Proofs by example

Benjamin Matschke
Boston University

Number Theory Seminar
Harvard, Oct. 2019
Proofs by example
To prove a general statement by verifying it for a single example.
PROOFS BY EXAMPLE

~ To prove a general statement by verifying it for a single example.

For instance: Statement: “All primes are even.”
To prove a general statement by verifying it for a single example.

For instance: Statement: “All primes are even.”
Example: 2.
Proofs by Example

~ To prove a general statement by verifying it for a single example.

For instance: Statement: “All primes are even.”
Example: 2.

Wikipedia: “Proof by example”
= inappropriate generalization
Proofs by Example

To prove a general statement by verifying it for a single example.

For instance: Statement: “All primes are even.”
Example: 2.

Wikipedia: “Proof by example”

= inappropriate generalization
= logical fallacy, in which one or more examples are claimed as “proof” for a more general statement.
To prove a general statement by verifying it for a single example.

For instance: Statement: “All primes are even.”
Example: 2.

Wikipedia: “Proof by example”
= inappropriate generalization
= logical fallacy, in which one or more examples are claimed as “proof” for a more general statement.

Related to “law of small numbers”: 
Proofs by Example

To prove a general statement by verifying it for a single example.

For instance: Statement: “All primes are even.”
Example: 2.

Wikipedia: “Proof by example”
= inappropriate generalization
= logical fallacy, in which one or more examples are claimed as “proof” for a more general statement.

Related to “law of small numbers”:
Initial data points do not always predict the subsequent ones.
To prove a general statement by verifying it for a single example.

For instance: Statement: “All primes are even.”
Example: 2.

Wikipedia: “Proof by example”
= inappropriate generalization
= logical fallacy, in which one or more examples are claimed as “proof” for a more general statement.

Related to “law of small numbers”:
Initial data points do not always predict the subsequent ones.
Example: 1, 1, 2, 3, 5, 8, 13, . . . ?
Another example: Thales’ theorem

Thales of Miletus
~ 600 BC
Another example: **Thales’ theorem**

\[ \alpha = 90^\circ \]

Thales of Miletus

\sim 600 BC
Another example: **Thales’ theorem**

Thales of Miletus

\[ \approx 89.97^\circ \]

\[ \sim 600 \text{ BC} \]
Another example: Thales’ theorem

\[ \angle C \approx 89.97° \]

\( \sim \) Can “Proof by example” work?

Thales of Miletus
\( \sim 600 \text{ BC} \)
Algebraic setting
Algebraic setting (first attempt):
Algebraic setting (first attempt):
Let $X = V(f_1, \ldots, f_m) \subseteq \mathbb{C}^n$ be algebraic variety, $\dim X = d$. 
Algebraic setting (first attempt):
Let $X = V(f_1, \ldots, f_m) \subseteq \mathbb{C}^n$ be algebraic variety, $\dim X = d$. Let $g(x_1, \ldots, x_n)$ be polynomial.
Algebraic setting (first attempt):
Let $X = V(f_1, \ldots, f_m) \subseteq \mathbb{C}^n$ be algebraic variety, $\dim X = d$. Let $g(x_1, \ldots, x_n)$ be polynomial.
Call $P \in X$ “sufficiently generic” for $g$ if

$$g(P) = 0 \implies g|_X = 0.$$
Algebraic setting (first attempt):
Let $X = V(f_1, \ldots, f_m) \subseteq \mathbb{C}^n$ be algebraic variety, $\dim X = d$.
Let $g(x_1, \ldots, x_n)$ be polynomial.
Call $P \in X$ “sufficiently generic” for $g$ if
\[ g(P) = 0 \implies g|_X = 0. \]
Algebraic setting (first attempt):
Let $X = V(f_1, \ldots, f_m) \subseteq \mathbb{C}^n$ be algebraic variety, $\dim X = d$.
Let $g(x_1, \ldots, x_n)$ be polynomial.
Call $P \in X$ “sufficiently generic” for $g$ if
\[ g(P) = 0 \implies g|_X = 0. \]

