Generating sets for powers of finite algebras and the complexity of quantified constraints

Barnaby Martin

Algorithms and Complexity Group, Durham University, UK
Acidissima gens, optima consulens, pessima faciens

York, 3rd May 2017

Let us study the growth rate of generating sets for direct powers of an algebra $\mathbb{A}$.

For $\mathbb{A}$ we have a function $f_{\mathbb{A}} : \mathbb{N} \to \mathbb{N}$, giving the cardinality of the minimal generating sets of the sequence

- $\mathbb{A}, \mathbb{A}^2, \mathbb{A}^3, \ldots$ as
- $f(1), f(2), f(3), \ldots$.

We say $\mathbb{A}$ has the g-GP if $f(m) \leq g(m)$ for all m.

(PGP) polynomial, when $f_{\mathbb{A}} = O(i^c)$, for some c; and

(EGP) exponential, when exists b so that $f_{\mathbb{A}} = \Omega(b^i)$.

History

Theorem (Wiegold 1987)

Let $\mathbb{B}$ be a finite semigroup. If $\mathbb{B}$ is a monoid then $\mathbb{B}$ has the (linear) PGP. Otherwise, $\mathbb{B}$ has the EGP.

Proof of PGP.

If $\mathbb{B}$ is a monoid with identity 1 and $|B| = n$, then

$$\begin{gathered}(B, 1, \ldots, 1, 1)\\(1, B, \ldots, 1, 1)\\\vdots\\(1, 1, \ldots, B, 1)\\(1, 1, \ldots, 1, B)\end{gathered}$$

is a generating set for $\mathbb{B}^m$ of size mn.

Theorem (Wiegold 1987)

Let $\mathbb{B}$ be a finite semigroup. If $\mathbb{B}$ is a monoid then $\mathbb{B}$ has the (linear) PGP. Otherwise, $\mathbb{B}$ has the EGP.

Proof of EGP.

Otherwise, without an identity, $\mathbb{B}$ and $\mathbb{B}^m$ have the properties that

$$|x \cdot B| \leq n-1, \text{ for each } x \in B.$$
$$|z \cdot B^m| \leq (n-1)^m, \text{ for each } z \in B^m.$$

Thus, a subset of B^m of size r can generate no more $r + r(n-1)^m$ elements in $\mathbb{B}^m$. Thus, a generating set must be of size $\geq \left(\frac{2n}{2n-1}\right)^m$.

Constraint Satisfaction Problems

The *constraint satisfaction problem* (CSP) is a popular formalism in Artificial Intelligence in which one is given

- a triple $(V, D, \mathcal{C})$ of variables, domain, constraints

and in which one asks for an assignment of the variables to the domain that satisfies the constraints.

A popular parameterisation involves fixing D and restricting

- the constraint language $\mathcal{C}$.

This can be formulated combinatorially as CSP($\mathcal{C}$) with

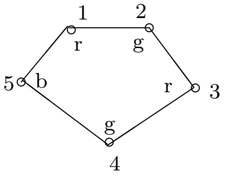
- Input: a structure $\mathcal{A}$.
- Question: does $\mathcal{A}$ have a homomorphism to $\mathcal{C}$?

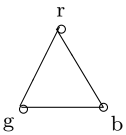
or logically as CSP($\mathcal{C}$) with

- Input: a sentence ϕ of $\{\exists, \wedge, =\}$-FO.
- Question: does $\mathcal{C} \models \phi$?

Example

$\mathrm{CSP}(\mathcal{K}_3)$, or $\mathrm{CSP}(\{r, g, b\}; \neq)$, is *Graph 3-colourability*.





Combinatorially, one looks for a homomorphism from $\mathcal{C}_5$ to $\mathcal{K}_3$.
Logically, one asks if $\mathcal{K}_3 \models \Phi$.

$$\begin{aligned}\Phi := \exists v_1, v_2, v_3, v_4, v_5 \quad & E(v_1, v_2) \wedge E(v_2, v_1) \wedge E(v_2, v_3) \wedge E(v_3, v_2) \\ & E(v_3, v_4) \wedge E(v_4, v_3) \wedge E(v_4, v_5) \\ & E(v_5, v_4) \wedge E(v_5, v_1) \wedge E(v_!, v_5).\end{aligned}$$

Quantified Constraint Satisfaction

The *quantified constraint satisfaction problem* QCSP($\mathcal{B}$) has

- Input: a sentence ϕ of $\{\forall, \exists, \wedge, =\}$-FO.
- Question: does $\mathcal{B} \models \phi$?

