Detecting Useless Critical Pairs

Cyrille Chenavier

Université Paris Diderot

1 Introduction

The critical pair/completion (CPC) technique was initiated in the mid sixties in three separated areas: theorem proving [12], polynomial ideal theory [3] and term rewriting [9]. For theoretical and practical reasons, improvements of CPC algorithms were developed in two main directions. The first one concerns strategies for selecting critical pairs. In [10], strategies consisting in adding the new critical pairs in a stack or in queue are investigated: the first one can fail even if another strategy succeeds whereas the second one always succeeds in the same situation. Other strategies consist in reducing critical pairs in parallel [1] and have shown to be efficient since the previously intractable cyclic 9 problem is solved using such a strategy in [6]. The second direction of improvement consists in finding criteria for detecting useless critical pairs. Buchberger introduced such a criterion in the context of polynomial ideal theory in [4] which was adapted to term rewriting systems in [13].

The presented work concerns the detection of useless critical pairs of rewriting systems whose underlying set of terms is a vector space. We are studying such rewriting systems since the theory of Gröbner bases concerns rewriting in a large class of algebraic structures (polynomial, tensor or Lie algebras, operads, invariant rings...) and we want that our framework generalises these various structures. For these structures, several criteria based on the so-called *syzygies* were introduced [7, 8, 11] for avoiding useless critical pairs during completion. As shown in [2], the computation of syzygies does not only enable us to reject critical pairs but to reject *useless reductions*. By useless reductions, we mean that all the critical pairs created from these reductions are useless. The downside of this approach is that useless reductions cannot be used to reduce terms into normal forms.

In this work, we introduce a lattice criterion for reducing the number of examinations of critical pairs. For that, we consider rewrite relations $\longrightarrow$ on a vector space V which admit decompositions

$$\longrightarrow \; = \bigcup_{i\,=\,1}^{n} \longrightarrow_i,$$

where each $\longrightarrow_i$ is also a rewrite relation on V. We propose an incremental completion procedure, that is we complete successively

$$\longrightarrow_{\leq i} \; = \bigcup_{j\,=\,1}^{i} \longrightarrow_j \, .$$

If $\longrightarrow_{\leq i}$ is already completed, we are looking for useless reductions of the form $v_1 \longrightarrow_{i+1} v_2$. In order to detect such reductions, we introduce in 2.2 the notion of *reduction operator*, which provide functional descriptions of rewriting systems. We recall in 2.3 that reduction operators admit a lattice structure, whose upper bound is written $\vee$. Letting N_i be the reduction operator normalising every element for the completion of $\longrightarrow_{\leq i}$ and T_{i+1} the reduction operator corresponding to the rewrite relation $\longrightarrow_{i+1}$, our criterion rejects the reductions $v_1 \longrightarrow_{i+1} v_2$ such that v_1 does belong to the image of $N_i \vee T_{i+1}$. In Section 3, we illustrate our criterion with a complete example.

B. Accatoli and B. Felgenhauer (eds.); IWC 2017, pp. 21–26

2 Reduction Operators

2.1. Notations. We fix a well-ordered set $(G, \ )$ and a commutative field $\mathbb{K}$. Every vector v of the vector space $\mathbb{K}G$ spanned by G admits a greatest element, written $\lg(v)$, in its decomposition with respect to G. We extend the order $<$ on G into an order on $\mathbb{K}G$ defined by $v_1 < v_2$ if $v_1 = 0$ and $v_2 \neq 0$ or if $\lg(v_1) < \lg(v_2)$.

2.2. Definition. A linear endomorphism T of $\mathbb{K}G$ is called a *reduction operator relative to* $(G, <)$ if it is a projector and if for every $g \in G$, we have $T(g) \leq g$. We write $\mathbf{RO}(G, <)$ the set of reduction operators relative to $(G, <)$ and for every $T \in \mathbf{RO}(G, <)$, we write

$$\mathrm{NF}(T) = \Big\{ g \in G \ \mid \ T(g) = g \Big\}.$$

2.3. Lattice Structure. Recall from [5, Proposition 2.1.14] that the map

$$\begin{aligned} \ker : \ \mathbf{RO}(G, <) &\longrightarrow \Big\{ \text{subspaces of } \mathbb{K}G \Big\}, \\ T &\longmapsto \ker(T) \end{aligned}$$

is a bijection. Given a subspace V of $\mathbb{K}G$, we write $\ker^{-1}(V)$ the unique reduction operator with kernel V. Then, $(\mathbf{RO}(G, <), \preceq, \wedge, \vee)$ is a lattice where

- **i.** $T_1 \preceq T_2$ if $\ker(T_2) \subseteq \ker(T_1)$,
- **ii.** $T_1 \wedge T_2 = \ker^{-1}(\ker(T_1) + \ker(T_2))$,
- **iii.** $T_1 \vee T_2 = \ker^{-1}(\ker(T_1) \cap \ker(T_2))$.

