Checking Equations in Finite Algebras

Vera Vértesi

Joint work with Csaba Szabó and Gábor Kun

Logic Colloquium 2004

Overview

- Equational Bound
  - ⋆ Membership problem and methods for checking
  - ⋆ Our and other results
  - ⋆ Application for flat graph and hypergraph algebras
- Identity Checking Problem
  - ⋆ Previous results for different algebras
  - ⋆ Different interpretations over rings
  - ⋆ Results

The Membership Problem

Given: $\mathcal{V} = \mathrm{Var}(\mathbf{A})$ variety, where $\mathbf{A}$ is a finite and finitely typed algebra

$$|\mathbf{A}| = m$$

Input: $\mathbf{B}$ finite algebra.

$$|\mathbf{B}| = n$$

Question: Is $\mathbf{B}$ in the variety generated by $\mathbf{A}$?

$$\mathbf{B} \overset{?}{\in} \mathrm{Var}(\mathbf{A})$$

Example

$\boldsymbol{\tau} = \langle \mathbf{1}, {}^{-1}, \cdot \rangle$

Claim: $\mathbf{A}$ finite Abelian group

$\mathbf{B} \in \mathrm{Var}(\mathbf{A})$, finite $\iff$ $\mathbf{B}$ is a finite Abelian group and

$$\exp \mathbf{B} \mid \exp \mathbf{A}$$

Identity basis of $\mathrm{Var}(\mathbf{A})$ is

$$\begin{aligned}
&x^{\exp \mathbf{A}} \equiv \mathbf{1} \\
&x \cdot \mathbf{1} \equiv \mathbf{1} \cdot x \equiv x \\
&x \cdot x^{-1} \equiv x^{-1} \cdot x \equiv \mathbf{1} \\
&x \cdot (y \cdot z) \equiv (x \cdot y) \cdot z \\
&x \cdot y \equiv y \cdot x
\end{aligned}$$

Method #1: Free algebra

$\mathbf{B} \in \mathrm{Var}(\mathbf{A}) \iff$ $\mathbf{B}$ is a homomorphic image of $\mathbf{F}_{\mathcal{V}}(n)$

$$\begin{array}{rcl} \overrightarrow{g_1} & = & \boxed{a_1 \quad a_{i_1} \quad \cdots \quad a_{k_1}} \\ \overrightarrow{g_2} & = & \boxed{a_2 \quad a_{i_2} \quad \cdots \quad a_{k_2}} \\ & & \vdots \qquad \vdots \qquad\qquad \vdots \\ \overrightarrow{g_n} & = & \boxed{a_n \quad a_{i_n} \quad \cdots \quad a_{k_n}} \end{array} \quad \updownarrow |\mathbf{B}|$$

$$\longleftrightarrow$$
$$|\mathbf{A}^{\mathbf{B}}|$$

$$\mathbf{F}_{\mathcal{V}}(n) = \langle \overrightarrow{g_1}, \overrightarrow{g_2}, \ldots, \overrightarrow{g_n} \rangle \subseteq \mathbf{A}^{\mathbf{A}^{\mathbf{B}}}$$

To be checked if $\begin{array}{c} g_1 \mapsto b_{i_1} \\ \vdots \\ g_n \mapsto b_{i_n} \end{array}$ extends to a homomorphism

Method #2: Checking Identities

$\mathbf{B} \in \mathrm{Var}(\mathbf{A}) \iff$ All identities of $\mathbf{A}$ holds in $\mathbf{B}$

Enough to check the identities of rank n

Moreover: $\mathbf{F}_{\mathcal{V}}(n) =$ equivalence classes of expressions

$T = \{t_1, t_2, \dots, t_k\}$ system of representatives ($k \leq m^{m^n}$)

Identities to be checked:

$$f(t_{i_1}, t_{i_2}, \dots, t_{i_r}) \equiv t \qquad t_{i_j}, t \in T,\ f \text{ operation}$$

Def. $\mathbf{A}$ *finitely based*, if every identity of $\mathbf{A}$ follows from a finite set of identities.

