THE DEGREE AS A MEASURE OF COMPLEXITY OF FUNCTIONS ON A UNIVERSAL ALGEBRA

Erhard Aichinger

PALS, February 16, 2021

Institute for Algebra, Austrian Science Fund FWF P33878

JOHANNES KEPLER
UNIVERSITY LINZ

Outline

In this talk, we will

1. discuss the degree of a function between abelian groups,
2. use it to derive properties of algebraic sets (= solution sets of polynomial equations),
3. relate degree to supernilpotency.

Polynomial Equations over Finite Fields

The Chevalley-Warning Theorem

Theorem (C. Chevalley and E. Warning 1935)

Let $p \in \mathbb{P}, m \in \mathbb{N}, q := p^m$, let $f_1, \dots, f_r \in \mathbb{F}_q[x_1, \dots, x_n]$, and let

$$v := \#\{\boldsymbol{a} \in \mathbb{F}_q^n \mid f_1(\boldsymbol{a}) = \cdots = f_r(\boldsymbol{a}) = 0\}.$$

We assume $n > \sum_{i=1}^{r} \deg(f_i)$. Then

1. $v \neq 1$ (Chevalley).
2. p divides v (Warning's First Theorem).

Proof of Chevalley's Theorem

- Suppose that $\boldsymbol{a} \in \mathbb{F}_q^n$ is the only solution of $f_1(\boldsymbol{a}) = \cdots = f_r(\boldsymbol{a}) = 0$.
- Then $g(\boldsymbol{x}) = \prod_{i=1}^r (1 - f_i(\boldsymbol{x} + \boldsymbol{a})^{q-1})$ satisfies $g(\boldsymbol{0}) = 1$ and $g(\boldsymbol{b}) = 0$ for $\boldsymbol{b} \neq \boldsymbol{0}$.
- Hence $g(\boldsymbol{x})$ and $\prod_{i=1}^n (1 - x_i^{q-1})$ induce the same function.
- Hence $\deg(g) \geq n(q-1)$.
- Thus $\sum_{i=1}^r \deg(f_i)\,(q-1) \geq n(q-1)$.
- Contradiction to $\sum_{i=1}^r \deg(f_i) < n$.

Proof of Chevalley's Theorem

Let $\chi : \mathbb{F}_q^n \to \mathbb{F}_q$, $\chi(0) = 1$, $\chi(a) = 0$ for $a \in \mathbb{F}_q^n \setminus \{0\}$.

We need an argument for:

Lemma

Every polynomial $p \in \mathbb{F}_q[x_1, \ldots, x_n]$ that induces χ has total degree $\geq n(q-1)$.

Proof using Alon's Combinatorial Nullstellensatz [N. Alon 1999]:

Suppose $\deg(p) < n(q-1)$.
Then the coefficient of $x_1^{q-1} \cdots x_n^{q-1}$ in $f := p(x_1, \ldots, x_n) - \prod_{i=1}^{n}(1 - x_i^{q-1})$ does not vanish.
Hence Alon's Theorem tells that f is not the zero-function.
Hence p does not induce χ.

Proof of Chevalley's Theorem

Lemma

Every polynomial $p \in \mathbb{F}_q[x_1, \dots, x_n]$ that induces χ has total degree $\geq n(q-1)$.

Proof using Warning's argument:

For $i < q - 1$, we have $\sum_{a \in \mathbb{F}_q} a^i = 0$.
Hence for each $f \in \mathbb{F}_q[x_1, \dots, x_n]$ with $\deg(f) < n(q-1)$, we have $\sum_{\boldsymbol{a} \in \mathbb{F}_q^n} f(\boldsymbol{a}) = 0$.
Since $\sum_{\boldsymbol{a} \in \mathbb{F}_q^n} \chi(\boldsymbol{a}) = 1$, we have $\deg(p) \geq n(q-1)$.

The Chevalley-Warning Theorem

Lemma

For each $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ with $\deg(f) < n(q-1)$, we have $\sum_{\boldsymbol{a} \in \mathbb{F}_q^n} f(\boldsymbol{a}) = 0$.

The number of solutions of $f_1(\boldsymbol{x}) = \cdots f_r(\boldsymbol{x}) = 0$ modulo p is given by

$$[v]_p = \sum_{\boldsymbol{a} \in \mathbb{F}_q^n} \prod_{i=1}^{r} (1 - f_i(\boldsymbol{a})^{q-1}).$$

Hence if $\sum_{i=1}^{r} \deg(f_i)(q-1) < n(q-1)$, then p divides v (Warning's First Theorem).

Functional degree

Definition of the degree for functions

We try to generalize the total degree of a polynomial function.
Setup: We let A, B be abelian groups, $f : A \to B$. (In the Chevalley-Warning Theorems $A = \mathbb{F}_q^n$ and $B = \mathbb{F}_q$.)
Goal:

- Find a definition for $\textsc{Fdeg}(f)$.
- Argue that the definition is useful.

Definition of the degree of a function

Setup: We let A, B be abelian groups, $f : A \to B$.
Definition through difference operator:

- For $a \in A$, $\Delta_a(f)\,(x) := f(x+a) - f(x)$.
- $\textsc{Fdeg}(f) :=$ the minimal $n \in \mathbb{N}_0$ with $\Delta_{a_1}\Delta_{a_2}\cdots\Delta_{a_{n+1}}\, f = 0$ for all $a_1, \ldots, a_{n+1} \in A$.

- **Intuitive:** $f : \mathbb{R} \to \mathbb{R}$ is a polynomial of degree $\leq 2 \Leftrightarrow f''' = 0$.
- **Problems:**
  - ☐ $\Delta_a(f \circ g) = \ ?$ ("Chain rule")
  - ☐ $f : \mathbb{Z}_2 \to \mathbb{Z}_3, f(0) = 1, f(1) = 2$ satisfies $\Delta_1 f = f$. Hence $\textsc{Fdeg}(f) = \infty$.

