WHEN IS THE VALUE OF A POLYNOMIAL DETERMINED BY THE VALUE OF OTHER POLYNOMIALS?

Erhard Aichinger, Institute for Algebra, Johannes Kepler University Linz
Supported by the Austrian Science Fund FWF : P33878
DMV-ÖMG Annual Conference 2021, Passau, September 2021

JOHANNES KEPLER UNIVERSITY LINZ

Outline

- We will investigate polynomials $g(t_1, \ldots, t_n)$ over algebraically closed fields whose values $g(\boldsymbol{a})$ are fully determined by the values $f_1(\boldsymbol{a}), \ldots, f_m(\boldsymbol{a})$ of some given polynomials.
- Often g is then a polynomial or rational function in $f_1, \ldots, f_m$.
- We are going to specify "often".

Determined Polynomials

Determined Polynomials

k field, $\quad m, n \in \mathbb{N}, \quad g, f_1, \ldots, f_m \in k[t_1, \ldots, t_n]$.

Definition. g is determined by $\boldsymbol{f} = (f_1, \ldots, f_m)$ if for all $\boldsymbol{a}, \boldsymbol{b} \in k^n$:

$$f_1(\boldsymbol{a}) = f_1(\boldsymbol{b}) \wedge \cdots \wedge f_m(\boldsymbol{a}) = f_m(\boldsymbol{b}) \implies g(\boldsymbol{a}) = g(\boldsymbol{b}).$$

Hence g is determined by $\boldsymbol{f}$ if and only if $\exists h : k^m \to k$ such that

$$g(\boldsymbol{a}) = h(f_1(\boldsymbol{a}), \ldots, f_m(\boldsymbol{a})) \text{ for all } \boldsymbol{a} \in k^n.$$

Examples of determined polynomials

- $t_1(t_1t_2)^2 - 3t_1^2(t_1t_2)$ is determined by $(t_1,\, t_1t_2)$.

Examples of determined polynomials

- $t_1(t_1t_2)^2 - 3t_1^2(t_1t_2)$ is determined by $(t_1,\, t_1t_2)$.
- Every $g \in k[f_1, \ldots, f_m]$ is $(f_1, \ldots, f_m)$-determined.

Examples of determined polynomials

- $t_1(t_1t_2)^2 - 3t_1^2(t_1t_2)$ is determined by (t_1, t_1t_2).
- Every $g \in k[f_1, \ldots, f_m]$ is $(f_1, \ldots, f_m)$-determined.
- $(k = \mathbb{C})$: $\frac{(t_1t_2)^2}{t_1} = t_1t_2^2$ is determined by (t_1, t_1t_2).

```
In[1]:= GroebnerBasis [ {a1 - b1, a1*a2 - b1*b2, -1 + (a1*a2^2 - b1*b2^2)*z} ]
Out[1]= {1}
```

Examples of determined polynomials

- $t_1(t_1t_2)^2 - 3t_1^2(t_1t_2)$ is determined by $(t_1,\, t_1t_2)$.
- Every $g \in k[f_1, \ldots, f_m]$ is $(f_1, \ldots, f_m)$-determined.
- $(k = \mathbb{C})$: $\frac{(t_1t_2)^2}{t_1} = t_1t_2^2$ is determined by $(t_1,\, t_1t_2)$.

```
In[1]:= GroebnerBasis [ {a1 - b1, a1*a2 - b1*b2, -1 + (a1*a2^2 - b1*b2^2)*z} ]
Out[1]= {1}
```

- $(k = \mathbb{C})$: $\frac{t_1t_2}{t_1} = t_2$ is not determined by $(t_1,\, t_1t_2)$

```
In[2]:= GroebnerBasis [ {a1 - b1, a1 a2 - b1 b2, -1 + (a2 - b2) z} ]
Out[2]= {-1 + a2 z - b2 z, b1, a1}
```

$\boldsymbol{a} = (0, 0)$, $\boldsymbol{b} = (0, 1)$ are witnesses.

