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 July 2022

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?

How many quantifiers?

We can ask: if a subset D is existentially definable, what is the "simplest" description which can be given to it?
We will measure complexity by number of quantifiers:

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 φ with m quantifiers. We denote it by $\mathrm{rk}_K^{\exists}(D)$. If D is not existentially definable, we set $\mathrm{rk}_K^{\exists}(D) = \infty$.

($\mathcal{L}_{\text{ring}}$ 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, $\mathrm{rk}_K^{\exists}(S_m(K)) \leq m$.
- 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.

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 $\mathrm{rk}^{\exists}_{\mathbb{Q}}(\mathbb{Q}_{\geq 0}) \leq 3$.

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 $\mathrm{rk}^{\exists}_{\mathbb{Q}}(\mathbb{Q}_{\geq 0}) = 3$?

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 $2 < \mathrm{rk}_{\mathbb{Q}}^{\exists}(D) < \infty$?

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 $D \subseteq \mathbb{Q}$.

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:

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

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

Can $\sigma_m(X)$ or $\pi_m(X_1, \dots, X_n)$ be written with fewer 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 fewer 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:

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 $\mathrm{rk}^{\exists}_{K}(D) = \mathrm{rk}^{\exists}_{\mathcal{L}_{\text{ring}}(K),\mathrm{Th}_{\mathcal{L}_{\text{ring}}(K)}(K)}(\varphi)$.
- 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 $\mathcal{L}_{\text{ring}}$ and with

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

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

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

University of Antwerp
Faculty of Science

Existential rank of formulas

In the language of rings $\mathcal{L}_{\text{ring}}$ 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	
$\sigma_m(X)$	m	
$\pi_m(X_1, \dots, X_m)$	m	

Existential rank of formulas

In the language of rings $\mathcal{L}_{\mathrm{ring}}$ 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	if $T =$ theory of fields with $2 \neq 0$
$\sigma_m(X)$	m	
$\pi_m(X_1, \ldots, X_m)$	m	

Existential rank of formulas

In the language of rings $\mathcal{L}_{\text{ring}}$ and with

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

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

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

Outline

1. Introduction ✓
2. Understanding existential rank of formulae: a model-theoretic framework
3. Lower bounds for existentially definable subsets of a field, uniform upper bounds for existentially definable subsets of a field

A condition to obtain lower bounds

Proposition

Let T be the theory of fields, $m \geq 1$. Consider for an existential $\mathcal{L}_{\text{ring}}$-formula $\varphi(X_1, \ldots, X_n)$ the following condition:

> *There exists an extension of fields L/K and $a \in K^n$ such that $L \models \varphi(a)$, but $K' \not\models \varphi(a)$ for every subextension K' of L/K generated by $m-1$ elements.* (*)

Then $\mathrm{rk}^{\exists}_{\mathcal{L}_{\text{ring}}, T}(\varphi) \geq m$.

A condition to obtain lower bounds

Proposition

Let T be the theory of fields, $m \geq 1$. Consider for an existential $\mathcal{L}_{\text{ring}}$-formula $\varphi(X_1, \ldots, X_n)$ the following condition:

There exists an extension of fields L/K and $a \in K^n$ such that $L \models \varphi(a)$, but $K' \not\models \varphi(a)$ for every subextension K' of L/K generated by $m-1$ elements. (*)

Then $\mathrm{rk}^{\exists}_{\mathcal{L}_{\text{ring}},T}(\varphi) \geq m$.

Proof: Suppose that $\psi(X_1, \ldots, X_n)$ is an existential $\mathcal{L}_{\text{ring}}$-formula with $m-1$ quantifiers equivalent to φ in all intermediate extensions of L/K. We have that $L \models \varphi(a)$ and hence $L \models \psi(a)$.

A condition to obtain lower bounds

Proposition

Let T be the theory of fields, $m \geq 1$. Consider for an existential $\mathcal{L}_{\text{ring}}$-formula $\varphi(X_1, \ldots, X_n)$ the following condition:

> *There exists an extension of fields L/K and $a \in K^n$ such that $L \models \varphi(a)$, but $K' \not\models \varphi(a)$ for every subextension K' of L/K generated by $m-1$ elements.* (*)

Then $\mathrm{rk}^{\exists}_{\mathcal{L}_{\text{ring}},T}(\varphi) \geq m$.

Proof: Suppose that $\psi(X_1, \ldots, X_n)$ is an existential $\mathcal{L}_{\text{ring}}$-formula with $m-1$ quantifiers equivalent to φ in all intermediate extensions of L/K. We have that $L \models \varphi(a)$ and hence $L \models \psi(a)$.

