Algebraic critical pair lemma

Cyrille Chenavier, Benjamin Dupont, and Philippe Malbos

[1] Johanes Kepler University, Linz, Austria, cyrille.chenavier@jku.at
[2,3] Université de Lyon, France, {bdupont,malbos}@math.univ-lyon1.fr

Abstract

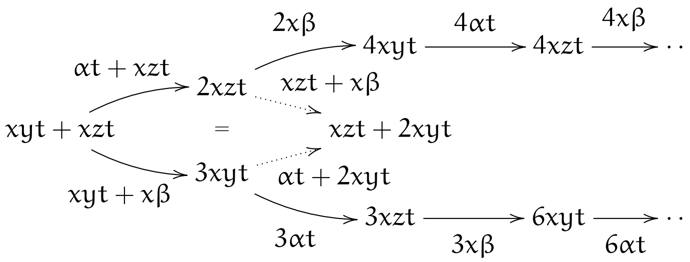
Convergent rewriting systems on algebraic structures give methods to prove coherence results and compute homological invariants of these structures. These methods are based on higher-dimensional extensions of the critical pair lemma that characterizes local confluence from confluence of critical pairs. The analysis of local confluence of rewriting systems on algebraic structures, such as groups or linear algebras, is complicated because of the underlying algebraic axioms, and local confluence properties require additional termination conditions. In this work, we define the structure of algebraic polygraph modulo that formalizes the interaction between the rules of the rewriting system and the inherent algebraic axioms, and we show a critical pair lemma algebraic polygraphs. We deduce from this result a critical pair lemma for rewriting systems on algebraic structures specified by rewriting systems convergent modulo AC. As an illustration, we explicit our constructions on linear rewriting systems.

1 Introduction

The critical-pair completion (CPC) is an approach developed in the mid sixties that combines completion procedure and the notion of critical pair [2]. It originates from theorem proving [12], polynomial ideal theory [1], and the word problem [9, 11]. In the mid eighties, CPC has found original and deep applications in algebra to solve coherence problems [14], or to compute homological invariants [13]. More recently, higher-dimensional extensions of the CPC approach were used for the computation of cofibrant replacements of algebraic and categorical structures [5, 6]. These constructions based on CPC are known for monoids, small categories, and algebras over a field. However, the extension of these methods to a wide range of algebraic structures is made difficult because of the interaction between the rewriting rules and the inherent axioms of the algebraic structure. For this reason, the higher-dimensional extensions of the CPC approach for a wide range of algebraic structures, including groups, Lie algebras, is still an open problem.

One of the main tools to reach confluence in CPC procedure for algebraic rewriting systems is the critical pair lemma, or critical branching lemma (CBL). Its proof is based on classification of the local branchings into *orthogonal* branchings, that is involving two rules that do not overlap, *overlapping* branchings involving two rules that overlap. A *critical branching* is a minimal overlapping application of two rules on the same redex. When the orthogonal branchings are confluent, if all critical branchings are confluent, then local confluence holds. Thus, the main argument to achieve CBL is to prove that orthogonal and overlapping branchings are confluent. For string and term rewriting systems, orthogonal branchings are always confluent, and confluence of critical branchings implies confluence of overlapping branchings. The situation is more complicated for rewriting systems on a linear structure.

The well known approaches of rewriting in the linear context consist in orienting the rules with respect to an ambient monomial order, and CBL is well known in this context. However, some algebras do not admit any higher-dimensional finite convergent presentation on a fixed set of generators with respect to a monomial order, [5]. However, when the orientation of rules does not depend on a monomial order, as in [5], the CBL requires additional assumptions, namely termination and positivity of reductions. A positive reduction for a linear rewriting system, as defined in [5], is the application of a reduction rule on a monomial that does not appear in the polynomial context. For instance, consider the linear rewriting system on an associative algebra over a field $\mathbb{K}$ given in [5] defined by rules $\alpha : xy \to xz$ and $\beta : zt \to 2yt$. It has no critical branching, but it has a non-confluent additive branching:



The dotted arrows correspond to non positive reductions. We note that the lack of termination is an obstruction to confluence of orthogonal branchings.

