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

\[ |A| = m \]

Input: \( B \) finite algebra.

\[ |B| = n \]

Question: Is \( B \) in the variety generated by \( A \)?

\[ B \in \text{Var}(A) \]
Example

\[ \tau = \langle 1, -1, \cdot \rangle \]

Claim: A finite Abelian group

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

\[ \exp B | \exp A \]

Identity basis of \( \text{Var}(A) \) is

\[ x^{\exp A} \equiv 1 \]

\[ x \cdot 1 \equiv 1 \cdot x \equiv x \]

\[ x \cdot x^{-1} \equiv x^{-1} \cdot x \equiv 1 \]

\[ x \cdot (y \cdot z) \equiv (x \cdot y) \cdot z \]

\[ x \cdot y \equiv y \cdot x \]
Method #1: Free algebra

\[ B \in \text{Var}(A) \iff B \text{ is a homomorphic image of } F_{\forall}(n) \]

\[ \overrightarrow{g_1} = \begin{pmatrix} a_1 & a_{i_1} & \cdots & a_{k_1} \\ \vdots & \vdots & & \vdots \\ a_n & a_{i_n} & \cdots & a_{k_n} \end{pmatrix} \]

\[ \overrightarrow{g_2} = \begin{pmatrix} a_2 & a_{i_2} & \cdots & a_{k_2} \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ a_n & a_{i_n} & \cdots & a_{k_n} \end{pmatrix} \]

\[ \overrightarrow{g_n} = \begin{pmatrix} a_n & a_{i_n} & \cdots & a_{k_n} \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ a_n & a_{i_n} & \cdots & a_{k_n} \end{pmatrix} \]

\[ F_{\forall}(n) = \langle \overrightarrow{g_1}, \overrightarrow{g_2}, \ldots, \overrightarrow{g_n} \rangle \subseteq A^{A^B} \]

To be checked if \( g_1 \mapsto b_{i_1} \)

\( \vdots \) extends to a homomorphism

\( g_n \mapsto b_{i_n} \)
Method #2: Checking Identities

\( B \in \text{Var}(A) \iff \) All identities of \( A \) holds in \( B \)

Enough to check the identities of rank \( n \)

Moreover: \( F_{\text{Var}}(n) = \) equivalence classes of expressions

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

Identities to be checked:

\[ f(t_{i_1}, t_{i_2}, \ldots, t_{i_r}) \equiv t \quad t_{i_j}, t \in T, \ f \text{ operation} \]

Def. A \textit{finitely based}, if every identity of \( A \) follows from a finite set of identities.

If \( A \) is finitely based \( \implies \) polynomial algorithm
\( \beta \)-function

\[ \mathcal{V} = \text{Var}(A) \]

\( \beta : \mathbb{N} \rightarrow \mathbb{N} \)

\[ \beta(n) = \min\{k : |B| \leq n, \text{it is enough to check the identities of not longer than } k \text{ to decide whether } B \in \mathcal{V}\} \]

\[ = \max\{l : \exists C \notin \mathcal{V}, |C| \leq n, \text{every identity in } A \text{ not longer than } l \text{ holds in } C\} + 1 \]

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

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

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

\( \forall \) finitely based \( \iff \) \( \beta \) bounded
Connections

\[ \forall \text{ finitely based} \quad \iff \quad \beta \text{ bounded} \]

\[ \beta \text{ bounded} \quad \implies \quad \forall \text{ finitely based} \]

finite set of identities

finite algebras

\( \mathcal{V}^k \)
Connections

\[ \forall \text{ finitely based} \quad \iff \quad \beta \text{ bounded} \]

\[ \beta \text{ bounded} \quad \implies \quad \forall \text{ finitely based} \]

or

\[ \forall \text{ inherently non-finitely based} \]

finite set of identities

finite algebras
Connections

\( \forall \) finitely based \( \iff \beta \) bounded

\( \beta \) bounded \( \implies \forall \) finitely based

or

\( \forall \) inherently non-finitely based

finite set of identities

such an example is not known
Results

Claim: (McNulty) A $\beta$-function exists and is recursive.

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

Well known: A finitely based $\iff$ $\beta$ bounded

E.g. (Székely) There exists an algebra such that the $\beta$-function is at least sublinear.

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

Theorem: The $\beta$-function is not bounded by any polynomial.
Graph Algebras (C. Shallon, 1979)

\(G(V, E)\) graph, \(E \subseteq V^2\)

\[\begin{align*}
\text{AG}\left(V \cup \{0\}, \cdot\right) \text{ graph algebra:} \\
0 \cdot x &= x \cdot 0 = 0 \\
x \cdot y &= \begin{cases} 
  x, & \text{if } (x, y) \in E \\
  0, & \text{otherwise}
\end{cases}
\end{align*}\]

\[
\begin{array}{cccccc}
\cdot & d & e & f & g & 0 \\
\hline
d & d & d & d & 0 & 0 \\
e & e & 0 & e & 0 & 0 \\
f & f & f & 0 & f & 0 \\
g & 0 & 0 & g & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0
\end{array}
\]
Hypergraph Algebras

Generalizations of the Graph Algebras:

\[ R(R, \alpha) \text{ relational structure / hypergraph, } \alpha \subseteq R^k \]

\[ A_R \left( R \cup \{0\}, f \right) \text{ hypergraph algebra:} \]

\[ f(x_1, \ldots, x_k) = \begin{cases} x_1, & \text{if } x_i \in R \text{ and } (x_1, \ldots, x_k) \in \alpha \\ 0, & \text{otherwise} \end{cases} \]
Flat Semilattices