If $\mathbf{A}$ is finitely based $\implies$ polynomial algorithm

β-function

$\mathcal{V} = \mathrm{Var}(\mathbf{A})$

$$\beta : \mathbb{N} \longrightarrow \mathbb{N}$$

$$\begin{aligned} \beta(n) &= \min\{k : |\mathbf{B}| \leq n, \text{it is enough to check the identities of} \\ &\quad \text{not longer than } k \text{ to decide whether } \mathbf{B} \in \mathcal{V}\} \\ &= \max\{l : \exists \mathbf{C} \notin \mathcal{V}, |\mathbf{C}| \leq n, \text{every identity in } \mathbf{A} \\ &\quad \text{not longer than } l \text{ holds in } \mathbf{C}\} + 1 \end{aligned}$$

$\Sigma_{\mathcal{V}}^{[k]}$: Identities of $\mathcal{V}$ not longer than k

$\mathcal{V}^k$: Variety defined by the identity set $\Sigma_{\mathcal{V}}^{[k]}$

$$\mathbf{B} \in \mathcal{V} \iff \mathbf{B} \models \Sigma_{\mathcal{V}}^{[\beta(n)]}$$

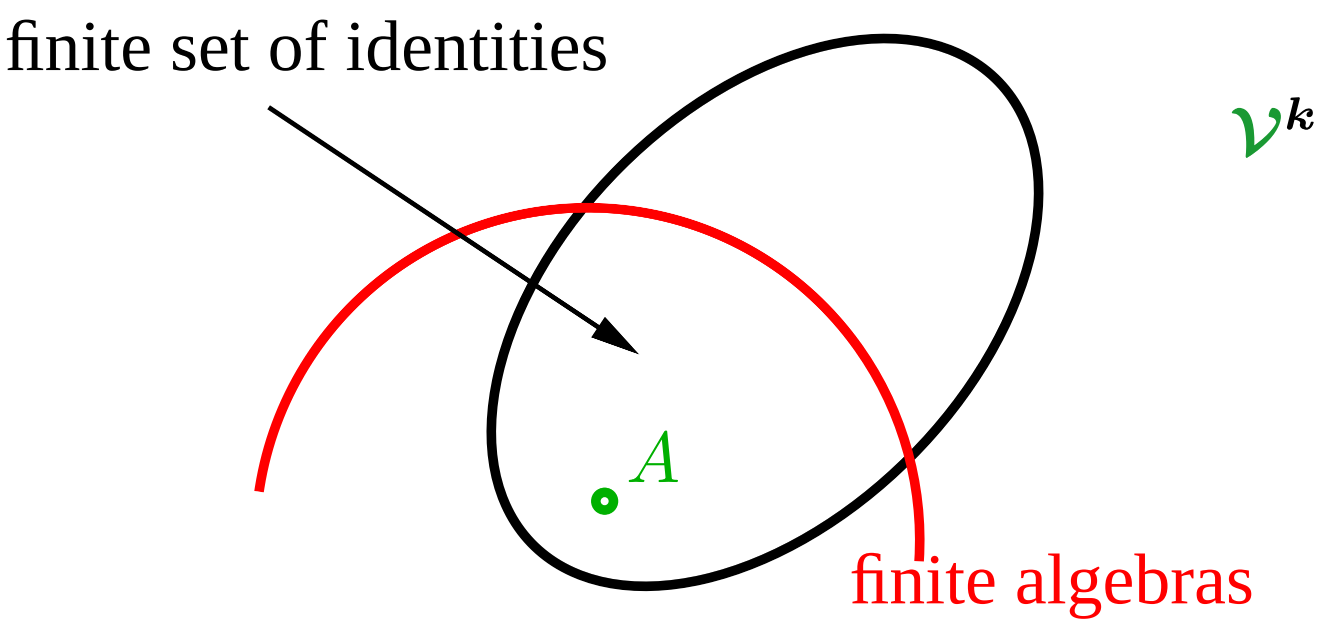
Connections

$\mathcal{V}$ finitely based $\quad \overset{\Longrightarrow}{\underset{?}{\Longleftarrow}} \quad \beta$ bounded

Connections

$$\mathcal{V} \text{ finitely based } \underset{\overset{?}{\Longleftarrow}}{\Longrightarrow} \beta \text{ bounded}$$