In this work we introduce an algebraic setting for the formulation of the CBL. We define the structure of algebraic polygraph modulo which formalizes the interaction between the rules of the rewriting system and the inherent axioms of the algebraic structure. We show a CBL for algebraic polygraphs modulo. We deduce from this result a CBL for rewriting systems on algebraic structures whose axioms are specified by term rewriting systems that are convergent modulo associativity and commutativity. Finally, we explicit our results in linear rewriting, and explain why termination is a necessary condition to characterize local confluence in that case.

In Section 2, we recall the categorical structure of cartesian polygraph introduced in [10]. In Section 3, we introduce the notion of algebraic polygraph modulo, and we refer the reader to [4] for a categorical interpretation of the given constructions. In Section 4, we present confluence property of algebraic polygraphs modulo from [4] and algebraic polygraphs modulo with respect a positive strategy σ. Finally, we state the algebraic critical branching lemma. This abstract is a short version of the preprint [3], where more detailed constructions and examples can be found.

2 Cartesian polygraphs

A *signature* is defined by a set P_0 of *sorts* and a set P_1 of *operations* on the free monoid over P_0. We denote by $s_0(\alpha)$ and $t_0(\alpha)$ the *arity* and *coarity* of $\alpha \in P_1$. When $s_1, \ldots, s_k$ are sorts, we denote $\underline{s} = s_1 \ldots s_k$ their product in the free monoid over P_0. We denote by $P_1^\times$ the free theory generated by a signature (P_0, P_1). Its 1-cells, also called *terms* on the signature (P_0, P_1) are defined inductively. The canonical projections $x_i^{\underline{s}} : \underline{s} \to s_i$ are *variables*, and for any terms $f : \underline{s} \to r$ and $f' : \underline{s} \to r'$ in $P_1^\times$, we denote by $\langle f, f' \rangle : \underline{s} \to rr'$, the *pairing* of terms f, f'. A *(cartesian) 2-polygraph* is a data made of a signature (P_0, P_1), and a set P_2 equipped with two maps $t_1, s_1 : P_2 \to P_1^\times$, satisfying the *globular conditions* $s_0 s_1 = s_0 t_1$ and $t_0 s_1 = t_0 t_1$. An element α of P_2 is called a *rule*, and relates terms of same arity and coarity.

2.1. Two-dimensional theories. Recall that a 2-*theory* is a 2-category with an additional cartesian structure on its 1-cells and 2-cells [10]. We denote by $P_2^\times$ the free 2-theory generated by a cartesian 2-polygraph (P_0, P_1, P_2). Its underlying 1-category is the free theory $P_1^\times$, and its 2-cells are defined inductively as follows. For $\alpha : f \Rightarrow f'$ in P_2 and $h \in P_1^\times$, there is a 2-cell $\alpha h : f \star h \Rightarrow f' \star h$ in $P_2^\times$, and for $\beta : g \Rightarrow g'$ in $P_2^\times$, there is a 2-cell $\langle \alpha, \beta \rangle : \langle f, g \rangle \Rightarrow \langle f', g' \rangle$.

Finally, there are 2-cells in $P_2^\times$ of the form $A[\alpha] : A[f] \Rightarrow A[f']$ where $A[\square]$ denotes an *algebraic context* of the form: $k\langle \mathrm{id}_{k_1}, \ldots, \square_i, \ldots, \mathrm{id}_{k_j}\rangle : \underline{s} \to r$, where $k_1, \ldots, k_j : \underline{s} \to \underline{r_i}$ and $k : \underline{r} \to r$ belong to $P_1^\times$, and $\square_i$ is the i-th element of the pairing. These 2-cells are required to satisfy *exchange relations*, see [10]. The source and target maps s_1, t_1 extend to $P_2^\times$ and we denote a_- and a_+ for $s_1(a)$ and $t_1(a)$. A *ground term* in $P_1^\times$ is a term with source $\mathbf{0}$. A 2-cell a in $P_2^\times$ is *ground* when a_- is a ground term. An algebraic context $A[\square] = f\langle f_1, \ldots, \square_i, \ldots f_{|\underline{r}|}\rangle$ is called *ground* when the f_i are ground terms.

The free $(2,1)$-theory generated by a cartesian 2-polygraph (P_0, P_1, P_2), denoted by $P_2^\top$, is the free 2-theory $P_2^\times$ whose any 2-cell is invertible with respect the $\star$-composition. The 2-cells of the $(2,1)$-theory $P_2^\top$ corresponds to elements of the equivalence relation generated by P_2.

