the arithmetic on the coefficients. So there are two relations, one is the usual "reduction relation" generated by the polynomial rewrite rules, the other is a "simplification relation" responsible for the arithmetic operations on the coefficients. The simplification relation need not be generated by rewrite rules. The main problem of course is to guarantee that these two relations behave well w.r.t. one another. This approach has been taken by Kandri–Rody and Kapur [KK 83]. The problem with [KK 83] is that it does not really show that the Knuth–Bendix procedure and the Buchberger algorithm can be viewed as special cases of a general procedure, but that the correctness proofs can be arranged in similar ways.

In [Wi 84] the author has combined various ideas of these papers together with [Hu 80] for demonstrating the exact nature of the relationship between BU and KB. The present paper continues this approach.

2. Confluence modulo a simplification relation

In the following we suppose that M is an arbitrary set, $\rightarrow$ a Noetherian relation on M (called a reduction relation), and $\Rightarrow$ a Noetherian confluent relation on M (called a simplification relation). By x, y, z, u, v, w we denote elements of M. $\leftarrow$, $\leftrightarrow$, $\rightarrow^+$, $\rightarrow^*$ are the inverse, the symmetric closure, the transitive closure, and the reflexive–transitive closure of $\rightarrow$, respectively. By $\xrightarrow{\text{rs}}$ we denote the union of these relations, i.e. $\xrightarrow{\text{rs}} = \rightarrow \cup \Rightarrow$.

Def.: $\rightarrow$ is *confluent modulo* $\Rightarrow$ iff for all x, y, x', y' such that $x' \leftarrow^* x \Leftrightarrow^* y \rightarrow^* y'$ there are x'', y'' such that $x' \rightarrow^* x'' \Leftrightarrow^* y'' \leftarrow^* y'$ (i.e., since $\Rightarrow$ is confluent, $x' \rightarrow^* x'' \Downarrow^* y'' \leftarrow^* y'$). (See the figure below.) ■

$$\begin{tikzcd}
x \arrow[r, Leftrightarrow, "*"] \arrow[d, "*"'] & y \arrow[d, "*"] \\
x' \arrow[d, dashed, "*"'] & y' \arrow[d, dashed, "*"] \\
x'' \arrow[r, Leftrightarrow, dashed, "*"] & y''
\end{tikzcd}$$

Lemma 2.1: Let $\rightarrow$ be confluent modulo $\Rightarrow$. Then for all x, y, z such that $y(\Leftarrow \cup \leftarrow)^* x \rightarrow^* z$ and y is irreducible modulo $\rightarrow \cup \Rightarrow$ and z is irreducible modulo $\rightarrow$, we have $z \Rightarrow^* y$. ■

Later on we will separate the reduction $\rightarrow$ of polynomials in the Gröbner basis algorithm from the simplification $\Rightarrow$ of the coefficients in the polynomials. What we ultimately want to achieve is that the combination $\rightarrow \cup \Rightarrow$ is a confluent relation. As the following theorem shows, it is enough to guarantee confluence of $\rightarrow$ modulo $\Rightarrow$.

Theorem 2.2: If $\rightarrow$ is confluent modulo $\Rightarrow$, then $\rightarrow \cup \Rightarrow$ is confluent.

Proof: Let $\rightarrow$ be confluent modulo $\Rightarrow$. Suppose x, y, z are such that $y(\Leftarrow \cup \leftarrow)^* x(\rightarrow \cup \Rightarrow)^* z$. Let x' be a normal form of x modulo $\rightarrow$ and y', z' be normal forms of y, z modulo $\rightarrow \cup \Rightarrow$, respectively. Then by Lemma 2.1 $y' \Leftarrow^* x' \Rightarrow^* z'$. Since y' and z' are also in normal form modulo $\Rightarrow$ and $\Rightarrow$ is confluent, we have $y' = z'$. (See the figure below.) ■

$$\begin{tikzcd}
 & x \arrow[dl, "\leftarrow \cup \Leftarrow"', "*"] \arrow[d, "*"] \arrow[dr, "\rightarrow \cup \Rightarrow", "*"'] & \\
y \arrow[d, "\rightarrow \cup \Rightarrow"', "*"] & x' \arrow[dl, Rightarrow, "*", "\text{Lemma 2.1}"'] \arrow[dr, Rightarrow, "*"', "\text{Lemma 2.1}"] & z \arrow[d, "\rightarrow \cup \Rightarrow", "*"'] \\
y' & = & z'
\end{tikzcd}$$

It is essential for an effective completion procedure that the confluence property of the reduction relation under consideration can be checked locally. This program can also be carried out for the notion of confluence modulo the simplification relation $\Rightarrow$.

