University of Antwerp
Faculty of Science

How many quantifiers are needed to existentially define a given subset of a field?

Based on joint work with Arno Fehm & Philip Dittmann

Nicolas Daans

18 June 2021

Existentially definable subsets

Let K be a field, $D \subseteq K^n$ for some $n \in \mathbb{N}$.
D is called *existentially definable (in K^n)* if $D = \varphi(K)$ for some existential formula φ in n free variables in the first-order language of rings with parameters from K.

Existentially definable subsets

Let K be a field, $D \subseteq K^n$ for some $n \in \mathbb{N}$.
D is called *existentially definable (in K^n)* if $D = \varphi(K)$ for some existential formula φ in n free variables in the first-order language of rings with parameters from K.

Equivalently,

$$D = \{\underline{x} \in K^n \mid f_1(\underline{x}, \underline{Y}), \ldots, f_r(\underline{x}, \underline{Y}) \text{ have a common zero in } K^m\}$$

for some $r, m \in \mathbb{N}$, $f_1, \ldots, f_r \in K[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$.

Existentially definable subsets

Examples of existentially definable subsets of fields ($n = 1$):

- Finite and cofinite subsets (quantifier-freely definable).

Existentially definable subsets

Examples of existentially definable subsets of fields ($n = 1$):

- Finite and cofinite subsets (quantifier-freely definable).
- The set of squares of the field K:

$$\square K = \{x \in K \mid \exists y \in K : x = y^2\}.$$

Existentially definable subsets

Examples of existentially definable subsets of fields ($n = 1$):

- Finite and cofinite subsets (quantifier-freely definable).
- The set of squares of the field K:

$$\square K = \{x \in K \mid \exists y \in K : x = y^2\}.$$

- For $K = \mathbb{Q}$, the set of non-negative rationals:

$$\mathbb{Q}_{\geq 0} = \{x \in \mathbb{Q} \mid \exists y_1, \ldots, y_4 \in \mathbb{Q} : x = y_1^2 + y_2^2 + y_3^2 + y_4^2\}.$$

Existentially definable subsets

Examples of existentially definable subsets of fields ($n = 1$):

- Finite and cofinite subsets (quantifier-freely definable).
- The set of squares of the field K:

$$\square K = \{x \in K \mid \exists y \in K : x = y^2\}.$$

- For $K = \mathbb{Q}$, the set of non-negative rationals:

$$\mathbb{Q}_{\geq 0} = \{x \in \mathbb{Q} \mid \exists y_1, \ldots, y_4 \in \mathbb{Q} : x = y_1^2 + y_2^2 + y_3^2 + y_4^2\}.$$

- The set of sums of m squares of a field, i.e.

$$S_m(K) = \left\{ x \in K \middle| \exists y_1, \ldots, y_m \in K : x = \sum_{i=1}^{m} y_i^2 \right\}.$$

Existentially definable subsets

- In general, to decide whether a given subset of a field K (or more generally, a subset of K^n) is existentially definable, is hard.

Existentially definable subsets

- In general, to decide whether a given subset of a field K (or more generally, a subset of K^n) is existentially definable, is hard.
- If K has a “rich arithmetic” (e.g. number field), many subsets could be existentially definable.

Existentially definable subsets

- In general, to decide whether a given subset of a field K (or more generally, a subset of K^n) is existentially definable, is hard.
- If K has a "rich arithmetic" (e.g. number field), many subsets could be existentially definable.
- e.g. **Question:** Is $\mathbb{Z}$ an existentially definable subset of $\mathbb{Q}$?

How many quantifiers?

We can ask: if a subset D is existentially definable, what is the "simplest" description which can be given to it?
There are different ways we could attach a number to an existentially definable set to express its simplicity or complexity. We will use the following:

Definition

Let K be a field, $n \in \mathbb{N}$, $D \subseteq K^n$. The *existential rank of D (in K^n)* is defined to be the smallest natural number m such that $D = \varphi(K)$ for some existential $\mathcal{L}_{\text{ring}}(K)$-formula with m quantifiers. We denote it by $\mathrm{rk}^{\exists}_K(D)$. If D is not existentially definable, we set $\mathrm{rk}^{\exists}_K(D) = \infty$.

($\mathcal{L}_{\text{ring}}$ is the language of rings, $\mathcal{L}_{\text{ring}}(K)$ the language of rings with parameters from K)

How many quantifiers?

- For any field K, $\mathrm{rk}^{\exists}_{K}(S_m(K)) \leq m$.

How many quantifiers?

- For any field K, $\mathrm{rk}^{\exists}_{K}(S_m(K)) \leq m$.
- Since for $K = \mathbb{Q}$ one has for all $m \geq 4$ that $S_m(\mathbb{Q}) = \mathbb{Q}_{\geq 0} = S_4(\mathbb{Q})$, we have $\mathrm{rk}^{\exists}_{\mathbb{Q}}(S_m(\mathbb{Q})) \leq 4$ for all m.