It is the CSP with $\forall$ returned.

"The QCSP might be thought of as the dissolute younger brother of its better-studied restriction, the CSP. . . . CSPs are ubiquitous in CS . . . , while QCSPs can not nearly claim to be so important in applications."

useful QCSPs	classified?
relativised ($\forall x \in X, \exists y \in Y$)	$\surd$
Boolean (QBF or QSAT)	$\surd$

". . . what is left of the true non-Boolean QCSP is a problem I believe to be mostly of interest to theorists."

First-order structures

Relational structures:

$$\mathcal{B} := (B; R_1, R_2, \ldots)$$

Functional structures:

$$\mathbb{B} := (D; f_1, f_2, \ldots)$$

$$\text{functional structures} \quad = \quad \text{algebras.}$$

What is the interplay between relational and functional structures?

$$\text{Model Theory} \quad = \quad \text{Logic} \quad + \quad \text{Universal Algebra}$$

All our structures are finite-domain.

Interplay

Let R be an m-ary relation on $\mathcal{B}$. We say that a k-ary operation $f : B^k \to B$ *preserves* R (or R is *invariant*) under f if:

$$
\begin{array}{llll}
f, & f, & \ldots, & f \\
(x_{11}, & x_{12}, & \ldots, & x_{1m}) \in R \\
(x_{21}, & x_{22}, & \ldots, & x_{2m}) \in R \\
\vdots & \vdots & & \vdots \\
(x_{k1}, & x_{k2}, & \ldots, & x_{km}) \in R \\
\hline
(y_1, & y_2, & \ldots, & y_m) \in R
\end{array}
$$

where each $y_i = f(x_{1i}, x_{2i}, \ldots, x_{ki})$.

- operations that preserve each of the relations of $\mathcal{B}$ are $\mathrm{Pol}(\mathcal{B})$
- relations invariant under each operation of $\mathbb{B}$ are $\mathrm{Inv}(\mathbb{B})$.

one-side of a Galois Correspondence

Let $\mathcal{B}$ and $\mathbb{B}$ be over the same finite domain B.

$$\mathrm{Inv}(\mathrm{Pol}(\mathcal{B})) = \langle \mathcal{B} \rangle_{\{\exists,\wedge,=\}}$$
$$\mathrm{Inv}(\mathrm{surPol}(\mathcal{B})) = \langle \mathcal{B} \rangle_{\{\forall,\exists,\wedge,=\}}$$

Idempotent operations are surjective! The algebraic definition for QCSP($\mathbb{B}$) has

- Input: a sentence ϕ of $\{\forall, \exists, \wedge\}$-FO with some relations $\mathcal{B} \in \mathrm{Inv}(\mathbb{B})$.
- Question: does $\mathcal{B} \models \phi$?

What if $\mathrm{Inv}(\mathbb{B})$ is infinite?

Infinite languages on a finite domain

Each relation R can be given as a list of tuples, but this is far too lengthy! How about a Boolean formula ϕ in atoms

- $v = v'$ and $v = c$,

where c is a domain element. The problem is that recognising, e.g., non-emptiness of the relation can be NP-hard! Following others, e.g. [Bodirsky & Dalmau 2006] we will ask for

- ϕ in DNF,

However, our main result will be a separation NP versus co-NP-hard, so this is not a big deal!

Infinite languages on a finite domain

Example 1.

$$\begin{array}{llll} \{ & (1,2), & (2,1), & \qquad (x \neq y \vee x = 1) \\ & (2,3), & (3,2), & \\ & (1,3), & (3,1), & \\ & (1,1) & \qquad \} & \end{array}$$

Example 2.

$$\begin{array}{lllll} \{ & (1,0,0), & (0,1,0), & (0,0,1), & \qquad (x \neq y \vee y \neq z) \\ & (1,1,0), & (1,0,1), & (1,1,0), & \} \end{array}$$

Back to PGP

Call an algebra $\mathbb{B}$ *k*-PGP-switchable if $\mathbb{B}^m$ is generated from the set of m-tuples of the form

- $(x_1, \ldots, x_1, x_2, \ldots x_2, \ldots, \ldots, x_{k'}, \ldots, x_{k'})$ for some $k' \leq k$.

switchability were originally introduced in connection with the QCSP by Hubie Chen!

Theorem (Chen 2008)

If $\mathbb{A}$ is switchable then QCSP($\mathbb{A}$) is in NP.

