How to express conjunction with few variables

Bernardo Rossi

Seminar Algebra and Discrete Mathematics
Institut für Algebra, JKU Linz

Boolean conjunction

The function $f\colon \{0,1\}^2 \to \{0,1\}$ defined by

$$\begin{aligned} f(0,0) &= 0 \\ f(0,1) &= 0 \\ f(1,0) &= 0 \\ f(1,1) &= 1 \end{aligned}$$

is called Boolean conjunction.
Usually $f(x,y)$ is denoted by $x \wedge y$ or $x \mathbin{\&} y$.

Boolean conjunction

The function $f\colon \{0,1\}^2 \to \{0,1\}$ defined by

$$\begin{aligned} f(0,0) &= 0 \\ f(0,1) &= 0 \\ f(1,0) &= 0 \\ f(1,1) &= 1 \end{aligned}$$

is called Boolean conjunction.
Usually $f(x,y)$ is denoted by $\boxed{x \wedge y}$ or $x \,\&\, y$.

we will use this notation

Generating functions

It is well known that each operation on $\{0,1\}$ can be defined starting from $\wedge$ and $\neg$, where $\neg\colon \{0,1\} \to \{0,1\}$ is

$$\neg(0) = 1 \quad \neg(1) = 0.$$

Generating functions

It is well known that each operation on $\{0,1\}$ can be defined starting from $\wedge$ and $\neg$, where $\neg\colon \{0,1\} \to \{0,1\}$ is

$$\neg(0) = 1 \quad \neg(1) = 0.$$

Example Let $\vee\colon \{0,1\}^2 \to \{0,1\}$ be

$$0 \vee 0 = 0 \quad 0 \vee 1 = 1 \quad 1 \vee 0 = 1 \quad 1 \vee 1 = 1.$$

Generating functions

It is well known that each operation on $\{0,1\}$ can be defined starting from $\wedge$ and $\neg$, where $\neg\colon \{0,1\} \to \{0,1\}$ is

$$\neg(0) = 1 \quad \neg(1) = 0.$$

Example Let $\vee\colon \{0,1\}^2 \to \{0,1\}$ be

$$0 \vee 0 = 0 \quad 0 \vee 1 = 1 \quad 1 \vee 0 = 1 \quad 1 \vee 1 = 1.$$

Then $x \vee y = \neg(\neg(x) \wedge \neg(y))$.

Generating conjunctions

When can we generate the function $\wedge$?

The answer is known and will be presented it in the next slides...

Generating conjunctions

When can we generate the function $\wedge$?

The answer is known and will be presented it in the next slides...

Before we consider some more examples...

Generating conjunctions

Example Let $f \colon \{0,1\}^n \to \{0,1\}$ be

$$f(a_1,\ldots,a_n) = \begin{cases} 0 & \text{if } 0 \in \{a_1,\ldots,a_n\} \\ 1 & \text{otherwise.} \end{cases}$$

Then

$$x_1 \wedge x_2 = f(x_1, x_2, \ldots, x_2).$$

Generating conjunctions

Example Let $f\colon \{0,1\}^n \to \{0,1\}$ be

$$f(a_1,\dots,a_n) = \begin{cases} 0 & \text{if } 0 \in \{a_1,\dots,a_n\} \\ 1 & \text{otherwise.} \end{cases}$$

Then

$$x_1 \wedge x_2 = f(x_1, x_2, \dots, x_2).$$

In fact

Generating conjunctions

Example Let $f\colon \{0,1\}^n \to \{0,1\}$ be

$$f(a_1,\dots,a_n) = \begin{cases} 0 & \text{if } 0 \in \{a_1,\dots,a_n\} \\ 1 & \text{otherwise.} \end{cases}$$

Then

$$x_1 \wedge x_2 = f(x_1, x_2, \dots, x_2).$$

In fact

$$f(0,0,\dots,0) = 0$$

Generating conjunctions

Example Let $f\colon \{0,1\}^n \to \{0,1\}$ be

$$f(a_1,\ldots,a_n) = \begin{cases} 0 & \text{if } 0 \in \{a_1,\ldots,a_n\} \\ 1 & \text{otherwise.} \end{cases}$$

