Normalized Rewriting – Application to Ground Completion and Standard Bases

Claude Marché

Lab. de Recherche en Informatique, Bât. 490, Université Paris-Sud et CNRS URA 410, 91405 Orsay cedex, France, E-mail: marche@lri.lri.fr

1 Introduction

We define a new kind of rewriting which is a variant of the usual notion of rewriting modulo an equational theory. This rewrite relation allows us to rewrite modulo theories for which the previous notion was not applicable, including identity, idempotency, Abelian group theory and commutative ring theory. We obtain a new completion algorithm which contains as instances many completion-like algorithms, for example AC (associative-commutative) completion algorithm, constrained AC1-completion, Buchberger's algorithm for computing standard bases of polynomial ideals over a commutative ring.

We investigate then the particular case of completion of ground equations, and we prove by a uniform method the termination of the completion process for a interesting class of equational theories, generalising the result of Narendran and Rusinowitch [23] for ground equations modulo AC, and the result of Buchberger for polynomial ideals, which is the case of ground equations modulo the theory of commutative rings. We obtain also new decidability results on the word problem in ground theories modulo AC and identity, idempotency, nilpotency (new results to our knowledge), and the cases of ground theories modulo the theory of Abelian groups and commutative rings, which is already known in the case when the signature contains only constants, but is new for extended signatures.

2 Rewriting modulo a theory presented by a canonical system

S-normalized rewriting, for an equational theory S, is a variant of the usual notion of rewriting modulo S, which has several advantages but needs S to be presented by a canonical rewrite system (modulo AC if there are AC operators).

For the usual notions on rewriting we refer to the survey of Dershowitz and Jouannaud [7].

2.1 Definition of normalized rewriting — termination

Let S be a set of rules, canonical modulo AC, let us denote by $s{\downarrow_S}$ the normal form of a term s.

Definition 1. Let R be a set of rules, the *S-normalized* rewrite relation generated by R, denoted $s \xrightarrow[R/S]{} t$, is given by:

$$s \xrightarrow[l \to r/S]{p,\sigma} t \iff \begin{cases} s' = s\downarrow_S \\ s'|_p =_{AC} l\sigma \\ t = s'[r\sigma]_p \end{cases}$$

Example 1. Let S be the canonical rewrite system for AC1$(+, 0)$, that is $\{x+0 \to x\}$. We have for example the reduction

$$-(a+b) \xrightarrow[-(x+y)\to(-x)+(-y)/S]{} (-a)+(-b)$$

but the following reduction is not valid

$$-(0+b) \xrightarrow[-(x+y)\to(-x)+(-y)/S]{} (-0)+(-b)$$

because the AC1-normal form of $-(0+b)$ is $(-b)$, which is not an instance of $-(x+y)$.

Termination of rewriting modulo a theory E (i.e. the usual notion) is rather difficult to check, because it needs a reduction ordering on terms compatible with E. On the contrary, termination of normalized rewriting needs only an ordering compatible with AC.

Let us assume now we have an AC-compatible reduction ordering $\succ$ such that each rule of S decreases w.r.t. $\succ$ that is $\xrightarrow[S]{} \subseteq \succ$. We have the following straightforward proposition.

Proposition 2 [21]. *Let R be a set of rules whose rules are decreasing w.r.t. $\succ$. Then the S-normalized rewriting by R terminates.*

2.2 Normalising pairs

We will give the completion algorithm adapted to normalized rewriting in the next section, but for that we need to define the notion of normalising pairs. This will allow us to give an orientation rule which will be general enough to contain as an instance many completion-like algorithms. For lack of space we just explain briefly where the notion of normalising pairs comes from, but the reader may look to [21] for more details.

Normalising pairs will allow in very general *orientation* rule in the completion process. Instead of building a unique rule from a given equation as in AC-completion, orientation in normalised completion will produce a set of rules and a set of equations: we will need to produce several rules at a time when using the symmetrisation technique, and we will need to keep some instances of the original equation as equations, as in AC1-constrained completion [10].

To define these normalising pairs, we need first to define a complexity measure on the algebra of equational proofs. Let $s\downarrow_p$ be the result of S-normalising s at position p (that is $s[(s|_p)\downarrow_S]_p$), and $c(s,p,t)$ be the multiset $\{s\}$ if $s|_p = s$ and $\{s\downarrow_p, t\downarrow_p\}$ otherwise. The complexity of a proof is the multiset of complexities of its

$$
\begin{aligned}
C(s \xleftrightarrow{\text{AC}} t) &= \langle \bot, && \{s\}, && \bot, \bot \rangle \\
C(s \xleftrightarrow[l=r]{\sigma,p} t) &= \langle \{s\downarrow_p, t\downarrow_p\}, && \{s,t\}, && \bot, \bot \rangle \\
C(s \xrightarrow[l\to r\downarrow_S]{\sigma} t) &= \langle \{c(s,p,t)\}, && \{s\}, && l, \; r\sigma \rangle \\
C(s \xrightarrow{S} t) &= \langle \bot, && \{s\}, && \bot, \bot \rangle
\end{aligned}
$$

Fig. 1. Elementary complexities of proofs

elementary sub-proofs, given on Figure 1. $\bot$ is a new minimal element, complexities are compared with the multiset extension of the lexicographic composition of $\succ_{mul}$ for the first two components, $\trianglerighteq_{\text{AC}}$ for the third and $\succ$ for the fourth. $\trianglerighteq_{\text{AC}}$ is the *encompassment* ordering, that is $s \trianglerighteq_{\text{AC}} t$ if $s|_p =_{\text{AC}} t\sigma$.