2.2. Rewriting properties of cartesian polygraphs. The algebraic contexts of a 2-polygraph P can be composed as follows $AA'[\square] := A[A'[\square]]$. One defines a *bi-context* as $B[\square_i, \square_j] := f\langle \mathrm{id}_{f_1}, \ldots, \square_i, \ldots, \square_j, \ldots, \mathrm{id}_{f_k}\rangle$ where the $f_k : \underline{s} \to \underline{r_k}$ and $f : \underline{r} \to r$ are terms in $P_1^\times$, and $\square_i$ (resp. $\square_j$) has to be filled by a term $g_i : \underline{s} \to \underline{r_i}$ (resp. $g_j : \underline{s} \to \underline{r_j}$). A 2-cell of the form $A[\alpha w]$ where A is an algebraic context, w is a term in $P_1^\times$ and $\alpha \in P_2$ is called a P-*rewriting step*. A P-*rewriting path* is a non-identity 2-cell of $P_2^\times$. Such a 2-cell can be decomposed as a $\star$-composition of rewriting steps $\alpha = A_1[\alpha_1 w_1] \star \ldots A_k[\alpha_k w_k]$.

3 Algebraic polygraphs modulo

Let (P_0, P_1) be a signature, and Q be a set of *generating ground terms* whose target is a sort in P_0. We denote by $P_1\langle Q\rangle$ the set of ground terms of the free theory $(P_1 \cup Q)^\times$. An *algebraic polygraph* is a data made of a 2-polygraph P, a family of set of constant 1-cells Q, and a cellular extension R of the set of ground terms $P_1\langle Q\rangle$, that is a set equipped with two source and target maps $R \to P_1\langle Q\rangle$. A R-*rewriting step* is a ground 2-cell in the free 2-theory $R^\times$ of the form $A[\alpha] : A[f] \to A[g]$, where $A[\square]$ is a ground context. A R-*rewriting path* is a finite or infinite sequence $a_1 \star \ldots \star a_k \star \ldots$ of R-rewriting steps a_i. The *size* of a R-rewriting path $\underline{a}$, denoted by $|\underline{a}|$, is the number of rewriting steps needed to write $\underline{a}$ as a composition as above. The cellular extension P_2 defined on $P_1^\times$ extends to a cellular extension on the free 1-theory $(P_1 \cup Q)^\times$ denoted by $\widehat{P}_2$. We denote by $P_2\langle Q\rangle$ the set of ground 2-cells in the free 2-theory $(\widehat{P}_2)^\times$. The algebraic polygraph $(P, Q, P_2\langle Q\rangle)$ is called the *algebraic polygraph of axioms*. We denote by $\overline{P\langle Q\rangle}$ the quotient of $P_1\langle Q\rangle$ by the congruence generated by relations in $P_2\langle Q\rangle$.

3.1. Positive strategies. Denote by $\overline{f}$ the image of a ground term f by the canonical projection $\pi : P_1\langle Q\rangle \to \overline{P\langle Q\rangle}$. Let $\sigma : \overline{P\langle Q\rangle} \to \mathsf{Set}$ be a map such that for any $\overline{f} \in \overline{P\langle Q\rangle}$, $\sigma(\overline{f})$ is a chosen non-empty subset of $\pi^{-1}(\overline{f})$. Such a map is called a *positive strategy* with respect to (P, Q). A R-rewriting step a is called σ-*positive* if a_- belongs to $\sigma(\overline{a_-})$, and a R-rewriting path $a_1 \star \ldots \star a_k$ is called σ-*positive* if any of its rewriting steps is positive.

We will use positive strategies wrt a 2-polygraph P such that $P_2 = P_2' \cup P_2''$, with P_2' confluent modulo P_2''. For every 1-cell $\overline{f}$ in $\overline{P\langle Q\rangle}$, we set $\sigma(\overline{f}) = \mathsf{NF}(f, P_2' \bmod P_2'')$, where $f \in \pi^{-1}(\overline{f})$, the set of normal forms of f for P_2' modulo P_2''. This is well-defined following [7], since if $f, f' \in \pi^{-1}(\overline{f})$, then $\mathsf{NF}(f, P_2' \bmod P"_2) \equiv_{P"_2} \mathsf{NF}(f', P_2' \bmod P"_2)$.

