

Quantified Constraint Satisfaction and the Polynomially Generated Powers Property

(Extended Abstract)

Hubie Chen

Departament de Tecnologies de la Informació i les Comunicacions
Universitat Pompeu Fabra
Barcelona, Spain
hubie.chen@upf.edu

Abstract. The quantified constraint satisfaction problem (QCSP) is the problem of deciding, given a relational structure and a sentence consisting of a quantifier prefix followed by a conjunction of atomic formulas, whether or not the sentence is true in the structure. The general intractability of the QCSP has led to the study of restricted versions of this problem. In this article, we study restricted versions of the QCSP that arise from prespecifying the relations that may occur via a set of relations called a *constraint language*. A basic tool used is a correspondence that associates an algebra to each constraint language; this algebra can be used to derive information on the behavior of the constraint language.

We identify a new combinatorial property on algebras, the *polynomially generated powers* (PGP) property, which we show is tightly connected to QCSP complexity. We also introduce another new property on algebras, *switchability*, which both implies the PGP property and implies positive complexity results on the QCSP. Our main result is a classification theorem on a class of three-element algebras: each algebra is either switchable and hence has the PGP, or provably lacks the PGP. The description of non-PGP algebras is remarkably simple and robust.

1 Introduction

Background. The *constraint satisfaction problem* (CSP) is the problem of deciding, given a relational structure and a *primitive positive sentence*

$$\exists x_1 \dots \exists x_m (R(x_{i_1}, \dots, x_{i_k}) \wedge \dots)$$

that is, a conjunction of atomic formulas in front of which all variables are existentially quantified, whether or not the sentence is true in the structure. The *quantified constraint satisfaction problem* (QCSP) is the generalization of the CSP where universal quantification is permitted in addition to existential quantification. Each of these problems constitutes a natural syntactic restriction of model checking in first-order logic.

The general intractability of the CSP and the QCSP—they are NP-complete and PSPACE-complete, respectively—has prompted the study of restricted versions of these problems. In this paper, we study restricted versions of the QCSP that are obtained by prespecifying the relations that may occur using a set of relations called a *constraint*

language.¹ This form of restriction has its origins in a 1978 paper of Schaefer [24], who gave a classification theorem showing that all constraint languages over a two-element domain give rise to a case of the CSP that is either polynomial-time tractable or NP-complete. The non-trivial tractable cases identified by this result are *2-SAT*, where each constraint is equivalent to a length 2 clause; *Horn-SAT*, where each constraint is equivalent to a propositional Horn clause, and *Affine-SAT*, where each constraint is an equation over the two-element field. The quantified generalizations of these three problems are known to be tractable [1,21,7,14], and a classification theorem on two-element QCSP complexity shows that all other constraint languages over a two-element domain give rise to a PSPACE-complete case of the QCSP [14,11].

An approach to studying the complexity of constraint languages based directly on concepts and tools from universal algebra was introduced by Bulatov, Jeavons and Krokhin [5]. The cornerstone of this approach is to associate, to each constraint language Γ , an algebra \mathbb{A}_Γ whose operations are the *polymorphisms* of Γ . (Roughly speaking, an operation f is a polymorphism of a constraint language Γ if each relation of Γ is closed under the coordinate-wise action of f .) This algebra is used to derive information about the constraint language. This approach has provided new and promising vistas on the complexity of constraint languages; one celebrated achievement that it has thus far yielded is the CSP complexity classification of constraint languages over a three-element domain by Bulatov [6]. One can further name [3,16,4,22,20] as a sampling of recent work using this viewpoint.

Contributions. In this paper, we develop the algebraic theory of the QCSP and present both structural algebraic results as well as new complexity results on the QCSP.

Our starting point is collapsibility, a previously studied property on algebras [12] which provides a sufficient condition on \mathbb{A}_Γ for the reducibility of the QCSP over Γ to the CSP over Γ (which in turn immediately gives an NP upper bound on the complexity of the QCSP). This condition was shown to hold on all algebras \mathbb{A}_Γ whose corresponding QCSP is polynomial-time tractable, in the two-element case. At its heart, the QCSP-to-CSP reduction provided by collapsibility exploits a property on algebras that we define here and call the *polynomially generated powers* (PGP) property: an algebra \mathbb{A} has the PGP property if its n th power \mathbb{A}^n has a polynomial-size generating set. Indeed, it can be directly shown that collapsibility of an algebra \mathbb{A} implies that \mathbb{A} has the PGP property via generating sets of a specific form.² Although the PGP property is, in

¹ It is worth mentioning that the complexity of the QCSP under *structural restrictions*—restrictions based on variable interaction—have also recently attracted attention: see for example the papers [9,13] by the present author (the latter with Dalmau), the paper [18] by Gottlob, Greco and Scarcello, and the paper [23] by Pan and Vardi.