Def.: $\to$ is *locally confluent modulo* $\Rightarrow$ iff
(L1) for all x, y, z with $y \leftarrow x \to z$ there are y', z' such that $y \to^* y' \Downarrow^* z' \leftarrow^* z$ and
(L2) for all x, y, z with $y \leftarrow x \Leftrightarrow z$ there are y', z' such that $y \to^* y' \Downarrow^* z' \leftarrow^* z$.
(See the figure below.) ■

(L1):
$$\begin{tikzcd}
 & x \arrow[dl] \arrow[dr] & \\
y \arrow[d, dashed, "*"'] & & z \arrow[d, dashed, "*"] \\
y' \arrow[rr, phantom, "\Downarrow^*"] & & z'
\end{tikzcd}$$

(L2):
$$\begin{tikzcd}
 & x \arrow[r, Leftrightarrow] \arrow[dl] & z \arrow[dd, dashed, "*"] \\
y \arrow[d, dashed, "*"'] & & \\
y' \arrow[rr, phantom, "\Downarrow^*"] & & z'
\end{tikzcd}$$

Def.: $\Rightarrow$ is *orthogonal to* $\to$ iff
(O1) for all x, y, y' with $x \Rightarrow y \to^+ y'$ there are x'', y'' such that $x \to^+ x'' \Downarrow^* y'' \leftarrow^* y'$ and
(O2) for all x, y, x' with $x' \leftarrow^+ x \Rightarrow y$ there are x'', y'' such that $x' \to^* x'' \Downarrow^* y'' \leftarrow^* y$.
(See the figure below.) ■

(O1):
$$\begin{tikzcd}
x \arrow[r, Rightarrow] \arrow[dd, dashed, "+"'] & y \arrow[dr, "+"] & \\
 & & y' \arrow[d, dashed, "*"] \\
x'' \arrow[rr, phantom, "\Downarrow^*"] & & y''
\end{tikzcd}$$

(O2):
$$\begin{tikzcd}
 & x \arrow[r, Rightarrow] \arrow[dl, "+"'] & y \arrow[dd, dashed, "*"] \\
x' \arrow[d, dashed, "*"'] & & \\
x'' \arrow[rr, phantom, "\Downarrow^*"] & & y''
\end{tikzcd}$$

With these definitions we get the following theorem.

Theorem 2.3: Let $\to \cup \Rightarrow$ be Noetherian, and $\Rightarrow$ orthogonal to $\to$. Then $\to$ is confluent modulo $\Rightarrow$ if and only if $\to$ is locally confluent modulo $\Rightarrow$.

Proof: Obviously confluence of $\to$ modulo $\Rightarrow$ implies local confluence of $\to$ modulo $\Rightarrow$.

So now assume that $\to$ is locally confluent modulo $\Rightarrow$. Let $\overset{\mathrm{rs2}}{\to}$ be the following relation on M^2:

$$\begin{aligned}
(x, y) \overset{\mathrm{rs2}}{\to} (x', y') \quad \text{iff} \quad & x \overset{\mathrm{rs}}{\to} x' \text{ and } y = y' \quad \text{or} \\
& x \overset{\mathrm{rs}}{\to} x' \text{ and } x \overset{\mathrm{rs}}{\to} y' \quad \text{or} \\
& x = x' \text{ and } y \overset{\mathrm{rs}}{\to} y' \quad \text{or} \\
& y \overset{\mathrm{rs}}{\to} x' \text{ and } y \overset{\mathrm{rs}}{\to} y'.
\end{aligned}$$

Then $\overset{\mathrm{rs2}}{\to}$ is a Noetherian relation on M^2. (This is a direct application of proposition 2.1 in [Hu 80].)

Now we show

$$\begin{aligned}
P(x, y): \quad & \text{if } x \Leftrightarrow^* y \text{ then} \\
& \text{for all } x', y' \text{ such that } x \to^* x' \text{ and } y \to^* y' \\
& \text{there are } \tilde{x}, \tilde{y} \text{ such that } x' \to^* \tilde{x} \Downarrow^* \tilde{y} \leftarrow^* y'
\end{aligned}$$

by Noetherian induction on $\overset{\mathrm{rs2}}{\to}$.

