THE DEGREE OF A FUNCTION BETWEEN TWO ABELIAN GROUPS

Erhard Aichinger and Jakob Moosbauer
Institute for Algebra
Austrian Science Fund FWF P29931

JOHANNES KEPLER
UNIVERSITY LINZ

Theorems involving the degree

Theorem (Chevalley 1935)

F a finite field, $f_1, \ldots, f_s \in F[x_1, \ldots, x_N]$.
If $\#\{\mathbf{a} \in F^N \mid f_i(\mathbf{a}) = \cdots = f_s(\mathbf{a}) = 0\} = 1$, then $\sum_{i=1}^{s} \deg(f_i) \geq N$.

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

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

The factor $m(q-1)$ is the maximal total degree of an m-ary reduced polynomial on $\mathbb{F}_q$. This factor therefore appears in the exponents of the polynomials bounding the complexity of PolSat$(\mathbf{A})$, PolEqv$(\mathbf{A})$ and k-PolSysSat$(\mathbf{A})$ for supernilpotent $\mathbf{A}$.

Definition of the degree for functions

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

- Define $\textsc{Fdeg}(f)$.
- 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 $a \in A$, $\Delta_a(f)\,(x) := f(x+a) - f(x)$.
- 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 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]

- 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]

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

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

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

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 $\textsc{FDeg}(f)$ to be the smallest $m \in \mathbb{N}_0$ such that

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

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

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

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

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 $\textsc{Fdeg}(\overline{f})$ 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

$\mathbb{F}_q$ a finite field of characteristic p, $f \in F[x_1, \ldots, x_n]$ with all exponents at most $q-1$. Then FDEG$(\overline{f}) = \deg_p(f)$.

Properties of the functional degree

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

Lemma

- $\textsc{Fdeg}(f + g) \leq \max(\textsc{Fdeg}(f), \textsc{Fdeg}(g))$.
- If $(B, +, \cdot)$ is a ring, then $\textsc{Fdeg}(f \cdot g) \leq \textsc{Fdeg}(f) + \textsc{Fdeg}(g)$.

Properties of the functional degree

Theorem (EA+JM 2019)

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

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 FDEG$(h) \leq 2$.

Functions of finite degree

Proposition

A, B finite abelian groups of coprime order, $C := A \times B$, $f : C^N \to C$ of finite degree. Then there are $g : A^N \to A$, $h : B^N \to B$ such that $f(\boldsymbol{a}, \boldsymbol{b}) = (g(\boldsymbol{a}), h(\boldsymbol{b}))$ for all $\boldsymbol{a} \in A^N$, $\boldsymbol{b} \in B^N$.

Proposition

An expansion of an abelian group is k-supernilpotent iff every function in its clone has functional degree at most k.

Hence finite supernilpotent expanded groups decompose into a product of prime power order expanded groups [Kearnes 1999].

Functions of maximal degree

Proposition

Let A, B be finite abelian groups. Then $\delta(A,B) := \max\{\text{FDEG}(f) \mid f : A \to B\} = \nu - 1$, where ν is the nilpotency degree of the augmentation ideal of $\mathbb{Z}_e[A]$ and $e := \exp(B)$.

Corollary

Let $p \in \mathbb{P}$, $A := \prod_{i=1}^{k} \mathbb{Z}_{p^{\alpha_i}}$, B abelian group of exponent p^β. Then

- $\delta(A,B) \leq (1 + \sum_{i=1}^{k}(p^{\alpha_i} - 1))\beta - 1$. [Karpilovsky 1987]
- $\delta(A,B) \leq \beta \sum_{i=1}^{k}(p^{\alpha_i} - 1)$.
- $\delta(A,\mathbb{Z}_p) = \sum_{i=1}^{k}(p^{\alpha_i} - 1)$. (Bound is sharp for $\beta = 1$)

Functions of maximal degree

Problem

For a finite abelian p-group $A = \prod_{i=1}^{k} \mathbb{Z}_{p^{\alpha_i}}$ and $\beta \in \mathbb{N}$, find the nilpotency degree ν of the augmentation ideal of $\mathbb{Z}_{p^\beta}[A]$.

Known: $1 + \sum_{i=1}^{k}(p^{\alpha_i} - 1) \leq \nu \leq 1 + \beta \sum_{i=1}^{k}(p^{\alpha_i} - 1)$.
Speculation from very few computations: For cylic $A = \mathbb{Z}_{p^\alpha}$, we have $\nu = \beta p^\alpha - (\beta - 1)p^{\alpha-1}$.

Applications

- Generalizations of the Chevalley Warning Theorems on the zeroes of polynomials ($\rightsquigarrow$ Jakob Moosbauer's talk).
- Improvements of the bounds in the

  nilpotent, finite type, prime power order $\Rightarrow$ *supernilpotent*

  Theorems, and hence in the exponents for PolSat($\mathbf{A}$), PolEqv($\mathbf{A}$) and k-PolSysSat($\mathbf{A}$) for supernilpotent $\mathbf{A}$.

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 $\big(m(p^\alpha - 1)\big)^{h-1}$.

More information on the functional degree:

Erhard Aichinger, Jakob Moosbauer: Chevalley Warning type results on abelian groups. arXiv 2019.