Then

$$x_1 \wedge x_2 = f(x_1, x_2, \ldots, x_2).$$

In fact

$$\begin{aligned} f(0,0,\ldots,0) &= 0 \\ f(1,0,\ldots,0) &= 0 \end{aligned}$$

Generating conjunctions

Example Let $f\colon \{0,1\}^n \to \{0,1\}$ be

$$f(a_1,\dots,a_n) = \begin{cases} 0 & \text{if } 0 \in \{a_1,\dots,a_n\} \\ 1 & \text{otherwise.} \end{cases}$$

Then

$$x_1 \wedge x_2 = f(x_1, x_2, \dots, x_2).$$

In fact

$$\begin{aligned} f(0,0,\dots,0) &= 0 \\ f(1,0,\dots,0) &= 0 \\ f(0,1,\dots,1) &= 0 \end{aligned}$$

Generating conjunctions

Example Let $f\colon \{0,1\}^n \to \{0,1\}$ be

$$f(a_1,\dots,a_n) = \begin{cases} 0 & \text{if } 0 \in \{a_1,\dots,a_n\} \\ 1 & \text{otherwise.} \end{cases}$$

Then

$$x_1 \wedge x_2 = f(x_1, x_2, \dots, x_2).$$

In fact

$$\begin{aligned} f(0,0,\dots,0) &= 0 \\ f(1,0,\dots,0) &= 0 \\ f(0,1,\dots,1) &= 0 \\ f(1,1,\dots,1) &= 1 \end{aligned}$$

Generating conjunctions

If we want to generate $\wedge$ from f, we need to identify variables.

Generating conjunctions

If we want to generate $\wedge$ from f, we need to identify variables.

In the language with only one functional symbol f, one needs to write $n > 2$ variable symbols to represent $\wedge$.

Generating conjunctions

If we want to generate $\wedge$ from f, we need to identify variables.

In the language with only one functional symbol f, one needs to write $n > 2$ variable symbols to represent $\wedge$.

When do we only need two variable symbols to represent $\wedge$?

Structure of the talk

Clones and Post's Lattice

Algebras, terms and polynomials

Short conjunctions

Applications to the study of the complexity of the polynomial satisfiability problem

Clones and Post's Lattice

Function composition

Let A be a set, let $f \in A^{A^n}$, let $g_1, \ldots, g_n \in A^{A^k}$.
The composition of f with $g_1, \ldots, g_n$ is the element of A^{A^k}

$$(f \circ (g_1, \ldots, g_n))(a_1, \ldots, a_k) = f(g_1(a_1, \ldots, a_k), \ldots, g_n(a_1, \ldots, a_k)).$$

Function composition

Let A be a set, let $f \in A^{A^n}$, let $g_1, \dots, g_n \in A^{A^k}$.
The composition of f with $g_1, \dots, g_n$ is the element of A^{A^k}

$$(f \circ (g_1, \dots, g_n))(a_1, \dots, a_k) = f(g_1(a_1, \dots, a_k), \dots, g_n(a_1, \dots, a_k)).$$

Example

Let $f = x_1^2 + x_2^2 \in \mathbb{R}^{\mathbb{R}^2}$
let $g_1 = \cos(x_1) \in \mathbb{R}^{\mathbb{R}^1}$
let $g_2 = \sin(x_1) \in \mathbb{R}^{\mathbb{R}^1}$. Then

$$(f \circ (g_1, g_2)) = \cos^2(x_1) + \sin^2(x_1) = 1 \in \mathbb{R}^{\mathbb{R}^1}.$$

Projections

Let A be a set and let $k, n \in \mathbb{N}$ with $k \leq n$.
The k-th n-ary projection is the function

$$\pi_k^n(a_1, \ldots, a_n) = a_k.$$

Clones

Let A be a set and let C be a set of operations on A.
C is a clone if

- C contains all projections π_k^n
- C is closed under composition.

