The size of generating sets of powers

Dmitriy Zhuk
zhuk.dmitriy@gmail.com

Department of Mathematics and Mechanics
Moscow State University

Arbeitstagung Allgemeine Algebra
90th Workshop on General Algebra
Novi Sad, Serbia, June 5-7, 2015

Let $\mathbb{A} = (A; F)$ be a finite algebra.
What can be the size of a generating set for $\mathbb{A}^n$?

Let $\mathbb{A} = (A; F)$ be a finite algebra.
What can be the size of a generating set for $\mathbb{A}^n$?
For $X \subseteq A$ by $\langle X \rangle$ we denote the subalgebra generated by X.

Example 1: $\mathbb{A} = (\{0, 1\}; \vee)$

$$\left\langle \begin{matrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \end{matrix} \right\rangle = \mathbb{A}^n$$

We need only $n+1$ tuples to generate $\mathbb{A}^n$.

Let $\mathbb{A} = (A; F)$ be a finite algebra.
What can be the size of a generating set for $\mathbb{A}^n$?
For $X \subseteq A$ by $\langle X \rangle$ we denote the algebra, generated by X.

Example 2: $\mathbb{A} = (\{0, 1\}; x + 1)$

We need at least 2^{n-1} tuples to generate $\mathbb{A}^n$.

Let $\mathbb{A} = (A; F)$ be a finite algebra.
What can be the size of a generating set for $\mathbb{A}^n$?
For $X \subseteq A$ by $\langle X \rangle$ we denote the algebra, generated by X.

Example 2: $\mathbb{A} = (\{0, 1\}; x + 1)$

We need at least 2^{n-1} tuples to generate $\mathbb{A}^n$.

Example 3: $\mathbb{A} = (\{0, 1, 2\}; s)$, where $s(x, y) = \begin{cases} 0, & \text{if } x \neq y \\ x, & \text{if } x = y \end{cases}$

We need at least 2^n tuples to generate $\mathbb{A}^n$.

An algebra $\mathbb{A}$ has the polynomially generated powers (PGP) property if its n-th power $\mathbb{A}^n$ has a polynomial-size generating set.
That is, there exists a polynomial p such that for every n the n-th power $\mathbb{A}^n$ can be generated by at most $p(n)$ tuples.

An algebra $\mathbb{A}$ has the exponentially generated powers (EGP) property if its n-th power $\mathbb{A}^n$ has a exponential-size generating set.
That is, there exists $b > 1$ and $C > 0$ such that for every n the n-th power $\mathbb{A}^n$ cannot be generated by less than Cb^n tuples.

An algebra $\mathbb{A}$ has the polynomially generated powers (PGP) property if its n-th power $\mathbb{A}^n$ has a polynomial-size generating set.
That is, there exists a polynomial p such that for every n the n-th power $\mathbb{A}^n$ can be generated by at most $p(n)$ tuples.

An algebra $\mathbb{A}$ has the exponentially generated powers (EGP) property if its n-th power $\mathbb{A}^n$ has a exponential-size generating set.
That is, there exists $b > 1$ and $C > 0$ such that for every n the n-th power $\mathbb{A}^n$ cannot be generated by less than Cb^n tuples.

Problems

- Is there anything between PGP property and EGP property?
- When does an algebra have PGP property?
- How to find a polynomial-size generating set?

- Connection with the Quantified Constraint Satisfaction Problem (see the previous talk).

- Connection with the Quantified Constraint Satisfaction Problem (see the previous talk).
- Just a very nice problem!

For a tuple $(a_1, \ldots, a_n)$ we say that $i \in \{1, 2, \ldots, n\}$ is a switch if $a_i \neq a_{i+1}$.

$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 2)$ has 2 switches.
$(2, 2, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$ has 3 switches.

For a tuple $(a_1, \ldots, a_n)$ we say that $i \in \{1, 2, \ldots, n\}$ is a switch if $a_i \neq a_{i+1}$.

$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 2)$ has 2 switches.
$(2, 2, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$ has 3 switches.

An algebra is called *k-switchable* if $\mathbb{A}^n$ is generated by all n-tuples with at most k switches.
An algebra is called *switchable* if it is k-switchable for some k.

Lemma (Switchability $\Rightarrow$ PGP property)

Suppose a finite algebra $\mathbb{A}$ is switchable, then it has PGP property.

Suppose $\alpha, \beta \subsetneq A$, $\alpha \cup \beta = A$.
An operation is called $\alpha\beta$-projective if there exists $j \in \{1, 2, \dots, n\}$ such that for every $(a_1, \dots, a_n) \in A^n$ and $S \in \{\alpha, \beta\}$ we have $f(a_1, \dots, a_{j-1}, S, a_{j+1}, \dots, a_n) \subseteq S$.