The definition of the degree

Setup: We let A, B be abelian groups, $f : A \to B$.

Definition through an abstract version of the difference operator:

[Vaughan-Lee 1983, Freese McKenzie 1987 (Chapter 14)]

- Group ring $\mathbb{Z}[A] := \{\sum_{a \in A} z_a \tau_a \mid (z_a)_{a \in A} \in \mathbb{Z}^{(A)}\}$.
- $\mathbb{Z}[A]$ acts on B^A by

$$\begin{array}{rcl} (\tau_a * f)\ (x) & = & f(x+a) \\ ((\sum_{a \in A} z_a \tau_a) * f)\ (x) & = & \sum_{a \in A} z_a f(x+a) \\ ((\tau_a - 1) * f)\ (x) & = & f(x+a) - f(x). \end{array}$$

- In this way, B^A is a $\mathbb{Z}[A]$-module.

The definition of the degree

Setup: We let A, B be abelian groups, $f : A \to B$.

Definition through an abstract version of the difference operator:

[Vaughan-Lee 1983, Freese McKenzie 1987 (Chapter 14)]

- $((\tau_a - 1) * f)(x) := f(x + a) - f(x)$.
- $I :=$ augmentation ideal of $\mathbb{Z}[A] =$ ideal generated by $\{\tau_a - 1 \mid a \in A\} = \{\sum_{a \in A} z_a \tau_a \in \mathbb{Z}[A] \mid \sum_{a \in A} z_a = 0\}$
- $\text{FDEG}(f) := \min(\{n \in \mathbb{N}_0 \mid I^{n+1} * f = 0\} \cup \{\infty\})$.

The definition of the degree

Setup: We let A, B be abelian groups, $f : A \to B$.

Definition through a functional equation: For functions on $\mathbb{R}$, we have:

Theorem (Fréchet 1909)

A polynomial of degree n in x is a continuous function verifying the identity

$$\begin{aligned} f(x_1 + x_2 + \ldots + x_{n+1}) - \sum_{\boldsymbol{n}} f(x_{i_1} + \ldots + x_{i_n}) \\ + \sum_{\boldsymbol{n-1}} f(x_{i_1} + \ldots + x_{i_{n-1}}) - \ldots \\ + (-1)^n \sum_{\boldsymbol{n}} f(x_{i_1}) + (-1)^{n+1} f(0) \equiv 0, \end{aligned}$$

whatever the constants $x_1, \ldots, x_{n+1}$ are without satisfying the analogous identities obtained by replacing the integer n with a smaller integer.

The definition of the degree

Setup: We let A, B be abelian groups, $f : A \to B$.
Definition through a functional equation:

We define $\text{FDEG}(f)$ to be the smallest $m \in \mathbb{N}_0$ such that

$$f(\sum_{i=1}^{m+1} x_i) = \sum_{S \subset [m+1]} (-1)^{m-|S|} f(\sum_{j \in S} x_j)$$

for all $x_1, \ldots, x_{m+1} \in A$.

$m = 0$: $f(x_1) = f(0)$.
$m = 1$: $f(x_1 + x_2) = f(x_1) + f(x_2) - f(0)$.
$m = 2$:
$f(x_1+x_2+x_3) = f(x_1+x_2)+f(x_1+x_3)+f(x_2+x_3)-f(x_1)-f(x_2)-f(x_3)+f(0)$.

The functional degree

Setup: We let A, B be abelian groups, $f : A \to B$.

Lemma

All three definitions yield the same degree.

Definition of the functional degree

$\textsc{Fdeg}(f) := \min\left(\{n \in \mathbb{N}_0 \mid (\mathrm{Aug}(\mathbb{Z}[A]))^{n+1} * f = 0\} \cup \{\infty\}\right)$.

- $\textsc{Fdeg}(f) = 0 \Leftrightarrow f$ is constant.
- $\textsc{Fdeg}(f) = 1 \Leftrightarrow f = c + h$ with c constant, h group homomorphism.
- Let $p \in \mathbb{P}$ and assume that A, B are finite abelian p-groups. Then $\textsc{Fdeg}(f) < \infty$. **Reason:** Nilpotency of $\mathrm{Aug}(\mathbb{Z}_{p^\beta}[A])$.

The degree of concrete functions

- Polynomials over prime fields:
  $A = \mathbb{F}_p^N$, $B = \mathbb{F}_p$, $f \in \mathbb{F}_p[x_1, \ldots, x_N]$ with all exponents $\leq p - 1$.
  Then FDEG$(\overline{f})$ is the total degree of f.
- Polynomials over finite fields:
  On $\mathbb{F}_{25}$, x^5 induces a homomorphism ($\Rightarrow$ degree 1).
  - $\mathbb{F}_q$ ... field with q elements of characteristic p.
  - For $n \in \mathbb{N}$, $s_p(n)$ is the digit sum in base p.
    $s_5(25) = 1$, $s_5(10) = 2$, $s_5(24) = 8$.
  - [Moreno Moreno 1995] The p-weight degree of $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ is defined by

$$\deg_p(x_1^{\alpha_1} \cdots x_N^{\alpha_N}) := \sum_{n=1}^{N} s_p(\alpha_n).$$

The functional degree of polynomial functions

Theorem

$\mathbb{F}$ a field, $f \in \mathbb{F}[x_1, \ldots, x_n]$.

- If $|\mathbb{F}| = q = p^m$, and if all exponents are at most $q-1$, then $\text{FDEG}(\overline{f}) = \deg_p(f)$.
- If $\mathbb{F}$ is infinite of characteristic $p \in \mathbb{P}$, then $\text{FDEG}(\overline{f}) = \deg_p(f)$.
- If $\mathbb{F}$ is of characteristic 0, then $\text{FDEG}(\overline{f}) = \deg(f)$.