Let $x, y, x', y' \in M$ be such that $x' \leftarrow^* x \Leftrightarrow^* y \rightarrow^* y'$. We show the existence of $\tilde{x}, \tilde{y}$ such that $x' \rightarrow^* \tilde{x} \Downarrow^* \tilde{y} \leftarrow^* y'$. We distinguish two cases.

Case 1: $x = y$. If $x' = x$ or $y' = y$, respectively, then we simply choose $\tilde{x} = \tilde{y} = y'$ or $\tilde{x} = \tilde{y} = x'$, respectively. Otherwise there are x_1, y_1 such that $x \rightarrow x_1 \rightarrow^* x'$, $y \rightarrow y_1 \rightarrow^* y'$. Applying property (L1) to x, x_1 and y_1, we get u, v, w such that $x_1 \rightarrow^* u \Rightarrow^* w \Leftarrow^* v \leftarrow^* y_1$. Let $\underline{x}', \underline{u}, \underline{v}, \underline{y}'$ be $\rightarrow$–normal form of x', u, v, y', respectively. Then by the induction hypothesis $P(x_1, x_1)$ there exists w_1 such that $\underline{x}' \Rightarrow^* w_1 \Leftarrow^* \underline{u}$ and w_1 is in $\Rightarrow$–normal form, by the induction hypothesis $P(u, v)$ there exists w_2 such that $\underline{u} \Rightarrow^* w_2 \Leftarrow^* \underline{v}$ and w_2 is in $\Rightarrow$–normal form, and by the induction hypothesis $P(y_1, y_1)$ there exists w_3 such that $\underline{v} \Rightarrow^* w_3 \Leftarrow^* \underline{y}'$ and w_3 is in $\Rightarrow$–normal form. Because of the confluence of $\Rightarrow$ we have $w_1 = w_2 = w_3$. (See Figure a.)

Case 2: $x \neq y$. Because of the confluence of $\Rightarrow$ we have $x \Downarrow^* y$. So w.l.o.g. there is u such that $x \Rightarrow u \Leftrightarrow^* y$.

Case 2a: $x' = x$. By the induction hypothesis $P(u, y)$ there are u', y'', w_1 such that $u \rightarrow^* u' \Rightarrow^* w_1 \Leftarrow^* y'' \leftarrow^* y'$. If $u' = u$ then we can choose $\tilde{x} = x'$, $\tilde{y} = y''$. (See Figure b.)

Otherwise there is u_1 such that $u \rightarrow u_1 \rightarrow^* u'$. By the orthogonality of $\Rightarrow$ to $\rightarrow$ there are x'', x''', u'', w_2 such that $x' \rightarrow x'' \rightarrow^* x''' \Rightarrow^* w_2 \Leftarrow^* u'' \leftarrow^* u_1$. Now we let $\underline{x}''', \underline{u}'', \underline{u}', \underline{y}''$ be $\rightarrow$–normal forms of x''', u'', u', y'', respectively. By the induction hypothesis $P(x''', u'')$ there is w_3 such that $\underline{x}''' \Rightarrow^* w_3 \Leftarrow^* \underline{u}''$ and w_3 is in $\Rightarrow$–normal form, by the induction hypothesis $P(u_1, u_1)$ there is w_4 such that $\underline{u}'' \Rightarrow^* w_4 \Leftarrow^* \underline{u}'$ and w_4 is in $\Rightarrow$–normal form, and by the induction hypothesis $P(u', y'')$ there is w_5 such that $\underline{u}' \Rightarrow^* w_5 \Leftarrow^* y''$ and w_5 is in $\Rightarrow$–normal form. Because of the confluence of $\Rightarrow$ we have $w_3 = w_4 = w_5$. (See Figure c.)

Case 2b: $x' \neq x$. In this case there is x_1 such that $x \rightarrow x_1 \rightarrow^* x'$. Applying property (L2) to x, u, x_1 we get v_1, v_2, w_1 such that $x_1 \rightarrow^* v_1 \Rightarrow^* w_1 \Leftarrow^* v_2 \leftarrow^* u$. By the induction hypothesis $P(u, y)$ there are v_3, y'', w_2 such that $v_2 \rightarrow^* v_3 \Rightarrow^* w_2 \Leftarrow^* y'' \leftarrow^* y'$. Now we let $\underline{x}', \underline{v}_1, \underline{v}_3, \underline{y}''$ be $\rightarrow$–normal forms of x', v_1, v_3, y'', respectively. By the induction hypothesis $P(x_1, x_1)$ there is w_3 such that $\underline{x}' \Rightarrow^* w_3 \Leftarrow^* \underline{v}_1$ and w_3 is in $\Rightarrow$–normal form, by the induction hypothesis $P(v_1, v_2)$ there is w_4 such that $\underline{v}_1 \Rightarrow^* w_4 \Leftarrow^* \underline{v}_3$ and w_4 is in $\Rightarrow$–normal form, and by the induction hypothesis $P(v_3, y'')$ there is w_5 such that $\underline{v}_3 \Rightarrow^* w_5 \Leftarrow^* \underline{y}''$ and w_5 is in $\Rightarrow$–normal form. Because of the confluence of $\Rightarrow$ we have $w_3 = w_4 = w_5$. (See Figure d.) ■