Definition 3. A pair $(\Theta(u,v), \Psi(u,v))$, where $\Theta(u,v)$ is a set of equations and $\Psi(u,v)$ is a set of rules, is S-*normalising* (w.r.t. $\succ$) if

1. every elementary proof of the form $s \xleftrightarrow[u=v]{\sigma} t$ or $s \xrightarrow[u\to v]{\sigma} t$ such that u, v, σ are in normal form for S, $u \succ v$, there exists a proof with a lower complexity between s and t using equations in $\Theta(u,v)$, rules in $\Psi(u,v)$, S-steps and AC-steps;
2. for all rule $l \to r$ in $\Psi(u,v)$, $\Theta(l,r) \subseteq \Theta(u,v)$ and $\Psi(l,r) \subseteq \Psi(u,v)$.

We first give a definition of a S-normalising pair for an arbitrary S. Let us denote by $\mathcal{FP}\text{os}(s)$ the set of non-variable positions of a term s and $\text{CSU}_{\text{AC}}(s,t)$ a complete set of AC-unifiers of s and t.

Definition 4. Let $\Theta_{gen}(u,v)$ be the union of

$$\{u\theta[r\theta]_q = v\theta \mid q \in \mathcal{FP}\text{os}(u), l \to r \in S, \theta \in \text{CSU}_{\text{AC}}(u|_q, l) \ S\text{-irreducible}\}$$

and

$$\{l\theta[v\theta]_q = r\theta \mid q \in \mathcal{FP}\text{os}(l), q \neq \Lambda, l \to r \in S, \theta \in \text{CSU}_{\text{AC}}(u, l|_q) \ S\text{-irreducible}\}$$

and let $\Psi_{gen}(u,v) = \{u \to v\}$.

Proposition 5. *The pair $(\Theta_{gen}(u,v), \Psi_{gen}(u,v))$ is S-normalising for any arbitrary theory S.*

Example 2. Let $S = \text{AC1} = \{z + 0 \to z\}$. Let us compute $\Theta_{gen}(-(x+y), (-x) + (-y))$: we have to unify $x + y$ and $z + 0$, leading to 4 unifiers

$$
\begin{cases} x \mapsto v_1 \\ y \mapsto 0 \\ z \mapsto v_1 \end{cases}
\begin{cases} x \mapsto 0 \\ y \mapsto v_1 \\ z \mapsto v_1 \end{cases}
\begin{cases} x \mapsto v_1 \\ y \mapsto v_2 + 0 \\ z \mapsto v_1 + v_2 \end{cases}
\begin{cases} x \mapsto v_1 + 0 \\ y \mapsto v_2 \\ z \mapsto v_1 + v_2 \end{cases}
$$

The last two are S-reducible hence we throw them away.

$$\Theta_{gen}(-(x+y),(-x)+(-y)) = \begin{cases} (-x) = (-x)+(-0) \\ (-y) = (-0)+(-y) \end{cases}$$

We see on this example that we get exactly the set of *forbidden instances* of $-(x+y) = (-x)+(-y)$ in constrained AC1-completion [10].

2.3 Normalized completion

ORIENT

$$E \cup \{u = v\}; R \;\vdash\; E \cup \Theta(u,v); R \cup \Psi(u,v)$$
$$\text{if } u = u{\downarrow_S},\ v = v{\downarrow_S},\ u \succ v$$

DEDUCE

$$E; R \;\vdash\; E \cup \{u = v\}; R \text{ if } u = v \in \mathrm{CP}_T(R)$$

NORMALIZE

$$E \cup \{u = v\}; R \;\vdash\; E \cup \{u{\downarrow_S} = v{\downarrow_S}\}; R$$

DELETE

$$E \cup \{u = v\}; R \;\vdash\; E; R \text{ if } u =_{\mathrm{AC}} v$$

COMPOSE

$$E; R \cup \{u \to v\} \;\vdash\; E; R \cup \{u \to v'\} \text{ if } v \xrightarrow[R/S]{} v'$$

SIMPLIFY

$$E \cup \{u = v\}; R \;\vdash\; E \cup \{u' = v\}; R \text{ if } u \xrightarrow[R/S]{} u'$$

COLLAPSE

$$E; R \cup \{u \to v\} \;\vdash\; E \cup \{u' = v\}; R \text{ if } \begin{cases} l \to r \in R \\ u \xrightarrow[l \to r/S]{\theta, p} u' \\ p \neq \Lambda \text{ or} \\ p = \Lambda \text{ and } \theta \text{ is not a renaming or} \\ p = \Lambda,\ \theta \text{ renaming and } u \succ r\theta \end{cases}$$

Fig. 2. Inference rules of generic S-normalized completion

Let us give now the completion algorithm corresponding to S-normalized rewriting. This algorithm is described by the set of inference rules of Figure 2. Orientation of an equation replace the given equation by its S-normalising pair, while deduction remains similar to the usual case ($\mathrm{CP}_T(R)$ denotes the set of critical pairs of R

modulo T), but a very important point is that unification can be done modulo any theory T between AC and $S \cup \mathrm{AC}$. This allows to choose a theory

1. not too “big” in order to keep unification decidable and finitary (for example we avoid ACD-unification);
2. not too “small” in order to have a small number of unifiers: if possible, we choose AC1 or ACI unification instead of AC-unification, because they generate much less solutions [16].