3.2. Algebraic polygraphs modulo. Given an algebraic polygraph $\mathcal{P} = (P, Q, R)$ and a positive strategy σ on $\mathcal{P}$, one denotes by ${}_P R_P$ the cellular extension of $P_1\langle Q\rangle$ whose elements are of the form $e \star a \star e'$, where e and e' are 2-cells in $P_2\langle Q\rangle^\top$ and a is a R-rewriting step such that $e_+ = a_-$ and $a_+ = e'_-$, see [4] for a detailed construction. A 2-cell $e \star a \star e'$ in ${}_P R_P$ is called σ-positive if a is a σ-positive R-rewriting step. An *algebraic polygraph modulo*, APM for short, is a data (P, Q, R, S) made of an algebraic polygraph (P, Q, R), and a cellular extension S of $P_1\langle Q\rangle$ such that $R \subseteq S \subseteq {}_P R_P$.

An algebraic polygraph (P, Q, R) is called *quasi-terminating* if for each sequence $(f_n)_{\in \mathbb{N}}$ of 1-cells of $P_1\langle Q\rangle$ such that for each $n \in \mathbb{N}$, there is a rewriting step $f_n \to f_{n+1}$, the sequence $(f_n)_{\in \mathbb{N}}$ contains an infinite number of occurrences of same 1-cell. An APM (P, Q, R, S) is called *quasi-terminating* if the algebraic polygraph (P, Q, S) is quasi-terminating. A 1-cell f of $P_1\langle Q\rangle$ is *quasi-irreducible* if for any S-rewriting step $f \to g$, there exists a S-rewriting sequence from g to f. A *quasi-normal form* of a 1-cell f in $P_1\langle Q\rangle$ is a quasi-irreducible 1-cell $\widetilde{f}$ of $P_1\langle Q\rangle$ such that there exists a S-rewriting sequence from f to $\widetilde{f}$. For a quasi-terminating APM, any 1-cell f of $P_1\langle Q\rangle$ admits at least a quasi-normal. A *quasi-normal form strategy* is a map $s : P_1\langle Q\rangle \to P_1\langle Q\rangle$ sending a 1-cell f on a chosen quasi-normal $\widetilde{f}$.

An *algebraic rewriting system* on (P, Q, R, S, σ) is a cellular extension $\overline{S}$ of $\overline{P}\langle Q\rangle$ defined by $\overline{S} = \{\overline{a} : \overline{a_-} \Rightarrow \overline{a_+} \mid a \in S\}$. Let us consider the subset $\overline{S}^{\sigma}$ of $\overline{S}$ defined by $\overline{S}^{\sigma} = \{\overline{a} : \overline{a_-} \Rightarrow \overline{a_+} \mid a \text{ is a } \sigma\text{-positive } S\text{-rule}\}$. A $\overline{S}$-*rewriting step* (resp. a $\overline{S}^{\sigma}$-rewriting step) is a 2-cell in $\overline{S}^{\times}$ (resp. $\overline{S}^{\sigma\times}$) of the form $\overline{C}[\overline{a}] : \overline{C}[\overline{a_-}] \Rightarrow \overline{C}[\overline{a_+}]$, where C is a ground context of $P_1\langle Q\rangle$ and $C[a]$ is a S-rewriting step (resp. σ-positive S-rewriting step). A $\overline{S}$-*rewriting path* is a sequence of $\overline{S}$-rewriting steps.

4 Confluence in algebraic polygraphs modulo

Let $\mathcal{P} = (P, Q, R, S)$ be an APM with a positivity strategy σ. A σ-*branching* of $\mathcal{P}$ is a triple (a, e, b) where a, b are σ-positive 2-cells of $S^{\times}$ and e is a 1-cell of $P_2\langle Q\rangle^{\top}$ such that $e_- = a_-$ and $e_+ = b_-$. It is *local* if a is a S-rewriting step, b is a 2-cell of $S^{\times}$ and e a 2-cell of $P_2\langle Q\rangle^{\top}$ such that $|e| + |b| = 1$. Note that the 2-cell b (resp. e) can be an identity 2-cell of $S^{\times}$ (resp of $P_2\langle Q\rangle^{\top}$), and in that case the σ-branching is of the form (a, e) (resp. (a, b)). Such a σ-branching is σ-*confluent modulo* if there exist σ-positive 2-cells a' and b' in $S^{\times}$ and a 2-cell e' of $P_2\langle Q\rangle^{\top}$ as depicted on the right. We say that the APM $\mathcal{P}$ is *confluent modulo* (resp. *locally confluent modulo*) if any σ-branching modulo (resp. local branching modulo) is confluent modulo.