The orthogonality of the simplification relation $\Rightarrow$ to the reduction relation $\rightarrow$ gives us freedom in the way these relations can be applied successively.

Lemma 2.4([Wi 84]): Let $\overset{rs}{\rightarrow}$ be Noetherian and $\Rightarrow$ orthogonal to $\rightarrow$. If $x \overset{rs}{\rightarrow}{}^* y$ and y in in $\overset{rs}{\rightarrow}$–normal form, then there exists z such that $x \rightarrow^* z \Rightarrow^* y$, where z is in $\rightarrow$–normal form. ■

$$\begin{tikzcd}
 & & & x = y \arrow[dl] \arrow[dr] & & & \\
 & & x_1 \arrow[dll, "*"] \arrow[d, "*"] & (\mathrm{L1}) & y_1 \arrow[d, "*"] \arrow[drr, "*"] & & \\
x' \arrow[ddd, "*"] & & u \arrow[dr, Rightarrow, "*"] \arrow[ddd, "*"] & & v \arrow[dl, Rightarrow, "*"] \arrow[ddd, "*"] & & y' \arrow[ddd, "*"] \\
 & & & w & & & \\
 & \begin{array}{c}\text{ind.hyp.}\\ P(x_1,x_1)\end{array} & & \begin{array}{c}\text{ind.hyp}\\ P(u,v)\end{array} & & \begin{array}{c}\text{ind.hyp.}\\ P(y_1,y_1)\end{array} & \\
\underline{x}' \arrow[dr, Rightarrow, "*"] & & \underline{u} \arrow[dl, Rightarrow, "*"] \arrow[dr, Rightarrow, "*"] & & \underline{v} \arrow[dl, Rightarrow, "*"] \arrow[dr, Rightarrow, "*"] & & \underline{y}' \arrow[dl, Rightarrow, "*"] \\
 & w_1 & = & w_2 & = & w_3 &
\end{tikzcd}$$

Figure a

$$\begin{tikzcd}
x' = x \arrow[dr, Rightarrow] & & & \\
 & u \arrow[rr, Leftrightarrow, "*"] \arrow[ddd, Rightarrow, "*"] & & y \arrow[d, "*"] \\
 & & & y' \arrow[d, "*"] \\
 & & & y'' \arrow[dll, Rightarrow, "*"] \\
 & w_1 & &
\end{tikzcd}$$

Figure b

$$\begin{tikzcd}
x' = x \arrow[d] \arrow[drrr, Rightarrow] & & & & & & \\
x'' \arrow[dd, "*"] & & & u \arrow[d] \arrow[rrr, Leftrightarrow, "*"] & & & y \arrow[d, "*"] \\
 & \text{orthogon.} & & u_1 \arrow[dl, "*"] \arrow[dr, "*"] & & \begin{array}{c}\text{ind.hyp.}\\ P(u,y)\end{array} & y' \arrow[d, "*"] \\
x''' \arrow[dr, Rightarrow, "*"] \arrow[ddd, "*"] & & u'' \arrow[dl, Rightarrow, "*"] \arrow[ddd, "*"] & & u' \arrow[dr, Rightarrow, "*"] \arrow[ddd, "*"] & & y'' \arrow[dl, Rightarrow, "*"] \arrow[ddd, "*"] \\
 & w_2 & & & & w_1 & \\
 & \begin{array}{c}\text{ind.hyp.}\\ P(x''',u'')\end{array} & & \begin{array}{c}\text{ind.hyp.}\\ P(u_1,u_1)\end{array} & & \begin{array}{c}\text{ind.hyp.}\\ P(u',y'')\end{array} & \\
\underline{x}''' \arrow[dr, Rightarrow, "*"] & & \underline{u}'' \arrow[dl, Rightarrow, "*"] \arrow[dr, Rightarrow, "*"] & & \underline{u}' \arrow[dl, Rightarrow, "*"] \arrow[dr, Rightarrow, "*"] & & \underline{y}'' \arrow[dl, Rightarrow, "*"] \\
 & w_3 & = & w_4 & = & w_5 &
\end{tikzcd}$$