Definition 6. A S-normalized completion algorithm takes as input a set of equations E_0 and an AC-reduction ordering $\succ$, and produces a finite or infinite sequence $(E_n; R_n)$ where $R_0 = \emptyset$ and for all i, $E_i; R_i \ \vdash \ E_{i+1}; R_{i+1}$. Let

$$E_\infty = \bigcup_{n=0}^{\infty} \left(\bigcap_{i=n}^{\infty} E_i \right) \ , \ R_\infty = \bigcup_{n=0}^{\infty} \left(\bigcap_{i=n}^{\infty} R_i \right)$$

Completion *fails* if E_∞ is not empty, *succeeds* otherwise. Completion *diverges* if the derivation is infinite.

A derivation $E_0; R_0 \ \vdash \ E_1; R_1 \ \vdash \ \ldots$ is *fair* if every critical pairs between two persisting rules are computed, i.e.:

$$CP_T(R_\infty) \subset \bigcup_{i=0}^{\infty} E_i.$$

A completion strategy is *fair* if any derivations it produces is fair.

The proof of the following completeness theorem is by the *normalisation proof method* [2, 3].

Theorem 7. *If (Θ, Ψ) is S-normalising, if completion is fair and does not fail, then*

$$\forall s,t \quad s =_{E_0 \cup \mathrm{AC} \cup S} t \Longleftrightarrow \exists u, v \quad s \xrightarrow[R_\infty/S]{*} u, \quad t \xrightarrow[R_\infty/S]{*} v, \quad u \xrightarrow[S]{*} u{\downarrow_S} =_{\mathrm{AC}} v{\downarrow_S} \xleftarrow[S]{*} v$$

2.4 Modularity

We show now that we can easily mix two theories if they don't share any symbol (i.e. are disjoint).

Theorem 8. *Let S_1 and S_2 be two disjoint canonical systems included in the same reduction ordering.*

(i) $S_1 \cup S_2$ *is canonical;*
(ii) *if* (Θ_1, Ψ_1) *is* S_1*-normalising and* (Θ_2, Ψ_2) *is* S_2*-normalising then* $(\Theta_1 \cup \Theta_2, \Psi_1 \cup \Psi_2)$ *is* $S_1 \cup S_2$*-normalising;*
(iii) *if for a set of rules* R, $\xrightarrow[R/S_1]{*}$ *and* $\xrightarrow[R/S_2]{*}$ *are convergent then* $\xrightarrow[R/(S_1 \cup S_2)]{*}$ *is convergent.*

2.5 Examples

We show now that it is interesting in some cases to give another form of normalising pair, to gain in efficiency. In particular, we will show that the algorithm for computing standard bases of polynomial ideals over $\mathbb{Z}$ is an instance of CR-normalized completion for a well-chosen CR-normalising pair.

2.6 Some shallow theories

Theory S	canonical system	$\Theta_S(u, v)$
$AC1(+, 0)$	$x + 0 \to x$	$\{u\theta = v\theta \mid \theta = x \mapsto 0, x + w \trianglelefteq u\}$
$ACI(+)$	$x + x \to x$	$\{u\sigma = v\sigma \mid \sigma = mgu_{AC}(l_1, l_2), l1 + l2 \trianglelefteq u\}$
$AC1I(+, 0)$	$x + x \to x,\ x + 0 \to x$	$\Theta_{AC1}(u, v) \cup \Theta_{ACI}(u, v)$
$AC0(., 0)$	$x.0 \to 0$	$\{u\theta = v\theta \mid \theta = x \mapsto 0, x.w \trianglelefteq u\}$
$ACN(+, 0)$	$x + x \to 0$	$\{u\sigma = v\sigma \mid \sigma = mgu_{AC}(l_1, l_2), l1 + l2 \trianglelefteq u\}$

Fig. 3. Set Θ_S for some shallow theories S

For theories S=AC1, ACI, AC1I, AC0, ACN, let $\Psi_S(u, v) = \{u \to v\}$ and Θ_S given in figure 3.

Proposition 9. *The pair defined above is S-normalising.*

Example 3. Figure 4 shows the completion of boolean rings theory modulo nilpotence of addition with identity 0, and idempotence of multiplication with identity 1.

2.7 Normalized completion modulo the theory of Abelian groups

$$S = AG \begin{cases} x + 0 \to x \\ x + (-x) \to 0 \\ -0 \to 0 \\ -(-x) \to x \\ -(x + y) \to (-x) + (-y) \end{cases} .$$

We give now an optimized AG-normalising pair which assumes that the ordering $\succ$ is the *rpo* with a precedence of the form $\cdots > - > + > 0$, and such that $+$ has the multiset status.

Definition 10. For an equation $u = v$ of the form $n_1u_1 + \cdots + n_ku_k = m_1t_1 + \cdots + m_lt_l$, with $\forall j \geq 2,\ u_1 \succ u_j$ and $\forall j,\ u_1 \succ t_j$, let

$$\begin{aligned} s &= n_1u_1 \\ t &= -n_2u_2 - \cdots - n_ku_k + m_1t_1 + \cdots + m_lt_l \end{aligned}$$