$$\beta \text{ bounded} \Longrightarrow \mathcal{V} \text{ finitely based}$$



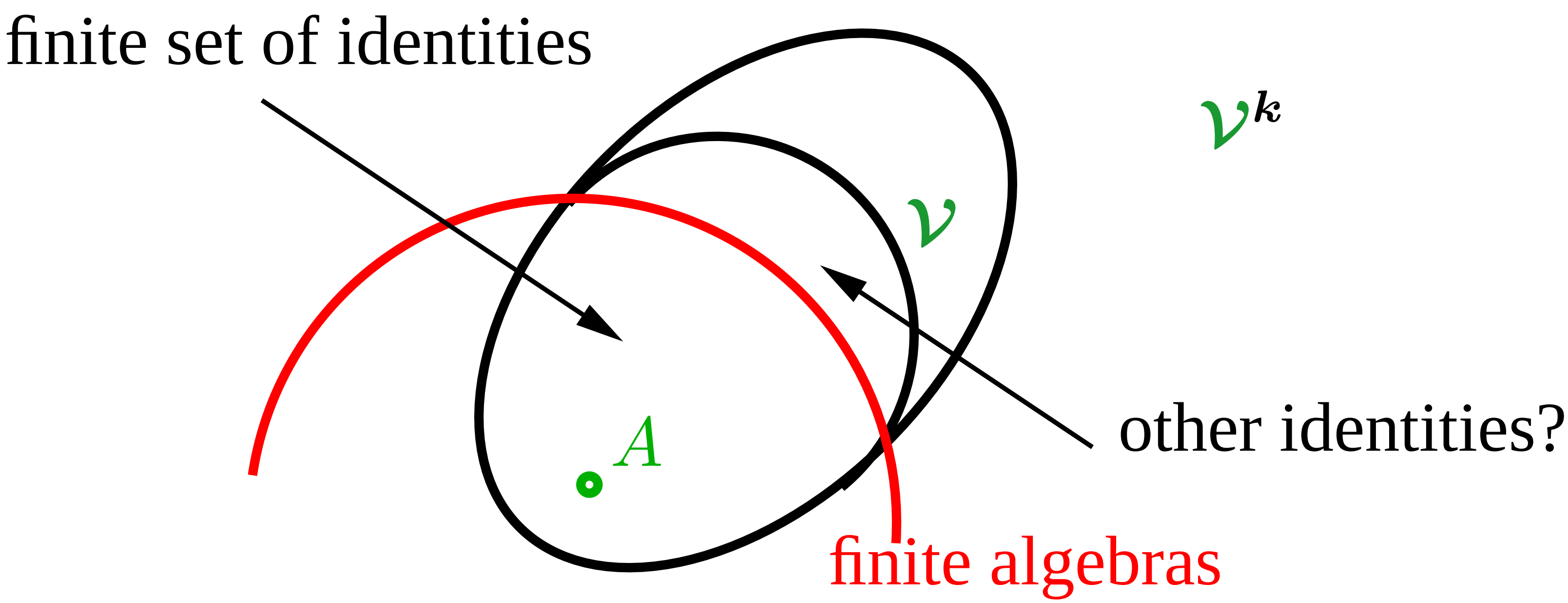
Connections

$\mathcal{V}$ finitely based $\underset{\overset{?}{\Longleftarrow}}{\Longrightarrow}$ β bounded