Example: Let $*$ be the **generic point** of $X$ in *scheme theoretic sense*.
Algebraic setting (first attempt):
Let $X = V(f_1, \ldots, f_m) \subseteq \mathbb{C}^n$ be algebraic variety, $\dim X = d$.
Let $g(x_1, \ldots, x_n)$ be polynomial.
Call $P \in X$ “sufficiently generic” for $g$ if
\[ g(P) = 0 \implies g|_X = 0. \]

Example: Let $\ast$ be the \textit{generic point} of $X$ in scheme theoretic sense.
Then $g(\ast) =$
Algebraic setting (first attempt):
Let \( X = V(f_1, \ldots, f_m) \subseteq \mathbb{C}^n \) be algebraic variety, \( \dim X = d \).
Let \( g(x_1, \ldots, x_n) \) be polynomial.
Call \( P \in X \) “sufficiently generic” for \( g \) if
\[
g(P) = 0 \implies g|_X = 0.
\]
Example: Let \( * \) be the generic point of \( X \) in scheme theoretic sense.
Then \( g(*) = g \mod I(X) \).
Algebraic setting (first attempt):

Let $X = V(f_1, \ldots, f_m) \subseteq \mathbb{C}^n$ be algebraic variety, $\dim X = d$.

Let $g(x_1, \ldots, x_n)$ be polynomial.

Call $P \in X$ “sufficiently generic” for $g$ if

$$g(P) = 0 \implies g|_X = 0.$$ 

Example: Let $\ast$ be the generic point of $X$ in scheme theoretic sense.

Then $g(\ast) = g \mod I(X)$. Thus $g(\ast) = 0$ iff $g|_X = 0$. 
Algebraic setting (first attempt):
Let $X = V(f_1, \ldots, f_m) \subseteq \mathbb{C}^n$ be algebraic variety, $\dim X = d$.
Let $g(x_1, \ldots, x_n)$ be polynomial.
Call $P \in X$ “sufficiently generic” for $g$ if
$$g(P) = 0 \quad \implies \quad g|_X = 0.$$ 

Example: Let $\ast$ be the generic point of $X$ in scheme theoretic sense.
Then $g(\ast) = g \mod I(X)$. Thus $g(\ast) = 0$ iff $g|_X = 0$.
$\implies$ Trivial!
Algebraic setting (first attempt):

Let $X = V(f_1, \ldots, f_m) \subseteq \mathbb{C}^n$ be algebraic variety, $\dim X = d$.

Let $g(x_1, \ldots, x_n)$ be polynomial.

Call $P \in X$ “sufficiently generic” for $g$ if

$$g(P) = 0 \implies g|_X = 0.$$  

Example: Let $\ast$ be the generic point of $X$ in scheme theoretic sense.

Then $g(\ast) = g \mod I(X)$. Thus $g(\ast) = 0$ iff $g|_X = 0$.

$\leadsto$ Trivial!

$\leadsto$ Useless...
Algebraic setting (first attempt):
Let \( X = V(f_1, \ldots, f_m) \subseteq \mathbb{C}^n \) be algebraic variety, \( \dim X = d \).
Let \( g(x_1, \ldots, x_n) \) be polynomial.
Call \( P \in X \) “sufficiently generic” for \( g \) if
\[
g(P) = 0 \implies g|_X = 0.
\]

Case \( X = \mathbb{C}^n \). Want \( P \) such that \( g(P) = 0 \implies g = 0. \)
**Algebraic setting** (first attempt):

Let $X = V(f_1, \ldots, f_m) \subseteq \mathbb{C}^n$ be algebraic variety, $\dim X = d$. 
Let $g(x_1, \ldots, x_n)$ be polynomial. 
Call $P \in X$ “sufficiently generic” for $g$ if 
\[ g(P) = 0 \implies g|_X = 0. \]

