UA IV
16.05

Algebras with few subpowers

Def. $\underline{A}$ ... finite algebra

$\underline{A}$ has few subpowers if $\exists p(n)$ polynomial such that

$|\{R \leq \underline{A}^n\}| \leq 2^{p(n)}$

For general $\underline{A}$:

$$2^{|A|^n} = |P(A^n)| \geq |\{R \leq \underline{A}^n\}| \geq |\{R \leq A^n, \text{pp-def from} =\}|$$
$$\geq 2^{n-1}$$

Examples

•) $\mathbb{Z}_p = (\mathbb{Z}_p, x-y+z)$

$R \leq \mathbb{Z}_p^n \Leftrightarrow R$ is affine subspace, i.e. given by

$A \cdot \bar{x} = \bar{b}$ for $A \in \mathbb{Z}_p^{n \times n}$, $\bar{b} \in \mathbb{Z}_p$

$\Rightarrow |\{R \leq \mathbb{Z}_p^n\}| \leq p^{n^2+n} = 2^{\log(p)\cdot(n^2+n)} \Rightarrow$ f.s.

We will see: $\underline{A}$ Mal'tsev $\Rightarrow$ $\underline{A}$ has few subpowers

•) $\underline{A} = (\{0,1\}, maj)$

then $R \leq \underline{A}^n \Leftrightarrow R = \bigwedge_{i,j} \underbrace{proj_{i,j} R(x_i, x_j)}_{\leq \underline{A}^2}$

$\Rightarrow |\{R \leq \underline{A}^n\}| \leq 2^{c \cdot \binom{n}{2}}$

In Practical: $\underline{A}$ has NU term $\Rightarrow$ $\underline{A}$ has few subpowers

$x \approx f(yx\ldots x) \approx f(xyx\ldots x) \approx \ldots \approx f(x\ldots xy)$

•) $\underline{A} = (A, \text{projections})$.

Then $|\{R \leq \underline{A}^n\}| = |\mathcal{P}(A^n)| = 2^{|A|^n}$

$\Rightarrow$ $\underline{A}$ does not have few subpowers.

•) There are Taylor algebras without few subpowers:

<u>In Practical:</u> $(\{0,1\}, \vee)$ does not have few subpowers.

<u>Def</u>: $\underline{A}$...algebra

•) $S \subseteq A$ is <u>independent</u> if (generalization of linearly independent)

$\forall a \in S: \ a \notin Sg_{\underline{A}}(S \setminus \{a\})$

•) $i_{\underline{A}}(n) := \max\{|S| \mid S \subseteq A^n \text{ is independent in } \underline{A}^n\}$

$$2^{i_{A}(n)} \underset{\mathrm{I}}{\leq} |\{R \leq \underline{A}^n\}| \underset{\mathrm{II}}{\leq} |A^n|^{i_{\underline{A}}(n)} = 2^{\log A \cdot n\, i_{A}(n)}$$

<u>Proof</u>

I Let $S = \{\bar{a}_1, \dots, \bar{a}_{i_A(n)}\}$ be an independent set in $\underline{A}^n$

then all $R_I := Sg_{\underline{A}^n}(\{a_i \mid i \in I\})$ are pairwise different for $I \subseteq [i_A(n)]$

II Every $R \leq \underline{A}^n$ has a minimal (and thus independent) generating set of size $\leq i_A(n)$.

$|A^n|^{i_A(n)}$ is a bound on ~~all~~ the number possible such generating sets.

$\square$

$\Rightarrow$ $\underline{A}$ has few subpowers $\Leftrightarrow$ $i_{\underline{A}}(n) \leq p(n)$ for a polynomial p.

1 If $\underline{B} \in HSP(\underline{A})$ then $i_B(n) \leq i_A(k \cdot n)$
finite for some k.

<u>Proof</u>. $\underline{B} \in HS(\underline{A}^k)$ for some $k \in \mathbb{N}$ i.e.

$\exists\, \underline{C} \leq \underline{A}^k$ and $f: C \twoheadrightarrow \underline{B}$ homom.

Let $\{\bar{b}_1, \dots, \bar{b}_e\}$ be independent in $\underline{B}^n$ and

$\{\bar{c}_1 \dots \bar{c}_e\} \subseteq C^n : f(\bar{c}_i) = b_i$.