Figure c

$$\begin{tikzcd}
 & & & x \arrow[dll] \arrow[dr, Rightarrow] & & & \\
 & x_1 \arrow[ddl, "*"] \arrow[ddr, "*"] & & & u \arrow[dd, "*"] \arrow[rr, Leftrightarrow, "*"] & & y \arrow[dd, "*"] \\
 & & & (\mathrm{L2}) & & \begin{array}{c}\text{ind.hyp.}\\ P(u,y)\end{array} & \\
x' \arrow[dddd, "*"] & & v_1 \arrow[dr, Rightarrow, "*"] \arrow[dddd, "*"] & & v_2 \arrow[dl, Rightarrow, "*"] \arrow[d, "*"] & & y' \arrow[d, "*"] \\
 & & & w_1 & v_3 \arrow[dr, Rightarrow, "*"] \arrow[ddd, "*"] & & y'' \arrow[dl, Rightarrow, "*"] \arrow[ddd, "*"] \\
 & & & & & w_2 & \\
 & \begin{array}{c}\text{ind.hyp.}\\ P(x_1,x_1)\end{array} & & \begin{array}{c}\text{ind.hyp.}\\ P(v_1,v_2)\end{array} & & \begin{array}{c}\text{ind.hyp.}\\ P(v_3,y'')\end{array} & \\
\underline{x}' \arrow[dr, Rightarrow, "*"] & & \underline{v}_1 \arrow[dl, Rightarrow, "*"] \arrow[dr, Rightarrow, "*"] & & \underline{v}_3 \arrow[dl, Rightarrow, "*"] \arrow[dr, Rightarrow, "*"] & & \underline{y}'' \arrow[dl, Rightarrow, "*"] \\
 & w_3 & = & w_4 & = & w_5 &
\end{tikzcd}$$

Figure d

We are especially interested in the case where the reduction relation $\rightarrow$ is induced by a rewrite rule system R, i.e. $\rightarrow\, = \,\rightarrow_R$, on a set of terms modulo an associative–commutative theory. The following theorem is proved in [Wi 84].

Theorem 2.5: Let T be an equational theory over the term algebra T, R a T–compatible rewrite rule system, $\Rightarrow$ a Noetherian confluent relation on $\mathsf{T}_{/T}$ which is stable and compatible (i.e. if $[s]_T \Rightarrow [t]_T$, σ a substitution, p an occurrence in u, then $[\sigma(s)]_T \Rightarrow [\sigma(t)]_T$ and $[u[p \leftarrow s]]_T \Rightarrow [u[p \leftarrow t]]_T$) such that $\rightarrow_R \cup \Rightarrow$ is Noetherian and $\Rightarrow$ is orthogonal to $\rightarrow_R$.
Then $\rightarrow_R$ is confluent modulo $\Rightarrow$ if and only if for all critical pairs $([s]_T, [t]_T)$ of R modulo T there are $[s']_T, [t']_T$ such that $[s]_T \rightarrow_R^* [s']_T \Downarrow^* [t']_T \leftarrow_R^* [t]_T$. ■

3. A common ancestor to BU and KB

Theorem 2.5 immediately leads to the following general completion procedure:

```
$R'$ ← COMPLETE($R, T, \Rightarrow$);
[$R$ is a finite Noetherian rewrite rule system over the term algebra $\mathsf{T}$,
$T$ an equational theory for which there exists a complete unification algorithm,
$\Rightarrow$ a Noetherian confluent stable and compatible relation over $\mathsf{T}_{/T}$,
such that $\rightarrow_R \cup \Rightarrow$ is Noetherian and $\Rightarrow$ is orthogonal to $\rightarrow_R$.
$R'$ is a finite Noetherian rewrite rule system such that
$(\rightarrow_R \cup \Rightarrow)^* \; = \; (\rightarrow_{R'} \cup \Rightarrow)^*$ and $\rightarrow_{R'}$ is confluent modulo $\Rightarrow$.]
$R'$ ← $T$–compatible extension of $R$;
while not all critical pairs of $R'$ have been considered do
    choose a critical pair $(c_1, c_2)$ of $R'$;
    reduce $(c_1, c_2)$ to normal forms $(d_1, d_2)$ modulo $\rightarrow_{R'} \cup \Rightarrow$;
    if $d_1 \neq d_2$ then
        if   terms $s, t$ can be constructed such that $d_1$ and $d_2$
             have a common successor modulo $\rightarrow_{R' \cup \{s \rightarrow t\}} \cup \Rightarrow$ and
             $\rightarrow_{R' \cup \{s \rightarrow t\}} \cup \Rightarrow$ is Noetherian
        then $R'$ ← $T$–compatibel extension of $R' \cup \{s \rightarrow t\}$
        else exit with failure
        endif
    endif
endwhile   ■
```