Examples of determined polynomials

- $t_1(t_1t_2)^2 - 3t_1^2(t_1t_2)$ is determined by $(t_1,\, t_1t_2)$.
- Every $g \in k[f_1, \ldots, f_m]$ is $(f_1, \ldots, f_m)$-determined.
- $(k = \mathbb{C})$: $\frac{(t_1t_2)^2}{t_1} = t_1t_2^2$ is determined by $(t_1,\, t_1t_2)$.

```
In[1]:= GroebnerBasis [ {a1 - b1, a1*a2 - b1*b2, -1 + (a1*a2^2 - b1*b2^2)*z} ]
Out[1]= {1}
```

- $(k = \mathbb{C})$: $\frac{t_1t_2}{t_1} = t_2$ is not determined by $(t_1,\, t_1t_2)$

```
In[2]:= GroebnerBasis [ {a1 - b1, a1 a2 - b1 b2, -1 + (a2 - b2) z} ]
Out[2]= {-1 + a2 z - b2 z, b1, a1}
```

  $\boldsymbol{a} = (0, 0)$, $\boldsymbol{b} = (0, 1)$ are witnesses.

- $g \in k(f_1, \ldots, f_m) \cap k[t_1, \ldots, t_n]$ provides no verdict on determinateness.

Examples of determined polynomials

- $(k = \mathbb{R})$: t is determined by t^3.

Examples of determined polynomials

- ($k = \mathbb{R}$) : t is determined by t^3.
- (k algebraically closed, characteristic $p > 0$) : $t^2 + 1$ is determined by $(t^2 + 1)^p$.

Determined $\Rightarrow$ rational function

Determined $\Rightarrow$ rational function

Theorem (EA 2015)

k ac field of char 0, $m, n \in \mathbb{N}$, $f_1, \ldots, f_m \in k[t_1, \ldots, t_n]$ algebraically independent over k. Then every $(f_1, \ldots, f_m)$-determined polynomial g lies in

$$k(f_1, \ldots, f_m) \cap k[t_1, \ldots, t_n].$$

Proof

- $P = \{(f_1(\boldsymbol{a}), \ldots, f_m(\boldsymbol{a})) \mid \boldsymbol{a} \in k^n\}$ is Zariski-dense in k^m,
- $D = \{(f_1(\boldsymbol{a}), \ldots, f_m(\boldsymbol{a}), g(\boldsymbol{a})) \mid \boldsymbol{a} \in k^n\}$ satisfies $\dim(\overline{D}) = m$.
  We use that g is $\boldsymbol{f}$-determined and that $\overline{D} = D \cup W$, where W is algebraic and $\dim(W) \leq m - 1$ (Closure Theorem).
- The minimal polynomial of g over $k[f_1, \ldots, f_m]$ has degree 1.
  Geometric intuition: degree of $\overline{D}$ should be 1.

Determined $\Rightarrow$ rational function

Theorem (EA 2015)

k ac field of char $p > 0$, $m, n \in \mathbb{N}$,
$f_1, \dots, f_m \in k[t_1, \dots, t_n]$ algebraically independent over k.
Then for every $(f_1, \dots, f_m)$-determined polynomial g there is $\nu \in \mathbb{N}$ with

$$g^{p^\nu} \in k(f_1, \dots, f_m) \cap k[t_1, \dots, t_n].$$

Proof

- Additional case: The minimal polynomial μ of g over $k[f_1, \dots, f_m]$ may have degree > 1.
- Then $\mu \in k[t^p]$.
- Repeat for g^p (induction).

Determined $\Rightarrow$ polynomial

Determined $\Rightarrow$ polynomial

- Limitation: $g = \frac{(t_1 t_2)^2}{t_1} = t_1 t_2^2$ is determined by $(t_1,\, t_1 t_2)$, but $g \notin \mathbb{C}[t_1,\, t_1 t_2]$.
- Reason: Each monomial μ in a $p \in \mathbb{C}[t_1,\, t_1 t_2]$ satisfies $\deg_{t_1}(\mu) \geq \deg_{t_2}(\mu)$.
- The mapping $\boldsymbol{f} : (x_1, x_2) \mapsto (x_1,\, x_1 x_2)$ satisfies

$$\begin{aligned}
\mathrm{range}(f) &= \mathbb{C}^2 \setminus \Big(\{(0,y) \mid y \in \mathbb{C}\} \setminus \{(0,0)\} \Big), \\
\mathbb{C}^2 \setminus \mathrm{range}(f) &= \{(0,y) \mid y \in \mathbb{C}\} \setminus \{(0,0)\}), \\
\dim(\mathbb{C}^2 \setminus \mathrm{range}(f)) &= 1 \not\leq 0.
\end{aligned}$$

- Key property: $\dim(\mathbb{C}^m \setminus \mathrm{range}(f)) \leq m - 2$.