How many quantifiers?

- For any field K, $\mathrm{rk}_K^{\exists}(S_m(K)) \leq m$.
- Since for $K = \mathbb{Q}$ one has for all $m \geq 4$ that $S_m(\mathbb{Q}) = \mathbb{Q}_{\geq 0} = S_4(\mathbb{Q})$, we have $\mathrm{rk}_{\mathbb{Q}}^{\exists}(S_m(\mathbb{Q})) \leq 4$ for all m.
- In fact, one has

$$\mathbb{Q}_{\geq 0} = S_3(\mathbb{Q}) \cup 2S_3(\mathbb{Q}),$$

so even $\mathrm{rk}_{\mathbb{Q}}^{\exists}(\mathbb{Q}_{\geq 0}) \leq 3$. **Question:** Do we have $\mathrm{rk}_{\mathbb{Q}}^{\exists}(\mathbb{Q}_{\geq 0}) = 3$?

How many quantifiers?

- For any field K, $\mathrm{rk}^{\exists}_{K}(S_m(K)) \leq m$.
- Since for $K = \mathbb{Q}$ one has for all $m \geq 4$ that $S_m(\mathbb{Q}) = \mathbb{Q}_{\geq 0} = S_4(\mathbb{Q})$, we have $\mathrm{rk}^{\exists}_{\mathbb{Q}}(S_m(\mathbb{Q})) \leq 4$ for all m.
- In fact, one has

$$\mathbb{Q}_{\geq 0} = S_3(\mathbb{Q}) \cup 2S_3(\mathbb{Q}),$$

  so even $\mathrm{rk}^{\exists}_{\mathbb{Q}}(\mathbb{Q}_{\geq 0}) \leq 3$. **Question:** Do we have $\mathrm{rk}^{\exists}_{\mathbb{Q}}(\mathbb{Q}_{\geq 0}) = 3$?
- **Question**: Is there any subset D of $\mathbb{Q}$ with $2 < \mathrm{rk}^{\exists}_{\mathbb{Q}}(D) < \infty$?

How many quantifiers?

- For any field K, $\mathrm{rk}_K^{\exists}(S_m(K)) \leq m$.
- Since for $K = \mathbb{Q}$ one has for all $m \geq 4$ that $S_m(\mathbb{Q}) = \mathbb{Q}_{\geq 0} = S_4(\mathbb{Q})$, we have $\mathrm{rk}_{\mathbb{Q}}^{\exists}(S_m(\mathbb{Q})) \leq 4$ for all m.
- In fact, one has

  $$\mathbb{Q}_{\geq 0} = S_3(\mathbb{Q}) \cup 2S_3(\mathbb{Q}),$$

  so even $\mathrm{rk}_{\mathbb{Q}}^{\exists}(\mathbb{Q}_{\geq 0}) \leq 3$. **Question:** Do we have $\mathrm{rk}_{\mathbb{Q}}^{\exists}(\mathbb{Q}_{\geq 0}) = 3$?
- **Question**: Is there any subset D of $\mathbb{Q}$ with $2 < \mathrm{rk}_{\mathbb{Q}}^{\exists}(D) < \infty$?
- If $\mathrm{rk}_{\mathbb{Q}}^{\exists}(\mathbb{Z}) < \infty$, then there exists $N \in \mathbb{N}$ such that $\mathrm{rk}_{\mathbb{Q}}^{\exists}(D) \leq N$ for all existentially definable $D \subseteq \mathbb{Q}$.

How many quantifiers?

- For any field K, $\mathrm{rk}^{\exists}_{K}(S_m(K)) \leq m$.
- Since for $K = \mathbb{Q}$ one has for all $m \geq 4$ that $S_m(\mathbb{Q}) = \mathbb{Q}_{\geq 0} = S_4(\mathbb{Q})$, we have $\mathrm{rk}^{\exists}_{\mathbb{Q}}(S_m(\mathbb{Q})) \leq 4$ for all m.
- In fact, one has

$$\mathbb{Q}_{\geq 0} = S_3(\mathbb{Q}) \cup 2S_3(\mathbb{Q}),$$

  so even $\mathrm{rk}^{\exists}_{\mathbb{Q}}(\mathbb{Q}_{\geq 0}) \leq 3$. **Question:** Do we have $\mathrm{rk}^{\exists}_{\mathbb{Q}}(\mathbb{Q}_{\geq 0}) = 3$?
- **Question**: Is there any subset D of $\mathbb{Q}$ with $2 < \mathrm{rk}^{\exists}_{\mathbb{Q}}(D) < \infty$?
- If $\mathrm{rk}^{\exists}_{\mathbb{Q}}(\mathbb{Z}) < \infty$, then there exists $N \in \mathbb{N}$ such that $\mathrm{rk}^{\exists}_{\mathbb{Q}}(D) \leq N$ for all existentially definable $D \subseteq \mathbb{Q}$.
- Determining $\mathrm{rk}^{\exists}_{K}(D)$ is in general hard.