Properties of the functional degree

For a function $f : (A, +) \longrightarrow (B, +)$, the functional degree does not use any syntactic representation of f.

Lemma

- $\textsf{F}\textsf{\small DEG}(f + g) \leq \max(\textsf{F}\textsf{\small DEG}(f), \textsf{F}\textsf{\small DEG}(g))$.
- If $(B, +, \cdot)$ is a ring, then $\textsf{F}\textsf{\small DEG}(f \cdot g) \leq \textsf{F}\textsf{\small DEG}(f) + \textsf{F}\textsf{\small DEG}(g)$.

Properties of the functional degree

Theorem [Leibman 2002]

Let $(A,+),(B,+),(C,+)$ be abelian groups, let $f : A \to B$ and $g : B \to C$ with $\textsc{Fdeg}(f) < \infty$ and $\textsc{Fdeg}(g) < \infty$. Then $\textsc{Fdeg}(g \circ f) \leq \textsc{Fdeg}(g) \cdot \textsc{Fdeg}(f)$.

Self-contained proof in [EA, Moosbauer, 2021].

The proof needs the following claim (stated here for $m = 2$): If there are $g_1, g_2, g_3 : A^2 \to B$ such that for all $x_1, x_2, x_3 \in A^3$,

$$h(x_1 + x_2 + x_3) = g_1(x_2, x_3) + g_2(x_1, x_3) + g_3(x_1, x_2),$$

then $\textsc{Fdeg}(h) \leq 2$.

Characterization of the degree

Theorem (cf. [EA, Moosbauer, 2021])

Let $(A, +)$ and $(B, +)$ be abelian groups, let $f : A \to B$, and let $m \in \mathbb{N}_0$. Then the following are equivalent:

1. $\mathrm{FDEG}(f) \leq m$.
2. For every $k > m$, we have $f(\sum_{i=1}^{k} x_i) = \sum_{S \subset [k]} (-1)^{k-|S|+1} f(\sum_{j \in S} x_j)$.
3. There exist functions $g_1, \ldots, g_{m+1} : A^{m+1} \to B$ such that for all $x_1, \ldots, x_{m+1} \in A$, we have

$$f(\sum_{i=1}^{m+1} x_i) = \sum_{i=1}^{m+1} g_i(x_1, \ldots, x_{m+1}),$$

   and for each $i \in [m+1]$, the function g_i does not depend on its i th argument.

Maximal degree

For two abelian groups A, B, we define

$$\delta(A,B) := \sup\left(\{\textsf{FDEG}(f) \mid f \in B^A\}\right).$$

Theorem [EA, Moosbauer 2021]

- $\delta(A,B) < \infty \iff |A| = 1$ or $|B| = 1$ or $\exists p \in \mathbb{P} :\ A$ is a finite p-group and B is a p-group of finite exponent.
- If $\exp(B) = n \in \mathbb{N}$, then $\delta(A,B) = \underbrace{\min\{m \in \mathbb{N} \mid (\mathrm{Aug}(\mathbb{Z}_n[A]))^m = 0\}}_{\text{nilpotency index of } \mathrm{Aug}(\mathbb{Z}_n[A])} - 1$.
- If $\exp(B) = n \in \mathbb{N}$, then the characteristic function $\chi(0) = b$ (of order n) and $\chi(a) = 0$ for $a \neq 0$ has degree $\delta(A,B)$.

General results on $\delta(A, B)$

$$\delta(A, B) := \sup\left(\{\text{FDEG}(f) \mid f \in B^A\}\right).$$

Lemma (EA, Moosbauer 2021)

Let A, B be abelian groups.

- $\delta(A, \mathbb{Z}_{p^\beta}) \leq \beta\, \delta(A, \mathbb{Z}_p)$.
- $\delta(A_1 \times A_2, B) \leq \delta(A_1, B) + \delta(A_2, B)$.

Known results on $\delta(A, B)$

$$\delta(A,B) := \sup\left(\{\textsf{FDEG}(f) \mid f \in B^A\}\right) = (\text{nilpotency index of } \operatorname{Aug}(\mathbb{Z}_{\exp(B)}[A])) - 1$$

$\delta(A,B)$	$B = \mathbb{Z}_p$	$B = \mathbb{Z}_{p^\beta}$

Known results on $\delta(A, B)$

$$\delta(A,B) := \sup\left(\{\textsf{FDEG}(f) \mid f \in B^A\}\right) = (\text{nilpotency index of } \operatorname{Aug}(\mathbb{Z}_{\exp(B)}[A])) - 1$$

$\delta(A, B)$	$B = \mathbb{Z}_p$	$B = \mathbb{Z}_{p^\beta}$
A is not a p-group	∞	∞

Known results on $\delta(A, B)$

$$\delta(A,B) := \sup\left(\{\mathrm{FDEG}(f) \mid f \in B^A\}\right) = (\text{nilpotency index of } \operatorname{Aug}(\mathbb{Z}_{\exp(B)}[A])) - 1$$

$\delta(A,B)$	$B = \mathbb{Z}_p$	$B = \mathbb{Z}_{p^\beta}$
A is not a p-group	∞	∞
$A = \mathbb{Z}_{p^\alpha}$	$p^\alpha - 1$ Karpilovsky 1987	

Known results on $\delta(A, B)$

$$\delta(A,B) := \sup\left(\{\textsf{FDEG}(f) \mid f \in B^A\}\right) = (\text{nilpotency index of } \operatorname{Aug}(\mathbb{Z}_{\exp(B)}[A])) - 1$$

$\delta(A, B)$	$B = \mathbb{Z}_p$	$B = \mathbb{Z}_{p^\beta}$
A is not a p-group	∞	∞
$A = \mathbb{Z}_{p^\alpha}$	$p^\alpha - 1$ Karpilovsky 1987	$\beta p^\alpha - (\beta - 1)p^{\alpha-1} - 1$ R. Wilson 2006