² In fact, as discussed in this paper (Section 2), \mathbb{A}_Γ having the PGP property, along with a mild computational assumption, yields a simple algorithm for the QCSP-to-CSP reduction on Π_2 formulas. This relationship can be used to present simple and self-contained proofs of this reduction on Π_2 formulas; examples of such proofs are given in [11, Section 1]. The essential proof technique applies across various constraint languages, and gives a uniform derivation of previously existing results in the literature, namely, the collapse results of Grädel [19] in descriptive complexity, as well as a theorem proved by Karpinski et al. [21] on the Π_2 fragment of *Quantified Horn-SAT*.

our view, a natural combinatorial property on algebras, to the best of our knowledge, it has not yet been systematically studied.

As we observe early on in this paper, in the two-element case, collapsibility “tells the full story” for the PGP property and also for polynomial-time tractability: for a constraint language Γ over a two-element set, either \mathbb{A}_Γ is collapsible, has the PGP, and the QCSP on Γ is polynomial-time tractable; or, \mathbb{A}_Γ does not have the PGP and the QCSP on Γ is PSPACE-complete. However, the three-element case is not yet understood, neither with respect to the PGP property nor with respect to QCSP complexity. A partial description of three-element non-collapsible idempotent algebras was achieved [12], but this result does not readily yield a characterization of the three-element idempotent algebras with respect to the PGP.³ The present investigation was initiated with the hope of understanding three-element idempotent algebras from the mentioned perspectives. In particular, two specific questions that we set out to answer were: Are there three-element idempotent algebras having the PGP property other than those that are collapsible, or does collapsibility give a full characterization of the PGP property for such algebras? And, for all such algebras \mathbb{A}_Γ having the PGP property, is this QCSP on Γ polynomial-time tractable, or at least reducible to the CSP?

This paper presents a classification of three-element idempotent algebras with respect to the PGP property, which identifies further, non-collapsible algebras having this property. In particular, we define a new property on algebras, *switchability*, and demonstrate that, even though switchability strictly generalizes collapsibility, it still implies both the PGP as well as a QCSP-to-CSP reduction. We then show our classification: for any three-element idempotent algebra \mathbb{A} lacking an algebraic sufficient condition for CSP/QCSP intractability (the “G-set condition”), either \mathbb{A} has switchability and indeed is polynomial-time tractable, or \mathbb{A} has a particular structure that readily implies absence of the PGP property. For the described class of algebras, we therefore answer both of the aforementioned research questions.⁴

On the “computer science” side, our introduction and study of switchability provide new polynomial-time tractable cases of the QCSP. Additionally, they give a sufficient condition for a QCSP-to-CSP reduction that is general in that it can be applied to universes of all sizes. We would like to emphasize that the description of non-switchable/non-PGP algebras given by our classification is robust in the sense that the terms of any such algebra may be viewed as a subclone of a single clone satisfying the description. In addition to being appealing in its own right, we believe that this description’s mathematical robustness will facilitate study of these algebras and their QCSP complexity.

Our classification in fact shows that the non-switchable/non-PGP algebras have the *exponentially generated powers* (EGP) property: for any sequence of generating sets X_1, X_2, \dots for the powers $\mathbb{A}^1, \mathbb{A}^2, \dots$ of such an algebra \mathbb{A} , these sets must have exponential size in that $|X_n|$ must be $\Omega(b^n)$ for some $b > 1$. We thus obtain a dichotomy

³ This paper focuses on the the QCSP where constants are permitted. It is known that to study this problem relative to a constraint language Γ , it suffices to study the algebra whose operations are the idempotent polymorphisms of Γ , hence our focus on idempotent algebras.

⁴ The first is answered by identifying new PGP algebras; the second, by showing these algebras to be polynomial-time tractable.

result with respect to a new combinatorial measure on algebras—the requisite size of generating sets for powers. Note that a dichotomy between the PGP property and EGP property is by no means entailed by the definitions of these two properties, as there are “intermediate” growth rates such as $n^{\log n}$ that are neither polynomial nor exponential, according to our definitions. Our dichotomy thus exhibits a chasm in the growth rates that occur naturally in this context, and it is curious that such intermediate growth rates do not occur.