Source	Script of completion
operators	Orienting the equation x+-(x) = 0
+,. : AC	into
0,1 : constant	{[1] x+-(x) -> 0} (1 rules)
- : 1	with critical equations
x,y,z : variable	{...} (3 equations)
	Orienting the equation 0 = -(0)
theory AC1N(+,0)	into
AC1I(.,1)	{[2] -(0) -> 0} (1 rules)
	with critical equations
axioms	{}
x+-(x) = 0;	Orienting the equation x.(y+z) = (x.y)+(x.z)
x.(y+z) = (x.y)+(x.z);	into
	{[3] x.(y+z) -> (x.y)+(x.z)} (1 rules)
order rpo 1>.>->+>0	with critical equations
	{...} (33 equations)
end	Orienting the equation x.0 = 0
	into
	{[4] x.0 -> 0} (1 rules)
	with critical equations
	{...} (7 equations)
	Orienting the equation x = -(-(x))
	into
	{[5] -(-(x)) -> x} (1 rules)
	with critical equations
	{}
	Orienting the equation y+-(x+y) = -(x)
	into
	{[6] y+-(x+y) -> -(x)} (1 rules)
	with critical equations
	{...} (28 equations)
	Orienting the equation x = -(x)
	into
	{[7] -(x) -> x} (1 rules)
	with critical equations
	{}
	Result:
	{[4] x.0 -> 0,
	[7] -(x) -> x,
	[3] x.(y+z) -> (x.y)+(x.z)} (3 rules)
	Number of calls to AC matching : 4615
	Number of successful calls : 500 (10%)
	Number of calls to AC unification : 21
	Number of critical pairs generated : 117
	User time : 4.970 s
	System time : 0.250 s

Fig. 4. Completion of Boolean rings modulo $ACN(+,0)$ and $AC1I(.,1)$

and

$$\Psi_{AG}(u,v) = \begin{cases} n_1u_1 \to -n_2u_2 - \cdots - n_ku_k + m_1t_1 + \cdots + m_lt_l \\ -u_1 \to (n_1-1)u_1 + n_2u_2 + \cdots + n_ku_k - m_1t_1 + \cdots - m_lt_l \end{cases}$$

$$\Theta_{AG}(u,v) = \Theta_{AC1}(s,t) \cup \Sigma_1(s,t) \cup \Sigma_2(s,t)$$

where

$$\Sigma_1(s,t) = CP_{AC}(s \to t, x + (-x) \to 0)$$
$$\Sigma_2(s,t) = \{s\sigma = t\sigma | \sigma = x \mapsto 0 \text{ or } -y \text{ or } y+z \text{ if } -x \in u\}$$

Proposition 11. *The pair (Θ_{AG}, Ψ_{AG}) is AG-normalising.*

We can remark that this AG-normalising pair is a generalization to the non-ground case of the symmetrization method of Le Chenadec [19].

Example 4. Figure 5 shows the completion of boolean rings theory modulo Abelian groups theory AG$(+,0,-)$ and idempotency AC1I$(.,1)$.

Example 5. Figure 6 compares completion of commutative rings modulo AC, AC1 and AG. Efficiency of AG-normalized completion is obvious.

2.8 Completion modulo the theory of commutative rings

$$S = CR \begin{cases} x + 0 \to x & x * (y+z) \to (x*y) + (x*z) \\ x + (-x) \to 0 & x * 1 \to x \\ -0 \to 0 & x * 0 \to 0 \\ -(-x) \to x & x * (-y) \to -(x*y) \\ -(x+y) \to (-x) + (-y) & \end{cases}$$

The ordering $\succ$ is the *extended-apo* [6, 21] with a precedence of the form $\cdots > * > - > + > 0$, such that $+$ and $*$ have multiset status.

Definition 12. Let $u = n_1u_1 + \cdots + n_ku_k$ and $v = m_1t_1 + \cdots + m_lt_l$, such that $\forall j \geq 2,\ u_1 \succ u_j$ and $\forall j,\ u_1 \succ t_j$, let

$$\begin{aligned} s &= n_1u_1 \\ t &= -n_2u_2 - \cdots - n_ku_k + m_1t_1 + \cdots + m_lt_l \\ \Sigma_1(u,v) &= CP_{AC}(s \to t, x + (-x) \to 0) \\ \Sigma_2(u,v) &= \{u\sigma = v\sigma | \sigma = x \mapsto 0 \text{ or } -y \text{ or } y+z \text{ if } -x \trianglelefteq u \\ \Sigma_3(u,v) &= \{u\sigma = v\sigma | \sigma = x \mapsto y+z \text{ or } -y \text{ if } x * w \trianglelefteq u \\ \Theta_{CR}(u,v) &= \Theta_{AC1}(s,t) \cup \Theta_{AC0}(s,t) \cup \Sigma_1(s,t) \cup \Sigma_2(s,t) \cup \Sigma_3(s,t) \\ \Psi_{CR}(u,v) &= \{n_1u_1 \to -n_2u_2 - \cdots - n_ku_k + m_1t_1 + \cdots + m_lt_l\} \\ &\cup \{-u_1 \to (n_1-1)u_1 + n_2u_2 + \cdots + n_ku_k - m_1t_1 + \cdots - m_lt_l \\ &\quad n_1x * u_1 \to -n_2x * u_2 - \cdots - n_kx * u_k + m_1x * t_1 + \cdots + m_lx * t_l \\ &\quad -x * u_1 \to (n_1-1)x * u_1 + n_2x * u_2 + \cdots + n_kx * u_k \\ &\qquad -m_1x * t_1 \cdots - m_lx * t_l \quad \} \\ &\quad \text{if } n_1 \geq 2, \text{ where } x \text{ is a new variable} \end{aligned}$$