There exists an intermediate extension K' of L/K generated by $m-1$ elements and such that $K' \models \psi(a)$. But then $K' \models \varphi(a)$. □

A condition to obtain lower bounds

Proposition

Let T be the theory of fields, $m \geq 1$. Consider for an existential $\mathcal{L}_{\text{ring}}$-formula $\varphi(X_1, \ldots, X_n)$ the following condition:

There exists an extension of fields L/K and $a \in K^n$ such that $L \models \varphi(a)$, but $K' \not\models \varphi(a)$ for every subextension K' of L/K generated by $m-1$ elements. (*)

Then $\mathrm{rk}^{\exists}_{\mathcal{L}_{\text{ring}},T}(\varphi) \geq m$.

Proof: Suppose that $\psi(X_1, \ldots, X_n)$ is an existential $\mathcal{L}_{\text{ring}}$-formula with $m-1$ quantifiers equivalent to φ in all intermediate extensions of L/K. We have that $L \models \varphi(a)$ and hence $L \models \psi(a)$.

There exists an intermediate extension K' of L/K generated by $m-1$ elements and such that $K' \models \psi(a)$. But then $K' \models \varphi(a)$. □

Note: the above argument even shows $\mathrm{rk}^{\exists}_{\mathcal{L}_{\text{ring}},T'}(\varphi) \geq m$ where T' is the union of T with the universal $\mathcal{L}_{\text{ring}}$-theory of L.

Sums of m squares

Consider the formula

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

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

Sums of m squares

Consider the formula

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

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

- 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 have $L \models \sigma_m(T)$, since $T = \sum_{i=1}^{m} U_i^2$.

Sums of m squares

Consider the formula

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

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

- 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 have $L \models \sigma_m(T)$, since $T = \sum_{i=1}^{m} U_i^2$.
- Any subfield K' of L/K generated by $m-1$ elements and for which $K' \models \sigma_m(T)$ must have transcendence degree at most $m-2$ over K.

Sums of m squares

- 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.

Sums of m squares

- 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.
- We conclude that $\mathrm{rk}^{\exists}_{\mathcal{L}_{\mathsf{ring}},T}(\sigma_m) \geq m$ by (*).

Sums of m squares

- 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.
- We conclude that $\mathrm{rk}^{\exists}_{\mathcal{L}_{\mathsf{ring}},T}(\sigma_m) \geq m$ by (*).

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

Sums of m squares

- 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.
- We conclude that $\mathrm{rk}^{\exists}_{\mathcal{L}_{\text{ring}},T}(\sigma_m) \geq m$ by (*).

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

Note: we did **not** show that there exists an intermediate field K' of L/K (or in fact any field) with $\mathrm{rk}^{\exists}_{K'}(S_m(K')) = m$.

Tuples of m squares

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

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

We argue similarly as before. Let $K = \mathbb{F}_2(T_1, \ldots, T_m)$ and $L = \mathbb{F}_2(\sqrt{T_1}, \ldots, \sqrt{T_m})$.

Tuples of m squares

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

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

We argue similarly as before. Let $K = \mathbb{F}_2(T_1, \ldots, T_m)$ and $L = \mathbb{F}_2(\sqrt{T_1}, \ldots, \sqrt{T_m})$.

- We have $K \models \pi_m(T_1, \ldots, T_m)$, but $K' \not\models \pi_m(T_1, \ldots, T_m)$ for any intermediate field K' of L/K generated by $m-1$ elements over K. Hence, there is no existential formula with $m-1$ quantifiers which is equivalent to π_m for all intermediate extensions of L/K.

Tuples of m squares

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

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

We argue similarly as before. Let $K = \mathbb{F}_2(T_1, \ldots, T_m)$ and $L = \mathbb{F}_2(\sqrt{T_1}, \ldots, \sqrt{T_m})$.

- We have $K \models \pi_m(T_1, \ldots, T_m)$, but $K' \not\models \pi_m(T_1, \ldots, T_m)$ for any intermediate field K' of L/K generated by $m-1$ elements over K. Hence, there is no existential formula with $m-1$ quantifiers which is equivalent to π_m for all intermediate extensions of L/K.
- Note: we did **not** show that there exists an intermediate extension K' of L/K (or in fact any field) for which $\mathrm{rk}^{\exists}_{K'}(\pi_m(K')) = m$.

Tuples of m squares

- If K is a field with $2 \neq 0$ and $a_1, \ldots, a_m \in K$, then 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) Thus, if T is the theory of fields in which $2 \neq 0$, no obstruction as in (*) exists.