Theorem (LICS 2015)

$\mathbb{A}$ is PGP-switchable iff it is switchable.

A number of algebraists worked on the PGP-EGP dichotomy conjecture.

Conjecture

Let $\mathbb{B}$ be a finite idempotent algebra, then either $\mathbb{B}$ has PGP or it has EGP.

In 2015, Dmitriy Zhuk solved it.

Theorem (Zhuk 2015)

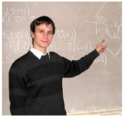
Let $\mathbb{B}$ be a finite algebra, then either $\mathbb{B}$ is PGP-switchable or it has EGP.

In order to prove this result, Zhuk assumes $\mathbb{B}$ is not PGP-switchable and finds the existence of a certain class of relations in $\mathrm{Inv}(\mathbb{B})$.

Church of Switchability

B. M.

switchability

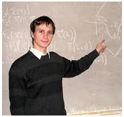


- H. Chen: *Quantified constraint satisfaction and the polynomially generated powers property*. ICALP 2008.
- D. Zhuk: *The Size of Generating Sets of Powers*. Arxiv 2015.

Church of Switchability

B. M.

switchability

- H. Chen: *Quantified constraint satisfaction and the polynomially generated powers property*. ICALP 2008.
- D. Zhuk: *The Size of Generating Sets of Powers*. Arxiv 2015.
- C. Carvalho, F. Madelaine, B. M.: *From Complexity to Algebra and Back: Digraph Classes, Collapsibility, and the PGP*. LICS 2015.

Notes & Queries

Henceforth, let $\mathbb{A}$ be an idempotent algebra on a finite domain A.

Conjecture (Chen Conjecture 2012)

Let $\mathcal{B}$ be a finite relational structure expanded with all constants. If Pol($\mathcal{B}$) has PGP, then QCSP($\mathcal{B}$) is in NP; otherwise QCSP($\mathcal{B}$) is Pspace-complete.

Theorem (Revised Chen Conjecture)

If $\mathrm{Inv}(\mathbb{A})$ satisfies PGP, then QCSP($\mathrm{Inv}(\mathbb{A})$) is in NP. Otherwise, if $\mathrm{Inv}(\mathbb{A})$ satisfies EGP, then QCSP($\mathrm{Inv}(\mathbb{A})$) is co-NP-hard.

Conjecture (Alternative Chen Conjecture)

If $\mathrm{Inv}(\mathbb{A})$ satisfies PGP, then for every finite reduct $\mathcal{B} \subseteq \mathrm{Inv}(\mathbb{A})$, QCSP($\mathcal{B}$) is in NP. Otherwise, there exists a finite reduct $\mathcal{B} \subseteq \mathrm{Inv}(\mathbb{A})$ so that QCSP($\mathcal{B}$) is co-NP-hard.

Notes & Queries

Henceforth, let $\mathbb{A}$ be an idempotent algebra on a finite domain A.

Conjecture (Chen Conjecture 2012)

Let $\mathcal{B}$ be a finite relational structure expanded with all constants. If Pol($\mathcal{B}$) has PGP, then QCSP($\mathcal{B}$) is in NP; otherwise QCSP($\mathcal{B}$) is Pspace-complete.

Theorem (Revised Chen Conjecture)

Either QCSP($\mathrm{Inv}(\mathbb{A})$) is co-NP-hard or QCSP($\mathrm{Inv}(\mathbb{A})$) has the same complexity as CSP($\mathrm{Inv}(\mathbb{A})$).

Conjecture (Alternative Chen Conjecture False)

If $\mathrm{Inv}(\mathbb{A})$ satisfies PGP, then for every finite reduct $\mathcal{B} \subseteq \mathrm{Inv}(\mathbb{A})$, QCSP($\mathcal{B}$) is in NP. Otherwise, there exists a finite reduct $\mathcal{B} \subseteq \mathrm{Inv}(\mathbb{A})$ so that QCSP($\mathcal{B}$) is co-NP-hard.

Tractability

We know from Zhuk 2015 that

$$\mathrm{PGP} \longrightarrow \text{PGP-switchability}$$

and from [LICS 2015]

$$\text{PGP-switchability} \longrightarrow \text{switchability}$$

whereupon Chen 2008 gives

$$\text{switchability} \longrightarrow \text{QCSP tractability.}$$

Henceforth, α, β be strict subsets of A so that $\alpha \cup \beta = A$.