Known results on $\delta(A, B)$

$$\delta(A,B) := \sup(\{\text{FDEG}(f) \mid f \in B^A\}) = (\text{nilpotency index of } \operatorname{Aug}(\mathbb{Z}_{\exp(B)}[A])) - 1$$

$\delta(A,B)$	$B = \mathbb{Z}_p$	$B = \mathbb{Z}_{p^\beta}$
A is not a p-group	∞	∞
$A = \mathbb{Z}_{p^\alpha}$	$p^\alpha - 1$ Karpilovsky 1987	$\beta p^\alpha - (\beta - 1)p^{\alpha-1} - 1$ R. Wilson 2006
$A = (\mathbb{Z}_p)^n$	$n(p-1)$ Karpilovski 1987	

Known results on $\delta(A, B)$

$$\delta(A,B) := \sup\left(\{\text{FDEG}(f) \mid f \in B^A\}\right) = (\text{nilpotency index of } \operatorname{Aug}(\mathbb{Z}_{\exp(B)}[A])) - 1$$

$\delta(A, B)$	$B = \mathbb{Z}_p$	$B = \mathbb{Z}_{p^\beta}$
A is not a p-group	∞	∞
$A = \mathbb{Z}_{p^\alpha}$	$p^\alpha - 1$ Karpilovsky 1987	$\beta p^\alpha - (\beta - 1)p^{\alpha-1} - 1$ R. Wilson 2006
$A = (\mathbb{Z}_p)^n$	$n(p-1)$ Karpilovski 1987	$\leq \beta n(p-1)$

Known results on $\delta(A, B)$

$$\delta(A,B) := \sup\left(\{\text{FDEG}(f) \mid f \in B^A\}\right) = (\text{nilpotency index of } \operatorname{Aug}(\mathbb{Z}_{\exp(B)}[A])) - 1$$

$\delta(A,B)$	$B = \mathbb{Z}_p$	$B = \mathbb{Z}_{p^\beta}$
A is not a p-group	∞	∞
$A = \mathbb{Z}_{p^\alpha}$	$p^\alpha - 1$ Karpilovsky 1987	$\beta p^\alpha - (\beta-1)p^{\alpha-1} - 1$ R. Wilson 2006
$A = (\mathbb{Z}_p)^n$	$n(p-1)$ Karpilovski 1987	$\leq \beta n(p-1)$ $(\beta+n-1)(p-1)$

Known results on $\delta(A, B)$

$$\delta(A,B) := \sup\left(\{\mathrm{FDEG}(f) \mid f \in B^A\}\right) = (\text{nilpotency index of } \operatorname{Aug}(\mathbb{Z}_{\exp(B)}[A])) - 1$$

$\delta(A, B)$	$B = \mathbb{Z}_p$	$B = \mathbb{Z}_{p^\beta}$
A is not a p-group	∞	∞
$A = \mathbb{Z}_{p^\alpha}$	$p^\alpha - 1$ Karpilovsky 1987	$\beta p^\alpha - (\beta - 1)p^{\alpha-1} - 1$ R. Wilson 2006
$A = (\mathbb{Z}_p)^n$	$n(p-1)$ Karpilovski 1987	$\leq \beta n(p-1)$ $(\beta + n - 1)(p - 1)$
$A = \prod_{i=1}^n \mathbb{Z}_{p^{\alpha_i}}$	$\sum_{i=1}^n (p^{\alpha_i} - 1)$ Karpilovsky 1987	

Known results on $\delta(A, B)$

$$\delta(A,B) := \sup\left(\{\text{FDEG}(f) \mid f \in B^A\}\right) = (\text{nilpotency index of } \mathrm{Aug}(\mathbb{Z}_{\exp(B)}[A])) - 1$$

$\delta(A,B)$	$B = \mathbb{Z}_p$	$B = \mathbb{Z}_{p^\beta}$
A is not a p-group	∞	∞
$A = \mathbb{Z}_{p^\alpha}$	$p^\alpha - 1$ Karpilovsky 1987	$\beta p^\alpha - (\beta-1)p^{\alpha-1} - 1$ R. Wilson 2006
$A = (\mathbb{Z}_p)^n$	$n(p-1)$ Karpilovski 1987	$\leq \beta n(p-1)$ $(\beta+n-1)(p-1)$
$A = \prod_{i=1}^n \mathbb{Z}_{p^{\alpha_i}}$	$\sum_{i=1}^n (p^{\alpha_i} - 1)$ Karpilovsky 1987	$< \infty$ OPEN

Equations over abelian groups

Warning's First Theorem

Abstract version Warning's Sum Lemma

Let p be a prime, let A be a finite abelian p-group, $f : A \to \mathbb{Z}_p$.
If $\text{FDEG}(f) < \delta(A, \mathbb{Z}_p)$, then $\sum_{x \in A} f(x) = 0$.

Proof:

- Let $I := \langle \tau_a - 1 \mid a \in A \rangle = \mathrm{Aug}(\mathbb{Z}[A])$.
- $\mathbb{Z}[A] * \chi = \mathbb{Z}_p^A$ and $\mathbb{Z}[A] * \chi = \langle \chi \rangle_{\text{vector-space}} + I * \chi$. Hence $I * \chi$ has codim 1 in $\mathbb{Z}_p^A$.
- $I * \chi \subseteq \{f \mid \sum_{a \in A} f(a) = 0\}$ because $\sum_{x \in A} (\tau_a - 1) * f(x) = \sum_{x \in A} f(x + a) - f(x) = 0$.
- $I * \chi \subseteq \{f \mid \text{FDEG}(f) < \delta(A, \mathbb{Z}_p)\}$.
- Hence $\{f \mid \sum_{a \in A} f(a) = 0\} = \{f \mid \text{FDEG}(f) < \delta(A, \mathbb{Z}_p)\}$.