Tuples of m squares

- If K is a field with $2 \neq 0$ and $a_1, \ldots, a_m \in K$, then 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) Thus, if T is the theory of fields in which $2 \neq 0$, no obstruction as in (*) exists.
- Does this already imply that $\mathrm{rk}^{\exists}_{\mathcal{L}_{\text{ring}}, T}(\pi_m) = 1$?

Quantitative preservation theorem

Yes.

Theorem ("Quantitative preservation theorem")

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:

(i) $\mathrm{rk}^{\exists}_{\mathcal{L},T}(\varphi) \leq m$.

(ii) *For every $L \models T$ and every $x \in \varphi(L)$ there is an $\mathcal{L}$-substructure K of L generated by x and m further elements such that $M \models \varphi(\rho(x))$ for every $\mathcal{L}$-embedding $\rho : K \to M$ where $M \models T$.*

Quantitative preservation theorem

Yes.

Theorem ("Quantitative preservation theorem")

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:

(i) $\mathrm{rk}^{\exists}_{\mathcal{L},T}(\varphi) \leq m$.

(ii) *For every $L \models T$ and every $x \in \varphi(L)$ there is an $\mathcal{L}$-substructure K of L generated by x and m further elements such that $M \models \varphi(\rho(x))$ for every $\mathcal{L}$-embedding $\rho : K \to M$ where $M \models T$.*

An example of a specialisation hereof:

Corollary

Let T be the union of the $\mathcal{L}_{\mathrm{ring}}$-theory of fields and some universal $\mathcal{L}_{\mathrm{ring}}$-theory. Let φ be an existential $\mathcal{L}_{\mathrm{ring}}$-formula and $m \in \mathbb{N}$. The following are equivalent:

(i) $\mathrm{rk}^{\exists}_{\mathcal{L}_{\mathrm{ring}},T}(\varphi) \leq m$.

(ii) *For every $L \models T$ and every $x \in \varphi(L)$, there exists a subfield K generated by x and m further elements of L such that $K \models \varphi(x)$.*

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 corollary. □

Explicit techniques

An example of an existential formula with one quantifier equivalent to π_2 for fields in which $2 \neq 0$ 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.

Outline

1. Introduction ✓
2. Understanding existential rank of formulae: a model-theoretic framework ✓
3. Lower bounds for existentially definable subsets of a field, uniform upper bounds for existentially definable subsets of a field

Sums and tuples of squares in a single field

Let $m \geq 1$.

- Through a limit construction, one can show that there exists a field K where $\mathrm{rk}^{\exists}_K(S_m(K)) = m$ for each $m \in \mathbb{N}$.

[1] A field K is called *large* if $K(\!(T)\!)/K$ is an existentially closed extension.

Sums and tuples of squares in a single field

Let $m \geq 1$.

- Through a limit construction, one can show that there exists a field K where $\mathrm{rk}^{\exists}_K(S_m(K)) = m$ for each $m \in \mathbb{N}$.
- If K is of characteristic 2, imperfect and large[1] (e.g. $K = \mathbb{F}_2(\!(T)\!)$), then $\mathrm{rk}^{\exists}_K(\pi_m(K)) = m$.

[1] A field K is called *large* if $K(\!(T)\!)/K$ is an existentially closed extension.

Sums and tuples of squares in a single field

Let $m \geq 1$.

- Through a limit construction, one can show that there exists a field K where $\mathrm{rk}_K^{\exists}(S_m(K)) = m$ for each $m \in \mathbb{N}$.
- If K is of characteristic 2, imperfect and large[1] (e.g. $K = \mathbb{F}_2(\!(T)\!)$), then $\mathrm{rk}_K^{\exists}(\pi_m(K)) = m$.
- If K is a finitely generated extension of a perfect field K_0, then $\mathrm{rk}_K^{\exists}(\pi_m(K)) = 1$.

[1] A field K is called *large* if $K(\!(T)\!)/K$ is an existentially closed extension.

Sums and tuples of squares in a single field

Let $m \geq 1$.

- Through a limit construction, one can show that there exists a field K where $\mathrm{rk}_K^{\exists}(S_m(K)) = m$ for each $m \in \mathbb{N}$.
- If K is of characteristic 2, imperfect and large[1] (e.g. $K = \mathbb{F}_2(\!(T)\!)$), then $\mathrm{rk}_K^{\exists}(\pi_m(K)) = m$.
- If K is a finitely generated extension of a perfect field K_0, then $\mathrm{rk}_K^{\exists}(\pi_m(K)) = 1$.
  In particular, although there is no existential formula with $m-1$ quantifiers equivalent to π_m simultaneously for all intermediate fields of $\mathbb{F}_2(\sqrt{T_1}, \ldots, \sqrt{T_m})/\mathbb{F}_2(T_1, \ldots, T_m)$, such a formula does exist for each intermediate field individually!