Source	Script of completion

operators
  +,. : AC
  0,1 : constant
  -   : 1
  x,y,z : variable
 	
theory AG(+,0,-)
       AC1I(.,1)
 	
axioms
  x.(y+z) = (x.y)+(x.z);
 	
order rpo 1>.>->+>0
 	
end
	Orienting the equation x.(y+z) = (x.y)+(x.z)
	into
	{[1] x.(y+z) -> (x.y)+(x.z)} (1 rules)
	with critical equations
	{...} (29 equations)
	Orienting the equation x.y = (x.y)+(x.0)
	into
	{[2] x.0 -> 0} (1 rules)
	with critical equations
	{...} (32 equations)
	Orienting the equation 0 = (x.-(z))+(x.z)
	into
	{[3] x.-(z) -> -(x.z)} (1 rules)
	with critical equations
	{...} (32 equations)
	Orienting the equation -(x)+-(x) = 0
	into
	{[5] x+x -> 0,
	[4] -(x) -> -(0)+x} (2 rules)
	with critical equations
	{...} (7 equations)
	
	Result:
	{[4] -(x) -> x,
	[5] x+x -> 0,
	[2] x.0 -> 0,
	[1] x.(y+z) -> (x.y)+(x.z)} (4 rules)
	
	Number of calls to AC matching : 7512
	Number of successful calls : 635 (8%)
	Number of calls to AC unification : 23
	Number of critical pairs generated : 138
	User time : 8.770 s
	System time : 0.240 s

Fig. 5. Boolean rings theory modulo $AG(+,0,-)$ and $AC1I(.,1)$

	modulo AC	modulo AC1	modulo AG
Computation time	53.69"	47.10"	2.88"
number of calls to AC unification	136	76	11
number of critical pairs	537	412	30
number of calls to AC matching	23925	21246	1229

Fig. 6. Commutative rings modulo AC, AC1 and AG

Proposition 13. *The pair (Θ_{CR}, Ψ_{CR}) is CR-normalising.*

We will see an example of CR-normalised completion in the next section.

3 Decidability of the E-ground word problem

Definition 14. For a given set of equations E, a *E-ground theory* is an equational theory presented by E and any set of ground equations. The *E-ground word problem* is the uniform word problem of E-ground theories.

Our aim is to give a decision procedure for the word problem of E-ground theories, for some interesting E, by building an E-normalized canonical system by completion. Hence, we now look to the problem of termination of S-normalized completion, if the equations given are ground. We prove this termination for various interesting S by an almost uniform method. This give then decidability results for the uniform word problem of S-ground theories, including some already known cases, such as the AC-ground case [23], AG-ground and CR-ground cases when they are only constants [19] which contains in particular the result of existence of standard bases of ideals of polynomials over $\mathbb{Z}$ [13, 11, 14].

3.1 General Results

We assume now that $\succ$ is total [23, 21]. Let F be the set of symbols which appear in S. Because of lack of space, we omit the proofs, they can be found in [21].

Definition 15. The *generator set* of a term u w.r.t. F is given by

$$\begin{cases} \gamma_F(u) = \{u\} \text{ if } \mathcal{H}\text{ead}(u) \notin F \\ \gamma_F(u) = \bigcup\limits_{1 \le i \le n} \gamma_F(u_i) \text{ if } u = f(u_1, \ldots, u_n) \text{ with } f \in F \end{cases}$$

Let E be a set of equations and R be a set of rules. The *generator set* of E and R is given by:

$$\begin{aligned} \Gamma_F(u,v) &= \gamma_F(u) \cup \gamma_F(v) \\ G_F(E,R) &= \bigcup_{u=v \in E} \Gamma_F(u,v) \cup \bigcup_{u \to v \in R} \Gamma_F(u,v) \end{aligned}$$

Theorem 16. *Let $E; R \overset{*}{\vdash} E'; R'$ be a sequence of inferences such that $E'; R'$ are no longer simplifyable, that is neither* Normalize, Delete, Simplify, Compose *nor* Collapse *can be applied. Then*

$$G_F(E,R) \succeq_{\text{mul}} G_F(E', R')$$

Definition 17. We say that the strategy *simplifies first* if the simplification rules (Delete, Normalize, Simplify, Compose and Collapse) have priority over Orient and Deduce.

Theorem 18. *If the strategy simplifies first, and completion diverges, then R_∞ is infinite, and contains infinitely many rules whose root symbol is in F.*

Now, for each of the following cases, in order to prove termination of completion, we suppose by contradiction that the completion diverges, we use the previous theorem to obtain infinitely many rules of a particular form, and then we apply a particular case Higman's lemma [9] which is the following.

Lemma 19. *If $\preceq$ is a well-quasi-ordering over a set $\mathcal{E}$, $\preceq_{mul}$ is a well-quasi-ordering over $\mathcal{M}(\mathcal{E})$. In particular, if F is a finite set and $M_1, M_2, \ldots$ is an infinite sequence of multisets of elements of F, there exist i and j such that $M_i \subseteq M_j$.*

3.2 Ground completion modulo AC1, ACI, AC1I, AC1N and AC0

If we specialize definition of normalising pairs to ground equations, in these cases, we obtain

$$\begin{cases} \Theta_S(u,v) = \emptyset \\ \Psi_S(u,v) = \{u \to v\} \end{cases}$$

To prove termination of completion, we assume by contradiction that the completion diverges, it can be easily seen that Orient and Deduce do not modify G_F, hence by theorem 18 we know then that there are infinitely many rules whose root symbol of the lefthand side is an AC symbol $+$. We have an infinite sequence of rules $l_1 = l_{1,1} + \cdots + l_{1,k_1} \to r_1, l_2 = l_{2,1} + \cdots + l_{2,k_2} \to r_2, \ldots$ in R_∞. Each $l_{i,j}$ belongs to $G_F(R_\infty)$, but this set is finite by theorem 16. We apply lemma 19 on multisets $M_1 = \{l_{1,1}, \ldots, l_{1,k_1}\}, M_2 = \{l_{2,1}, \ldots, l_{2,k_2}\}, \ldots$ hence there exist i and j such that $M_i \subseteq M_j$ (modulo AC), hence l_i is a subterm modulo AC of l_j, hence $l_j \to r_j$ is simplifyable, a contradiction.