Warning's First Theorem

Theorem [EA, Moosbauer 2021]

Let p be a prime, let A be a finite abelian p-group with $|A| > 1$, and let $f_1, \ldots, f_r : A^n \to A$ be functions with

$$n > \sum_{i=1}^{r} \text{FDEG}(f_i).$$

Then p divides $v = |\{\boldsymbol{a} \in A^n \mid f_1(\boldsymbol{a}) = \cdots = f_r(\boldsymbol{a}) = 0\}|$.

Proof:

- $\chi : A \to \mathbb{Z}_p$ has degree $\delta(A, \mathbb{Z}_p)$.
- $\boldsymbol{a} \mapsto \prod_{i=1}^{r} \chi\left(f_i(a_1, \ldots, a_n)\right)$ has degree $\leq \sum_{i=1}^{r} \text{FDEG}(f_i)\, \delta(A, \mathbb{Z}_p)$.
- Hence $\boldsymbol{a} \mapsto \prod_{i=1}^{r} \chi(f_i(a_1, \ldots, a_n))$ has degree $< n\delta(A, \mathbb{Z}_p) = \delta(A^n, \mathbb{Z}_p)$.
- By the Sum-Lemma $[v]_p = \sum_{\boldsymbol{a} \in A^n} \prod_{i=1}^{r} \chi(f_i(a_1, \ldots, a_n)) = 0$.

Warning's First Theorem

Setting $A := F$, we obtain:

Theorem (Warning 1935; Moreno and Moreno 1995)

Let p be a prime, let F be a finite field of characteristic p, let $r, n \in \mathbb{N}$, and let $f_1, \ldots, f_r \in F[x_1, \ldots, x_n]$. We assume that $n > \sum_{j=1}^{r} \deg_p(f_j)$. Then p divides $|V(f_1, \ldots, f_r)|$.

Warning's First Thm for noncommutative rings [EA, Moosbauer 2021]

Let $p \in \mathbb{P}$, let $\alpha \in \mathbb{N}$, let R be a (not necessarily commutative) ring with $|R| = p^\alpha$, let $n \in \mathbb{N}$, let $X = \{x_1, \ldots, x_n\}$, and let $f_1, \ldots, f_r$ be polynomial expressions over R in the variables X. If $n > \sum_{i=1}^{r} \deg(f_i)$, then p divides $|V(f_1, \ldots, f_r)|$.

Warning's First Theorem with restricted domain

Restricted Domain versions have been established, e.g., by [P.L. Clark, 2014] and [D. Brink, 2011].

Theorem [EA, Moosbauer 2021]

Let p be a prime, $\alpha \in \mathbb{N}$, and let F be a finite field with $q = p^\alpha$ elements. Let $f_1, \ldots, f_r \in F[x_1, \ldots, x_n]$, let A be a subgroup of $(F^n, +)$ with p^M elements. We assume that

$$M > \alpha \sum_{j=1}^{r} \deg_p(f_j).$$

Then p divides the cardinality of $\{\boldsymbol{a} \in A \mid f_1(\boldsymbol{a}) = \cdots = f_r(\boldsymbol{a}) = 0\}$.

Warning's Second Theorem

Theorem (E. Warning, 1935)

F a finite field, $f_1, \ldots, f_s \in F[x_1, \ldots, x_n]$.
If $V(f_1, \ldots, f_s) \neq \varnothing$, then $\#V(f_1, \ldots, f_n) \geq |F|^{n - \sum_{i=1}^{s} \deg(f_i)}$.

Remarks:

1. Warning considered the case $s = 1$ (Satz 3).
2. The bound can be attained: $\#V(x_1, \ldots, x_s) = |F|^{n-s}$.

Warning's Second Theorem is useful

Let F be a finite field.

- The problem

  Input $f \in F[x_i \mid i \in \mathbb{N}]$ (possibly not in expanded form). **Output** YES iff $V(f) \neq \varnothing$

  is NP-complete.
- Its fixed parameter version for fixed degree D with

  Input $f \in F[x_i \mid i \in \mathbb{N}]$ with $\deg(f) \leq D$

  is in RP (randomized polynomial time). **Proof:** If f has N variables and is solvable, then a random $\boldsymbol{a} \in F^n$ is a solution with probability $\geq |F|^{-D}$.
- Such (and better) results were used in [Kawałek and Krzaczkowski, 2020] to provide a linear time Monte-Carlo algorithm to solve equations over nilpotent groups.

Improvements of Warning's Second Theorem

Theorem (E. Warning, 1935)

F a finite field, $f_1, \ldots, f_s \in F[x_1, \ldots, x_n]$.
If $V(f_1, \ldots, f_s) \neq \varnothing$, then $\#V(f_1, \ldots, f_s) \geq |F|^{n - \sum_{i=1}^{s} \deg(f_i)}$.

- [Heath-Brown, 2011]: if $V(f_1, \ldots, f_s)$ is not a linear manifold and $|F| \geq 4$, then $\#V(f_1, \ldots, f_n) \geq 2q^{n-d}$. ($q := |F|$, $d := \sum_{i=1}^{s} \deg(f_i)$)
- [Moreno Moreno 1995]: $\deg(f)$ can be replaced by the p-weight degree $\deg_p(f)$, where $p = \mathrm{char}(F)$,

$$\deg_p(x_1^{\alpha_1} \cdots x_N^{\alpha_N}) := \sum_{n=1}^{N} s_p(\alpha_n),$$

$s_p(n)$ is the digit sum in base p.

Warning's Second Theorem for abelian groups

Theorem (E. Warning, 1935)

F a finite field, $f_1, \dots, f_s \in F[x_1, \dots, x_n]$.