[1] A field K is called *large* if $K(\!(T)\!)/K$ is an existentially closed extension.

Existential rank of a field

For a field K, we define

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

Existential rank of a field

For a field K, we define

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

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

Existential rank of a field

For a field K, we define

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

- If K is finite or algebraically closed, then $\mathrm{rk}^{\exists,1}(K) = 0$.
- If $K = \mathbb{R}$, $K = \mathbb{Q}_p$ for some prime number p, or K is perfect pseudo-algebraically closed (e.g. an infinite algebraic extension of a finite field), then $\mathrm{rk}^{\exists,1}(K) \leq 1$.

Existential rank of a field

For a field K, we define

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

- If K is finite or algebraically closed, then $\mathrm{rk}^{\exists,1}(K) = 0$.
- If $K = \mathbb{R}$, $K = \mathbb{Q}_p$ for some prime number p, or K is perfect pseudo-algebraically closed (e.g. an infinite algebraic extension of a finite field), then $\mathrm{rk}^{\exists,1}(K) \leq 1$.
- If K is large and imperfect (e.g. $K = \mathbb{F}_p(\!(T)\!)$) then $\mathrm{rk}^{\exists,1}(K) = \infty$.

Existential rank of a field

For a field K, we define

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

- If K is finite or algebraically closed, then $\mathrm{rk}^{\exists,1}(K) = 0$.
- If $K = \mathbb{R}$, $K = \mathbb{Q}_p$ for some prime number p, or K is perfect pseudo-algebraically closed (e.g. an infinite algebraic extension of a finite field), then $\mathrm{rk}^{\exists,1}(K) \leq 1$.
- If K is large and imperfect (e.g. $K = \mathbb{F}_p(\!(T)\!)$) then $\mathrm{rk}^{\exists,1}(K) = \infty$.
- (Pasten [Pas22], building on Kollár [Kol08]) If K is large and uncountable (e.g. $K = \mathbb{C}$), then $\mathrm{rk}^{\exists,1}(K(T)) = \infty$.

Existential rank of a field

For a field K, we define

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

- If K is finite or algebraically closed, then $\mathrm{rk}^{\exists,1}(K) = 0$.
- If $K = \mathbb{R}$, $K = \mathbb{Q}_p$ for some prime number p, or K is perfect pseudo-algebraically closed (e.g. an infinite algebraic extension of a finite field), then $\mathrm{rk}^{\exists,1}(K) \leq 1$.
- If K is large and imperfect (e.g. $K = \mathbb{F}_p(\!(T)\!)$) then $\mathrm{rk}^{\exists,1}(K) = \infty$.
- (Pasten [Pas22], building on Kollár [Kol08]) If K is large and uncountable (e.g. $K = \mathbb{C}$), then $\mathrm{rk}^{\exists,1}(K(T)) = \infty$.
- If K is an infinite, finitely generated 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 $\mathbb{Q}$.

Existential rank of a field

For a field K, we define

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

- If K is finite or algebraically closed, then $\mathrm{rk}^{\exists,1}(K) = 0$.
- If $K = \mathbb{R}$, $K = \mathbb{Q}_p$ for some prime number p, or K is perfect pseudo-algebraically closed (e.g. an infinite algebraic extension of a finite field), then $\mathrm{rk}^{\exists,1}(K) \leq 1$.
- If K is large and imperfect (e.g. $K = \mathbb{F}_p(\!(T)\!)$) then $\mathrm{rk}^{\exists,1}(K) = \infty$.
- (Pasten [Pas22], building on Kollár [Kol08]) If K is large and uncountable (e.g. $K = \mathbb{C}$), then $\mathrm{rk}^{\exists,1}(K(T)) = \infty$.
- If K is an infinite, finitely generated 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* 153.2 (2003), pp. 361–372.

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

[Pas22] Hector Pasten. "Notes on the DPRM property for listable structures". In: *The Journal of Symbolic Logic* 87.1 (2022), pp. 273–312.

