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 $A$.

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

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

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

- *(PGP)* polynomial, when $f_A = O(i^c)$, for some $c$; and
- *(EGP)* exponential, when exists $b$ so that $f_A = \Omega(b^i)$.
History

Theorem (Wiegold 1987)

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

Proof of PGP.
If $B$ is a monoid with identity $1$ and $|B| = n$, then

$$(B, 1, \ldots, 1, 1)$$
$$(1, B, \ldots, 1, 1)$$
$$\vdots$$
$$(1, 1, \ldots, B, 1)$$
$$(1, 1, \ldots, 1, B)$$

is a generating set for $B^m$ of size $mn$. 
Theorem (Wiegold 1987)

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

Proof of EGP.

Otherwise, without an identity, \( B \) and \( B^m \) 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 \( B^m \). 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 \((V, D, C)\) 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 \(C\).

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

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

or logically as \(\text{CSP}(C)\) with

- Input: a sentence \(\phi\) of \(\{\exists, \land, =\}\)-FO.
- Question: does \(C \models \phi\)?
Example

CSP(\(K_3\)), or CSP(\(\{r, g, b\}; \neq\)), is \textit{Graph 3-colourability}.

Combinatorially, one looks for a \textit{homomorphism} from \(C_5\) to \(K_3\). Logically, one asks if \(K_3 \models \Phi\).

\[
\Phi := \exists v_1, v_2, v_3, v_4, v_5 \quad E(v_1, v_2) \land E(v_2, v_1) \land E(v_2, v_3) \land E(v_3, v_2) \\
E(v_3, v_4) \land E(v_4, v_3) \land E(v_4, v_5) \\
E(v_5, v_4) \land E(v_5, v_1) \land E(v_1, v_5).
\]
The **quantified constraint satisfaction problem** QCSP(\(\mathcal{B}\)) has

- **Input**: a sentence \(\phi\) of \(\{\forall, \exists, \land, =\}\)-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.”

<table>
<thead>
<tr>
<th>useful QCSPs</th>
<th>classified?</th>
</tr>
</thead>
<tbody>
<tr>
<td>relativised ((\forall x \in X, \exists y \in Y))</td>
<td>√</td>
</tr>
<tr>
<td>Boolean (QBF or QSAT)</td>
<td>√</td>
</tr>
</tbody>
</table>

“. . . 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:

\[ \mathcal{B} := (D; f_1, f_2, \ldots) \]

functional structures = algebras.

What is the interplay between relational and functional structures?

Model Theory = Logic + Universal Algebra

All our structures are finite-domain.
Let $R$ be an $m$-ary relation on $\mathcal{B}$. We say that a $k$-ary operation $f : B^k \rightarrow B$ preserves $R$ (or $R$ is invariant) under $f$ if:

\[
\begin{align*}
    f, & \quad f, \quad \ldots, \quad f \\
    (x_{11}, & \quad x_{12}, \quad \ldots, \quad x_{1m}) \in R \\
    (x_{21}, & \quad x_{22}, \quad \ldots, \quad x_{2m}) \in R \\
    \vdots & \quad \vdots \\
    (x_{k1}, & \quad x_{k2}, \quad \ldots, \quad x_{km}) \in R \\
    (y_1, & \quad y_2, \quad \ldots, \quad y_m) \in R
\end{align*}
\]

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

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

DANGER Acid
one-side of a Galois Correspondence

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

\[
\text{Inv}(\text{Pol}(\mathcal{B})) = \langle \mathcal{B} \rangle_{\exists, \wedge, =} \\
\text{Inv}(\text{surPol}(\mathcal{B})) = \langle \mathcal{B} \rangle_{\forall, \exists, \wedge, =}
\]

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

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

What if $\text{Inv}(\mathcal{B})$ 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 $\phi$ 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

- $\phi$ in DNF,

However, our main result will be a separation $\text{NP}$ versus $\text{co-NP}$-hard, so this is not a big deal!
Infinite languages on a finite domain

Example 1.

\{ (1, 2), (2, 1), (2, 3), (3, 2), (1, 3), (3, 1), (1, 1) \}

Example 2.

\{ (1, 0, 0), (0, 1, 0), (0, 0, 1), (1, 1, 0), (1, 0, 1), (1, 1, 0) \}
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 $B$ be a finite idempotent algebra, then either $B$ has PGP or it has EGP.

In 2015, Dmitriy Zhuk solved it.

**Theorem (Zhuk 2015)**

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

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

B. M.

\[ \text{switchability} \]

Church of Switchability

B. M.

switchability


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

**Conjecture (Chen Conjecture 2012)**

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

**Theorem (Revised Chen Conjecture)**

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

**Conjecture (Alternative Chen Conjecture)**

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

Henceforth, let $A$ be an idempotent algebra on a finite domain $A$.

**Conjecture (Chen Conjecture 2012)**

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

**Theorem (Revised Chen Conjecture)**

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

**Conjecture (Alternative Chen Conjecture False)**

If $\text{Inv}(A)$ satisfies PGP, then for every finite reduct $B \subseteq \text{Inv}(A)$, $QCSP(B)$ is in NP. Otherwise, there exists a finite reduct $B \subseteq \text{Inv}(A)$ so that $QCSP(B)$ is co-NP-hard.
We know from Zhuk 2015 that

\[ \text{PGP} \quad \rightarrow \quad \text{PGP-switchability} \]

and from [LICS 2015]

\[ \text{PGP-switchability} \quad \rightarrow \quad \text{switchability} \]

whereupon Chen 2008 gives

\[ \text{switchability} \quad \rightarrow \quad \text{QCSP tractability}. \]
Henceforth, $\alpha, \beta$ be strict subsets of $A$ so that $\alpha \cup \beta = A$.

**Theorem (Zhuk 2015)**

*Algebra $\mathbb{A}$ (idempotent) has EGP iff exists such $\alpha, \beta$ with*

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

*where $\rho(x, y) = (\alpha \times \alpha) \cup (\beta \times \beta)$, is in $\text{Inv}(\mathbb{A})$, 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*

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

*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 $\alpha, \beta$ with $\tau_k(x_1, y_1, z_1 \ldots, x_k, y_k, z_k)$ in $\text{Inv}(\mathbb{A})$, for each $k \in \mathbb{N}$.*
co-NP-hardness

**Theorem**

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

**Proof.**

Reduce from the complement of (monotone) 3-$\text{not-all-equal-sat}$.

$$\exists x_1^1, x_1^2, x_1^3, \ldots, \ldots, x_m^1, x_m^2, x_m^3 \; \text{NAE}(x_1^1, x_1^2, x_1^3) \land \ldots \land \text{NAE}(x_m^1, x_m^2, x_m^3)$$

becomes

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

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

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

has a DNF representation that is polynomially-sized in $m$. 
Recall, \( \alpha, \beta \) 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 \( \alpha \cap \beta \).

**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 $A$ be an algebra. Either

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

Or even

Conjecture

Let $A$ be an algebra on a 3-element domain. Either

- $QCSP(\text{Inv}(A))$ is in NP, or
- $QCSP(\text{Inv}(A))$ is co-NP-complete, or
- $QCSP(\text{Inv}(A))$ 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*

- \( \Pi_k\)-CSP\( (\text{Inv}(\mathbb{A})) \) *is in NP, for all \( k \); or*
- \( \Pi_k\)-CSP\( (\text{Inv}(\mathbb{A})) \) *is co-NP-complete, for all \( k \); or*
- \( \Pi_k\)-CSP\( (\text{Inv}(\mathbb{A})) \) *is \( \Pi^P_2 \)-hard, for some \( k \).*