The procedure COMPLETE can be specialized both to the Knuth–Bendix procedure and to the Buchberger algorithm. We get KB from COMPLETE by letting $\Rightarrow$ be the identity and $T = \emptyset$.

It is a little bit more complicated to specialize COMPLETE to BU. We have to meet the following requirements:

(C1) give an injective mapping from the polynomial ring $K[x_1, \ldots, x_n]$ into some term algebra T modulo an equational theory T,

(C2) give a simplification relation $\Rightarrow$ on $\mathsf{T}_{/T}$, (C3) construct a rewrite rule system R for a given basis F of a polynomial ideal

such that

(P1) $\rightarrow_R \cup \Rightarrow$ simulates $\rightarrow_F$, i.e. every reduction step modulo $\rightarrow_F$ can be considered as a series of reduction steps modulo $\rightarrow_R \cup \Rightarrow$,
(P2) there exists a finite complete unification algorithm for T,
(P3) R is a finite Noetherian rewrite rule system,
(P4) $\Rightarrow$ is a Noetherian confluent stable and compatible relation over $\mathsf{T}_{/T}$,
(P5) $\rightarrow_R \cup \Rightarrow$ is Noetherian,
(P6) $\Rightarrow$ is orthogonal to $\rightarrow_R$.

Ad (C1): The term algebra T contains the binary function symbols $\oplus, \otimes$, the unary function symbol $\ominus$, the constants $X_1, \ldots, X_n$ and a for every $a \in K$, and the denumerable set of variables $V = \{x_0, x_1, \ldots\}$ (for convenience we denote the first variables by $x, y, z, w, \ldots$, similarly for the constants X_i). As the equational theory T we choose the associative-commutative theory of $\oplus$ and $\otimes$, i.e. a basis for T is

$$\{x \oplus y = y \oplus x,\ (x \oplus y) \oplus z = x \oplus (y \oplus z),\ x \otimes y = y \otimes x,\ (x \otimes y) \otimes z = x \otimes (y \otimes z)\}.$$

A nonzero polynomial $f = \sum_{i=1}^{m} a_i X_1^{e_{i1}} \cdots X_n^{e_{in}}$ is mapped onto the equivalence class of $s_1 \oplus (s_2 \oplus \cdots \oplus (s_{m-1} \oplus s_m) \cdots)$ modulo T, where s_i is the obvious description of $a_i X_1^{e_{i1}} \cdots X_n^{e_{in}}$ in T. The zero polynomial is mapped onto the constant 0. This mapping is called *term*. We let $\otimes$ have higher precedence than $\oplus$, so that we can omit parentheses because of the associativity of the operators. So, for instance, the polynomial $3x^2y^2 - 2x^2y + 4x - 5 \in \mathbb{Q}[x, y]$ is mapped onto the equivalence class $[3 \otimes X \otimes X \otimes Y \otimes Y \oplus (-2) \otimes X \otimes X \otimes Y \oplus 4 \otimes X \oplus (-5)]_T$. *term* is an injective mapping from $K[x_1, \ldots, x_n]$ onto $\mathsf{T}_{/T}$.

Ad (C2): The simplification relation $\Rightarrow$ on $\mathsf{T}_{/T}$ is defined in such a way that it simulates the operations involving the const:.nts of the coefficient field K.

$$\begin{array}{ll} [s]_T \Rightarrow [t]_T \ :\Longleftrightarrow & \text{there are } s' \equiv_T s, t' \equiv_T t, \text{ such that} \\ & t' = s'[p \leftarrow u] \text{ for some occurrence } p \text{ in } s' \text{ and } s'/_p \hookrightarrow u, \end{array}$$

where for coefficients $a_1, a_2 \in K$ and terms $s \in \mathsf{T}$:

$$\begin{array}{ll} a_1 \otimes a_2 \hookrightarrow a_1 \cdot a_2 & a_1 \oplus a_2 \hookrightarrow a_1 + a_2 \\ \ominus a_1 \hookrightarrow -a_1 & \ominus(a_1 \otimes s) \hookrightarrow (-a_1) \otimes s \\ a_1 \otimes s \oplus a_2 \otimes s \hookrightarrow (a_1 + a_2) \otimes s & 0 \oplus a_1 \otimes s \hookrightarrow a_1 \otimes s \\ 0 \otimes s \hookrightarrow 0 & \end{array}$$

The relation $\Rightarrow$ is well-defined on $\mathsf{T}_{/T}$.