2.4. Confluence. Let $F \subset \mathbf{RO}(G, <)$. We write

$$\mathrm{NF}(F) = \bigcap_{T \in F} \mathrm{NF}(T) \ \text{ and } \ \wedge F = \ker^{-1}\left(\sum_{T \in F} \ker(T) \right).$$

The set F is said to be *confluent* if we have the equality $\mathrm{NF}(\wedge F) = \mathrm{NF}(F)$. Recall from [5, Corollary 2.3.9] that F is confluent if and only if the reduction relation defined by

$$v \underset{F}{\longrightarrow} T(v),$$

for every $T \in F$ and every $v \notin \mathrm{im}(T)$, is confluent.

2.5. Completion. Let F be a subset of $\mathbf{RO}(G, <)$. A *completion* of F is a set $F' \subset \mathbf{RO}(G, <)$ such that

- **i.** F' is confluent,
- **ii.** $F \subseteq F'$ and $\wedge F' = \wedge F$.

We let

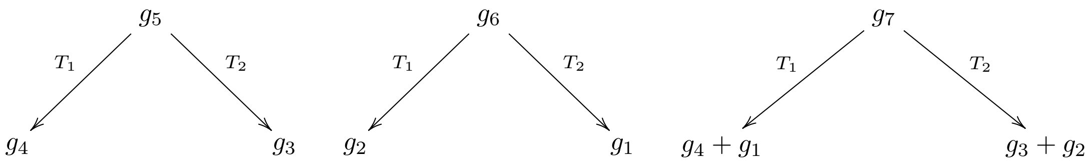
$$C^F = (\wedge F) \vee \left(\vee \overline{F} \right),$$

where $\vee \overline{F}$ is equal to $\ker^{-1}(\mathbb{K}\mathrm{NF}(F))$. Recall from [5, Theorem 3.2.6] that $F \cup \left\{ C^F \right\}$ is a completion of F.

2.6. Example. We consider $G = (g_1 < g_2 < g_3 < g_4 < g_5 < g_6 < g_7)$. We let $P = (T_1,\ T_2)$, where

$$T_1 = \begin{pmatrix} 1&0&0&0&0&0&1\\ 0&1&0&0&0&1&0\\ 0&0&1&0&0&0&0\\ 0&0&0&1&1&0&1\\ 0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0 \end{pmatrix} \text{ and } T_2 = \begin{pmatrix} 1&0&0&0&0&1&0\\ 0&1&0&0&0&0&1\\ 0&0&1&0&1&0&1\\ 0&0&0&1&0&0&0\\ 0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0 \end{pmatrix},$$

where the matrices are considered with respect to the basis G. The pair P represents the following reductions:



We have

$$C^P = \begin{pmatrix} 1&1&0&0&0&0&0\\ 0&0&0&0&0&0&0\\ 0&0&1&1&0&0&0\\ 0&0&0&0&0&0&0\\ 0&0&0&0&1&0&0\\ 0&0&0&0&0&1&0\\ 0&0&0&0&0&0&1 \end{pmatrix}.$$

2.7. Remark. In the previous example, we remark that C^P is equal to $C^{P'}$, where P' is the pair obtained by considering the restrictions of T_1 and T_2 to the vector space spanned by $G \setminus \{g_7\}$. Hence, this example shows that there exist elements of G that we can avoid during a completion procedure. Our purpose in the sequel is to provide a criterion using the lattice structure to detect these useless elements.

2.8. Restrictions and Extensions of Reduction Operators. Let $P = (T_1,\ T_2)$ be a pair of reduction operators relative to $(G,\ <)$. We consider the pair $P' = (T_1',\ T_2')$ of reduction operators relative to $\left(\mathrm{NF}\,(T_1 \vee T_2)\,,\ <\right)$ defined by $T_i'(g) = T_i(g)$ for every $g \in \mathrm{NF}\,(T_1 \vee T_2)$ and $i = 1$ or 2.