β bounded $\Longrightarrow$ $\mathcal{V}$ finitely based

or

$\mathcal{V}$ inherently non-finitely based



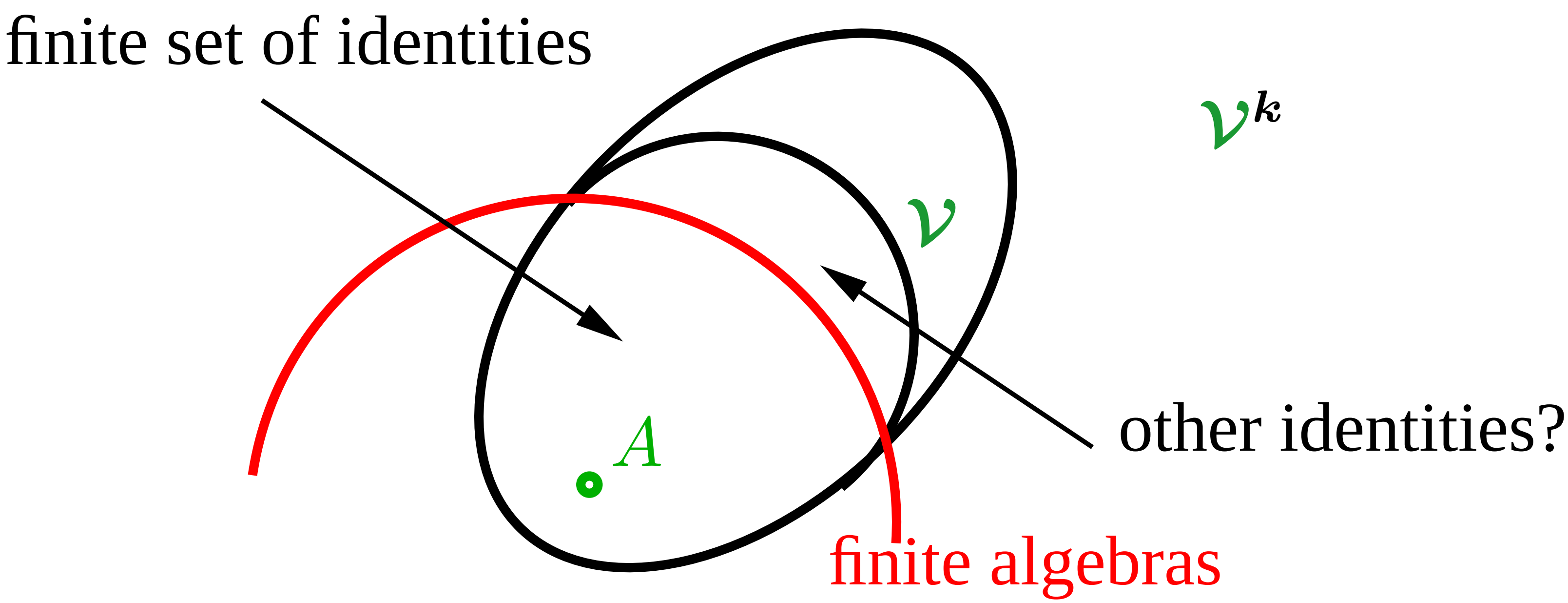
Connections

$\mathcal{V}$ finitely based $\overset{\Longrightarrow}{\underset{?}{\Longleftarrow}}$ β bounded

β bounded $\Longrightarrow$ $\mathcal{V}$ finitely based

or

$\mathcal{V}$ inherently non-finitely based



Such an example is not known

Results

Claim: (*McNulty*) A β-function exists and is recursive.

Claim: $\beta(n) = \mathcal{O}(m^{m^n})$

Well known: $\mathbf{A}$ finitely based $\implies$ β bounded

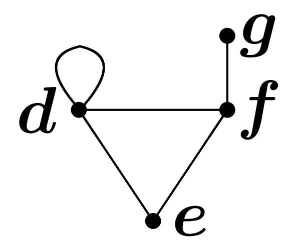
E.g. (*Székely*) There exists an algebra such that the β-function is at least sublinear.

Construction: (*Kun, W*): For every k there is an algebra such that $\beta(n) \sim n^k$.

Theorem: The β-function is not bounded by any polinomial.

Graph Algebras (C. Shallon, 1979)

$\mathbf{G}(V, E)$ *graph*, $E \subseteq V^2$



$\mathbf{A}_{\mathbf{G}}(\overbrace{V \cup \{0\}}^{A_{\mathrm{G}}}, \cdot)$ *graph algebra:*

$$0 \cdot x = x \cdot 0 = 0$$

$$x \cdot y = \begin{cases} x, & \text{if } (x, y) \in E \\ 0 & \text{otherwise} \end{cases}$$

$\cdot$	d	e	f	g	0
d	d	d	d	0	0
e	e	0	e	0	0
f	f	f	0	f	0
g	0	0	g	0	0
0	0	0	0	0	0

Hypergraph Algebras

Generalizations of the Graph Algebras:

$\mathbf{R}(\boldsymbol{R}, \boldsymbol{\alpha})$ *relational structure / hypergraph*, $\boldsymbol{\alpha} \subseteq \boldsymbol{R}^{\boldsymbol{k}}$

$\mathbf{A}_{\mathrm{R}}(\overbrace{\boldsymbol{R} \cup \{\mathbf{0}\}}^{\boldsymbol{A}_{\mathrm{R}}}, \boldsymbol{f})$ *hypergraph algebra:*

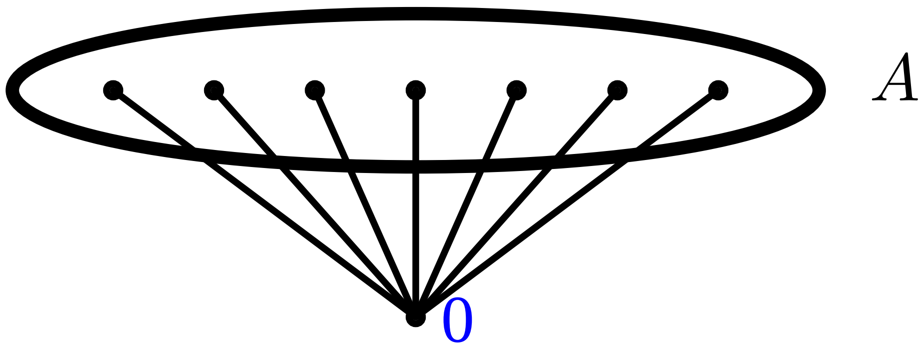
$$\boldsymbol{f}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{\boldsymbol{k}}) = \begin{cases} \boldsymbol{x}_1, & \text{if } \boldsymbol{x}_{\boldsymbol{i}} \in \boldsymbol{R} \text{ and } (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{\boldsymbol{k}}) \in \boldsymbol{\alpha} \\ \mathbf{0} & \text{otherwise} \end{cases}$$