Theorem 20. *Every AC1-ground theory (resp. ACI, AC1I, ACN, AC0) has a AC1-normalized (resp. ACI-, AC1I-, ACN-, AC0-) canonical system, and consequently has a decidable word problem.*

3.3 Ground completion modulo the theory of Abelian groups

For an AC-compatible total reduction ordering, we use the *rpo* with a total precedence such that $\cdots > - > + > 0$, with multiset status for $+$ and lexicographic status for the other symbols. In the ground case, $\Theta_{AG}(u,v)$ becomes empty.

We can remark now that we have obtained an algorithm similar to the completion with symmetrization of Le Chenadec [19]. In fact here this is slightly more general since we allow non constant symbols. The termination of completion (already shown by Le Chenadec) is analogous to the AC1 case, with $F = \{+, -, 0\}$.

Theorem 21. *Every AG-ground equational theory has an AG-normalized canonical system, hence its word problem is decidable.*

Example 6. Figure 7 gives benchmarks of completion of a finitely presented group $\langle a, b, c; -3a + 2b + 3c = 0, 2a + 2b - 2c = 0 \rangle$. The AG-normalized canonical system contains $a \to 4b + c$, $10b \to 0$ et $-b \to 9b$, this shows in particular that the group is isomorphic to $\mathbb{Z}/_{10\mathbb{Z}} \times \mathbb{Z}$.

	modulo AC	modulo AC1	modulo AG
Computation time	4' 30"	3' 37"	1" 7
number of calls to AC unification	96	82	9
number of critical pairs	804	779	4
number of calls to AC matching	119823	117289	773

Fig. 7. Completion of a finitely generated Abelian group

3.4 Ground Completion modulo the theory of commutative rings

We need a total AC-compatible reduction ordering which orients the rules of the usual canonical system for commutative rings. It is not easy to define such an ordering, we assume here we have such an ordering, the reader may look to [21] for information.

In the normalising pair, the set Θ becomes empty in the ground case.

Example 7. $\Psi_{CR}(2(a*a)-3(b*b*b),-a+4b)$ contains the rules

$$\begin{cases} 2(a*a) \rightarrow -a+3(b*b*b)+4b \\ 2(a*a*z) \rightarrow -a*z+3(b*b*b*z)+4(b*z) \\ -(a*a) \rightarrow a*a+a-3(b*b*b)-4b \\ -(a*a*z) \rightarrow a*a*z+a*z-3(b*b*b*z)-4(b*z) \end{cases}$$

The completion algorithm obtained is similar to Buchberger's algorithm for computing standard bases of polynomial ideals over $\mathbb{Z}$ [11, 15]. This is also analogous to the technique of symmetrization of Le Chenadec.

The proof of termination of completion is similar to the one for Abelian groups, this generalize the proof of termination, known for the Buchberger's and the Le Chenadec's algorithms, to the general case where there are non constant symbols.

Theorem 22. *Every CR-ground theory has a CR-normalized canonical system, and consequently has a decidable word problem.*

Example 8. To illustrate how a standard basis is computed by the normalized completion algorithm, let us show how to compute a basis for the ideal $(2X^2Y - Y, 3XY^2 - X)$. The source file to give to our implementation and the result is shown figure 8, which corresponds to the basis $\{2X^2Y-Y, X^2Y^2-X^2+Y^2, 3Y^2-2X^2, 2X^3-X\}$.

Of course, this method is less efficient than algorithms dedicated to standard bases computation, because we still use general AC unification and general AC matching, which costs much time.

Source	Script of completion
operators	Result:
+,* : AC	{[12] (x*Y*Y)+(x*Y*Y)+(x*Y*Y) -> (x*X*X)+(x*X*X),
0,1 : constant	[17] (X*X*X)+(X*X*X) -> X,
- : unary	[16] (x*X*X*X)+(x*X*X*X) -> x*X,
X,Y,Z : constant	[9] X*X*Y*Y -> (Y*Y)+(Y*Y)+-(X*X),
x,y,z : variable	[1] -(x*X*X*Y) -> -(x*Y)+(x*X*X*Y),
	[14] -(x*X*X*X) -> -(x*X)+(x*X*X*X),
theory CR(+,0,-,*,1)	[3] (x*X*X*Y)+(x*X*X*Y) -> x*Y,
	[13] (Y*Y)+(Y*Y)+(Y*Y) -> (X*X)+(X*X),
axioms	[2] -(X*X*Y) -> -(Y)+(X*X*Y),
(X*X*Y) + (X*X*Y) +	[15] -(X*X*X) -> -(X)+(X*X*X),
-(Y) = 0;	[4] (X*X*Y)+(X*X*Y) -> Y,
(X*Y*Y) + (X*Y*Y) +	[11] -(Y*Y) -> -(X*X)+-(X*X)+(Y*Y)+(Y*Y),
(X*Y*Y) + -(X) = 0;	[10] -(x*Y*Y) -> -(x*X*X)+-(x*X*X)+(x*Y*Y)+(x*Y*Y)}
	(13 rules)
order	
rpo Y>X>1>*>->0>+ ;	Number of calls to AC matching : 17369
+ mul, * mul	Number of successful calls : 581 (3%)
	Number of calls to AC unification : 184
end	Number of critical pairs generated : 119
	User time : 24.780 s
	System time : 0.470 s

Fig. 8. Computation of a standard basis

4 Undecidability results

We have obtained decidability results in the previous section. We recall now already known undecidability results (see figure 9).