Let $\tilde{G}$ be a subset of G and let $T \in \mathbf{RO}\left(\tilde{G},\ <\right)$. Let $\overline{T} \in \mathbf{RO}\,(G,\ <)$ defined by

$$\overline{T}(g) = \begin{cases} T(g), & \text{if } g \in \tilde{G} \\ g, & \text{otherwise} \end{cases}$$

for every $g \in G$.

2.9. Proposition. *Let $F = (T_1, \cdots, T_n)$ be a finite set of reduction operators. For every $2 \leq i \leq n$, we let $P_i = (T_1 \wedge \cdots \wedge T_{i-1}, T_i)$. Then,*

$$F \cup \left\{ \overline{C^{P'_2}} \wedge \cdots \wedge \overline{C^{P'_n}} \right\},$$

is a completion of F.

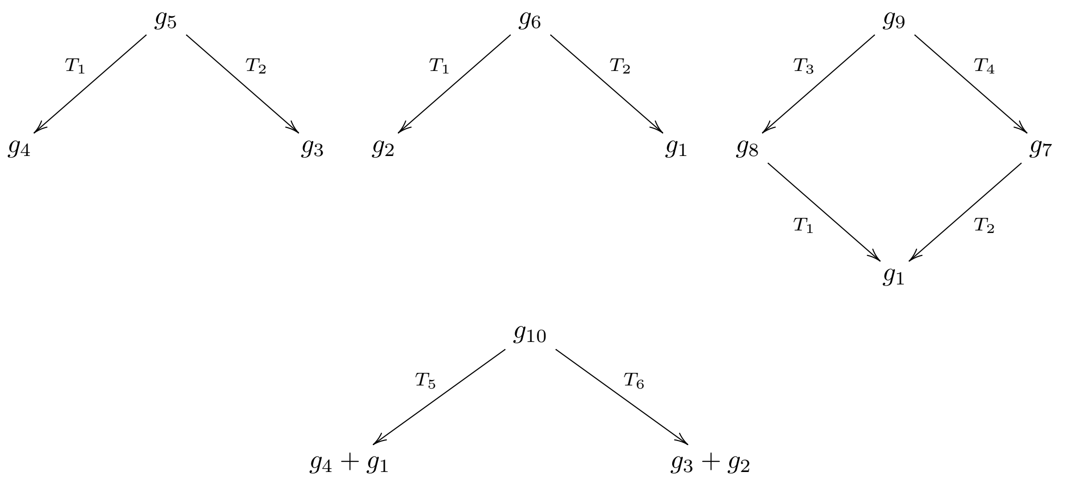
2.10. Remark.

i. The previous proposition means that the reductions $g \underset{T_i}{\longrightarrow} g$ are useless for completion whenever g is a normal form for $(T_1 \wedge \cdots \wedge T_{i-1}) \vee T_i$.

ii. In the previous proposition, we could replace the construction $\overline{C^{P'_2}} \wedge \cdots \wedge \overline{C^{P'_n}}$ by $\overline{C^{F'}}$, where F' is obtained by considering the restrictions of elements of F to the union of the sets NF $((T_1 \wedge \cdots \wedge T_{i-1}) \vee T_i)$. The construction $\overline{C^{P'_2}} \wedge \cdots \wedge \overline{C^{P'_n}}$ means that we complete successively completions of (T_1, T_2), (T_1, T_2, T_3), ..., $(T_1, \cdots, T_n) = F$. We illustrate this step by step construction in the next section.

3 Example

3.1. Initial Data. Consider $G = (g_1 < g_2 < g_3 < g_4 < g_5 < g_6 < g_7 < g_8 < g_9 < g_{10})$ and $F = (T_1, T_2, T_3, T_4, T_5, T_6)$ represented by the following reductions:



3.2. Organisation. We compute C^F step by step. We initialize the completion with

$$C = \mathrm{Id}_{\mathbb{K}G}.$$

At each step i, we select the elements g of G reducible both for $T_1 \wedge \cdots \wedge T_{i-1}$ and by T_i. If g is reducible by $(T_1 \wedge \cdots \wedge T_{i-1}) \vee T_i$, we do not consider g in the completion process.

We do not give the details of the computations. They were treated using the online implementation of reduction operators available on the website www.irif.fr/~chenavier.

3.3. Step 1. We consider $P_2 = (T_1,\ T_2)$. We have two elements of G reducible by T_1 and T_2: g_5 and g_6. Moreover, $T_1 \vee T_2$ is equal to the identity matrix of $\mathbb{K}G$, so that we need to consider both g_5 and g_6. We obtain that $C = C^{P_2}$ maps g_4 to g_3 and g_2 to g_1.