We conclude this introduction with a brief methodological/philosophical discussion of this article’s approach and context. On the one hand, an algebraic notion was introduced by complexity considerations: the definition of the PGP property was inspired by considering the Π_2 fragment of the QCSP. On the other hand, algebraic investigation led to insight on complexity: during the course of obtaining the results in this article, the author identified some non-collapsible algebras to have the PGP property prior to establishing any complexity-theoretic result on any of them (in particular, before proving that any of them possessed a QCSP-to-CSP reduction). It is our understanding that the recent investigations on the so-called *few subalgebras property* followed a similar storyline: a purely combinatorial property on algebras was defined from computational considerations [15,10], a classification of such algebras with respect to the property was established [2], and then the algebras possessing the property were shown to entail a desirable computational property—in this case, CSP tractability [20].⁵ We believe and hope that the CSP and its variants will continue to effect this mutual cross-pollination between algebra and complexity, and certainly look forward to further work along these lines.

Preliminaries. Our notations and definitions are fairly standard, and similar to those used in [12]. Here, we confine ourselves to a few remarks. We use $[n]$ to denote the set containing the first n positive integers, $\{1, \dots, n\}$. We use $\text{QCSP}_c(\Gamma)$ to denote the QCSP over constraint language Γ where constants may appear in constraints; $\text{CSP}_c(\Gamma)$ is the restriction of $\text{QCSP}_c(\Gamma)$ to formulas having only existential quantifiers. We use $\text{QCSP}(\Gamma)$ and $\text{CSP}(\Gamma)$ to denote the same problems, but where constants may not appear in constraints.

2 Properties

In this section, we introduce the two combinatorial properties on algebras—the *polynomially generated powers* and the *exponentially generated powers* properties—that will be studied.

For an algebra \mathbb{A} and a subset $X \subseteq A$, we use $\langle X \rangle$ to denote the intersection of all \mathbb{A} -subalgebras containing X (that is, the smallest subalgebra of \mathbb{A} containing X). We call $\langle X \rangle$ the subalgebra *generated* by X . We say that a function $f : \mathbb{N} \rightarrow \mathbb{N}$ is a *polynomial* if there exists $k \geq 1$ such that $f(n)$ is $O(n^k)$.

⁵ A remark: M. Valeriote has communicated to us that in studying the few subalgebras property, it was observed by the authors of [2] that the few subalgebras property implies the PGP property. The converse does not hold: the algebra $(\{0, 1\}, \{\wedge\})$ is an example of an algebra having the PGP property but not having the few subalgebras property.

Definition 1. An algebra \mathbb{A} has the polynomially generated powers (PGP) property if there exists a polynomial $p(n)$ such that for all $n \geq 1$, there exists a subset $X_n \subseteq A^n$ of size $|X_n| \leq p(n)$ that generates the algebra \mathbb{A}^n .

We now show that the PGP property, along with a polynomial-time algorithm that computes generating sets, implies a reduction from the Π_2 fragment of the QCSP to the CSP.

Proposition 1. Let Γ be a constraint language. If \mathbb{A}_Γ has the PGP property and there exists an algorithm that outputs a generating set X_n for \mathbb{A}_Γ^n in polynomial time (in n), then Π_2 -QCSP $_c(\Gamma)$ reduces to CSP $_c(\Gamma)$.

This proposition is implicit in [11]. As noted there, it can be readily used to derive the collapse results of Grädel [19] in descriptive complexity, as well as a theorem proved by Karpinski et al. [21] on the Π_2 fragment of *Quantified Horn-SAT*. We refer the reader to [11] for further discussion.

Definition 2. An algebra \mathbb{A} has the exponentially generated powers (EGP) property if for any sequence of subsets $X_1 \subseteq A^1, X_2 \subseteq A^2, X_3 \subseteq A^3, \dots$ where for all $n \geq 1$ the subset X_n generates \mathbb{A}^n , there exists $b > 1$ such that the size function $|X_n|$ is $\Omega(b^n)$.

The following proposition furnishes examples of algebras having the EGP property. Say that an operation $f : A^k \rightarrow A$ is *essentially unary* if there exists a coordinate i and a unary operation $g : A \rightarrow A$ such that $f(a_1, \dots, a_k) = g(a_i)$ for all $(a_1, \dots, a_k) \in A^k$. Say that an algebra is *essentially unary* if all of its operations are essentially unary.

Proposition 2. An essentially unary algebra \mathbb{A} with finite universe of non-trivial size has the EGP property.

3 Collapsibility

In this section, we review the notion of collapsibility as well as the results on this notion that will be relevant to the present work. This section should be taken as a presentation of previous work; other than Propositions 4, 5, and 7, the results and concepts are either explicit or implicit in [12].