Almost surjective maps

Definition. k ac field, $\boldsymbol{f} = (f_1, \dots, f_m) \in (k[t_1, \dots, t_n])^m$.
$\boldsymbol{f}$ is almost surjective on k : $\iff \dim(\overline{k^m \setminus \operatorname{range}(\boldsymbol{f})}) \leq m - 2$.

Almost surjective maps exist:

- $(t_1^3,\ t_2^2 - t_2 + 1)$ is surjective ($\dim(\varnothing) := -1$), hence almost surjective.
- ($k = \mathbb{C}$) : $\boldsymbol{f} = \begin{pmatrix} t_1 \\ t_2 \\ t_1 t_3 + t_2 t_4 \end{pmatrix}$ satisfies $\mathbb{C}^3 \setminus \{(0,0,z) \mid z \in \mathbb{C}\} \subseteq \operatorname{range}(\boldsymbol{f})$, $\dim(\overline{\mathbb{C}^m \setminus \operatorname{range}(\boldsymbol{f})}) = 1 \leq 3 - 2$. Hence $\boldsymbol{f}$ is almost surjective.
- ($k = \mathbb{C}$) : $(t_1,\ t_1 t_2)$ is not almost surjective.
- $(f_1, \dots, f_m)$ almost surjective $\Longrightarrow (f_1, \dots, f_m)$ are algebraically independent over k, and $\operatorname{range}(\boldsymbol{f})$ is Zariski-dense in k^m.

Determined $\Rightarrow$ polynomial

Theorem (EA 2015)

k ac field of char 0, $m, n \in \mathbb{N}$, $\boldsymbol{f} = (f_1, \ldots, f_m) \in k[t_1, \ldots, t_n]^m$ algebraically independent over k. TFAE:

1. Every $\boldsymbol{f}$-determined polynomial g lies in $k[f_1, \ldots, f_m]$.
2. $\boldsymbol{f}$ is almost surjective.

Proof of (2)$\Rightarrow$ (1):

- From above: $g \in k(f_1, \ldots, f_m)$.
- Main Lemma: $\boldsymbol{f}$ almost surjective $\Longrightarrow$
  $k(f_1, \ldots, f_m) \cap k[t_1, \ldots, t_n] = k[f_1, \ldots, f_m]$.
  Adaption of [van den Essen (2000), Theorem 4.2.1].

There is a version for characteristic p.

Compositions that are polynomials

Compositions that are polynomials

Corollary (Folklore) Let $h : \mathbb{C} \to \mathbb{C}$ be an arbitrary function, and let $f \in \mathbb{C}[t]$ nonconstant.
If $h \circ f$ is a polynomial function, then h is a polynomial function.

- Hence $\sqrt[3]{x} \circ x^{12} = x^4$ works in $\mathbb{R}$, but not in $\mathbb{C}$.

Theorem (EA 2015)

k ac field of char 0, $m, n \in \mathbb{N}$, $\boldsymbol{f} = (f_1, \ldots, f_m) \in k[t_1, \ldots, t_n]^m$ such that $\boldsymbol{f}$ is almost surjective,
$h : k^m \to k$ arbitrary mapping.
If $h \circ \boldsymbol{f}$ is a polynomial function (from k^n to k), then h is a polynomial (on the range of $\boldsymbol{f}$).