3.4. Step 2. We consider the pair $P_3 = (T_1 \wedge T_2,\ T_3)$. There is no element reducible by $T_1 \wedge T_2$ and by T_3, so that there is no completion at this step.

3.5. Step 3. We consider $P_4 = (T_1 \wedge T_2 \wedge T_3,\ T_4)$. There is one element reducible both by $T_1 \wedge T_2 \wedge T_3$ and T_4: g_9. Moreover, $(T_1 \wedge T_2 \wedge T_3) \vee T_4$ maps g_9 to g_7, i.e., $\mathrm{Red}\left((T_1 \wedge T_2 \wedge T_3) \vee T_4\right)$ is reduced to $\{g_9\}$. Hence, there is no completion at this step.

3.6. Step 4. We consider $P_5 = (T_1 \wedge T_2 \wedge T_3 \wedge T_4,\ T_5)$. There is no element reducible by $T_1 \wedge T_2 \wedge T_3 \wedge T_4$ and by T_5, so that there is no completion at this step.

3.7. Step 5. We consider $P_6 = (T_1 \wedge T_2 \wedge T_3 \wedge T_4 \wedge T_5,\ T_6)$. There is one element reducible both by $T_1 \wedge T_2 \wedge T_3 \wedge T_4 \wedge T_5$ and T_6: g_{10}. Moreover, $(T_1 \wedge T_2 \wedge T_3 \wedge T_4 \wedge T_5) \vee T_6$ maps g_{10} to $g_3 + g_2$, that is $\mathrm{Red}\left((T_1 \wedge T_2 \wedge T_3 \wedge T_4 \wedge T_5) \vee T_6\right)$ is reduced to $\{g_{10}\}$. Hence, there is no completion at this step and the completion terminates with

$$C^F = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

References

[1] Beatrice Amrhein, Reinhard Bündgen, and Wolfgang Küchlin. Parallel completion techniques. In *Symbolic rewriting techniques (Ascona, 1995)*, volume 15 of *Progr. Comput. Sci. Appl. Logic*, pages 1–34. Birkhäuser, Basel, 1998.

[2] Alberto Arri and John Perry. The F5 criterion revised. *J. Symbolic Comput.*, 46(9):1017–1029, 2011.

[3] Bruno Buchberger. Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal. *Universitat Innsbruck, Austria, Ph. D. Thesis*, 1965.

[4] Bruno Buchberger. A criterion for detecting unnecessary reductions in the construction of Gröbner-bases. In *Symbolic and algebraic computation (EUROSAM '79, Internat. Sympos., Marseille, 1979)*, volume 72 of *Lecture Notes in Comput. Sci.*, pages 3–21. Springer, Berlin-New York, 1979.

[5] Cyrille Chenavier. Reduction Operators and Completion of Rewriting Systems. *J. Symbolic Comput.*, 2017.

[6] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases (F_4). *J. Pure Appl. Algebra*, 139(1-3):61–88, 1999. Effective methods in algebraic geometry (Saint-Malo, 1998).

[7] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, pages 75–83 (electronic). ACM, New York, 2002.

[8] Rüdiger Gebauer and H. Michael Möller. On an installation of Buchberger's algorithm. *J. Symbolic Comput.*, 6(2-3):275–286, 1988. Computational aspects of commutative algebra.

[9] Donald E. Knuth and Peter B. Bendix. Simple word problems in universal algebras. In *Computational Problems in Abstract Algebra (Proc. Conf., Oxford, 1967)*, pages 263–297. Pergamon, Oxford, 1970.

[10] Wolfgang Küchlin. A theorem-proving approach to the knuth-bendix completion algorithm. *Computer Algebra*, pages 101–108, 1982.

[11] Hans-Michael Möller, Teo Mora, and Carlo Traverso. Gröbner bases computation using syzygies. In *Papers from the international symposium on Symbolic and algebraic computation*, pages 320–328. ACM, 1992.

[12] John A. Robinson. A machine-oriented logic based on the resolution principle. *J. Assoc. Comput. Mach.*, 12:23–41, 1965.

[13] Franz Winkler. Reducing the complexity of the Knuth-Bendix completion algorithm: a "unification" of different approaches. In *EUROCAL '85, Vol. 2 (Linz, 1985)*, volume 204 of *Lecture Notes in Comput. Sci.*, pages 378–389. Springer, Berlin, 1985.