Definition 3. Let $n \geq 1$ and \mathbb{A} be an algebra. A rectangular adversary (of length n) is a set of tuples having the form $B_1 \times \dots \times B_n$, where $B_i \subseteq A$ for all $i \in [n]$.⁶

Definition 4. Let $n, w \geq 1$ and \mathbb{A} be an algebra. Say that a rectangular adversary $B_1 \times \dots \times B_n$ is w -bounded if there exists a value $a \in A$ and a subset $S \subseteq [n]$ with $|S| \leq w$ such that $B_s = A$ for all $s \in S$ and $B_i = \{a\}$ for all $i \in [n] \setminus S$. That is, a rectangular adversary is w -bounded if w or fewer of its sets are equal to A , and the rest are equal to $\{a\}$ for the same constant $a \in A$.

⁶ We remark that what we call a *rectangular adversary* here is simply called an *adversary* in [12].

Definition 5. An algebra \mathbb{A} is collapsible if there exists $w \geq 1$ such that for all $n \geq 1$, there exist an \mathbb{A} -term operation $f : A^k \rightarrow A$ and w -bounded rectangular adversaries (of length n) $B_{11} \times \cdots \times B_{1n}, \dots, B_{k1} \times \cdots \times B_{kn}$ such that for all $j \in [n]$, $A = f(B_{1j}, \dots, B_{kj})$.

The following is the primary computational property of collapsibility.

Theorem 3. [12] Let Γ be a constraint language. If \mathbb{A}_Γ is collapsible, then $\text{QCSP}_c(\Gamma)$ reduces to $\text{CSP}_c(\Gamma)$.

We show that collapsibility directly implies the PGP.

Proposition 4. If an algebra \mathbb{A} is collapsible, then it has the polynomially generated powers property.

We may now observe that collapsibility characterizes the PGP property in the two-element case. We have the following dichotomy result.

Proposition 5. Let \mathbb{A} be an algebra having a 2-element universe. Either \mathbb{A} is collapsible and has the PGP property, or \mathbb{A} has the EGP property.

We can remark that, in the two-element case, the boundary line between the PGP property and the EGP property matches the boundary between the tractability and intractability of $\text{QCSP}(\Gamma)$: for a constraint language Γ over a two-element set, when \mathbb{A}_Γ has the PGP property, $\text{QCSP}(\Gamma)$ is polynomial-time tractable; and, when \mathbb{A}_Γ has the EGP property, $\text{QCSP}(\Gamma)$ is PSPACE-complete. (This is readily derived from the dichotomy on two-element $\text{QCSP}(\Gamma)$ complexity [14, 11] and the proof of Proposition 5.)

The following theorem was the result of attempts to understand those algebras which are not collapsible, nor have a G-set.

Theorem 6. [12] Let \mathbb{A} be an idempotent algebra having three-element universe A . Either:

1. \mathbb{A} is collapsible and for any constraint language Γ with $\mathbb{A}_\Gamma = \mathbb{A}$, $\text{QCSP}_c(\Gamma)$ is in P ;
2. \mathbb{A} has a G-set as factor and for any constraint language Γ with $\mathbb{A}_\Gamma = \mathbb{A}$, $\text{QCSP}_c(\Gamma)$ is NP-hard; or,
3. There is a way to label the elements of A as $\{a, b, c\}$ such that:
 - the size 2 subalgebras of \mathbb{A} are $\{a, c\}$ and $\{b, c\}$, which we denote by α and β respectively,
 - \mathbb{A} has as a term operation the semilattice operation $s_{abc} : A \times A \rightarrow A$ defined by $s_{abc}(x, y) = c$ if $x \neq y$, and $s_{abc}(x, y) = x$ if $x = y$, and
 - for every term operation $f : A^k \rightarrow A$ of \mathbb{A} and subalgebras $S_1, \dots, S_k \in \{\alpha, \beta\}$, there exists $T \in \{\alpha, \beta\}$ such that $f(S_1, \dots, S_k) \subseteq T$.⁷

⁷ Regarding the statement of this theorem, we remark that it is not the case that for every three-element idempotent algebra \mathbb{A} there exists a constraint language Γ such that $\mathbb{A} = \mathbb{A}_\Gamma$; the operations of an algebra of the form \mathbb{A}_Γ are closed under taking term operations, which is not required of an algebra in general.

The algebras \mathbb{A}_Γ for which the tractability/intractability of $\text{QCSP}_c(\Gamma)$ is not yet fully understood are those of type (3). These fall into a “gap”: on the one hand, we cannot derive tractability using the condition of collapsibility; on the other hand, we cannot derive intractability using the G-set condition. We hence refer to them as *gap algebras*.

Definition 6. A gap algebra is a three-element idempotent algebra that is not collapsible and has no G-set as factor.

We now introduce some terminology that can be used to discuss gap algebras, but also apply more generally to three-element algebras.