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

Bonus slides

4 Bonus slides

- Tuples of pth powers in characteristic p
- Existential vs positive-existential
- Large fields

Tuples of pth powers in characteristic p

Let K be a field which is finitely generated over a perfect field K_0 of characteristic $p > 0$. There exists $r \in \mathbb{N} \setminus p\mathbb{N}$ (depending on K) such that for all $x, y \in K$ we have that

$$\exists z_1, z_2 \in K : x = z_1^p \wedge x = z_2^p$$

if and only if there exists $z \in K$ such that

$$(x^r + 1 = 0 \wedge y = z^p) \vee (x^r + 1 \neq 0$$
$$\wedge (x^r + 1)^{p+1} y + (x^r + 1)^{p+1} y^{p^2} + (x^r + 1)^{2p+1} + x^r + 1 = z^p)$$

If K is imperfect, then r cannot be bounded uniformly for all finite separable extensions of K.

Existential vs positive-existential

For a language $\mathcal{L}$, an $\mathcal{L}$-theory T and an $\mathcal{L}$-formula φ, we define its *existential rank*

$$\mathrm{rk}^{\exists}_{\mathcal{L},T}(\varphi) = \inf \left\{ m \in \mathbb{N} \;\middle|\; \begin{array}{l} \varphi \text{ is equivalent modulo } T \text{ to an} \\ \text{existential } \mathcal{L}\text{-formula with } m \text{ quantifiers} \end{array} \right\}$$

and its positive-existential rank

$$\mathrm{rk}^{\exists+}_{\mathcal{L},T}(\varphi) = \inf \left\{ m \in \mathbb{N} \;\middle|\; \begin{array}{l} \varphi \text{ is equivalent modulo } T \text{ to a positive} \\ \text{existential } \mathcal{L}\text{-formula with } m \text{ quantifiers} \end{array} \right\}.$$

Clearly one always has $\mathrm{rk}^{\exists}_{\mathcal{L},T}(\varphi) \leq \mathrm{rk}^{\exists+}_{\mathcal{L},T}(\varphi)$.

Existential vs positive-existential

Let $\mathcal{L} = \mathcal{L}_{\text{ring}}$, T a theory containing the theory of fields, φ an $\mathcal{L}_{\text{ring}}$-formula. Then precisely one of the following occurs:

1. $\mathrm{rk}^{\exists}_{\mathcal{L}_{\text{ring}},T}(\varphi) = \mathrm{rk}^{\exists^+}_{\mathcal{L}_{\text{ring}},T}(\varphi)$,
2. $\mathrm{rk}^{\exists}_{\mathcal{L}_{\text{ring}},T}(\varphi) = 0$ and $\mathrm{rk}^{\exists^+}_{\mathcal{L}_{\text{ring}},T}(\varphi) = 1$,
3. $\mathrm{rk}^{\exists}_{\mathcal{L}_{\text{ring}},T}(\varphi) = 1$ and $\mathrm{rk}^{\exists^+}_{\mathcal{L}_{\text{ring}},T}(\varphi) = 2$.

Furthermore, case (3) only occurs in very special cases; e.g. it requires that T has both finite and infinite models.

Existential vs positive-existential

Let $\mathcal{L} = \mathcal{L}_{\mathsf{ring}}$, T a theory containing the theory of fields, φ an $\mathcal{L}_{\mathsf{ring}}$-formula. Then precisely one of the following occurs:

1. $\mathrm{rk}^{\exists}_{\mathcal{L}_{\mathsf{ring}},T}(\varphi) = \mathrm{rk}^{\exists^+}_{\mathcal{L}_{\mathsf{ring}},T}(\varphi)$,
2. $\mathrm{rk}^{\exists}_{\mathcal{L}_{\mathsf{ring}},T}(\varphi) = 0$ and $\mathrm{rk}^{\exists^+}_{\mathcal{L}_{\mathsf{ring}},T}(\varphi) = 1$,
3. $\mathrm{rk}^{\exists}_{\mathcal{L}_{\mathsf{ring}},T}(\varphi) = 1$ and $\mathrm{rk}^{\exists^+}_{\mathcal{L}_{\mathsf{ring}},T}(\varphi) = 2$.

Furthermore, case (3) only occurs in very special cases; e.g. it requires that T has both finite and infinite models.
Examples with T the theory of fields:

- The formula $x \neq 0$ is an example of case (2).
- The formula $\exists y(y^2 \neq y)$ is an example of case (3).

Large fields

- A field K is called *large* if K is existentially closed in the field of formal Laurent series $K((T))$.
- Equivalently, a field K is large if every smooth curve over K has either zero or infinitely many K-rational points.
- Examples of large fields: henselian valued fields (e.g. $\mathbb{Q}_p$, $K((T))$), real closed fields (e.g. $\mathbb{R}$), pseudo-algebraically closed fields (e.g. non-principal ultraproducts of finite fields, separably closed fields)