Existential rank of formulas

Consider for each $m \in \mathbb{N}$ the following formulas in the language of rings:

$$\sigma_m(X) = \exists Y_1, \ldots, Y_m(X \doteq \sum_{i=1}^{m} Y_i^2)$$

$$\pi_m(X_1, \ldots, X_m) = \exists Y_1, \ldots, Y_m(\bigwedge_{i=1}^{m} X_i \doteq Y_i^2)$$

Can $\sigma_m(X)$ or $\pi_m(X_1, \ldots, X_n)$ be written with less quantifiers "independently of the underlying field"? I.e. can $S_m(K)$ and $(\square K)^m$ be defined *uniformly in the class of fields* with less than m quantifiers?

Existential rank of formulas

Definition

Let $\mathcal{L}$ be a first-order language, φ an $\mathcal{L}$-formula, T an $\mathcal{L}$-theory. The *$\mathcal{L}$-existential rank of φ modulo T*, denoted by $\mathrm{rk}^{\exists}_{\mathcal{L},T}(\varphi)$ is the smallest integer m such that $T \models \varphi \leftrightarrow \psi$ for some existential $\mathcal{L}$-formula ψ with m quantifiers. We set $\mathrm{rk}^{\exists}_{\mathcal{L},T}(\varphi) = \infty$ if no such integer m exists.

Remarks:

- We recover from this the existential rank of a subset $D = \varphi(K)$ of some field K, namely $\mathrm{rk}^{\exists}_{K}(D) = \mathrm{rk}^{\exists}_{\mathcal{L}_{\mathrm{ring}}(K), \mathrm{Th}_{\mathcal{L}_{\mathrm{ring}}(K)}(K)}(\varphi)$.

Existential rank of formulas

Definition

Let $\mathcal{L}$ be a first-order language, φ an $\mathcal{L}$-formula, T an $\mathcal{L}$-theory. The *$\mathcal{L}$-existential rank of φ modulo T*, denoted by $\mathrm{rk}^{\exists}_{\mathcal{L},T}(\varphi)$ is the smallest integer m such that $T \models \varphi \leftrightarrow \psi$ for some existential $\mathcal{L}$-formula ψ with m quantifiers. We set $\mathrm{rk}^{\exists}_{\mathcal{L},T}(\varphi) = \infty$ if no such integer m exists.

Remarks:

- We recover from this the existential rank of a subset $D = \varphi(K)$ of some field K, namely $\mathrm{rk}^{\exists}_{K}(D) = \mathrm{rk}^{\exists}_{\mathcal{L}_{\mathrm{ring}}(K), \mathrm{Th}_{\mathcal{L}_{\mathrm{ring}}(K)}(K)}(\varphi)$.
- For $\mathcal{L}$-formulas φ_1, φ_2 and an $\mathcal{L}$-theory T one has

$$\mathrm{rk}^{\exists}_{\mathcal{L},T}(\varphi_1 \wedge \varphi_2) \leq \mathrm{rk}^{\exists}_{\mathcal{L},T}(\varphi_1) + \mathrm{rk}^{\exists}_{\mathcal{L},T}(\varphi_2)$$
$$\mathrm{rk}^{\exists}_{\mathcal{L},T}(\varphi_1 \vee \varphi_2) \leq \max\{\mathrm{rk}^{\exists}_{\mathcal{L},T}(\varphi_1), \mathrm{rk}^{\exists}_{\mathcal{L},T}(\varphi_2)\}$$

Existential rank of formulas

In the language of rings and with

$$\sigma_m(X) = \exists Y_1, \ldots, Y_m (X \doteq \sum_{i=1}^{m} Y_i^2)$$

$$\pi_m(X_1, \ldots, X_m) = \exists Y_1, \ldots, Y_m (\bigwedge_{i=1}^{m} X_i \doteq Y_i^2)$$

$\mathrm{rk}^{\exists}_{\mathcal{L}_{\mathrm{ring}}, T}$	if T = theory of fields	
$\sigma_m(X)$		
$\pi_m(X_1, \ldots, X_m)$		

Existential rank of formulas

In the language of rings and with

$$\sigma_m(X) = \exists Y_1, \ldots, Y_m (X \doteq \sum_{i=1}^{m} Y_i^2)$$

$$\pi_m(X_1, \ldots, X_m) = \exists Y_1, \ldots, Y_m (\bigwedge_{i=1}^{m} X_i \doteq Y_i^2)$$

$\mathrm{rk}^{\exists}_{\mathcal{L}_{\mathrm{ring}}, T}$	if T = theory of fields	
$\sigma_m(X)$	m	
$\pi_m(X_1, \ldots, X_m)$	m	