Definition 7. Let A be a three-element set, and let α and β be distinct two-element subsets of A .

- We say that an operation $f : A^k \rightarrow A$ can be realized as an operation $g : \{\alpha, \beta\}^k \rightarrow \{\alpha, \beta\}$ if for all $S_1, \dots, S_k \in \{\alpha, \beta\}$, it holds that $f(S_1, \dots, S_k) \subseteq g(S_1, \dots, S_k)$.
- We say that an operation $f : A^k \rightarrow A$ is $\alpha\beta$ -projective if it can be realized by an operation g on $\{\alpha, \beta\}$ that is a projection.

We remark that any term operation f of a gap algebra can be realized as an operation g , by the third condition given on such algebras by Theorem 6, with respect to the α and β described in that theorem.

We now define the notion of an $\alpha\beta$ -projective algebra.

Definition 8. Let \mathbb{A} be an algebra with three-element universe A . We say that \mathbb{A} is $\alpha\beta$ -projective if there exist distinct two-element subsets α and β of A with respect to which all operations of \mathbb{A} are $\alpha\beta$ -projective.

Note that the notion of $\alpha\beta$ -projective operation is robust: the composition of $\alpha\beta$ -projective operations is also an $\alpha\beta$ -projective operation. As all projections are $\alpha\beta$ -projective, all term operations of an $\alpha\beta$ -projective algebra are $\alpha\beta$ -projective.

Proposition 7. An algebra that is $\alpha\beta$ -projective has the EGP property.

4 A Curious Operation

In this section, we focus on a particular algebra that is defined by a single operation. Define $r : \{a, b, c\}^4 \rightarrow \{a, b, c\}$ to be the operation where

$$r(a, b, b, b) = r(b, a, b, b) = r(b, b, b, b) = b$$

and

$$r(a, a, b, a) = r(a, a, a, b) = r(a, a, a, a) = a$$

and is equal to c otherwise. Define \mathbb{A}_r to be the algebra $(\{a, b, c\}, \{r\})$. Note that \mathbb{A}_r has s_{abc} as a term operation: $s_{abc}(x, y) = r(x, x, y, y)$; hence, \mathbb{A}_r has no G-set factor.

Does \mathbb{A}_r have the PGP property? We may observe that \mathbb{A}_r is not $\alpha\beta$ -projective, rendering this sufficient condition for the EGP property unusable here. We do this as

follows. An algebra cannot be $\alpha\beta$ -projective with respect to a two-element subset that is not a subalgebra; hence, if \mathbb{A}_r is $\alpha\beta$ -projective at all, it must be $\alpha\beta$ -projective with respect to the two two-element subalgebras $\alpha = \{a, c\}$ and $\beta = \{b, c\}$ of \mathbb{A}_r . However, from the relationships

$$b = r(a, b, b, b) \in r(\alpha, \beta, \beta, \beta) \not\subseteq \alpha$$

$$b = r(b, a, b, b) \in r(\beta, \alpha, \beta, \beta) \not\subseteq \alpha$$

$$a = r(a, a, b, a) \in r(\alpha, \alpha, \beta, \alpha) \not\subseteq \beta$$

$$a = r(a, a, a, b) \in r(\alpha, \alpha, \alpha, \beta) \not\subseteq \beta$$

we may see that r cannot be realized as any of the arity 4 projections (on $\{\alpha, \beta\}$), and hence is not $\alpha\beta$ -projective. Indeed, one might view r as being “diagonalized away” from being $\alpha\beta$ -projective.

So, we were unable to apply our sufficient condition for the EGP property to \mathbb{A}_r . What about trying to show that \mathbb{A}_r satisfies collapsibility, our sufficient condition for the PGP property? This fails as well.

Proposition 8. *The algebra \mathbb{A}_r is not collapsible.*

As we have now obtained that the algebra \mathbb{A}_r has no G-set, is not $\alpha\beta$ -projective, and is not collapsible, we have that \mathbb{A}_r is a non- $\alpha\beta$ -projective gap algebra. We now show that this algebra has the PGP property.

Proposition 9. *The algebra \mathbb{A}_r has the PGP property.*

The proof of this proposition uses the following definition. For a tuple $(t_1, \dots, t_n) \in T^n$ over a set T , say that a coordinate $i \in [n - 1]$ is a *switch* (of the tuple) if $t_i \neq t_{i+1}$.