1. Decidability of word problem of ground equational theories has been shown first in 1954 by Ackermann [1].
2. Decidability of word problem in AC-ground theories has been proved by Narendran and Rusinovitch in 1991 [23], and is known since 1963 by Emilicev [8] in the particular case of finitely presented commutative semi-groups.
3. Undecidability of word problem in A-ground theories is known since 1947 because it is a consequence of undecidability of word porblem in Thue systems, proved independently by Post and Markov [26, 22].
4. Undecidability of word problem of G-ground theories is a consequence of the undecidability of word problem in finitely presented groups, and is known since 1955 by Novikov and Boone [24, 4, 28].
5. Undecidability of word problem of ACD-ground theories has been proved by Marché in 1991 [20].
6. Decidability of word problem in AC1, ACI or ACI ground theories is a consequence of the existence of a normalized canonical system.

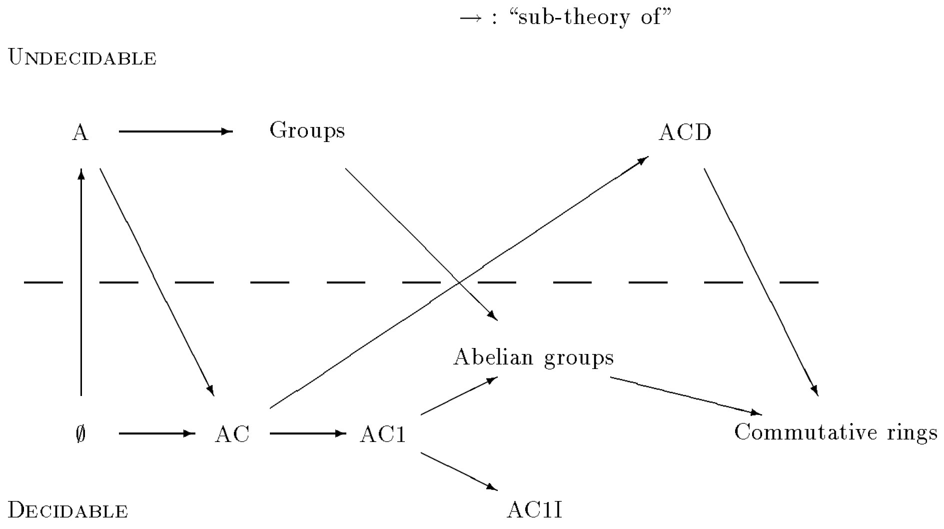

Fig. 9. Decidability of the E-ground word problem for some E

7. Decidability of word problem in AG-ground theories is known since 1966 [27] for the particular case of finitely presented Abelian groups, and a consequence of the existence of an AG-normalized canonical system in the general case.
8. Decidability of word problem in CR-ground theories is known since 1984 [12, 13] for the particular case of polynomial ideals, and a consequence of the existence of an CR-normalized canonical system in the general case.

5 Conclusion

The notion of S-normalized rewriting and S-normalized completion algorithm, whose completeness has been proved for an arbitrary S, allows us to unify in a single way a variety of completion-like algorithm, as shown on figure 10.

References

1. W. Ackermann. *Solvable Cases of the Decision Problem.* North-Holland, Amsterdam, 1954.
2. Leo Bachmair. *Proof Methods for Equational Theories.* PhD thesis, University of Illinois at Urbana-Champaign, 1987.
3. Leo Bachmair and Nachum Dershowitz. Completion for rewriting modulo a congruence. *Theoretical Computer Science*, 67(2&3):173–201, October 1989.
4. W. Boone. The word problem. *Annals of Math.*, 70:207–265, 1959.