**Case** $X = \mathbb{C}^n$. Want $P$ such that 
\[ g(P) = 0 \implies g = 0. \]

**Schwartz-Zippel lemma** (1979–80; Ore 1922):
If $A \subset \mathbb{C}$ finite, $p_1, \ldots, p_n$ independent and uniformly at random from $A$, then 
\[ g \neq 0 \implies P[g(p_1, \ldots, p_n) = 0] \leq \frac{\deg g}{|A|}. \]
Algebraic setting (first attempt):

Let \( X = V(f_1, \ldots, f_m) \subseteq \mathbb{C}^n \) be algebraic variety, \( \dim X = d \).
Let \( g(x_1, \ldots, x_n) \) be polynomial.
Call \( P \in X \) “sufficiently generic” for \( g \) if

\[
g(P) = 0 \implies g|_X = 0.
\]

Case \( X = \mathbb{C}^n \). Want \( P \) such that \( g(P) = 0 \implies g = 0 \).
Algebraic setting (first attempt):

Let $X = V(f_1, \ldots, f_m) \subseteq \mathbb{C}^n$ be algebraic variety, $\dim X = d$. Let $g(x_1, \ldots, x_n)$ be polynomial.

Call $P \in X$ “sufficiently generic” for $g$ if

$$g(P) = 0 \implies g|_X = 0.$$ 

Case $X = \mathbb{C}^n$. Want $P$ such that $g(P) = 0 \implies g = 0$.

Combinatorial Nullstellensatz (Alon 1999, weak):

If $A \subseteq \mathbb{C}$, $|A| > \deg g$, then

$$g(A \times \ldots \times A) = 0 \implies g = 0.$$
Algebraic setting (first attempt):
Let \( X = V(f_1, \ldots, f_m) \subseteq \mathbb{C}^n \) be algebraic variety, \( \dim X = d \).
Let \( g(x_1, \ldots, x_n) \) be polynomial.
Call \( P \in X \) “sufficiently generic” for \( g \) if
\[
g(P) = 0 \quad \implies \quad g|_X = 0.
\]

Case \( X = \mathbb{C} \). Want \( P \) such that \( g(P) = 0 \quad \implies \quad g = 0 \).
Algebraic setting (first attempt):
Let \( X = V(f_1, \ldots, f_m) \subseteq \mathbb{C}^n \) be algebraic variety, \( \dim X = d \).
Let \( g(x_1, \ldots, x_n) \) be polynomial.
Call \( P \in X \) “sufficiently generic” for \( g \) if
\[
g(P) = 0 \implies g|_X = 0.
\]

Case \( X = \mathbb{C} \). Want \( P \) such that \( g(P) = 0 \implies g = 0 \).

**Lagrange’s theorem** (1798):
If \( g(t) = a_0 + a_1 t + \ldots + a_{n-1} t^{n-1} + t^n \), then
\[
|x| > \max \left( 1, \sum |a_i| \right) \implies g(x) \neq 0.
\]
Proofs by example

Want:

- sufficiently generic example $P$,
- example $P$ easy to construct,
- $g(P)$ easy to compute,
- allow for numerical margin of error.
Main theorem (over \( \mathbb{Q} \) with standard \(|\ .\ |\) (2019)).
Let
\[ X = V(f_1, \ldots, f_m) \subseteq \mathbb{Q}^n \text{ irreducible, } \dim X = d, \]
\[ g \text{ polynomial,} \]
\[ H := "\text{arithmetic complexity" of } (f_1, \ldots, f_m, g), \]
\[ P = (p_1, \ldots, p_n) \in \mathbb{Q}^n \text{ such that} \]
\[ 0 \ll_H h(p_1) \ll_H h(p_2) \ll_H \ldots \ll_H h(p_d). \]