Flat Semilattices

$\mathbf{A}$: arbitrary algebra

New operation : $\wedge$

$$x \wedge y = \begin{cases} x, & \text{if } x = y \\ 0 & \text{otherwise} \end{cases}$$



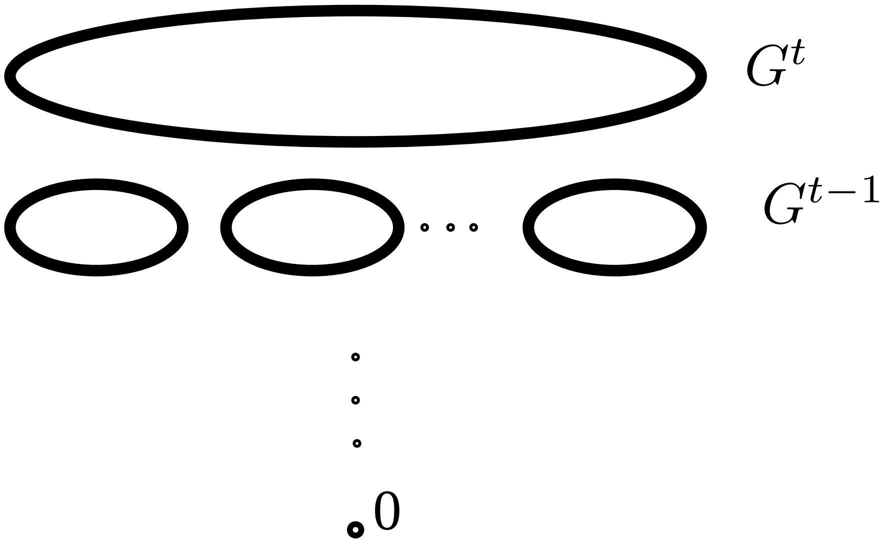
flat semilattice operation

$$\mathbf{F_G}(\overbrace{V \cup \{0\}}^{F_G}, \cdot, \wedge)$$ *flat graph algebra*

$$x \cdot y = \begin{cases} x, & \text{if } (x, y) \in E \\ 0 & \text{otherwise} \end{cases}$$

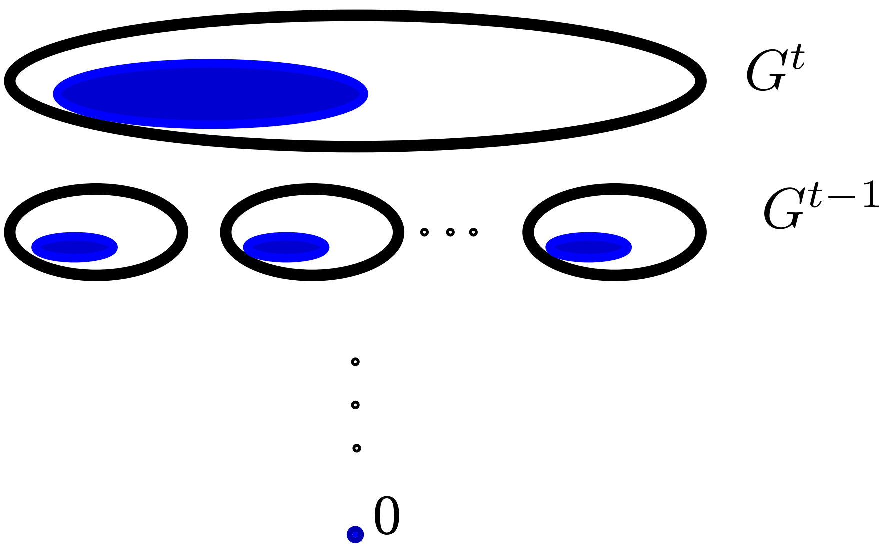
$$\mathbf{F_R}(\overbrace{R \cup \{0\}}^{F_R}, f, \wedge)$$ *flat hypergraph algebra*