In the next sections, we will see that the algebra \mathbb{A}_r is a member of a class of algebras that we introduce called *switchable* algebras—algebras which, as with collapsible algebras, both have the PGP property and imply a QCSP-to-CSP reduction. The condition of switchability generalizes the condition of collapsibility; the algebra \mathbb{A}_r will witness that switchability is a strict generalization of collapsibility.⁸

5 Switchability

The goal of this section is to present the notion of *switchability* as well as some of its basic properties. We review and introduce some basic concepts concerning quantified formulas to be used (Section 5.1), present a notion of composition for sets of tuples that is used in the definition of switchability (Section 5.2), and then proceed to develop the notion of switchability (Section 5.3).

⁸ In the present section, we showed that the algebra \mathbb{A}_r is not collapsible (Proposition 8); it follows from Theorem 17 that the algebra \mathbb{A}_r is switchable.

5.1 Truth and Adversaries

We now review a characterization of truth for quantified constraint formulas. This characterization comes from the concept of Skolemization [17]. When Φ is a quantified constraint formula, let V^Φ denote the variables of Φ , let E^Φ denote the existentially quantified variables of Φ , let U^Φ denote the universally quantified variables of Φ , and for each $x \in E^\Phi$, let U_x^Φ denote the variables in U^Φ that come before x in the quantifier prefix of Φ . (We may drop the Φ superscript if the formula is clear from the context.) Let $[B \rightarrow A]$ denote the set of functions mapping from B to A .

Definition 9. A strategy for a quantified constraint formula Φ is a sequence of partial functions

$$\sigma = \{\sigma_x : [U_x^\Phi \rightarrow A] \rightarrow A\}_{x \in E^\Phi}.$$

That is, a strategy has a mapping σ_x for each existentially quantified variable $x \in E^\Phi$, which tells how to set the variable x in response to an assignment to the universal variables coming before x . Let $\tau : U^\Phi \rightarrow A$ be an assignment to the universal variables. We define $\langle \sigma, \tau \rangle$ to be the mapping from V^Φ to A such that $\langle \sigma, \tau \rangle(v) = \tau(v)$ for all $v \in U^\Phi$, and $\langle \sigma, \tau \rangle(x) = \sigma_x(\tau|_{U_x^\Phi})$ for all $x \in E^\Phi$. The mapping $\langle \sigma, \tau \rangle$ is undefined if $\sigma_x(\tau|_{U_x^\Phi})$ is not defined for all $x \in E^\Phi$. The intuitive point here is that a strategy σ along with an assignment τ to the universally quantified variables naturally yields an assignment $\langle \sigma, \tau \rangle$ to all of the variables, so long as the mappings σ_x are defined at the relevant points.

We have the following characterization of truth for quantified constraint formulas.

Fact 10. A quantified constraint formula Φ is true if and only if there exists a strategy σ for Φ such that for all mappings $\tau : U^\Phi \rightarrow A$, the assignment $\langle \sigma, \tau \rangle$ is defined and satisfies the constraints of Φ .

Note that a strategy satisfying the condition of Fact 10 must consist only of total functions. We have defined a strategy to be a sequence of *partial* functions as we will be interested in strategies σ that need not yield an assignment $\langle \sigma, \tau \rangle$ for all τ .

Definition 10. An adversary is a set of tuples on a set A , all of the same length; the length of an adversary is considered to be the length of one (any) of its tuples.

Let us say that an adversary \mathcal{A} is an adversary for a quantified constraint formula Φ if the length of \mathcal{A} matches the number of universally quantified variables in Φ . When this is the case, the adversary \mathcal{A} naturally induces the set of assignments $\mathcal{A}[\Phi] = \{\tau \in [U^\Phi \rightarrow A] \mid (\exists(a_1, \dots, a_n) \in \mathcal{A})(\forall i \in [n])(\tau(y_i) = a_i)\}$. Here, we assume that y_1, \dots, y_n are the universally quantified variables of Φ , ordered according to quantifier prefix, from outside to inside.

We say that an adversary is Φ -winnable if in the modified game, the existential player can win: that is, if there is a strategy that can handle all assignments that the adversary gives rise to, as formalized in the following definition.

Definition 11. Let Φ be a quantified constraint formula, and let \mathcal{A} be an adversary for Φ . We say that \mathcal{A} is Φ -winnable if there exists a strategy σ for Φ such that for all assignments $\tau \in \mathcal{A}[\Phi]$, the assignment $\langle \sigma, \tau \rangle$ is defined and satisfies the constraints of Φ .

We have previously given a characterization of truth for quantified constraint formulas (Fact 10). This characterization can be formulated in the terminology just introduced.