Then $\{\bar{c}_1 \dots \bar{c}_e\}$ independent in $\underline{C}^n \leq (\underline{A}^k)^n = \underline{A}^{k \cdot n}$

$\Rightarrow i_B(n) \leq i_A(k \cdot n)$ $\square$

$\Rightarrow$ few subpower property preserved under HSP.

Is there a Mal'tsev condition describing it? YES!

<u>Theorem</u> (Idziak, Marković, McKenzie, Valeriote, Willard '10)

For $\underline{A}$ finite, either

1) $\underline{A}$ has <u>no cube term</u> and $i_A(n) = 2^{\Theta(n)}$

2) $\underline{A}$ has a <u>cube term</u> and <u>few subpowers</u>.

more precisely: <u>k-cube term</u> $\Leftrightarrow i_A(n) = O(n^{k-1})$

<u>Def</u> recall „<u>Berto cube terms</u>":

$$t\begin{pmatrix} x & * & \cdots & * \\ * & x & & \vdots \\ \vdots & & \ddots & * \\ * & \cdots & * & x \end{pmatrix} = \begin{pmatrix} y \\ y \\ \vdots \\ y \end{pmatrix}$$

$* \in \{x, y\}$

Def t is <u>$(k\text{-})$cube term</u>, if

$$t\underbrace{\begin{pmatrix} x & y & \cdots & x \\ x & x & & y \\ \vdots & \vdots & & \vdots \\ x & x & \cdots & y \end{pmatrix}}_{\text{columns = all vectors in } \{x,y\}^k \setminus \{(y\,y\ldots y)\}} \approx \begin{pmatrix} y \\ y \\ \vdots \\ y \end{pmatrix}$$

e.g. $k=2$

$$t\begin{pmatrix} x & y & x \\ x & x & y \end{pmatrix} = \begin{pmatrix} y \\ y \end{pmatrix} \ldots \text{ Mal'tsev term}$$

(up to permutation of var.)

$k=3$

$$t\begin{pmatrix} x & y & x & x & y & y & x \\ x & x & y & x & y & x & y \\ x & x & x & y & x & y & y \end{pmatrix} \approx \begin{pmatrix} y \\ y \\ y \end{pmatrix}$$

<u>Easy exercise</u>: $\exists$ cube term $\Leftrightarrow$ $\exists$ Bonto cube term.

<u>Lemma</u>

Let $\underline{F} = \underline{F}_{HSP(\underline{A})}(x,y) \leq \underline{A}^{A^2}$ be the free algebra generated by $\{x,y\}$.

Then 1) If $i_F(k) < 2^k \Rightarrow \underline{A}$ has k-cube term.

2) If $i_F(m) < \binom{m}{k} \Rightarrow \underline{A}$ has k-cube term.

<u>Proof</u>

(1) Let $\bar{v}_1, \bar{v}_2 \ldots \bar{v}_{2^k}$ be an enumeration of $\{x,y\}^k$

Since $i_F(k) < 2^k$ this is <u>not</u> an independent set $\Rightarrow$

wlog. $\exists f \in Clo\,\underline{A}$: $f(\bar{v}_1, \bar{v}_2 \ldots \bar{v}_{2^k-1}) = \bar{v}_{2^k}$

(else we relabel the $\bar{v}_i$'s)

by switching x and y in given rows, we can assume $\bar{v}_{2^k} = \begin{pmatrix} y \\ \vdots \\ y \end{pmatrix}$

$\Rightarrow f$ is k-cube term.