Flat Graph Algebra Varieties



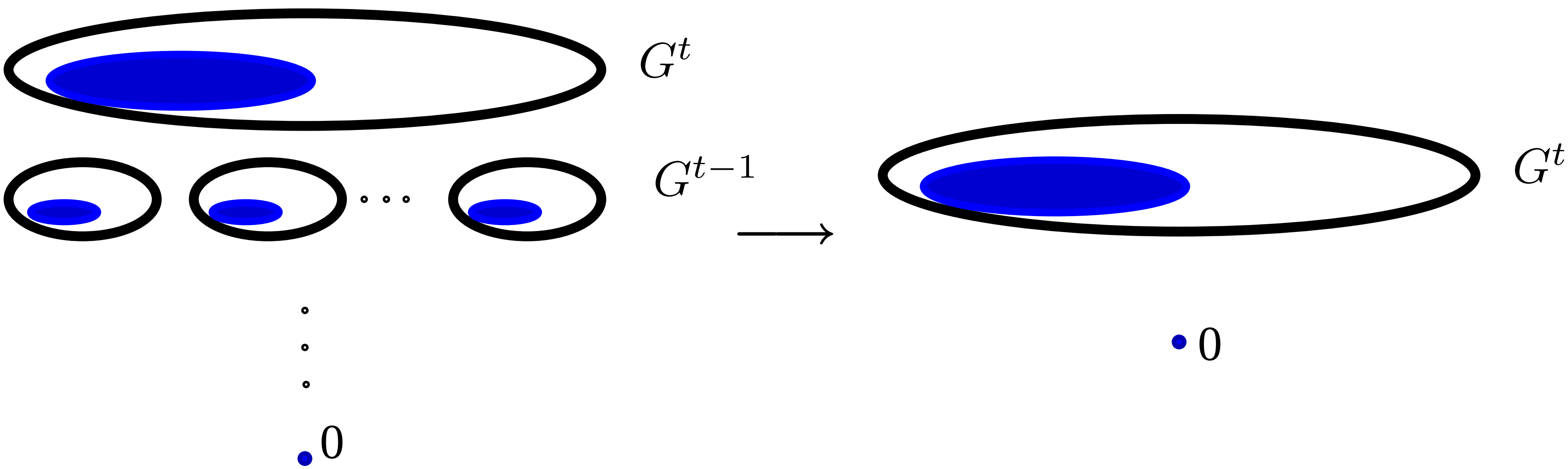
. . . a direct product . . .

Flat Graph Algebra Varieties



. . . a direct product's subalgebra

Flat Graph Algebra Varieties



homomorphic image of a direct product's subalgebra

So if $\mathbf{H} \subseteq \mathbf{G}^t$ is an induced subgraph $\implies$ $\mathbf{F_H} \in \mathrm{Var}(\mathbf{F_G})$

Subdirectly Irreducible Flat Graph Algebras

Theorem: (*Willard, 1996*) Let $\mathbf{F_G} = \langle F_G, \cdot, \wedge \rangle$ be a finite flat graph algebra, and $\mathbf{D} \in \mathrm{Var}(\mathbf{F_G})$ a finite algebra. Then the following are equivalent:

1. $\mathbf{D}$ is subdirectly irreducible
2. $\mathbf{D} = \mathbf{F_H}$ is a finite flat graph algebra, where $\mathbf{H}$ is a connected induced subgraph of $\mathbf{G}^t$ for some $t \in \mathbb{N}$.
3. $\mathbf{D}$ is simple.

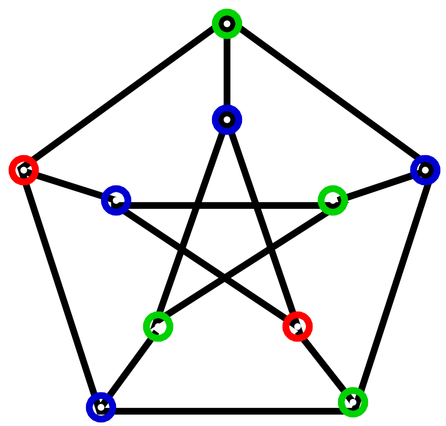
Theorem: (*Birkhoff*) Every algebra is a subdirect product of subdirectly irreducible ones.

Corollary: It is enough to know β's order of magnitude for subdirectly irreducible algebras.

Corollary: It is enough to investigate the connected induced subgraphs of $\mathbf{G}^t$.

Graph r-Coloring

Def. A graph $\mathbf{G}$ is *r-colorable* if its vertices can be colored with r colors so that there is no edge between vertices of the same color.



Def. $\mathbf{G}$ *r-critical*, if $\mathbf{G}$ is not r-colorable, but removing any edges of $\mathbf{G}$ results in an r-colorable graph.