Suppose $\alpha, \beta \subsetneq A$, $\alpha \cup \beta = A$.
An operation is called $\alpha\beta$-projective if there exists $j \in \{1, 2, \ldots, n\}$ such that for every $(a_1, \ldots, a_n) \in A^n$ and $S \in \{\alpha, \beta\}$ we have
$f(a_1, \ldots, a_{j-1}, S, a_{j+1}, \ldots, a_n) \subseteq S$.
An algebra $\mathbb{A}$ is called $\alpha\beta$-projective if every operation in $\mathbb{A}$ is $\alpha\beta$-projective.

Suppose $\alpha, \beta \subsetneq A$, $\alpha \cup \beta = A$.
An operation is called $\alpha\beta$-projective if there exists $j \in \{1, 2, \ldots, n\}$ such that for every $(a_1, \ldots, a_n) \in A^n$ and $S \in \{\alpha, \beta\}$ we have $f(a_1, \ldots, a_{j-1}, S, a_{j+1}, \ldots, a_n) \subseteq S$.
An algebra $\mathbb{A}$ is called $\alpha\beta$-projective if every operation in $\mathbb{A}$ is $\alpha\beta$-projective.

Lemma(Hubie Chen)

Suppose a finite algebra $\mathbb{A}$ is $\alpha\beta$-projective for some α and β. Then $\mathbb{A}$ has EGP property.

Suppose $\alpha, \beta \subsetneq A$, $\alpha \cup \beta = A$.
An operation is called $\alpha\beta$-projective if there exists $j \in \{1, 2, \dots, n\}$ such that for every $(a_1, \dots, a_n) \in A^n$ and $S \in \{\alpha, \beta\}$ we have $f(a_1, \dots, a_{j-1}, S, a_{j+1}, \dots, a_n) \subseteq S$.
An algebra $\mathbb{A}$ is called $\alpha\beta$-projective if every operation in $\mathbb{A}$ is $\alpha\beta$-projective.

Lemma(Hubie Chen)

Suppose a finite algebra $\mathbb{A}$ is $\alpha\beta$-projective for some α and β. Then $\mathbb{A}$ has EGP property.

Example

The operation $s(x, y) = \begin{cases} 0, & \text{if } x \neq y \\ x, & \text{if } x = y \end{cases}$ is {0,1}{0,2}-projective.

Theorem (Hubie Chen)

Suppose $\mathbb{A}$ is an idempotent finite algebra not having a G-set on 3 elements. Then either $\mathbb{A}$ is switchable, or $\mathbb{A}$ is $\alpha\beta$-projective.

Corollary

Suppose $\mathbb{A}$ is an idempotent finite algebra not having a G-set on 3 elements. Then either it has PGP property, or it has EGP property.

Theorem : Non Switchable $\Rightarrow$ EGP property

Suppose a finite algebra $\mathbb{A}$ is not switchable, then it has EGP property.

Main Result

Theorem : Non Switchable $\Rightarrow$ EGP property

Suppose a finite algebra $\mathbb{A}$ is not switchable, then it has EGP property.

Corollary

Suppose $\mathbb{A}$ is a finite algebra. Then either it has PGP property, or it has EGP property.

Theorem : Non Switchable $\Rightarrow$ EGP property

Suppose a finite algebra $\mathbb{A}$ is not switchable, then it has EGP property.

Corollary

Suppose $\mathbb{A}$ is a finite algebra. Then either it has PGP property, or it has EGP property.

Theorem

Suppose $\mathbb{A}$ is a finite idempotent algebra. Then either $\mathbb{A}$ is switchable, or $\mathbb{A}$ is $\alpha\beta$-projective.

Proof

Theorem : Not Switchable ⇒ EGP property

Suppose a finite algebra $\mathbb{A}$ is not switchable, then it has EGP property.

Theorem : Not Switchable $\Rightarrow$ EGP property

Suppose a finite algebra $\mathbb{A}$ is not switchable, then it has EGP property.

Not Switchable $\Rightarrow$ Not k-switchable for every k

Theorem : Not Switchable $\Rightarrow$ EGP property

Suppose a finite algebra $\mathbb{A}$ is not switchable, then it has EGP property.

Not Switchable $\Rightarrow$ Not k-switchable for every k
There exists $n > k$ such that $\mathbb{A}^n$ is not generated by all n-tuples with at most k switches.
By σ we denote the relation generated by all such tuples.

Theorem : Not Switchable $\Rightarrow$ EGP property

Suppose a finite algebra $\mathbb{A}$ is not switchable, then it has EGP property.