Ad (C3): We start with the rules of the canonical rewrite rule system for the ring structure modulo the AC-theory T which are not already incorporated in $\Rightarrow$, i.e.

$$\begin{array}{ll} x \otimes (y \oplus z) \rightarrow (x \otimes y) \oplus (x \otimes z) & \ominus(\ominus x) \rightarrow x \\ \ominus(x \oplus y) \rightarrow (\ominus x) \oplus (\ominus y) & x \otimes (\ominus y) \rightarrow \ominus(x \otimes y) \end{array}$$

We call this rewrite rule system R_r.

For every polynomial f in the ideal basis F we include the following rule in the rewrite sytem R_F:

$$term(lt(f)) \rightarrow \ominus term(red(f)),$$

where $lt(f)$ is the leading term of f and $red(f)$ is the reductum of f.

We let the rewrite rule system R be the union of R_r and R_F. ■

This completes the simulation (C1) — (C3). Now it can be shown that (P1) — (P6) hold [Wi 84]. We illustrate this simulation of BU by the following example.

Example: We consider the ideal basis

$$F = \{\underbrace{x^2y - x^2 + 2xy}_{f_1},\ \underbrace{y^2 - y + 1}_{f_2}\} \subseteq \mathrm{Q}[x,y].$$

The power products are ordered according to the graduated lexicographic ordering. First there is only one critical pair of F, namely the one resulting from the reduction of x^2y^2 modulo f_1 and f_2, respectively.

$$\begin{tikzcd}[row sep=tiny] & x^2y - 2xy^2 \quad \rightarrow_{f_1} \quad -2xy^2 + x^2 - 2xy \quad \rightarrow_{f_2} \quad x^2 - 4xy + 2x \\ x^2y^2 \arrow[ur, "f_1"] \arrow[dr, "f_2"'] & \\ & x^2y - x^2 \quad \rightarrow_{f_1} -2xy \end{tikzcd}$$

So we add $f_3 = x^2 - 2xy + 2x$ to the ideal basis and proceed. All the other critical pairs lead to common successors, so $\{f_1, f_2, f_3\}$ is a Gröbner basis for the ideal.

The rewrite rule system corresponding to F is

$$R_F = \{(1):\ \underbrace{X \otimes X \otimes Y}_{s_1} \to \underbrace{X \otimes X \oplus (-2) \otimes X \otimes Y}_{t_1},\quad (2):\ \underbrace{Y \otimes Y}_{s_2} \to \underbrace{Y \oplus (-1)}_{t_2}\}.$$

Applying the procedure COMPLETE to $R = R_r \cup R_F$, we first have to construct a T–compatible extension $R^e$of R. Because T is an AC–theory, this means adding a new rule $u \circ s \to u \circ t$ (u a new variable) for every rule $s \to t$ with outermost operator $\circ \in \{\oplus, \otimes\}$.

$$R' = R^e = R_r \cup R_r^e \cup R_F \cup$$
$$\underbrace{\{\underbrace{u \otimes X \otimes X \otimes Y}_{s_1^e} \to \underbrace{u \otimes (X \otimes X \oplus (-2) \otimes X \otimes Y)}_{t_1^e}, \underbrace{v \otimes Y \otimes Y}_{s_2^e} \to \underbrace{v \otimes (Y \oplus (-1))}_{t_2^e}\}}_{R_F^e}.$$

The only interesting critical pair results from unifying s_1^e and s_2^e by the unifier $\sigma = \{u \leftarrow Y,\ v \leftarrow X \otimes X\}$. For brevity, we will omit the operator $\otimes$ from now on.