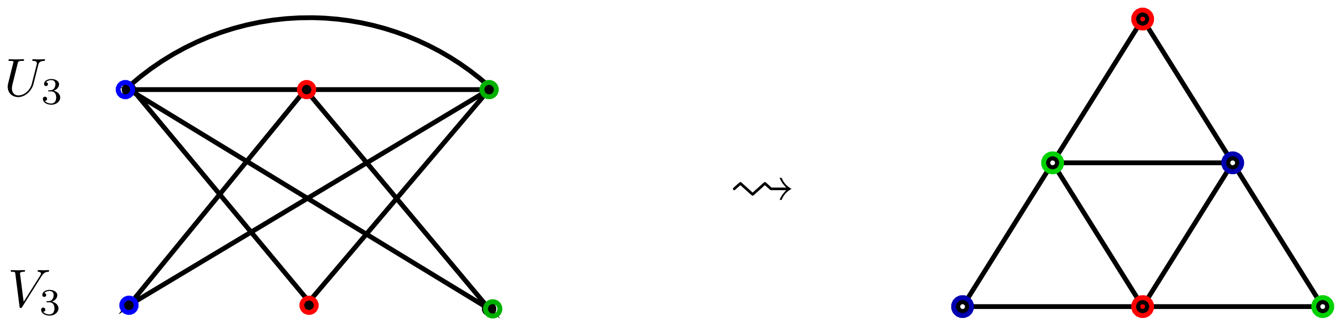
E.g. 2-critical graphs are the odd circles

Theorem: (*Toft, 1972*) For every $r \geq 3$ there is an r-critical graph $\mathbf{H}_{r\text{-crit}}$ with n vertices and $\sim n^2$ edges.

r-Colorable Graphs

$$\mathbf{G}_r = (\{\overbrace{v_1, \ldots, v_r}^{V_r}, \overbrace{u_1, \ldots, u_r}^{U_r}\}, E_r)$$

$$(x, y) \in E \iff \begin{cases} x, y \in \mathrm{U}_r \\ x = v_i \in \mathrm{V}_r, y = u_j \in \mathrm{U}_r, i \neq j \\ x = u_i \in \mathrm{U}_r, y = v_j \in \mathrm{V}_r, i \neq j \end{cases}$$



Theorem: $\mathbf{H} = (U, F)$ is a connected r-colorable graph $\iff$ $\mathbf{H}$ connected induced subgraph of G_r^t for some $t \in \mathbb{N}$.

β-Function for Flat Graph Algebras

Reminder: The subdirectly irreducibles in $\mathrm{Var}(\mathbf{F}_{\mathbf{G}_r})$ are those graph algebras belonging to r-colorable graphs.

Theorem: (*Kun, W*) For a flat graph algebra $\mathbf{F}_{\mathbf{G}_r}$ $\beta(n) \sim n^2$.

Proof of $\beta(n) = \Omega(n^2)$

Let $\mathbf{H}_{r\text{-crit}}$ be an r-critical graph, then $\mathbf{F}_{\mathbf{H}_{r\text{-crit}}} \notin \mathrm{Var}(\mathbf{F}_{\mathbf{G}_r})$, thus $\exists p \equiv q$ identity:

$$\mathbf{F}_{\mathbf{G}_r} \models p \equiv q \qquad \text{but} \qquad \mathbf{F}_{\mathbf{H}_{r\text{-crit}}} \not\models p \equiv q$$

So there is an evaluation $u_1, \ldots, u_k \in \mathbf{F}_{\mathbf{H}_{r\text{-crit}}}$ so that $p(u_1, \ldots, u_k) \neq q(u_1, \ldots, u_k)$. If there was an edge (u, v) where $u \cdot v$ did not occur while evaluating $p(u_1, \ldots, u_k)$ and $q(u_1, \ldots, u_k)$, then $p \not\equiv q$ would be true by removing the edge (u, v). But since $\mathbf{H}_{r\text{-crit}}$ is critical, then by removing one edge we get an r-colorable graph, so $p \equiv q$ holds. $\lightning$ $\square$

β-Function for Flat Hypergraph Algebras

Theorem: (*Willard, 1996*) Let $\mathbf{F_R} = \langle \boldsymbol{F_{\mathrm{R}}}, \boldsymbol{f}, \wedge \rangle$ be a finite flat hypergraph algebra, and $\mathbf{D} \in \mathrm{Var}(\mathbf{F_R})$ a finite algebra. Then the following are equivalent:

1. $\mathbf{D}$ is subdirectly irreducible
2. $\mathbf{D} = \mathbf{F_S}$ is a finite flat hypergraph algebra, where $\mathbf{S}$ is a connected induced subhypergraph of $\mathbf{R}^{t}$ for some $t \in \mathbb{N}$.
3. $\mathbf{D}$ is simple.

Theorem: (*Toft, 1972*) For every $r \geq 3$ there is an r-critical k-hypergraph with n vertices and $\sim n^{k}$ edges.

Theorem: (*Kun, W*) The subdirectly irreducible algebras of $\mathrm{Var}(\mathbf{F}_{\mathbf{G}_{r,k}})$ are the flat hypergraph algebras belong to r-colorable k-hypergraphs.