Existential rank of formulas

In the language of rings and with

$$\sigma_m(X) = \exists Y_1, \dots, Y_m (X \doteq \sum_{i=1}^{m} Y_i^2)$$

$$\pi_m(X_1, \dots, X_m) = \exists Y_1, \dots, Y_m (\bigwedge_{i=1}^{m} X_i \doteq Y_i^2)$$

$\mathrm{rk}^{\exists}_{\mathcal{L}_{\text{ring}}, T}$	if T = theory of fields	if T = theory of fields with $2 \neq 0$
$\sigma_m(X)$	m	
$\pi_m(X_1, \dots, X_m)$	m	

Existential rank of formulas

In the language of rings and with

$$\sigma_m(X) = \exists Y_1, \dots, Y_m (X \doteq \sum_{i=1}^{m} Y_i^2)$$

$$\pi_m(X_1, \dots, X_m) = \exists Y_1, \dots, Y_m (\bigwedge_{i=1}^{m} X_i \doteq Y_i^2)$$

$\mathrm{rk}^{\exists}_{\mathcal{L}_{\mathrm{ring}}, T}$	if T = theory of fields	if T = theory of fields with $2 \neq 0$
$\sigma_m(X)$	m	m
$\pi_m(X_1, \dots, X_m)$	m	1

Outline

1. Introduction
2. Understanding existential rank of formulae: a model-theoretic framework
3. Outlook: lower bounds for existentially definable sets, existential rank of a field

Sums of m squares

Assume that

$$\sigma_m(X) = \exists Y_1, \ldots, Y_m(X \doteq \sum_{i=1}^{m} Y_i^2)$$

is equivalent to an existential formula $\psi(X)$ with $m-1$ existential quantifiers for all fields in which $2 \neq 0$. We want to reach a contradiction.

Sums of m squares

Assume that

$$\sigma_m(X) = \exists Y_1, \ldots, Y_m (X \doteq \sum_{i=1}^{m} Y_i^2)$$

is equivalent to an existential formula $\psi(X)$ with $m-1$ existential quantifiers for all fields in which $2 \neq 0$. We want to reach a contradiction.

Consider $K = \mathbb{R}(T)$, $L = K(U_1, \ldots, U_{m-1})(\sqrt{T - \sum_{i=1}^{m-1} U_i^2})$; set $U_m = \sqrt{T - \sum_{i=1}^{m-1} U_i^2} \in L$. We see that:

University of Antwerp
Faculty of Science

Sums of m squares

Assume that

$$\sigma_m(X) = \exists Y_1, \ldots, Y_m(X \doteq \sum_{i=1}^{m} Y_i^2)$$

is equivalent to an existential formula $\psi(X)$ with $m-1$ existential quantifiers for all fields in which $2 \neq 0$. We want to reach a contradiction.

Consider $K = \mathbb{R}(T)$, $L = K(U_1, \ldots, U_{m-1})(\sqrt{T - \sum_{i=1}^{m-1} U_i^2})$; set $U_m = \sqrt{T - \sum_{i=1}^{m-1} U_i^2} \in L$. We see that:

- $L \models \sigma_m(T)$ (witness $(U_1, \ldots, U_m)$),

Sums of m squares

Assume that

$$\sigma_m(X) = \exists Y_1, \ldots, Y_m (X \doteq \sum_{i=1}^{m} Y_i^2)$$

is equivalent to an existential formula $\psi(X)$ with $m-1$ existential quantifiers for all fields in which $2 \neq 0$. We want to reach a contradiction.

Consider $K = \mathbb{R}(T)$, $L = K(U_1, \ldots, U_{m-1})(\sqrt{T - \sum_{i=1}^{m-1} U_i^2})$; set $U_m = \sqrt{T - \sum_{i=1}^{m-1} U_i^2} \in L$. We see that:

- $L \models \sigma_m(T)$ (witness $(U_1, \ldots, U_m)$),
- $L \models \psi(T)$

University of Antwerp
Faculty of Science

Sums of m squares

- There exists an intermediate field K' of L/K generated by $m-1$ elements over K such that $K' \models \psi(T)$.

Sums of m squares

- There exists an intermediate field K' of L/K generated by $m-1$ elements over K such that $K' \models \psi(T)$.
- $K' \models \sigma_m(T)$, i.e. T is a sum of m squares in K'.

Sums of m squares

- There exists an intermediate field K' of L/K generated by $m-1$ elements over K such that $K' \models \psi(T)$.
- $K' \models \sigma_m(T)$, i.e. T is a sum of m squares in K'.
- K' has transcendence degree at most $m-2$ over K.

Sums of m squares

- There exists an intermediate field K' of L/K generated by $m-1$ elements over K such that $K' \models \psi(T)$.
- $K' \models \sigma_m(T)$, i.e. T is a sum of m squares in K'.
- K' has transcendence degree at most $m-2$ over K.
- But by results on the essential dimension of quadrics (Karpenko, Merkurjev [KM03]), T is not a sum of m squares in any intermediate field of L/K of transcendence degree less than $m-1$ over K. Contradiction.