Not Switchable $\Rightarrow$ Not k-switchable for every k
There exists $n > k$ such that $\mathbb{A}^n$ is not generated by all n-tuples with at most k switches.
By σ we denote the relation generated by all such tuples.
Let α be a tuple from $A^n \setminus \sigma$ with the minimal number of switches.

$$\alpha = (\underbrace{a_1, \dots, a_1}_{n_1}, \underbrace{a_2, \dots, a_2}_{n_2}, \dots, \underbrace{a_m, \dots, a_m}_{n_m}).$$

Theorem : Not Switchable $\Rightarrow$ EGP property

Suppose a finite algebra $\mathbb{A}$ is not switchable, then it has EGP property.

Not Switchable $\Rightarrow$ Not k-switchable for every k
There exists $n > k$ such that $\mathbb{A}^n$ is not generated by all n-tuples with at most k switches.
By σ we denote the relation generated by all such tuples.
Let α be a tuple from $A^n \setminus \sigma$ with the minimal number of switches.

$$\alpha = (\underbrace{a_1, \ldots, a_1}_{n_1}, \underbrace{a_2, \ldots, a_2}_{n_2}, \ldots, \underbrace{a_m, \ldots, a_m}_{n_m}).$$

Put $\rho(x_1, \ldots, x_m) = \sigma(\underbrace{x_1, \ldots, x_1}_{n_1}, \underbrace{x_2, \ldots, x_2}_{n_2}, \ldots, \underbrace{x_m, \ldots, x_m}_{n_m}).$

- ρ is an invariant of $\mathbb{A}$, $\rho \neq A^m$.
- $(\exists i\colon c_i = c_{i+1}) \Rightarrow (c_1, \ldots, c_m) \in \rho$.

Proof

(ALMOST TRUE) for every n we can get a relation ρ of arity $2n^2$ such

- ρ is an invariant of $\mathbb{A}$, $(a, b, a, b, a, b, a, b, \ldots, a, b) \notin \rho$.
- $\exists i\colon c_i = d_i \Rightarrow (c_1, d_1, c_2, d_2, \ldots, c_{n^2}, d_{n^2}) \in \rho$.

(ALMOST TRUE) for every n we can get a relation ρ of arity $2n^2$ such

- ρ is an invariant of $\mathbb{A}$, $(a, b, a, b, a, b, a, b, \ldots, a, b) \notin \rho$.
- $\exists i \colon c_i = d_i \Rightarrow (c_1, d_1, c_2, d_2, \ldots, c_{n^2}, d_{n^2}) \in \rho$.

Put $\delta(x_1, \ldots, x_n, y_1, \ldots, y_n) =$
$\rho(x_1, y_1, x_1, y_2, x_1, y_3, \ldots, x_1, y_n, x_2, y_1, \ldots, x_n, y_n)$.

- δ is an invariant of $\mathbb{A}$, $(\underbrace{a, a, \ldots, a}_{n}, \underbrace{b, b, \ldots, b}_{n}) \notin \delta$.
- $\exists i, j \colon c_i = d_j \Rightarrow (c_1, \ldots, c_n, d_1, \ldots, d_n) \in \delta$.

Proof

(ALMOST TRUE) for every n we can get a relation ρ of arity $2n^2$ such

- ρ is an invariant of $\mathbb{A}$, $(a, b, a, b, a, b, a, b, \dots, a, b) \notin \rho$.
- $\exists i\colon c_i = d_i \Rightarrow (c_1, d_1, c_2, d_2, \dots, c_{n^2}, d_{n^2}) \in \rho$.

Put $\delta(x_1, \dots, x_n, y_1, \dots, y_n) =$
$\rho(x_1, y_1, x_1, y_2, x_1, y_3, \dots, x_1, y_n, x_2, y_1, \dots, x_n, y_n)$.

- δ is an invariant of $\mathbb{A}$, $(\underbrace{a, a, \dots, a}_{n}, \underbrace{b, b, \dots, b}_{n}) \notin \delta$.
- $\exists i, j\colon c_i = d_j \Rightarrow (c_1, \dots, c_n, d_1, \dots, d_n) \in \delta$.

Final step

We consider $2n!$ relations obtained from δ by a permutation of variables.

Proof

(ALMOST TRUE) for every n we can get a relation ρ of arity $2n^2$ such

- ρ is an invariant of $\mathbb{A}$, $(a, b, a, b, a, b, a, b, \dots, a, b) \notin \rho$.
- $\exists i\colon c_i = d_i \Rightarrow (c_1, d_1, c_2, d_2, \dots, c_{n^2}, d_{n^2}) \in \rho$.

Put $\delta(x_1, \dots, x_n, y_1, \dots, y_n) =$
$\rho(x_1, y_1, x_1, y_2, x_1, y_3, \dots, x_1, y_n, x_2, y_1, \dots, x_n, y_n)$.

- δ is an invariant of $\mathbb{A}$, $(\underbrace{a, a, \dots, a}_{n}, \underbrace{b, b, \dots, b}_{n}) \notin \delta$.
- $\exists i, j\colon c_i = d_j \Rightarrow (c_1, \dots, c_n, d_1, \dots, d_n) \in \delta$.