If $V(f_1, \dots, f_s) \neq \varnothing$, then $\#V(f_1, \dots, f_s) \geq |F|^{n - \sum_{i=1}^{s} \deg(f_i)}$.

Theorem [EA, Moosbauer 2021]

Let $f_1, \dots, f_r \colon {\mathbb{Z}_p}^{\alpha} \to {\mathbb{Z}_p}^{\beta}$. If $V(f_1, \dots f_r) \neq \varnothing$, then

$$\#V(f_1, \dots, f_r) \geq p^{\alpha - \beta \sum_{i=1}^{r} \textsc{Fdeg}(f_i)}.$$

Supernilpotency

Supernilpotent algebras

Definition

Let $k \in \mathbb{N}$. The algebra $\mathbf{A}$ is k-supernilpotent if

$\forall n_1, \ldots, n_{k+1} \in \mathbb{N}_0$, $\forall\ \sum_{i=1}^{k+1} n_i$-ary term functions t of $\mathbf{A}$,
$\forall \langle (a_1^{(i)}, a_2^{(i)}) \mid i \in \{1, \ldots, k+1\} \rangle \in \prod_{i=1}^{k} (A^{n_i} \times A^{n_i})$, the following holds:

If for all $f : \{1, \ldots, k\} \to \{1, 2\}$ such that f is not constantly 2, we have

$$t(a_{f(1)}^{(1)}, \ldots, a_{f(k)}^{(k)}, a_1^{(k+1)}) = t(a_{f(1)}^{(1)}, \ldots, a_{f(k)}^{(k)}, a_2^{(k+1)}),$$

then

$$t(a_2^{(1)}, \ldots, a_2^{(k)}, a_1^{(k+1)}) = t(a_2^{(1)}, \ldots, a_2^{(k)}, a_2^{(k+1)}).$$

Supernilpotent algebras

Definition

The algebra $\mathbf{A}$ is 1-supernilpotent if

$\forall n_1, n_2 \in \mathbb{N}_0$, $\forall\ n_1 + n_2$-ary term functions t of $\mathbf{A}$,
$\forall a_1^{(1)}, a_2^{(1)} \in A^{n_1},\ a_1^{(2)}, a_2^{(2)} \in A^{n_2}$, the following holds:

$$t(a_1^{(1)}, a_1^{(2)}) = t(a_1^{(1)}, a_2^{(2)}) \Longrightarrow t(a_2^{(1)}, a_1^{(2)}) = t(a_2^{(1)}, a_2^{(2)}).$$

Hence $\mathbf{A}$ is 1-supernilpotent iff it is abelian.

Supernilpotent algebras

Definition

The algebra $\mathbf{A}$ is 1-supernilpotent if

$\forall n_1, n_2 \in \mathbb{N}_0$, $\forall\ n_1 + n_2$-ary term functions t of $\mathbf{A}$,
$\forall \boldsymbol{a}, \boldsymbol{b} \in A^{n_1},\ \boldsymbol{c}, \boldsymbol{d} \in A^{n_2}$, the following holds:

$$t(\boldsymbol{a}, \boldsymbol{c}) = t(\boldsymbol{a}, \boldsymbol{d}) \Longrightarrow t(\boldsymbol{b}, \boldsymbol{c}) = t(\boldsymbol{b}, \boldsymbol{d}).$$

Hence $\mathbf{A}$ is 1-supernilpotent iff it is abelian.

Supernilpotent algebras

Definition

The algebra $\mathbf{A}$ is 2-supernilpotent if

$\forall n_1, n_2, n_3 \in \mathbb{N}_0$, $\forall \sum_{i=1}^{3} n_i$-ary term functions t of $\mathbf{A}$,
$\forall \langle (\boldsymbol{a}^{(i)}, \boldsymbol{b}^{(i)}) \mid i \in \{1, \ldots, 3\} \rangle \in \prod_{i=1}^{k} (A^{n_i} \times A^{n_i})$, the following holds:

$$\left.\begin{array}{l} t(\boldsymbol{a}^{(1)}, \boldsymbol{a}^{(2)}, \boldsymbol{a}^{(3)}) = t(\boldsymbol{a}^{(1)}, \boldsymbol{a}^{(2)}, \boldsymbol{b}^{(3)}) \\ t(\boldsymbol{b}^{(1)}, \boldsymbol{a}^{(2)}, \boldsymbol{a}^{(3)}) = t(\boldsymbol{b}^{(1)}, \boldsymbol{a}^{(2)}, \boldsymbol{b}^{(3)}) \\ t(\boldsymbol{a}^{(1)}, \boldsymbol{b}^{(2)}, \boldsymbol{a}^{(3)}) = t(\boldsymbol{a}^{(1)}, \boldsymbol{b}^{(2)}, \boldsymbol{b}^{(3)}) \end{array}\right\} \Longrightarrow t(\boldsymbol{b}^{(1)}, \boldsymbol{b}^{(2)}, \boldsymbol{a}^{(3)}) = t(\boldsymbol{b}^{(2)}, \boldsymbol{b}^{(2)}, \boldsymbol{b}^{(3)}).$$

Comments on “supernilpotent”

- Supernilpotent expanded groups were defined in [Aichinger, Ecker 2006].
- Supernilpotent algebras were defined in [Aichinger, Mudrinski 2010] as those satisfying $[1, \ldots, 1] = 0$ for the higher commutator operation from [Bulatov 2001].
- For algebras with Mal’cev term, supernilpotent implies nilpotent (nested commutator property (HC8)) [EA, Mudrinski 2010].
- Supernilpotent $\Rightarrow$ Nilpotent:
  - not true in general [Moore, Moorhead 2019].
  - true for finite algebras [Kearnes, Szendrei 2020] and Taylor algebras [Wires 2019 and Moorhead 2021].