Sums of m squares

- There exists an intermediate field K' of L/K generated by $m-1$ elements over K such that $K' \models \psi(T)$.
- $K' \models \sigma_m(T)$, i.e. T is a sum of m squares in K'.
- K' has transcendence degree at most $m-2$ over K.
- But by results on the essential dimension of quadrics (Karpenko, Merkurjev [KM03]), T is not a sum of m squares in any intermediate field of L/K of transcendence degree less than $m-1$ over K. Contradiction.

We conclude that $\mathrm{rk}^{\exists}_{\mathcal{L}_{\mathrm{ring}},T}(\sigma_m) = m$ where T is the theory of fields (or even the theory of fields of characteristic 0).

Sums of m squares

- There exists an intermediate field K' of L/K generated by $m-1$ elements over K such that $K' \models \psi(T)$.
- $K' \models \sigma_m(T)$, i.e. T is a sum of m squares in K'.
- K' has transcendence degree at most $m-2$ over K.
- But by results on the essential dimension of quadrics (Karpenko, Merkurjev [KM03]), T is not a sum of m squares in any intermediate field of L/K of transcendence degree less than $m-1$ over K. Contradiction.

We conclude that $\mathrm{rk}^{\exists}_{\mathcal{L}_{\text{ring}},T}(\sigma_m) = m$ where T is the theory of fields (or even the theory of fields of characteristic 0).

Note: we did **not** show that there exists a field K with $\mathrm{rk}^{\exists}_{K}(S_m(K)) = m$.

Tuples of m squares

For $m \in \mathbb{N}$ we had

$$\pi_m(X_1, \dots, X_m) = \exists Y_1, \dots, Y_m (\bigwedge_{i=1}^{m} X_i \doteq Y_i^2).$$

- By similar arguments as before, this time arguing via the extension $\mathbb{F}_2(\sqrt{T_1}, \dots, \sqrt{T_m})/\mathbb{F}_2(T_1, \dots, T_m)$, one sees that $\mathrm{rk}^{\exists}_{\mathcal{L}_{\text{ring}}, T}(\pi_m) = m$ where T is the theory of fields in which $2 = 0$.

Tuples of m squares

For $m \in \mathbb{N}$ we had

$$\pi_m(X_1, \ldots, X_m) = \exists Y_1, \ldots, Y_m (\bigwedge_{i=1}^{m} X_i \doteq Y_i^2).$$

- By similar arguments as before, this time arguing via the extension $\mathbb{F}_2(\sqrt{T_1}, \ldots, \sqrt{T_m})/\mathbb{F}_2(T_1, \ldots, T_m)$, one sees that $\mathrm{rk}^{\exists}_{\mathcal{L}_{\text{ring}}, T}(\pi_m) = m$ where T is the theory of fields in which $2 = 0$.
- However, for fields in which $2 \neq 0$ this argument fails: for any such field K and $a_1, \ldots, a_m \in K$, the extension $K(\sqrt{a_1}, \ldots, \sqrt{a_n})/K$ is a separable finite extension and thus generated by one element. (Primitive Element Theorem)

Tuples of m squares

Let T be the theory of fields with $2 \neq 0$.

- Let $\mathcal{C}$ be the set of quantifier-free $\mathcal{L}_{\text{ring}}$-formulas $\psi(Y, X_1, \ldots, X_m)$ for which

$$T \models \exists Y \psi(Y, X_1, \ldots, X_m) \to \pi_m(X_1, \ldots, X_m).$$

Tuples of m squares

Let T be the theory of fields with $2 \neq 0$.

- Let $\mathcal{C}$ be the set of quantifier-free $\mathcal{L}_{\text{ring}}$-formulas $\psi(Y, X_1, \ldots, X_m)$ for which

$$T \models \exists Y \psi(Y, X_1, \ldots, X_m) \rightarrow \pi_m(X_1, \ldots, X_m).$$

- **Claim:** For any $K \models T$ and $a_1, \ldots, a_m \in \square K$, there is some $\psi \in \mathcal{C}$ such that $K \models \exists Y \psi(Y, a_1, \ldots, a_m)$.

Tuples of m squares

Let T be the theory of fields with $2 \neq 0$.

- Let $\mathcal{C}$ be the set of quantifier-free $\mathcal{L}_{\text{ring}}$-formulas $\psi(Y, X_1, \ldots, X_m)$ for which
$$T \models \exists Y \psi(Y, X_1, \ldots, X_m) \to \pi_m(X_1, \ldots, X_m).$$
- **Claim:** For any $K \models T$ and $a_1, \ldots, a_m \in \square K$, there is some $\psi \in \mathcal{C}$ such that $K \models \exists Y \psi(Y, a_1, \ldots, a_m)$.
  - Let K_0 be the smallest subfield of K containing $a_1, \ldots, a_m$, set $L = K_0(\sqrt{a_1}, \ldots, \sqrt{a_m})$, and let b be a primitive element of L/K_0.