$$\begin{tikzcd}[column sep=small] & {[\sigma(s_1^e)]_T = [XXYY]_T = [\sigma(s_2^e)]_T} \arrow[dl, "(1^e)"'] \arrow[dr, "(2^e)"] & \\ {[Y(XX \oplus (-2)XY)]_T \rightarrow_{R_r}} & & {[XX(Y \oplus (-1))]_T \rightarrow_{R_r}} \end{tikzcd}$$

$$\begin{array}{ll} [XXY \oplus (-2)XYY]_T \rightarrow_{(1)} & [XXY \oplus (-1)XX]_T \rightarrow_{(1)} \\ [XX \oplus (-2)XY \oplus (-2)XYY]_T \rightarrow_{(2)} & [XX \oplus (-2)XY \oplus (-1)XX]_T \Rightarrow^* \\ [XX \oplus (-2)XY \oplus (-2)XY \oplus (-2)(-1)X]_T \Rightarrow^* & [(-2)XY]_T \\ [XX \oplus (-4)XY \oplus 2X]_T & \end{array}$$

We add the new rule (3) : $XX \to 2XY \oplus (-2)X$ to R' in order to guarantee a common successor of the two normal forms of $[XXYY]_T$ modulo $\rightarrow_{R'} \cup \Rightarrow$. We also have to add the extended rule, so that R' remains T–compatible.

All the other critical pairs of R' have common successors. So $\rightarrow'_R$ with $R' = R_r \cup R^e_r \cup \{(1),(2),(3)\} \cup \{(1^e),(2^e),(3^e)\}$ is confluent modulo $\Rightarrow$. ■

We want to point out that we do not claim or intend to be able to improve the efficiency of BU or KB by such a simulation. However, we think that the general completion procedure COMPLETE might help to understand the intricate relationship between two important algorithmic concepts for constructing canonical rewrite systems.

References

[Bu 65] B. Buchberger: *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* Dissertation, Univ. Innsbruck, Austria (1965).

[Bu 85a] B. Buchberger: "Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory". In: *Multidimensional Systems Theory*, N.K. Bose (ed.), 184–232, D. Reidel Publ. Comp. (1985).

[Bu 85b] B. Buchberger: "Basic Features and Development of the Critical-Pair/Completion Procedure", *Rewriting Techniques and Applications*, J.-P. Jouannaud (ed.), Springer Lecture Notes in Comp. Sci. 202, 1–45 (1985).

[BL 83] B. Buchberger, R. Loos: "Algebraic Simplification", in: *Computer Algebra — Symbolic and Algebraic Computation, 2nd ed.*, Buchberger, Collins, Loos (eds.), Springer-Verlag, 11–44 (1983).

[Hu 80] G.P. Huet: "Confluent Reductions: Abstract Properties and Applications to Term Rewriting Systems", *J.ACM* **27/4**, 797–821 (1980).

[HO 80] G.P. Huet, D.C. Oppen: "Equations and Rewrite Rules — A Survey", in: *Formal Language Theory*, R.V. Book (ed.), Academic Press, 349–405 (1980).

[KK 83] A. Kandri-Rody, D. Kapur: "On Relationship between Buchberger's Grobner Basis Algorithm and the Knuth-Bendix Completion Procedure", General Electric Technical Report No. 83CRD286, Schenectady, New York (1983).

[KB 67] D.E. Knuth, P.B. Bendix: "Simple Word Problems in Universal Algebra", *Proc. of the Conf. on Computational Problems in Abstract Algebra*, Oxford, 1967, J. Leech (ed.), Pergamon Press (1970).

[Le 86] P. Le Chenandec: *Canonical Forms in Finitely Presented Algebras*, Pitman, London (1986).

[Ll 83] R. Llopis de Trias: "Canonical Forms for Residue Classes of Polynomial Ideals and Term Rewriting Systems", Techn. Rep., Univ. Autonoma de Madrid, Division de Matematicas (1983).

[Lo 81] R. Loos: "Term Reduction Systems and Algebraic Algorithms", *Proc. 5th GI Workshop on Artif. Intell.*, Bad Honnef, Springer–Verlag, Informatik Fachberichte 47, 214–234 (1981).

[PS 81] G.E. Peterson, M.E. Stickel: "Complete Sets of Reductions for Some Equational Theories", *J.ACM* **28/2**, 233–264 (1981).

[Ra 79] P. Raulefs, J. Siekmann, P. Szabó, E. Unvericht: "A Short Survey on the State of the Art in Matching and Unification Problems", *SIGSAM Bull.* **13/2**, 14–20 (1979).

[Wi 84] F. Winkler: *The Church–Rosser Property in Computer Algebra and Special Theorem Proving: An Investigation of Critical-Pair/Completion Algorithms.* Dissertation, Univ. Linz (1984).