Theorem: (*Kun, W*) For a flat hypergraph algebra $\mathbf{F}_{\mathbf{G}_{r,k}}$ $\beta(n) \sim n^{k}$.

The Identity Checking Problem

- TERM-EQ($\mathbf{A}$)

  Given: $\mathbf{A}$ a finite and finitely typed algebra

  Input: $t \overset{?}{\equiv} s$ identity, where t and s are terms

  Question: Is $t = s$ for every substitution over $\mathbf{A}$?

- E.g. $\left(x_1^{-1}x_2^{-1}x_1x_2\right)^3 \overset{?}{\equiv} x_2^6$ in S_3

$$\begin{array}{ccc} \left(x_1^{-1}x_2^{-1}x_1x_2\right)^3 & \overset{?}{\equiv} & x_2^6 \\ \| & & \| \\ [x_1, x_2]^3 \equiv id & & id \end{array}$$

  $[x_1, x_2] \in S_3' = A_3$

- E.g. $x^p \overset{?}{\equiv} x$ in $\mathbb{Z}_p$

Groups

- Theorem: *Lawrence*, *Willard* (1993)
  TERM-EQ is coNP-complete for G finite nonsolvable groups.

- Theorem: *Goldmann*, *Russel* (2001)
  For nilpotent groups TERM-EQ is in P.

- Theorem: *Horváth*, *Kun*, *Szabó*, *W* (2003)
  TERM-EQ is in P for metacyclic groups (semidirect product of cyclic groups).

- The question is open for other finite groups.

Semigroups

Are there any semigroups so that TERM-EQ is coNP-complete?

- *Volkov* (2002)
  #elements $\approx \mathbf{2^{1700}}$
- *Kisielewicz* (2002)
  few thousand
- *Szabó*, *W* (2002)
  13
- *Klima* (2003)
  6

Other semigroups?

Rings

Theorem: *Burris*, *Lawrence* (1993)
For a finite ring $\mathcal{R}$ $\text{TERM-EQ}(\mathcal{R})$ is in P, if $\mathcal{R}$ is nilpotent,
$\text{TERM-EQ}(\mathcal{R})$ is coNP-complete otherwise

TERM:

- any
  E.g. $(x+y)^n$

- TERM_Σ (sum of monomials)
  E.g. $x_1x_2^3x_3 + x_1 + x_2x_1x_3 + x_{19}$
  $\text{TERM}_\Sigma\text{-EQ}(\mathcal{R})$ problem

- monomial
  just in the multiplicative semigroup
  TERM-EQ problem for the multiplicative semigroup

$\mathrm{TERM}_\Sigma\text{-}\mathrm{EQ}(\mathcal{R})$ -Problem

- Theorem: *Lawrence*, *Willard* (1997)
  If $\mathcal{R} = M_n(\mathbb{F})$ is a finite simple matrix ring whose invertible elements form a nonsolvable group, then $\mathrm{TERM}_\Sigma\text{-}\mathrm{EQ}(\mathcal{R})$ is coNP-complete.

- Theorem: *Szabó*, *W* (2002)
  $\mathrm{TERM}_\Sigma\text{-}\mathrm{EQ}(M_2(\mathbb{Z}_2))$ and $\mathrm{TERM}_\Sigma\text{-}\mathrm{EQ}(M_2(\mathbb{Z}_3))$ are coNP-complete.

- Conclusion: For a finite simple matrix ring $M_n(\mathbb{F})$,
  $\mathrm{TERM}_\Sigma\text{-}\mathrm{EQ}(M_n(\mathbb{F}))$ is in P if it is commutative;
  Otherwise it is coNP-complete.

Multiplicative Semigroup of Rings

- Theorem: *Szabó*, *W* (2002-2003)
  TERM-EQ is in P for the multiplicative semigroup of a finite simple matrix ring if it is commutative;
  Otherwise it is coNP-complete.

Let $\mathcal{R}$ be a finite ring,
$\mathcal{J}(\mathcal{R})$ denotes its Jacobson-radical.
Then $\mathcal{R}/\mathcal{J}(\mathcal{R}) = M_{n_1}(\mathbb{F}_1) \oplus \cdots \oplus M_{n_k}(\mathbb{F}_k)$

- Theorem: For a finite ring $\mathcal{R}$ $\mathrm{TERM}_\Sigma\text{-}\mathrm{EQ}(\mathcal{R})$ is in P
  if $\mathcal{R}/\mathcal{J}(\mathcal{R})$ is commutative;
  Otherwise it is coNP-complete.