$$\begin{array}{ccccc} f & \xrightarrow{a} & f' & \overset{a'}{\dashrightarrow} & h \\ {\scriptstyle e}\downarrow & & & & \downarrow{\scriptstyle e'} \\ g & \xrightarrow[b]{} & g' & \underset{b'}{\dashrightarrow} & h' \end{array}$$

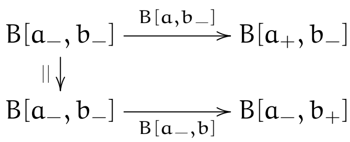
4.1. Theorem (Newman lemma modulo for algebraic polygraphs modulo). *Let $\mathcal{P}$ be a quasi-terminating APM, and σ be a positive strategy on $\mathcal{P}$. If $\mathcal{P}$ is locally σ-confluent modulo, then it is σ-confluent modulo.*

The proof of this result, and of Thm. 4.4 are based on the principle of double induction on the distance to the quasi-normal form, and are extensions to quasi-terminating setting of Huet's constructions based on double induction principle [7] in the terminating setting. Let $d : P_1\langle Q\rangle \to \mathbb{N}$ maping a 1-cell f to the length $d(f)$ of the shortest ${}_P R_P$-rewriting path from f to $\widetilde{f}$, that we extend to a map on σ-branchings (a, e, b) by setting $d(a, e, b) := d(a_-) + d(b_-)$. We define a well-founded order $\prec$ on the set of σ-branchings of $\mathcal{P}$ by $(a, e, b) \prec (a', e', b')$ if $d(a, e, b) < d(a', e', b')$.

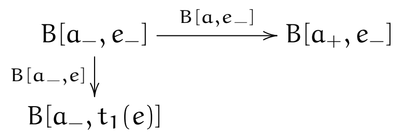
4.2. Classification of local σ-branchings modulo. The local σ-branchings modulo of S can be classified in the following families:

$$A[a_+] \xleftarrow{a} A[a_-] \xrightarrow{a} A[a_+] \qquad A[a_+] \xleftarrow{a} A[a_-] = A[A'[b_-]] \xrightarrow{b} A[A'[b_+]]$$

Trivial *Inclusion independant*



Orthogonal

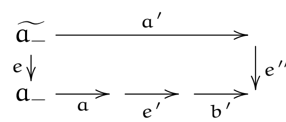


Orthogonal modulo

together with symmetries on orthogonal σ-branchings modulo, for some σ-positive S-rewriting steps a, b, 2-cell e in $P_2\langle Q\rangle^\top$, ground contexts A, A', and ground bi-contexts B, B'. The remaining local σ-branchings modulo are called *non-orthogonal* σ-branchings modulo.

We define an order relation on σ-branchings modulo of $\mathcal{P} = (P, Q, R, S)$ by setting $(a, e, b) \sqsubseteq (A[a], A[e], A[b])$ for a ground context A. A *critical σ-branching modulo* is a local σ-branching modulo P which is non trivial, non orthogonal and minimal wrt the order relation $\sqsubseteq$.

4.3. Positive confluence. An APM (P, Q, R, S) with a positive strategy σ is called σ-*positively confluent* if, for any S-rewriting step f, there exists a representing $\widetilde{a_-} \in \sigma(a_-)$ of a_- and two σ-positive S-reductions a' and b' of size at most 1 as in the following on the right.