Supernilpotent algebras

Theorem

Let $k \in \mathbb{N}$, $\mathbf{A}$ an algebra. TFAE:

1. $\mathbf{A}$ is k-supernilpotent.
2. $\mathbf{A}$ satisfies $[1, \ldots, 1] = 0$ ($k + 1$ times 1).

Supernilpotent algebras in congruence modular varieties

Definition

A term $w(x_1, \dots, x_{r+1})$ in the language of $\mathbf{A}$ is a commutator term of rank r for $\mathbf{A}$ if

$$\mathbf{A} \models w(z, x_2, \dots, x_r, z) \approx w(x_1, z, \dots, x_r, z) \approx \cdots \approx w(x_1, x_2, \dots, z, z) \approx z.$$

A commutator term $w(x_1, \dots, x_{r+1})$ is called trivial if $\mathbf{A} \models w(x_1, \dots, x_r, z) \approx z$.

A commutator term in the language of ($\mathbf{A}$ + constants) is a commutator polynomial.

Supernilpotent algebras

Theorem

Let $k \in \mathbb{N}$, $\mathbf{A}$ an algebra in a congruence modular variety. TFAE:

1. $\mathbf{A}$ is k-supernilpotent.
2. $\mathbf{A}$ is nilpotent, and all nontrivial commutator polynomials are of rank $\leq k$.

For (1)$\Rightarrow$(2), [Wires 2019] produces a Mal'cev term. Then apply [EA, Mudrinski 2010].

Two descriptions of supernilpotency in cp varieties in terms of

- identities (as opposed to quasi-identities),
- invariant relations

can be found in [Opršal 2016].

Supernilpotent algebras

Theorem

Let $k \in \mathbb{N}$, $\mathbf{A}$ a finite algebra in a congruence modular variety. TFAE:

1. $\mathbf{A}$ is k-supernilpotent.
2. $\mathbf{A}$ is nilpotent, and all nontrivial commutator terms are of rank $\leq k$.
3. $f(n) = \log_2(|\mathrm{Clo}_n(\mathbf{A})|)$ is a polynomial of degree k.

Proof: Use [Berman, Blok 1987], [Freese, McKenzie 1987], [Hobby McKenzie 1988], [EA, Mudrinski 2010], [Wires 2019].

Supernilpotent expanded groups

Theorem

Let $k \in \mathbb{N}$, $\mathbf{A}$ an expanded group. TFAE:

1. $\mathbf{A}$ is k-supernilpotent.
2. For every $p \in \mathsf{Pol}_{k+1}(\mathbf{A})$ with

$$\forall a_1, \ldots, a_{k+1} : 0 \in \{a_1, \ldots, a_{k+1}\} \Rightarrow p(a_1, \ldots, a_{k+1}) = 0$$

   we have $\forall \boldsymbol{a} \in A^{k+1} : p(\boldsymbol{a}) = 0$. (Every nonzero absorbing polynomial function has at most k arguments).

Supernilpotent expanded abelian groups

Theorem

Let $k \in \mathbb{N}$, $\mathbf{A}$ an expansion of an abelian group. TFAE:

1. $\mathbf{A}$ is k-supernilpotent.
2. Every nonzero absorbing polynomial function has at most k arguments.
3. Every function in $\mathrm{Clo}(\mathbf{A})$ has functional degree at most k.

Theorem

Let $k \in \mathbb{N}$, $\mathbb{A}$ a field, and let $\mathbf{A} = (A, +, -, 0, F)$ with $F \subseteq$ Pol$(\mathbb{A})$. TFAE:

1. $\mathbf{A}$ is k-supernilpotent.
2. Every nonzero absorbing polynomial function has at most k arguments.
3. Every function in $\mathrm{Clo}(\mathbf{A})$ has functional degree at most k.
4. Every function in $\mathrm{Clo}(\mathbf{A})$ can be represented by a polynomial in $\mathbb{A}[x_1, x_2 \ldots]$ each of whose monomials contains only k variables.

The Structure of Supernilpotent Algebras

Structure of supernilpotent algebras

Theorem [Kearnes 1999], [Berman, Blok 1987], [Freese, McKenzie 1987]

$\mathbf{A}$ in a cm variety, finitely many basic operations. Then $\mathbf{A}$ is supernilpotent $\iff$ $\mathbf{A}$ is nilpotent and isomorphic to a product of algebras of prime power order.

Our goal: Find f such that
k-nilpotent and prime power order $\implies f(k,.)$-supernilpotent.

Bounds on the supernilpotency degree

Examples:

- k-nilpotent groups and rings are k-supernilpotent.
- For each $k \in \mathbb{N}$ and $m \geq 2$, there is a k-nilpotent expanded group of of supernilpotency class m^{k-1} [EA, Mudrinski 2013].

We will now outline a proof of
nilpotent & prime power order $\Longrightarrow$ supernilpotent.
Can we do it for

- Expanded groups?
- Expansions of elementary abelian groups = reducts of fields?

Reducts of Fields

Clones of polynomials

For $A, B \subseteq \mathbb{K}[x_i \mid i \in \mathbb{N}] = \bigcup_{n\in\mathbb{N}} \mathbb{K}[x_1, \ldots, x_n]$, we define (following [Couceiro, Foldes 2009])

$$AB = \{p(q_1, \ldots, q_n) \,\big|\, n \in \mathbb{N}, p \in A \cap \mathbb{K}[x_1, \ldots, x_n], q_1, \ldots, q_n \in B\}.$$

$C \subseteq \mathbb{K}[x_i \mid i \in \mathbb{N}]$ is a **clone of polynomials** if for each $i \in \mathbb{N}$, $x_i \in C$ and $CC \subseteq C$.

A polynomial f is **homovariate** if all of its monomials contain the same variables.

- $5x_1x_2^3x_4 - 2x_1^{17}x_2x_4^3 + x_1^6x_2^3x_4^{20}$, $x_2 + 6x_2^4$, and 2 are all homovariate.
- None of $x_1 + x_2$, $1 + 3x_1^3 + x_1^5$ is homovariate.

