Algebraic Independence Testing over Arbitrary Fields

Prerona Chatterjee

WIT 2018

June, 2018

Algebraic Independence

When are $v_1, \ldots, v_n$ linearly independent?

$$\sum_{i=1}^{n} \alpha_i v_i = 0 \Leftrightarrow \alpha_i = 0 \text{ for every } i.$$

Algebraic Independence

When are $v_1, \ldots, v_n$ linearly independent?

$$\sum_{i=1}^{n} \alpha_i v_i = 0 \Leftrightarrow \alpha_i = 0 \text{ for every } i.$$

When are $f_1, \ldots, f_k$ algebraically independent?

$$\sum_{\mathbf{e}:\sum e_i \leq d} \alpha_{\mathbf{e}} \prod_{i=1}^{k} f_i^{e_i} = 0 \Leftrightarrow \alpha_{\mathbf{e}} = 0 \text{ for every } d, \mathbf{e} = (e_1, \ldots, e_k).$$

Algebraic Independence

When are $v_1, \ldots, v_n$ linearly independent?

$$\sum_{i=1}^{n} \alpha_i v_i = 0 \Leftrightarrow \alpha_i = 0 \text{ for every } i.$$

When are $f_1, \ldots, f_k$ algebraically independent?

$$\sum_{\mathbf{e}:\sum e_i \le d} \alpha_{\mathbf{e}} \prod_{i=1}^{k} f_i^{e_i} = 0 \Leftrightarrow \alpha_{\mathbf{e}} = 0 \text{ for every } d, \mathbf{e} = (e_1, \ldots, e_k).$$

Question: Can we test algebraic independence efficiently?

Algebraic Independence

When are $v_1, \ldots, v_n$ linearly independent?

$$\sum_{i=1}^{n} \alpha_i v_i = 0 \Leftrightarrow \alpha_i = 0 \text{ for every } i.$$

When are $f_1, \ldots, f_k$ algebraically independent?

$$\sum_{\mathbf{e}:\sum e_i \le d} \alpha_{\mathbf{e}} \prod_{i=1}^{k} f_i^{e_i} = 0 \Leftrightarrow \alpha_{\mathbf{e}} = 0 \text{ for every } d, \mathbf{e} = (e_1, \ldots, e_k).$$

Question: Can we test algebraic independence efficiently?

[Kay09], [GSS18] : Even checking if $\alpha_{\mathbf{0}}$ is always zero is NP-hard.

Checking algebraic independence over characteristic zero fields

In a world where positive numbers don't add up to give zero:

For $f_1, f_2, \ldots, f_k \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ and $\mathbf{f} = (f_1, f_2, \ldots, f_k)$,

$$\mathbf{J_x}(\mathbf{f}) = \begin{bmatrix} \partial_{x_1}(f_1) & \partial_{x_2}(f_1) & \ldots & \partial_{x_n}(f_1) \\ \partial_{x_1}(f_2) & \partial_{x_2}(f_2) & \ldots & \partial_{x_n}(f_2) \\ \vdots & \vdots & \ddots & \vdots \\ \partial_{x_1}(f_k) & \partial_{x_2}(f_k) & \ldots & \partial_{x_n}(f_k) \end{bmatrix}$$

Checking algebraic independence over characteristic zero fields

In a world where positive numbers don't add up to give zero:

For $f_1, f_2, \ldots, f_k \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ and $\mathbf{f} = (f_1, f_2, \ldots, f_k)$,

$$\mathbf{J_x(f)} = \begin{bmatrix} \partial_{x_1}(f_1) & \partial_{x_2}(f_1) & \ldots & \partial_{x_n}(f_1) \\ \partial_{x_1}(f_2) & \partial_{x_2}(f_2) & \ldots & \partial_{x_n}(f_2) \\ \vdots & \vdots & \ddots & \vdots \\ \partial_{x_1}(f_k) & \partial_{x_2}(f_k) & \ldots & \partial_{x_n}(f_k) \end{bmatrix}$$

The Jacobian Criterion [Jac41]: $\{f_1, f_2, \ldots, f_k\}$ is algebraically independent if and only if its Jacobian matrix is full rank.

It doesn't work over arbitrary fields

In a world where 1 added up p times is zero:

$$f_1 = x^p,\ f_2 = y^p\ :\ \text{Algebraically Independent over } \mathbb{F}_p.$$

It doesn't work over arbitrary fields

In a world where 1 **added up** p **times is zero**:

$f_1 = x^p,\ f_2 = y^p$: Algebraically Independent over $\mathbb{F}_p$.

$$\mathbf{J}_{x,y} = \begin{bmatrix} px^{p-1} & 0 \\ 0 & py^{p-1} \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

It doesn't work over arbitrary fields

In a world where 1 added up p times is zero:

$$f_1 = x^p,\ f_2 = y^p : \text{ Algebraically Independent over } \mathbb{F}_p.$$

$$\mathbf{J}_{x,y} = \begin{bmatrix} px^{p-1} & 0 \\ 0 & py^{p-1} \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$f_1 = xy^{p-1},\ f_2 = x^{p-1}y : \text{ Algebraically Independent over } \mathbb{F}_p.$$

It doesn't work over arbitrary fields

In a world where 1 added up p times is zero:

$$f_1 = x^p,\ f_2 = y^p \ :\ \text{Algebraically Independent over } \mathbb{F}_p.$$

$$\mathbf{J}_{x,y} = \begin{bmatrix} px^{p-1} & 0 \\ 0 & py^{p-1} \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$f_1 = xy^{p-1},\ f_2 = x^{p-1}y \ :\ \text{Algebraically Independent over } \mathbb{F}_p.$$

$$\mathbf{J}_{x,y} = \begin{bmatrix} y^{p-1} & (p-1)xy^{p-2} \\ (p-1)x^{p-2}y & x^{p-1} \end{bmatrix} = \begin{bmatrix} y^{p-1} & -xy^{p-2} \\ -x^{p-2}y & x^{p-1} \end{bmatrix}$$

Checking algebraic independence over arbitrary fields

How hard is the problem?

[GSS18]: The question of checking whether a given set of polynomials are algebraically independent or not, is in AM $\cap$ co-AM and so "should not be" NP-hard.

Checking algebraic independence over arbitrary fields

How hard is the problem?

[GSS18]: The question of checking whether a given set of polynomials are algebraically independent or not, is in AM $\cap$ co-AM and so "should not be" NP-hard.

Is there any criterion?

[PSS16]: Gives a "Jacobian-like" criterion for algebraic independence, that can be efficiently tested only in a "very special" case.

Checking algebraic independence over arbitrary fields

How hard is the problem?

[GSS18]: The question of checking whether a given set of polynomials are algebraically independent or not, is in AM $\cap$ co-AM and so "should not be" NP-hard.

Is there any criterion?

[PSS16]: Gives a "Jacobian-like" criterion for algebraic independence, that can be efficiently tested only in a "very special" case.

What I am interested in: Is there a criterion that leads to an efficient test for Algebraic Independence in general?

Thank you!