4.4. Theorem (Terminating critical branching theorem modulo). *Let (P, Q, R, S) be a quasi-terminating and positively σ-confluent APM with a positive strategy σ. Then it is locally σ-confluent modulo if and only if the two following properties hold:*

a_0) *any critical σ-branching modulo (a, b) made of S-rewriting steps is σ-confluent modulo.*

b_0) *any critical σ-branching modulo (a, e), with a S-rewriting step and e is a 2-cell in $P_2\langle Q\rangle^\top$ of length 1, is σ-confluent modulo.*

When all the reductions are positive, that is $S(\overline{u}) = \pi^{-1}(\overline{u})$ for any $\overline{u}$, the quasi-termination assumption in Prop. 4.4 are not needed. In that case, the positive confluence is always satisfied.

4.5. Algebraic critical branching lemma. Let $\mathcal{A}$ be an algebraic rewriting system on an APM $\mathcal{P} = (P, Q, R, S)$. The *critical branchings* of $\mathcal{A}$ are the projections of the critical σ-branchings modulo of $\mathcal{P}$ of the form $\mathbf{a}_0$), that is pairs $(\overline{a}, \overline{b})$ of $\overline{S}^\sigma$-rewriting steps such that there is a σ-branching modulo in $\mathcal{P}$ with source $(\widetilde{a_-}, \widetilde{b_-})$. From Prop. 4.4, we deduce our main result.

4.6. Theorem. *Let $\mathcal{P} = (P, Q, R, S)$ be an APM such that ${}_P R_P$ is quasi-terminating and positively confluent. Let $\mathcal{A}$ be an algebraic rewriting system on $\mathcal{P}$. Then $\mathcal{A}$ is locally confluent if and only if its critical branchings are confluent.*

4.7. CBL for linear rewriting. Suppose that P contains the convergent 2-polygraph modulo AC that presents the theory of modules over commutative rings given in [8], denoted by RMod. If P_2'' is the 2-polygraph of associativity and commutativity relations, and P_2' is RMod, then Thm. 4.6 corresponds to CBL for linear rewriting systems proved in [5]. Indeed, given an APM (P, Q, R, S) with the σ-strategy defined in 3.1, one proves that the positivity confluence of S with respect to σ implies the factorization property of [5]. This property means that any rewriting step a of $\overline{S}$ can be decomposed as $a = b \star c^{-1}$ where b and c are either rewriting steps of $\overline{S}^\sigma$ or identities. Finally, the quasi-termination assumption of ${}_P R_P$ is equivalent to the termination assumption in [5].

References

[1] B. Buchberger. *An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal*. PhD thesis, University of Innsbruck, Austria, 1965.

[2] B. Buchberger. History and basic features of the critical-pair/completion procedure. *J. Symbolic Comput.*, 3(1-2):3–38, 1987. Rewriting techniques and applications (Dijon, 1985).

[3] Cyrille Chenavier, Benjamin Dupont, and Philippe Malbos. Algebraic polygraphs modulo and linear rewriting. preprint, arXiv:2004.14361, 2020.

[4] B. Dupont and P. Malbos. Coherent confluence modulo relations and double groupoids. arXiv:1810.08184, Hal-01898868, 2018.

[5] Y. Guiraud, E. Hoffbeck, and P. Malbos. Convergent presentations and polygraphic resolutions of associative algebras. *Math. Z.*, 2019.

[6] Y. Guiraud and P. Malbos. Higher-dimensional normalisation strategies for acyclicity. *Adv. Math.*, 231(3-4):2294–2351, 2012.

[7] G. Huet. Confluent reductions: abstract properties and applications to term rewriting systems. *J. Assoc. Comput. Mach.*, 27(4):797–821, 1980.

[8] J.-M. Hullot. A catalogue of canonical term rewriting systems. 1980. SRI International, Technical Report CSL 113.

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

[10] P. Malbos and S. Mimram. Cartesian polygraphic resolutions. in progress, 2020.

[11] M. Nivat. Congruences parfaites et quasi-parfaites. In *Séminaire P. Dubreil, 25e année (1971/72), Algèbre, Fasc. 1, Exp. No. 7*, page 9. Secrétariat Mathématique, Paris, 1973.

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

[13] C. Squier and F. Otto. The word problem for finitely presented monoids and finite canonical rewriting systems. In *RTA, 1987*, volume 256 of *LNCS*, pages 74–82. 1987.

[14] C. C. Squier, F. Otto, and Y. Kobayashi. A finiteness condition for rewriting systems. *TCS*, 131(2):271–294, 1994.