Tuples of m squares

Let T be the theory of fields with $2 \neq 0$.

- Let $\mathcal{C}$ be the set of quantifier-free $\mathcal{L}_{\text{ring}}$-formulas $\psi(Y, X_1, \ldots, X_m)$ for which

$$T \models \exists Y \psi(Y, X_1, \ldots, X_m) \to \pi_m(X_1, \ldots, X_m).$$

- **Claim:** For any $K \models T$ and $a_1, \ldots, a_m \in \Box K$, there is some $\psi \in \mathcal{C}$ such that $K \models \exists Y \psi(Y, a_1, \ldots, a_m)$.
  - Let K_0 be the smallest subfield of K containing $a_1, \ldots, a_m$, set $L = K_0(\sqrt{a_1}, \ldots, \sqrt{a_m})$, and let b be a primitive element of L/K_0.
  - Denoting by D the quantifier-free $\mathcal{L}_{\text{ring}}(X_1, \ldots, X_m, Y)$-theory of L (where we interpret X_i as a_i and Y as b), we get $D \cup T \models \pi_m(X_1, \ldots, X_m)$.

Tuples of m squares

Let T be the theory of fields with $2 \neq 0$.

- Let $\mathcal{C}$ be the set of quantifier-free $\mathcal{L}_{\text{ring}}$-formulas $\psi(Y, X_1, \ldots, X_m)$ for which
$$T \models \exists Y \psi(Y, X_1, \ldots, X_m) \to \pi_m(X_1, \ldots, X_m).$$
- **Claim:** For any $K \models T$ and $a_1, \ldots, a_m \in \square K$, there is some $\psi \in \mathcal{C}$ such that $K \models \exists Y \psi(Y, a_1, \ldots, a_m)$.
  - Let K_0 be the smallest subfield of K containing $a_1, \ldots, a_m$, set $L = K_0(\sqrt{a_1}, \ldots, \sqrt{a_m})$, and let b be a primitive element of L/K_0.
  - Denoting by D the quantifier-free $\mathcal{L}_{\text{ring}}(X_1, \ldots, X_m, Y)$-theory of L (where we interpret X_i as a_i and Y as b), we get $D \cup T \models \pi_m(X_1, \ldots, X_m)$.
  - By the Compactness Theorem, there exist $\psi_1, \ldots, \psi_r \in D$ such that
$$T \models \exists Y (\bigwedge_{i=1}^{r} \psi_i) \to \pi_m(X_1, \ldots, X_m),$$
proving the claim.

Tuples of m squares

Let T be the theory of fields with $2 \neq 0$.

- Let $\mathcal{C}$ be the set of quantifier-free $\mathcal{L}_{\text{ring}}$-formulas $\psi(Y, X_1, \ldots, X_m)$ for which

$$T \models \exists Y \psi(Y, X_1, \ldots, X_m) \to \pi_m(X_1, \ldots, X_m).$$

- For any $K \models T$ and $a_1, \ldots, a_m \in \Box K$, there is some $\psi \in \mathcal{C}$ such that $K \models \exists Y \psi(Y, a_1, \ldots, a_m)$.

Tuples of m squares

Let T be the theory of fields with $2 \neq 0$.

- Let $\mathcal{C}$ be the set of quantifier-free $\mathcal{L}_{\text{ring}}$-formulas $\psi(Y, X_1, \ldots, X_m)$ for which

$$T \models \exists Y \psi(Y, X_1, \ldots, X_m) \to \pi_m(X_1, \ldots, X_m).$$

- For any $K \models T$ and $a_1, \ldots, a_m \in \square K$, there is some $\psi \in \mathcal{C}$ such that $K \models \exists Y \psi(Y, a_1, \ldots, a_m)$.
- By the Compactness Theorem, there exist $\varphi_1, \ldots, \varphi_s \in \mathcal{C}$ such that $T \models \exists Y (\bigvee_{i=1}^{s} \varphi_i) \leftrightarrow \pi_m$. We conclude that π_m is indeed equivalent to an existential formula with one quantifier modulo T.

Tuples of m squares

An example of an existential formula with one quantifier equivalent to π_2 is given by

$$\exists Y((X_1 - X_2)^2 Y^4 - 2(X_1 + X_2)Y^2 + 1 \doteq 0 \vee (X_1 \doteq 0 \wedge X_2 \doteq 0)).$$

Explicit techniques to construct existential formulas equivalent to a given formula and with the optimal number of quantifiers, will be discussed in upcoming work with Karim Becher.