Fact 11. *The adversary A^n is Φ -winnable if and only if Φ is true.*

5.2 Reactive Composition

Let $f : A^k \rightarrow A$ be an operation and let $\mathcal{A}, \mathcal{B}_1, \dots, \mathcal{B}_k$ be adversaries of length n . We say that \mathcal{A} is *f-reactively composable* from $\mathcal{B}_1, \dots, \mathcal{B}_k$, denoted $\mathcal{A} \trianglelefteq f(\mathcal{B}_1, \dots, \mathcal{B}_k)$, if there exist partial functions $g_i^j : A^i \rightarrow A$ for $i \in [n], j \in [k]$ such that, for every tuple $(a_1, \dots, a_n) \in \mathcal{A}$:

- for every $j \in [k]$, the values $g_1^j(a_1), g_2^j(a_1, a_2), \dots, g_n^j(a_1, \dots, a_n)$ are defined,
- for every $j \in [k]$, the tuple $(g_1^j(a_1), g_2^j(a_1, a_2), \dots, g_n^j(a_1, \dots, a_n))$ is contained in \mathcal{B}_j , and
- for each $i \in [n]$, $a_i = f(g_i^1(a_1, \dots, a_i), \dots, g_i^k(a_1, \dots, a_i))$.

When \mathbb{A} is an algebra and $\mathcal{A}, \mathcal{B}_1, \dots, \mathcal{B}_k$ are adversaries of the same length, we say that \mathcal{A} is *\mathbb{A} -reactively composable* from $\mathcal{B}_1, \dots, \mathcal{B}_k$ if there exists a term operation f of \mathbb{A} such that $\mathcal{A} \trianglelefteq f(\mathcal{B}_1, \dots, \mathcal{B}_k)$.

Theorem 12. *Let Φ be a quantified constraint formula, assume that $f : A^k \rightarrow A$ is an idempotent polymorphism of all relations of Φ , and let $\mathcal{A}, \mathcal{B}_1, \dots, \mathcal{B}_k$ be adversaries for Φ . If each of the adversaries $\mathcal{B}_1, \dots, \mathcal{B}_k$ is Φ -winnable and $\mathcal{A} \trianglelefteq f(\mathcal{B}_1, \dots, \mathcal{B}_k)$, then the adversary \mathcal{A} is Φ -winnable.*

The notion of reactive composition as well as this theorem appeared in [8], although in a slightly different formulation.

Proposition 13. *Let \mathbb{A} be an algebra, and let S and S' be sets of adversaries, all of the same length. If an adversary \mathcal{A} is \mathbb{A} -reactively composable from adversaries in S' , and all adversaries in S' are \mathbb{A} -reactively composable from adversaries in S , then \mathcal{A} is \mathbb{A} -reactively composable from adversaries in S .*

5.3 Definition and Basic Properties

Recall that we define the *switches* of a tuple $\bar{s} = (s_1, \dots, s_n) \in S^n$ over a set S to be the coordinates $\{i \in [n-1] \mid s_i \neq s_{i+1}\}$; the number of switches of \bar{s} is the cardinality of this set.

Definition 12. *Let $T \subseteq A^n$ be a set of tuples, and let $w \geq 1$. Define $\mathcal{S}(T, w)$ to be the set $\{\bar{t} \in T \mid \bar{t} \text{ has } w \text{ or fewer switches}\}$.*

Definition 13. *An algebra \mathbb{A} is *switchable* if there exists $w \geq 1$ such that for all $n \geq 1$, there exists an \mathbb{A} -term operation $f : A^k \rightarrow A$ such that*

$$A^n \trianglelefteq f(\mathcal{S}(A^n, w), \dots, \mathcal{S}(A^n, w)).$$

Observe that, for a fixed $w \geq 1$, the set $\mathcal{S}(A^n, w)$ has polynomial size in n : a tuple in this set is determined by the location of its switches and a tuple over A of length up to $w + 1$ specifying, in order, the values it takes on. We may thus upper bound the size of $\mathcal{S}(A^n, w)$ by $\binom{n}{1} + \dots + \binom{n}{w} \cdot (|A|^{w+1})$ which is $O(n^w)$.

Proposition 14. *Let \mathbb{A} be an algebra. If \mathbb{A} is collapsible, then \mathbb{A} is switchable.*

Theorem 15. *Let Γ be a constraint language. If \mathbb{A}_Γ is switchable, then $\text{QCSP}_c(\Gamma)$ reduces to $\text{CSP}_c(\Gamma)$.*

Theorem 16. *Let \mathbb{A} be an algebra. If \mathbb{A} is switchable, then \mathbb{A} has the PGP property.*

6 Classification Theorem

Theorem 17. *(Classification theorem) A three-element idempotent algebra not having a G -set is either switchable or is $\alpha\beta$ -projective.*

Notice that the terms of an $\alpha\beta$ -projective algebra may be viewed as a subclone of the clone containing all $\alpha\beta$ -projective operations.