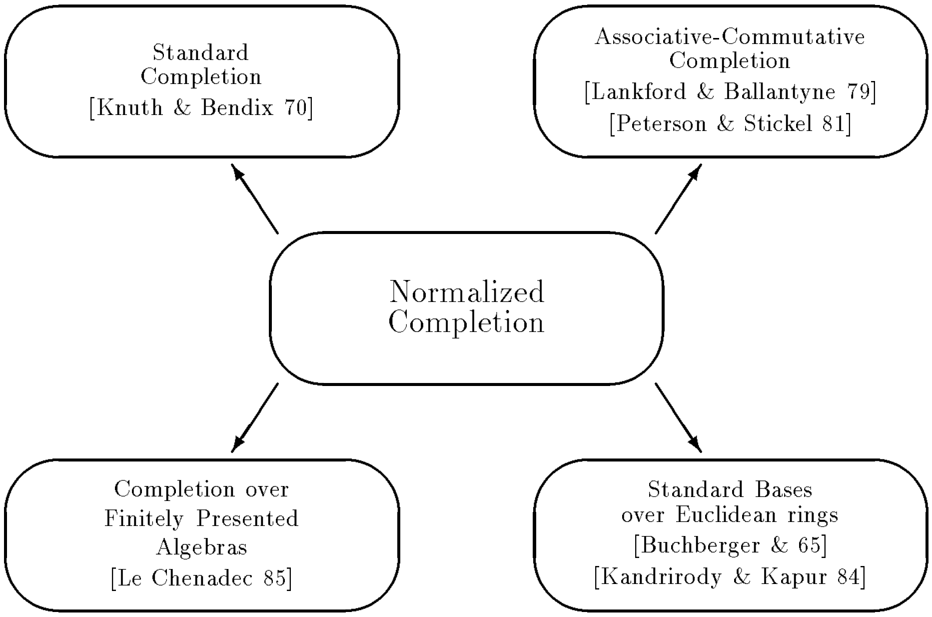

Fig. 10. Various instances of normalized completion

5. Bruno Buchberger. *An Algorithm for Finding a Basis for the Residue Class Ring of a Zero-Dimensional Ideal.* PhD thesis, University of Innsbruck, Austria, 1965. (in German).
6. Catherine Delor and Laurence Puel. Extension of the associative path ordering to a chain of associative-commutative symbols. In *Proc. 5th Rewriting Techniques and Applications, Montréal, LNCS 690*, 1993.
7. Nachum Dershowitz and Jean-Pierre Jouannaud. Rewrite systems. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume B, pages 243–309. North-Holland, 1990.
8. V. A. Emiličev. On algorithmic decidability of certain mass problems in the theory of commutative semigroups. *Sbirsk. Mat. Ž*, 4:788–798, 1963. In russian.
9. Graham Higman. Ordering by divisibility in abstract algebras. *Proceedings of the London Mathematical Society*, 2(3):326–336, September 1952.
10. Jean-Pierre Jouannaud and Claude Marché. Termination and completion modulo associativity, commutativity and identity. *Theoretical Computer Science*, 104:29–51, 1992.
11. Abdelilah Kandri-Rody and Deepak Kapur. An algorithm for computing the Gröbner basis of a polynomial ideal over an Euclidean ring. Technical Report 84CRD045, CRD, General Electric Company, Schenectady, New-York, December 1984.
12. Abdelilah Kandri-Rody and Deepak Kapur. Algorithms for computing gröbner bases of polynomial ideals over various Euclidian rings. In *Proc. Eurosam 84, Cambridge,*

England. Springer-Verlag, 1984.
13. Abdelilah Kandri-Rody and Deepak Kapur. Computing the grobner basis of an ideal in polynomial rings over the integers. In V.E. Golden and M.A. Hussain, editors, *Proc. of the Thirds MACSYMA Users'Conference*, July 1984.
14. Abdelilah Kandri-Rody, Deepak Kapur, and Franz Winkler. Knuth-Bendix procedure and Buchberger algorithm — a synthesis. In *Proc. of the 20th Int. Symp. on Symbolic and Algebraic Computation, Portland, Oregon*, pages 55–67, 1989.
15. Deepak Kapur and Paliath Narendran. Constructing Gröbner bases for a polynomial ideal. Presented at the workshop *Combinatorial algorithms in algebraic structures* at Europaische Akademie, Otzenhause, 1985.
16. Claude Kirchner, editor. *Unification*. Academic Press, 1990.
17. Donald E. Knuth and Peter B. Bendix. Simple word problems in universal algebras. In J. Leech, editor, *Computational Problems in Abstract Algebra*, pages 263–297. Pergamon Press, 1970.
18. Dallas S. Lankford and A. M. Ballantyne. Decision procedures for simple equational theories with commutative-associative axioms: Complete sets of commutative-associative reductions. Research Report Memo ATP-39, Department of Mathematics and Computer Science, University of Texas, Austin, Texas, USA, August 1977.
19. Philippe Le Chenadec. *Canonical forms in finitely presented algebras*. Pitman, London, 1986.
20. Claude Marché. The word problem of ACD-ground theories is undecidable. *International Journal of Foundations of Computer Science*, 3(1):81–92, 1992.
21. Claude Marché. Réécriture modulo une théorie présentée par un système convergent et décidabilité des problèmes du mot dans certains classes de théories équationnelles. Thèse de Doctorat, Université de Paris-Sud, France, 1993.
22. A. A. Markov. On the impossibility of certain algorithms in the theory of associative systems. *Dokl. Akad. Nauk SSSR*, 55(7):587–590, 1947. In Russian, English translation in C.R. Acad. Sci. URSS, 55, 533-586.
23. Paliath Narendran and Michaël Rusinowitch. Any ground associative-commutative theory has a finite canonical system. In Ronald V. Book, editor, *Proc. 4th Rewriting Techniques and Applications, LNCS 488*, Como, Italy, April 1991. Springer-Verlag.
24. P. S. Novikov. On the algorithmic unsolvability of the word problem in group theory. *Trudy Mat. Inst. Steklov*, 44:1–143, 1955. in Russian.
25. Gerald E. Peterson and Mark E. Stickel. Complete sets of reductions for some equational theories. *Journal of the ACM*, 28(2):233–264, April 1981.
26. Emil L. Post. Recursive unsolvability of a problem of Thue. *Journal of Symbolic Logic*, 13:1–11, 1947.
27. D. A. Smith. A basis algorithm for finitely generated Abelian groups. *Maths. Algorithms*, I(1), 1966.
28. John Stillwell. The word problem and the isomorphism problem for groups. *Bulletin of the American Mathematical Society*, 6(1):33–56, January 1982.

This article was processed using the LaTeX macro package with LLNCS style