Quantitative preservation theorem

Proposition

Let φ be an $\mathcal{L}_{\text{ring}}$-formula, $m \in \mathbb{N}$, T the theory of fields. The following are equivalent:

1. $\mathrm{rk}^{\exists}_{\mathcal{L}_{\text{ring}},T}(\varphi) \leq m$.
2. *For every field K and every $\underline{x} \in \varphi(K)$ there is a subfield K' of K generated by $\underline{x}$ and m further elements such that $K' \models \varphi(\underline{x})$.*

Quantitative preservation theorem

Proposition

Let φ be an $\mathcal{L}_{\text{ring}}$-formula, $m \in \mathbb{N}$, T the theory of fields. The following are equivalent:

1. $\mathrm{rk}^{\exists}_{\mathcal{L}_{\text{ring}},T}(\varphi) \leq m$.
2. *For every field K and every $\underline{x} \in \varphi(K)$ there is a subfield K' of K generated by $\underline{x}$ and m further elements such that $K' \models \varphi(\underline{x})$.*

This principle generalises to arbitrary languages and theories:

Proposition

Let $\mathcal{L}$ be a first-order language, φ an $\mathcal{L}$-formula, T an $\mathcal{L}$-theory, $m \in \mathbb{N}$. The following are equivalent:

1. $\mathrm{rk}^{\exists}_{\mathcal{L},T}(\varphi) \leq m$.
2. *For every $K \models T$ and every $\underline{x} \in \varphi(K)$ there is an $\mathcal{L}$-substructure A of K generated by $\underline{x}$ and m further elements such that $L \models \varphi(\rho(\underline{x}))$ for every $\mathcal{L}$-embedding $\rho : A \to L$ where $L \models T$.*

Another application

Corollary

Let T be the theory of fields of characteristic 0. For $\mathcal{L}$-formulas φ_1, φ_2 with $\mathrm{rk}^{\exists}_{\mathcal{L}_{\text{ring}},T}(\varphi_1), \mathrm{rk}^{\exists}_{\mathcal{L}_{\text{ring}},T}(\varphi_2) \geq 1$ one has

$$\mathrm{rk}^{\exists}_{\mathcal{L}_{\text{ring}},T}(\varphi_1 \wedge \varphi_2) \leq \mathrm{rk}^{\exists}_{\mathcal{L}_{\text{ring}},T}(\varphi_1) + \mathrm{rk}^{\exists}_{\mathcal{L}_{\text{ring}},T}(\varphi_2) - 1.$$

Proof idea.

If L_1/K and L_2/K are field extensions in characteristic 0 which are not purely transcendental and which are generated by m_1 respectively m_2 elements, then any compositum $L_1 L_2$ is generated by $m_1 + m_2 - 1$ elements over K. Now invoke the previous proposition. □

Outlook: lower bounds for existentially definable sets

- (Pasten [Pas21], building on Kollár [Kol08]) In $K = \mathbb{C}(T)$, for every $m \in \mathbb{N}^+$ the set

$$D_m = \{a_0 + a_1 T + \ldots + a_m T^m \mid a_0, \ldots, a_m \in \mathbb{C}\}$$

has $\mathrm{rk}_K^{\exists}(D_m) = m$.

Outlook: lower bounds for existentially definable sets

- (Pasten [Pas21], building on Kollár [Kol08]) In $K = \mathbb{C}(T)$, for every $m \in \mathbb{N}^+$ the set

$$D_m = \{a_0 + a_1 T + \ldots + a_m T^m \mid a_0, \ldots, a_m \in \mathbb{C}\}$$

  has $\mathrm{rk}^{\exists}_K(D_m) = m$.
- There exists a field K such that for all $m \in \mathbb{N}$, $\mathrm{rk}^{\exists}_K(S_m(K)) = m$.

Outlook: lower bounds for existentially definable sets

- (Pasten [Pas21], building on Kollár [Kol08]) In $K = \mathbb{C}(T)$, for every $m \in \mathbb{N}^+$ the set

  $$D_m = \{a_0 + a_1 T + \ldots + a_m T^m \mid a_0, \ldots, a_m \in \mathbb{C}\}$$

  has $\mathrm{rk}^{\exists}_K(D_m) = m$.
- There exists a field K such that for all $m \in \mathbb{N}$, $\mathrm{rk}^{\exists}_K(S_m(K)) = m$.
- If K is a large imperfect field of characteristic 2 (e.g. $K = \mathbb{F}_2((T))$), then $\mathrm{rk}^{\exists}_K((\Box K)^m) = m$ for all $m \in \mathbb{N}$.