6.1 Corollaries

Corollary 1. *A three-element idempotent algebra not having a G -set either has the PGP property, or has the EGP property.*

Corollary 2. *For every 3-element constraint language Γ , either $\text{QCSP}_c(\Gamma)$ is in P , $\text{QCSP}_c(\Gamma)$ is NP -hard, or the algebra \mathbb{A}_Γ is $\alpha\beta$ -projective.*

Acknowledgements. The author thanks Víctor Dalmau for useful discussions, Manuel Bodirsky for suggestions on a draft of this paper, and Matt Valeriote for helpful remarks and aid with terminological decisions. Some of the results and ideas in this paper were presented at the Workshop on Universal Algebra and the Constraint Satisfaction Problem held at Vanderbilt University in June 2007; the author thanks the participants of this workshop for their interest.

References

1. Aspvall, B., Plass, M.F., Tarjan, R.E.: A linear-time algorithm for testing the truth of certain quantified boolean formulas. *Information Processing Letters* 8(3), 121–123 (1979)
2. Berman, J., Idziak, P., Markovic, P., McKenzie, R., Valeriote, M., Willard, R.: Varieties with few subalgebras of powers (submitted for publication)
3. Bulatov, A.: Tractable conservative constraint satisfaction problems. In: *Proceedings of 18th IEEE Symposium on Logic in Computer Science (LICS 2003)*, pp. 321–330 (2003)
4. Bulatov, A., Dalmau, V.: A simple algorithm for mal'tsev constraints. *SIAM Journal of Computing* 36(1), 16–27 (2006)
5. Bulatov, A., Jeavons, P., Krokhin, A.: Classifying the complexity of constraints using finite algebras. *SIAM J. Computing* 34(3), 720–742 (2005)

6. Bulatov, A.A.: A dichotomy theorem for constraint satisfaction problems on a 3-element set. *Journal of the ACM (J. ACM)* 53 (2006)
7. Büning, H.K., Karpinski, M., Flögel, A.: Resolution for quantified boolean formulas. *Information and Computation* 117(1), 12–18 (1995)
8. Chen, H.: The computational complexity of quantified constraint satisfaction. Ph.D. thesis, Cornell University (August 2004)
9. Chen, H.: Quantified constraint satisfaction and bounded treewidth. In: ECAI (2004)
10. Chen, H.: The expressive rate of constraints. *Annals of Mathematics and Artificial Intelligence* 44(4), 341–352 (2005)
11. Chen, H.: A rendezvous of logic, complexity, and algebra. *SIGACT News Logic Column* (December 2006)
12. Chen, H.: The complexity of quantified constraint satisfaction: Collapsibility, sink algebras, and the three-element case. *SIAM Journal on Computing* 37(5), 1674–1701 (2008)
13. Chen, H., Dalmau, V.: From pebble games to tractability: An ambidextrous consistency algorithm for quantified constraint satisfaction. In: Ong, L. (ed.) *CSL 2005. LNCS*, vol. 3634, Springer, Heidelberg (2005)
14. Creignou, N., Khanna, S., Sudan, M.: *Complexity Classification of Boolean Constraint Satisfaction Problems*. *SIAM Monographs on Discrete Mathematics and Applications*. Society for Industrial and Applied Mathematics (2001)
15. Dalmau, V.: Computational complexity of problems over generalized formulas. Ph.D. Thesis, UPC
16. Dalmau, V.: Generalized majority-minority operations are tractable. In: LICS (2005)
17. Ebbinghaus, H.D., Flum, J., Thomas, W.: *Mathematical Logic*. Springer, Heidelberg (1984)
18. Gottlob, G., Greco, G., Scarcello, F.: The complexity of quantified constraint satisfaction problems under structural restrictions. In: IJCAI (2005)
19. Grädel, E.: Capturing complexity classes by fragments of second order logic. *Theoretical Computer Science* 101, 35–57 (1992)
20. Idziak, P., Markovic, P., McKenzie, R., Valeriote, M., Willard, R.: Tractability and learnability arising from algebras with few subpowers (extended abstract). In: LICS (2007)
21. Karpinski, M., Büning, H.K., Schmitt, P.H.: On the computational complexity of quantified horn clauses. In: *CSL 1987*, pp. 129–137 (1987)
22. Kiss, E., Valeriote, M.: On tractability and congruence distributivity. In: LICS (2006)
23. Pan, G., Vardi, M.Y.: Fixed-parameter hierarchies inside pspace. In: LICS (2006)
24. Schaefer, T.J.: The complexity of satisfiability problems. In: *Proceedings of the ACM Symposium on Theory of Computing (STOC)*, pp. 216–226 (1978)