Theorem (EA 2015)

k ac field of char $p > 0$, $m, n \in \mathbb{N}$, $\boldsymbol{f} = (f_1, \ldots, f_m) \in k[t_1, \ldots, t_n]^m$ such that $\boldsymbol{f}$ is almost surjective,
$h : k^m \to k$ arbitrary mapping.
If $h \circ \boldsymbol{f}$ is a polynomial function (from k^n to k), then there is a polynomial $H(x_1, \ldots, x_m) \in k[x_1, \ldots, x_m]$ and $\nu \in \mathbb{N}$ such that

$$h(\boldsymbol{b}) = \sqrt[p^\nu]{H(\boldsymbol{b})} \text{ for all } \boldsymbol{b} \in k^m.$$

Didactical application

Corollary. If $f \in \mathbb{C}[t_1,\, t_2, t_3]$ satisfies $f(t_1, t_2, t_3) = f(t_{\pi(1)}, t_{\pi(2)}, t_{\pi(3)})$ for all $\pi \in S_3$, then there is $p \in \mathbb{C}[x_1, x_2, x_3]$ such that $f = p(t_1 + t_2 + t_3, t_1t_2 + t_1t_3 + t_2t_3, t_1t_2t_3)$.

Proof.

- $\boldsymbol{s} = \begin{pmatrix} t_1 + t_2 + t_3 \\ t_1t_2 + t_1t_3 + t_2t_3 \\ t_1t_2t_3 \end{pmatrix}$ is surjective:
  for finding the pre-image of $(\gamma_1, \gamma_2, \gamma_3)$, factor $x^3 + \gamma_1 x^2 + \gamma_2 x + \gamma_3$ into $(x + \tau_1)(x + \tau_2)(x + \tau_3)$.
- Since f is symmetric, f is determined by $(t_1 + t_2 + t_3,\ t_1t_2 + t_1t_3 + t_2t_3,\ t_1t_2t_3)$.
- Hence $\exists p \in \mathbb{C}[x_1, x_2, x_3] : f = p \circ \boldsymbol{s}$.

Further development: when the range of f is not dense

Open questions

Can "algebraic independence" be dropped? (Jaime Gutierrez)

Lemma (EA 2021)

k ac field, let $m, n \in \mathbb{N}$, and let $f_1, \ldots, f_m, g \in k[t_1, \ldots, t_n]$. We assume that for all $(y_1, \ldots, y_m) \in k^m$, the set

$$\{g(\boldsymbol{a}) \mid \boldsymbol{a} \in k^n, f_1(\boldsymbol{a}) = y_1, \ldots, f_m(\boldsymbol{a}) = y_m\}$$

is finite. Then g is algebraic over $k[f_1, \ldots, f_m]$.

Question: Is the following true (in char 0)?

If all the sets have at most 1 element, then $g \in k(f_1, \ldots, f_m)$.

Question with probably known answer

The example of an almost surjective and not surjective mapping was $\mathbb{C}^4 \to \mathbb{C}^3$,

$$(t_1, t_2, t_3, t_4) \mapsto \begin{pmatrix} t_1 \\ t_2 \\ t_1 t_3 + t_2 t_4 \end{pmatrix}.$$

Question: Is there an almost surjective and not surjective polynomial mapping from $\mathbb{C}^m$ to $\mathbb{C}^m$? (This means $\dim(\mathbb{C}^m \setminus \mathrm{range}(\boldsymbol{f})) \leq m - 2$.)

Question with probably known answer

The example of an almost surjective and not surjective mapping was $\mathbb{C}^4 \to \mathbb{C}^3$,

$$(t_1, t_2, t_3, t_4) \mapsto \begin{pmatrix} t_1 \\ t_2 \\ t_1 t_3 + t_2 t_4 \end{pmatrix}.$$

Question: Is there an almost surjective and not surjective polynomial mapping from $\mathbb{C}^m$ to $\mathbb{C}^m$? (This means $\dim(\mathbb{C}^m \setminus \operatorname{range}(\boldsymbol{f})) \leq m - 2$.)
Partial answers:

- **No** for $m = 1$.
- For $m = 2$, we would need a mapping $\boldsymbol{f} : \mathbb{C}^2 \to \mathbb{C}^2$ with cofinite range.

Written Material

Most results in this talk can be found in

E. Aichinger. On function compositions that are polynomials. *Journal of Commutative Algebra*, **7**(3) : 303-315, 2015.