\( A \): arbitrary algebra

New operation: \( \land \)

\[ x \land y = \begin{cases} x, & \text{if } x = y \\ 0, & \text{otherwise} \end{cases} \]

flat semilattice operation

\[ F_G(V \cup \{0\}, \cdot, \land) \text{ flat graph algebra} \]

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

\[ F_R(R \cup \{0\}, f, \land) \text{ flat hypergraph algebra} \]
Flat Graph Algebra Varieties

... a direct product ...
Flat Graph Algebra Varieties

\[ G^t \]

\[ G^{t-1} \]

\[ \ldots \]

\[ 0 \]

\ldots a direct product’s subalgebra
Flat Graph Algebra Varieties

homomorphic image of a direct product's subalgebra

So if $H \subseteq G^t$ is an induced subgraph $\implies F_H \in \text{Var}(F_G)$
Subdirectly Irreducible Flat Graph Algebras

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

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

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

Corollary: It is enough to know $\beta$’s order of magnitude for subdirectly irreducible algebras.

Corollary: It is enough to investigate the connected induced subgraphs of $G^t$. 
**Graph \( r \)-Coloring**

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

![Graph Coloring Diagram](image)

**Def.** \( G \) is **\( r \)-critical**, if \( G \) is not \( r \)-colorable, but removing any edges of \( G \) 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 \( H_{r \text{-crit}} \) with \( n \) vertices and \( \sim n^2 \) edges.
$r$-Colorable Graphs

$G_r = (\{ v_1, \ldots, v_r, u_1, \ldots, u_r \}, E_r)$

$(x, y) \in E \iff \begin{cases} 
  x, y \in U_r \\
  x = v_i \in V_r, y = u_j \in U_r, i \neq j \\
  x = u_i \in U_r, y = v_j \in V_r, i \neq j 
\end{cases}$

Theorem: $H = (U, F)$ is a connected $r$-colorable graph

$\iff$ $H$ connected induced subgraph of $G_r^t$ for some $t \in \mathbb{N}$. 
**β-Function for Flat Graph Algebras**

Reminder: The subdirectly irreducibles in $\text{Var}(F_{G_r})$ are those graph algebras belonging to $r$-colorable graphs.

**Theorem:** (Kun, W) For a flat graph algebra $F_{G_r}$, $\beta(n) \sim n^2$.

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

Let $H_{r\text{-crit}}$ be an $r$-critical graph, then $F_{H_{r\text{-crit}}} \notin \text{Var}(F_{G_r})$, thus $\exists p \equiv q$ identity:

$$F_{G_r} \models p \equiv q \quad \text{but} \quad F_{H_{r\text{-crit}}} \not\models p \equiv q$$

So there is an evaluation $u_1, \ldots, u_k \in F_{H_{r\text{-crit}}}$ 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 $H_{r\text{-crit}}$ is critical, then by removing one edge we get an $r$-colorable graph, so $p \equiv q$ holds. $\square$
β-Function for Flat Hypergraph Algebras

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

1. $D$ is subdirectly irreducible
2. $D = F_S$ is a finite flat hypergraph algebra, where $S$ is a connected induced subhypergraph of $R^t$ for some $t \in \mathbb{N}$.
3. $D$ 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 $\text{Var}(F_{G_{r,k}})$ are the flat hypergraph algebras belong to $r$-colorable $k$-hypergraphs.

Theorem: (Kun, W) For a flat hypergraph algebra $F_{G_{r,k}}$

$\beta(n) \sim n^k$. 
The Identity Checking Problem

- **TERM-EQ(A)**

  Given: \( A \) a finite and finitely typed algebra

  Input: \( t \equiv s \) identity, where \( t \) and \( s \) are terms

  Question: Is \( t = s \) for every substitution over \( A \)?

- E.g. \( (x_1^{-1}x_2^{-1}x_1x_2)^3 \equiv x_2^6 \) in \( S_3 \)

- E.g. \( [x_1, x_2]^3 \equiv id \) in \( S_3' = A_3 \)

- E.g. \( x^p \equiv x \) in \( \mathbb{Z}_p \)
Groups

  TERM-EQ is coNP-complete for $G$ finite nonsolvable groups.

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

  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 \textsc{Term-Eq} is coNP-complete?

- \textit{Volkov} (2002)
  \#elements \approx 2^{1700}

- \textit{Kisielewicz} (2002)
  few thousand

  13

- \textit{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. $(x + y)^n$
- $\text{TERM}_\Sigma$ (sum of monomials)
  - E.g. $x_1x_2^3x_3 + x_1 + x_2x_1x_3 + x_{19}$
  - $\text{TERM}_\Sigma$-EQ($\mathcal{R}$) problem
- monomial
  - just in the multiplicative semigroup
  - $\text{TERM}$-EQ problem for the multiplicative semigroup
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 $\text{TERM}_\Sigma\text{-EQ}(\mathcal{R})$ is coNP-complete.

$\text{TERM}_\Sigma\text{-EQ}(M_2(\mathbb{Z}_2))$ and $\text{TERM}_\Sigma\text{-EQ}(M_2(\mathbb{Z}_3))$ are coNP-complete.

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

  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 $\mathcal{R}/\mathcal{J}(\mathcal{R}) = M_{n_1}(F_1) \oplus \cdots \oplus M_{n_k}(F_k)$

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