Outlook: lower bounds for existentially definable sets

- (Pasten [Pas21], building on Kollár [Kol08]) In $K = \mathbb{C}(T)$, for every $m \in \mathbb{N}^+$ the set

$$D_m = \{a_0 + a_1 T + \ldots + a_m T^m \mid a_0, \ldots, a_m \in \mathbb{C}\}$$

  has $\mathrm{rk}_K^{\exists}(D_m) = m$.
- There exists a field K such that for all $m \in \mathbb{N}$, $\mathrm{rk}_K^{\exists}(S_m(K)) = m$.
- If K is a large imperfect field of characteristic 2 (e.g. $K = \mathbb{F}_2((T))$), then $\mathrm{rk}_K^{\exists}((\square K)^m) = m$ for all $m \in \mathbb{N}$.
- On the other hand, if K is a finitely generated field (e.g. $K = \mathbb{F}_2(T)$), then $\mathrm{rk}_K^{\exists}((\square K)^m) = 1$ for all $m \in \mathbb{N}^+$.

Outlook: existential rank of a field

For a field K, we define

$$\mathrm{rk}^{\exists,1}(K) = \sup\{\mathrm{rk}^{\exists}(D) \mid D \subseteq K \text{ existentially definable in } K\}.$$

- If K is finite or algebraically closed, then $\mathrm{rk}^{\exists,1}(K) = 0$.

Outlook: existential rank of a field

For a field K, we define

$$\mathrm{rk}^{\exists,1}(K) = \sup\{\mathrm{rk}^{\exists}(D) \mid D \subseteq K \text{ existentially definable in } K\}.$$

- If K is finite or algebraically closed, then $\mathrm{rk}^{\exists,1}(K) = 0$.
- If K is real closed, p-adically closed, or perfect pseudo-algebraically closed, then $\mathrm{rk}^{\exists,1}(K) \leq 1$.

Outlook: existential rank of a field

For a field K, we define

$$\mathrm{rk}^{\exists,1}(K) = \sup\{\mathrm{rk}^{\exists}(D) \mid D \subseteq K \text{ existentially definable in } K\}.$$

- If K is finite or algebraically closed, then $\mathrm{rk}^{\exists,1}(K) = 0$.
- If K is real closed, p-adically closed, or perfect pseudo-algebraically closed, then $\mathrm{rk}^{\exists,1}(K) \leq 1$.
- If K is large and imperfect (e.g. $K = \mathbb{F}_p((T))$) then $\mathrm{rk}^{\exists,1}(K) = \infty$.

Outlook: existential rank of a field

For a field K, we define

$$\mathrm{rk}^{\exists,1}(K) = \sup\{\mathrm{rk}^{\exists}(D) \mid D \subseteq K \text{ existentially definable in } K\}.$$

- If K is finite or algebraically closed, then $\mathrm{rk}^{\exists,1}(K) = 0$.
- If K is real closed, p-adically closed, or perfect pseudo-algebraically closed, then $\mathrm{rk}^{\exists,1}(K) \leq 1$.
- If K is large and imperfect (e.g. $K = \mathbb{F}_p((T))$) then $\mathrm{rk}^{\exists,1}(K) = \infty$.
- If K is a global field, then $\mathrm{rk}^{\exists,1}(K) \geq 2$. If $\mathrm{rk}^{\exists,1}(\mathbb{Q}) < \infty$, then $\mathbb{Z}$ is not existentially definable in $\mathbb{Q}$.

Outlook: existential rank of a field

For a field K, we define

$$\mathrm{rk}^{\exists,1}(K) = \sup\{\mathrm{rk}^{\exists}(D) \mid D \subseteq K \text{ existentially definable in } K\}.$$

- If K is finite or algebraically closed, then $\mathrm{rk}^{\exists,1}(K) = 0$.
- If K is real closed, p-adically closed, or perfect pseudo-algebraically closed, then $\mathrm{rk}^{\exists,1}(K) \leq 1$.
- If K is large and imperfect (e.g. $K = \mathbb{F}_p((T))$) then $\mathrm{rk}^{\exists,1}(K) = \infty$.
- If K is a global field, then $\mathrm{rk}^{\exists,1}(K) \geq 2$. If $\mathrm{rk}^{\exists,1}(\mathbb{Q}) < \infty$, then $\mathbb{Z}$ is not existentially definable in $\mathbb{Q}$.
- **Question:** Is there a field K with $\mathrm{rk}^{\exists,1}(K) \notin \{0, 1, \infty\}$?

References

[DDF21] Nicolas Daans, Philip Dittmann, and Arno Fehm. "Existential rank and essential dimension of diophantine sets". available as arXiv:2102.06941. 2021.

[KM03] Nikita Karpenko and Alexander Merkurjev. "Essential dimension of quadrics". In: *Inventiones Mathematicae* 153 (2003), pp. 361–372.

[Kol08] János Kollár. "Diophantine subsets of function fields of curves". In: *Algebra & Number Theory* 2.3 (2008), pp. 299–311.

[Pas21] Hector Pasten. "Notes on the DPRM property for listable structures". available as arXiv:2012.14054. Jan. 2021.

Nicolas Daans
E-mail: `nicolas.daans@uantwerpen.be`
Office: M.G.223