Theorem (Zhuk 2015)

Algebra $\mathbb{A}$ (idempotent) has EGP iff exists such α, β with

$$\sigma_k(x_1, y_1, \ldots, x_k, y_k) := \rho(x_1, y_1) \vee \ldots \vee \rho(x_k, y_k),$$

where $\rho(x, y) = (\alpha \times \alpha) \cup (\beta \times \beta)$, is in $\mathrm{Inv}(\mathbb{A})$, for each $k \in \mathbb{N}$.

We prefer the relation $\tau_k(x_1, y_1, z_1 \ldots, x_k, y_k, z_k)$ defined by

$$\tau_k(x_1, y_1, z_1 \ldots, x_k, y_k, z_k) := \rho'(x_1, y_1, z_1) \vee \ldots \vee \rho'(x_k, y_k, z_k),$$

where $\rho'(x, y, z) = (\alpha \times \alpha \times \alpha) \cup (\beta \times \beta \times \beta)$.

Corollary

Algebra $\mathbb{A}$ (idempotent) has EGP iff exists such α, β with $\tau_k(x_1, y_1, z_1 \ldots, x_k, y_k, z_k)$ in $\mathrm{Inv}(\mathbb{A})$, for each $k \in \mathbb{N}$.

co-NP-hardness

Theorem

If $\mathrm{Inv}(\mathbb{A})$ *satisfies EGP, then QCSP*$(\mathrm{Inv}(\mathbb{A}))$ *is co-NP-hard.*

Proof.

Reduce from the complement of (monotone) 3-*not-all-equal-sat*.

$$\exists x_1^1, x_1^2, x_1^3, \ldots, \ldots, x_m^1, x_m^2, x_m^3 \ \mathrm{NAE}(x_1^1, x_1^2, x_1^3) \wedge \ldots \wedge \mathrm{NAE}(x_m^1, x_m^2, x_m^3)$$

becomes

$$\forall x_1^1, x_1^2, x_1^3, \ldots, \ldots, x_m^1, x_m^2, x_m^3 \ \rho'(x_1^1, x_1^2, x_1^3) \vee \ldots \vee \rho'(x_m^1, x_m^2, x_m^3)$$

where we note that $\tau_m(x_1, y_1, z_1 \ldots, x_m, y_m, z_m) :=$

$$\rho'(x_1, y_1, z_1) \vee \ldots \vee \rho'(x_m, y_m, z_m)$$

has a DNF representation that is polynomially-sized in m.

Recall, α, β be strict subsets of A so that $\alpha \cup \beta = A$. Now ask further that $\alpha \cap \beta \neq \emptyset$.

Corollary

$QCSP(A; \{\tau_n : n \in \mathbb{N}\}, \{a : a \in A\})$ is co-NP-hard.

In fact,

Proposition

$QCSP(A; \{\tau_n : n \in \mathbb{N}\}, \{a : a \in A\})$ is in co-NP.

Proof.

Roughly speaking, evaluate all existential variables to something in $\alpha \cap \beta$. $\square$

Proposition

For every finite reduct $\mathcal{B}$ of $(A; \{\tau_n : n \in \mathbb{N}\}, \{a : a \in A\})$, $QCSP(\mathcal{B})$ is in NL.

Conjecture

Let $\mathbb{A}$ *be an algebra. Either*

- *QCSP*$(\mathrm{Inv}(\mathbb{A}))$ *is in NP, or*
- *QCSP*$(\mathrm{Inv}(\mathbb{A}))$ *is co-NP-complete, or*
- *QCSP*$(\mathrm{Inv}(\mathbb{A}))$ *is Pspace-complete.*

Or even

Conjecture

Let $\mathbb{A}$ *be an algebra on a 3-element domain. Either*

- *QCSP*$(\mathrm{Inv}(\mathbb{A}))$ *is in NP, or*
- *QCSP*$(\mathrm{Inv}(\mathbb{A}))$ *is co-NP-complete, or*
- *QCSP*$(\mathrm{Inv}(\mathbb{A}))$ *is Pspace-complete.*

3-element vignette

The closest we can do is

Theorem

Let $\mathbb{A}$ be an algebra on a 3-element domain. Either

- Π_k*-CSP*$(\mathrm{Inv}(\mathbb{A}))$ *is in NP, for all* k*; or*
- Π_k*-CSP*$(\mathrm{Inv}(\mathbb{A}))$ *is co-NP-complete, for all* k*; or*
- Π_k*-CSP*$(\mathrm{Inv}(\mathbb{A}))$ *is* Π_2^{P}*-hard, for some* k*.*