Let \( \varepsilon := \varepsilon(H, h(p_d)) \). Then
\[
\text{if } \left\{ \begin{array}{l}
|f_i(P)| \leq \varepsilon \quad \forall i \quad \text{and} \\
|g(P)| \leq \varepsilon
\end{array} \right\} \implies g|_X = 0.
\]
Remarks

▶ “Robust one-point Nullstellensatz”
▶ Based on
  ▶ arithmetic Nullstellensatz [Krick–Pardo–Sombra]
  ▶ new effective Łojasiewicz inequality
▶ Way to remove irreducibility assumption on $X$.
▶ Way to remove knowledge of dimension of $X$.
▶ Motivates other “robust Nullstellensätze”.
▶ Motivates more general combinatorial Nullstellensätze.
A comparison:

Let $X = V(f_1, \ldots, f_m)$.

**Hilbert’s Nullstellensatz:**

$g|_X = 0 \iff g^N = \sum_i \lambda_i f_i$ for some $N$ and some polynomials $\lambda_i$

**Proof by example scheme:**

$g|_X = 0 \iff g(P) \approx 0$ for some sufficiently generic $P$ close to $X$
A comparison:

Let $X = V(f_1, \ldots, f_m)$.

**Hilbert’s Nullstellensatz:**

$g|_X = 0 \iff g^N = \sum_i \lambda_i f_i$ for some $N$ and some polynomials $\lambda_i$

**Proof by example scheme:**

$g|_X = 0 \iff g(P) \approx 0$ for some sufficiently generic $P$ close to $X$

$\implies$ new **witness** for $g|_X = 0$. 
Example: **Thales’ theorem**
Example: **Thales’ theorem**

![Diagram of Thales' theorem with points A, B, C, and angle α labeled. The diagram illustrates a right triangle within a semicircle with p1 and p2 marked.]

Choose $p_1 = 0.1234567890123$. Compute $p_2 = \sqrt{1 - p_2^2}$ up to 1300 digits of precision. $\Rightarrow$ works!
Example: Thales’ theorem

Choose \( p_1 = 0.1234567890123 \).
Example: Thales’ theorem

Choose $p_1 = 0.1234567890123$.

Compute $p_2 = \sqrt{1 - p_1^2}$ up to 1300 digits of precision.
Example: Thales’ theorem

Choose $p_1 = 0.1234567890123$.

Compute $p_2 = \sqrt{1 - p_1^2}$ up to 1300 digits of precision.

$\leadsto$ works!
Measuring dimension by example:
Measuring dimension by example:

If

- \( P \) sufficiently generic and close to \( X \), and
- \(| \det([e_1, e_2, \ldots, e_d, \nabla f_1(P), \ldots, \nabla f_{n-d}(P)])| > \varepsilon \),

then \( \dim X = d \).
Measuring dimension by example:

If

- $P$ sufficiently generic and close to $X$, and
- $| \det([e_1, e_2, \ldots, e_d, \nabla f_1(P), \ldots, \nabla f_{n-d}(P)])| > \varepsilon$,  

then $\dim X = d$.

Note: $\varepsilon$ is mild.

Equivalence if $X$ is smooth.
Can we decide *whether or not* $g|_x = 0$?
Can we decide whether or not $g|_x = 0$? – Yes!

~~ Dichotomy theorem:
Can we decide whether or not $g|_X = 0$? – Yes!

⇒ Dichotomy theorem:

If $P$ sufficiently generic and close enough to $X$, then either

Case 1: $|g(P)| \leq \varepsilon$ and $g|_X = 0$.

Case 2: $|g(P)| \geq 2\varepsilon$ and $g|_X \neq 0$. 
PROOFS BY EXAMPLE

Future topics:

1. Better bounds
2. Equivalence to arithmetic Nullstellensatz
3. Combinatorial Nullstellensatz for varieties
   - Proofs by examples (e.g. Thales, Pappus, Desargues)
   - Robust combinatorial/probabilistic Nullstellensätze
4. Comparison with Gröbner bases
5. Continuation of sequences
Thank you