Clones of polynomials

The function defined by

$$f(x_1, x_2, x_4) := 5x_1x_2^3x_4 - 2x_1^{17}x_2x_4^3 + x_1^6x_2^3x_4^{20}$$

is **absorbing**, meaning that $f(0, y, z) = f(x, 0, z) = f(x, y, 0) = 0$ for all x, y, z.

Theorem [EA, 2019]

Let $\mathbb{K}$ be a field, let $F \subseteq \mathbb{K}[x_i \mid i \in \mathbb{N}]$, $\deg(f) \leq n$ for all $f \in F$. Let $L := \mathrm{Clop}(\{x_1+x_2, -x_1, 0\})$. Then there exists a set $H \subseteq \mathbb{K}[x_1, \ldots, x_n]$ of homovariate polynomials such that

$$L\ \mathrm{Clop}(H) = \mathrm{Clop}(F \cup \{x_1 + x_2, -x_1, 0\})$$

and $\deg(h) \leq n$ for all $h \in H$.

Nilpotency and Supernilpotency

Let C be a clone of polynomials on $\mathbb{K}$ that contains $x_1 + x_2$ and $-x_1$. Let $H \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be such that all $h \in H$ are homovariate, and $L\ \mathrm{Clop}(H) = C$.

- If the algebra $\mathbf{K} = (\mathbb{K}, \overline{C})$ is k**-nilpotent**, then each function in $\overline{\mathrm{Clop}(H)}$ depends on $\leq n^{k-1}$ arguments.
- The algebra $\mathbf{K} = (\mathbb{K}, \overline{C})$ is s**-supernilpotent** if each absorbing polynomial function of $\mathbf{K}$ depends on $\leq s$ arguments.

On the implication nilpotent $\Rightarrow$ supernilpotent

Let C be a clone of polynomials on $\mathbb{K}$ that contains $x_1 + x_2$ and $-x_1$.
Let $H \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be such that all $h \in H$ are homovariate, and
$L \ \mathrm{Clop}(H) = C$.

Then:

$\mathbf{K} = (\mathbb{K}, \overline{C})$ is k-nilpotent
$\Rightarrow$ each function in $\overline{\mathrm{Clop}(H)}$ depends on $\leq n^{k-1}$ arguments
$\Rightarrow$ each absorbing polynomial function of $\mathbf{K} = (K, \overline{L \ \mathrm{Clop}(H)})$
depends on $\leq n^{k-1}$ arguments
$\Rightarrow$ $\mathbf{K}$ is n^{k-1}-supernilpotent.

Expansions of additive groups of fields

Theorem

Let $(A, +, *)$ be a field, and let $\mathbf{A} = (A, +, -, 0, (f_i)_{i \in I})$ be an algebra. Assume

- For each $i \in I$, $\deg(f_i) \leq n$,
- $\mathbf{A}$ is nilpotent of class at most k.

Then all absorbing polynomial functions of $\mathbf{A}$ are of essential arity at most n^{k-1}.

Theorem [EA, 2019]

Let $\mathbb{A} = (A, +, *)$ be a field, and let $\mathbf{A} = (A, +, -, 0, (f_i)_{i \in I})$ be an expansion of $(A, +)$ with polynomial functions of $\mathbb{A}$ of total degree $\leq n$. Then:

- If $\mathbf{A}$ is k-nilpotent, it is n^{k-1}-supernilpotent.

Coordinatization

Coordinatization

We have seen a result on the structure of **nilpotent expansions of** $((\mathbb{Z}_p)^n, +)$.

It would be nice to have a result on **nilpotent algebras of prime power order in congruence modular varieties**.

To this end, we will expand such algebras with a group operation.

Coordinatization

Theorem. Let $\mathbf{A} = (A, (f_i)_{i \in \mathbb{N}})$ be a nilpotent algebra in a congruence modular variety, $|A| = p^n$ with p prime.

Then there exists $+ : A \times A \to A$ and $* : A \times A \to A$ such that

- $(A, +, *)$ is a field and hence $(A, +) \cong (\mathbb{Z}_p^n, +)$.
- $\mathbf{A}' = (A, (f_i)_{i \in \mathbb{N}}, +)$ is nilpotent.

Structure of nilpotent algebras

Theorem

Let $\mathbf{A}$ be a finite nilpotent algebra in a congruence modular variety that is a direct product of algebras of prime power order, with all fundamental operations of arity at most m, $|A| > 1$. Let

$$s := \big(m(|A| - 1)\big)^{(\log_2(|A|)-1)}.$$

Then $\mathbf{A}$ is s-supernilpotent and there is a polynomial $p \in \mathbb{R}[x]$ of degree $\leq s$ such that the free spectrum satisfies

$$f_{\mathbf{A}}(n) = \mathrm{Clo}_n(\mathbf{A}) = 2^{p(n)} \text{ for all } n \in \mathbb{N}.$$

Theorem (Vaughan-Lee 1983, Freese McKenzie 1987, EA+JM 2019)

$\mathbf{A}$: nilpotent, in cm variety, prime power order $q = p^\alpha$, all fundamental operations at most m-ary. $h :=$ height of Con$(\mathbf{A})$.
Then $\mathbf{A}$ is supernilpotent of degree at most $\big(m\,\alpha(p-1)\big)^{h-1}$.

- The old bound was $\big(m(p^\alpha - 1)\big)^{h-1}$.
- We can take h as the p-nilpotency degree of $\mathbf{A}$.

Written Material:

- E. Aichinger. Bounding the free spectrum of nilpotent algebras of prime power order. *Israel Journal of Mathematics* 230 (2019): 919-947.
- E. Aichinger and J. Moosbauer, Chevalley-Warning type results on abelian groups, *Journal of Algebra* 569 (2021): 30-66.