Final step

We consider $2n!$ relations obtained from δ by a permutation of variables. Any 2n-tuple omits at most $2^{|A|} \cdot (n!)^2$ relations.

(ALMOST TRUE) for every n we can get a relation ρ of arity $2n^2$ such

- ρ is an invariant of $\mathbb{A}$, $(a, b, a, b, a, b, a, b, \dots, a, b) \notin \rho$.
- $\exists i\colon c_i = d_i \Rightarrow (c_1, d_1, c_2, d_2, \dots, c_{n^2}, d_{n^2}) \in \rho$.

Put $\delta(x_1, \dots, x_n, y_1, \dots, y_n) =$
$\rho(x_1, y_1, x_1, y_2, x_1, y_3, \dots, x_1, y_n, x_2, y_1, \dots, x_n, y_n)$.

- δ is an invariant of $\mathbb{A}$, $(\underbrace{a, a, \dots, a}_{n}, \underbrace{b, b, \dots, b}_{n}) \notin \delta$.
- $\exists i, j\colon c_i = d_j \Rightarrow (c_1, \dots, c_n, d_1, \dots, d_n) \in \delta$.

Final step

We consider $2n!$ relations obtained from δ by a permutation of variables. Any 2n-tuple omits at most $2^{|A|} \cdot (n!)^2$ relations. To generate $\mathbb{A}^{2n}$ we need at least $(2n!)/(2^{|A|} \cdot (n!)^2) > 2^{n-|A|}$ tuples.

Proof

(ALMOST TRUE) for every n we can get a relation ρ of arity $2n^2$ such

- ρ is an invariant of $\mathbb{A}$, $(a, b, a, b, a, b, a, b, \dots, a, b) \notin \rho$.
- $\exists i\colon c_i = d_i \Rightarrow (c_1, d_1, c_2, d_2, \dots, c_{n^2}, d_{n^2}) \in \rho$.

Put $\delta(x_1, \dots, x_n, y_1, \dots, y_n) =$
$\rho(x_1, y_1, x_1, y_2, x_1, y_3, \dots, x_1, y_n, x_2, y_1, \dots, x_n, y_n)$.

- δ is an invariant of $\mathbb{A}$, $(\underbrace{a, a, \dots, a}_{n}, \underbrace{b, b, \dots, b}_{n}) \notin \delta$.
- $\exists i, j\colon c_i = d_j \Rightarrow (c_1, \dots, c_n, d_1, \dots, d_n) \in \delta$.

Final step

We consider $2n!$ relations obtained from δ by a permutation of variables. Any 2n-tuple omits at most $2^{|A|} \cdot (n!)^2$ relations. To generate $\mathbb{A}^{2n}$ we need at least $(2n!)/(2^{|A|} \cdot (n!)^2) > 2^{n-|A|}$ tuples. Success.

An algebra $\mathbb{A}$ is called k-collapsible, if $\mathbb{A}^n$ is generated by all the tuples where at least $(n-k)$ elements are equal.
An algebra $\mathbb{A}$ is collapsible, if it is k-collapsible for some k.

An algebra $\mathbb{A}$ is called k-collapsible, if $\mathbb{A}^n$ is generated by all the tuples where at least $(n-k)$ elements are equal.
An algebra $\mathbb{A}$ is collapsible, if it is k-collapsible for some k.

Lemma (Hubie Chen)

Collapsibility $\Rightarrow$ Switchability.
Switchability $\not\Rightarrow$ Collapsibility.

An algebra $\mathbb{A}$ is called k-collapsible, if $\mathbb{A}^n$ is generated by all the tuples where at least $(n-k)$ elements are equal.
An algebra $\mathbb{A}$ is collapsible, if it is k-collapsible for some k.

Lemma (Hubie Chen)

Collapsibility $\Rightarrow$ Switchability.
Switchability $\not\Rightarrow$ Collapsibility.

Conjecture (Barnaby Martin)

Suppose $\mathbb{A}$ is a finitely related algebra.
Then Switchability $\Leftrightarrow$ Collapsibility.

An algebra $\mathbb{A}$ is called k-collapsible, if $\mathbb{A}^n$ is generated by all the tuples where at least $(n-k)$ elements are equal.
An algebra $\mathbb{A}$ is collapsible, if it is k-collapsible for some k.

Lemma (Hubie Chen)

Collapsibility $\Rightarrow$ Switchability.
Switchability $\not\Rightarrow$ Collapsibility.

Conjecture (Barnaby Martin)

Suppose $\mathbb{A}$ is a finitely related algebra.
Then Switchability $\Leftrightarrow$ Collapsibility.

Almost Theorem

The conjecture holds for idempotent algebras on 3 elements.

Thank you for your attention