(2) ... similar proof $\square$

Together with 1 this implies:

$$\begin{aligned} i_{\underline{A}}(n) &= 2^{o(n)} \\ &\text{(subexponential)} \end{aligned} \quad \Rightarrow \underline{A} \text{ has cube-term}$$

$$i_{\underline{A}}(n) = O(n^k) \quad \Rightarrow \underline{A} \text{ has } k\text{-cube term.}$$

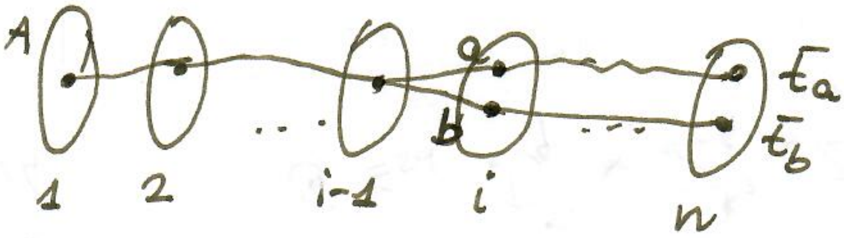
Proving the other direction of Theorem is harder

we only show: <u>Theorem 2</u>

$$\left[\begin{array}{l} \underline{A} \text{ Mal'tser} \\ \quad (2\text{-cube term}) \end{array} \Rightarrow i_{\underline{A}}(n) = O(n). \right]$$

<u>Def</u>. For any $R \leq \underline{A}^n$, the <u>signature $Sig(R)$</u> is the set of all triples (i, a, b) $i \in [n]$, $a, b \in A$, s.t.

$\exists \bar{t}_a, \bar{t}_b \in R$:



<u>Lemma</u> Let

$\underline{A}$ ... Mal'tser algebra

$R \leq \underline{A}^n$, $S \subseteq R$ with $Sig(S) = Sig(R)$

$\Rightarrow Sg_{\underline{A}^n}(S) = R$.

<u>Proof</u>:

Induction on n.

$n = 1$ ✓

for $n-1 \to n$:

By induction hypothesis:

$$\circledast \quad Sg_{\underline{A}^{n-1}}(pr_{[n-1]} S) = pr_{[n-1]} Sg(S) = pr_{[n-1]} R$$

Let $\bar{r} = (r_1 \dots r_{n-1}, r_n) \in R$

by $\circledast$ $\exists\ \bar{s} = (r_1 \dots r_{n-1}, s_n) \in Sg(S)$

since $\Rightarrow (n, r_n, s_n) \in Sig(R) = Sig(S)$

$\Rightarrow \exists\ \bar{t}_{r_n}, \bar{t}_{s_n} \in S$, withnessing (n, r_n, s_n)

$\bar{t}_{r_n} = (t_1 \dots t_{n-1}, r_n)$ $\quad$ $\bar{t}_{s_n} = (t_1 \dots t_{n-1}, s_n)$

then $m(\bar{s}, \bar{t}_{s_n}, \bar{t}_{r_n}) = m\begin{pmatrix} r_1 & t_1 & t_1 \\ \vdots & & \\ r_{n-1} & t_{n-1} & t_{n-1} \\ s_n & s_n & r_n \end{pmatrix} = \begin{pmatrix} r_1 \\ \vdots \\ r_{n-1} \\ r_n \end{pmatrix} = \bar{r}$ $\square$

We call a small such subset, i.e.

- $Sig(S) = Sig(R)$
- $|S| \leq 2 \cdot |Sig(R)| \quad (\leq 2n \cdot |A|^2)$

a <u>compact representation</u> of $R \leq \underline{A}^n$.

Every $R \leq \underline{A}^n$, in $\underline{A}$ Mal'tsev is generated by a compact representation.

Compact representations have many applications (e.g. CSP algorithms, Subpower membership problem).

Proof of Theorem 2:

Let $\underline{A}$ be Mal'tsev, and

$\bar{a}_1, \bar{a}_2 \ldots \bar{a}_m \in A^n$ be an independent set in $\underline{A}^n$.

We define $R_i := Sg_{A^n}(\bar{a}_1 \ldots \bar{a}_i)$.

It is not hard to find compact representations ~~B~~ S_i of R_i, such that $S_1 \subseteq S_2 \subseteq \ldots \subseteq S_m$. (exercise)

Since $R_i \subsetneq R_{i+1}$ (by independence), also $S_i \subsetneq S_{i+1}$

$\Rightarrow m \leq |S_m| \leq 2n \cdot |A|^2 = O(n)$.

$\Rightarrow i_A(n) \leq O(n)$

$\square$

Generalization of compact representations for k-cube terms can be used to prove Theorem 1, and

e.g. ~~...~~ algorithms for CSPs ~~...~~ with k-cube polymorphisms.