Clones

Let A be a set and let C be a set of operations on A.
C is a clone if

- C contains all projections π_k^n
- C is closed under composition.

Example Let $\mathbf{G}$ be a group.
The functions induced by words of the form

$$g_1 x_1^{l_1} g_2 x_2^{l_2} \dots g_n x_n^{l_n} g_{n+1}$$

with $n \in \mathbb{N}$ form a clone on G.

Clones

Let A be a set and let C be a set of operations on A.
C is a clone if

- C contains all projections π_k^n
- C is closed under composition.

Example Let $\mathbf{G}$ be a group.
The functions induced by words of the form

$$g_1 x_1^{l_1} g_2 x_2^{l_2} \dots g_n x_n^{l_n} g_{n+1}$$

with $n \in \mathbb{N}$ form a clone on G.

Example Let $\mathbf{K}$ be a field. The functions induced on K by the elements of $\mathbf{K}[x_1, \dots, x_n]$ (i.e. the polynimial functions) form a clone on K.

Clones

Less meaningful, but yet useful examples:

Example The set of all operations on a set A is a clone $\mathcal{O}_A$.

Clones

Less meaningful, but yet useful examples:

Example The set of all operations on a set A is a clone $\mathcal{O}_A$.

Example The set of projections on a set A is a clone $\mathcal{J}_A$.

Clones

Less meaningful, but yet useful examples:

Example The set of all operations on a set A is a clone $\mathcal{O}_A$.

Example The set of projections on a set A is a clone $\mathcal{J}_A$.

Theorem

The set $\mathcal{L}_A$ of the clones on a set A is a complete lattice with respect to set inclusion with top element $\mathcal{O}_A$ and bottom element $\mathcal{J}_A$.

Generating clones

Asking if an operation f on a set A can be defined starting from operations $g_1, \ldots, g_k$ is equivalent to the question:

Does f belong to the smallest clone that contains $g_1, \ldots, g_k$?

Generating clones

Asking if an operation f on a set A can be defined starting from operations $g_1, \ldots, g_k$ is equivalent to the question:

Does f belong to the smallest clone that contains $g_1, \ldots, g_k$?

Example Let $A = \{0, 1\}$. The clone generated by $\wedge, \neg$ is $\mathcal{O}_A$.

Generating clones

Asking if an operation f on a set A can be defined starting from operations $g_1, \dots, g_k$ is equivalent to the question:

Does f belong to the smallest clone that contains $g_1, \dots, g_k$?

Example Let $A = \{0, 1\}$. The clone generated by $\wedge, \neg$ is $\mathcal{O}_A$.

Example Let $A = \{0, 1\}$. The clone generated by $\wedge, \vee, 0, 1$ is the clone of monotone operations.

Clones on finite sets

Theorem [Ágoston, Demetrovics, Hánnak, 1983]

Let A be a finite set with at least three elements.
The following sets have cardinality $2^{\aleph_0}$:

- $\mathbb{R}$;

Clones on finite sets

Theorem [Ágoston, Demetrovics, Hánnak, 1983]

Let A be a finite set with at least three elements.
The following sets have cardinality $2^{\aleph_0}$:

- $\mathbb{R}$;
- $\{\mathrm{L} \in \mathcal{L}_A \mid \mathrm{L}$ contains all constant operations on $A\}$;

Clones on finite sets

Theorem [Ágoston, Demetrovics, Hánnak, 1983]

Let A be a finite set with at least three elements.
The following sets have cardinality $2^{\aleph_0}$:

- $\mathbb{R}$;
- $\{\mathrm{L} \in \mathcal{L}_{\mathrm{A}} \mid \mathrm{L}$ contains all constant operations on $A\}$;
- $\mathcal{P}(\mathcal{O}_{\mathrm{A}})$.

Post's Lattice

Theorem [Post, 1944]

On the two-element set there are

- $\aleph_0$ distinct clones;
- $\aleph_0$ distinct clones that contain $\wedge$;
- 7 distinct clones that contain all constants.

Post's Lattice

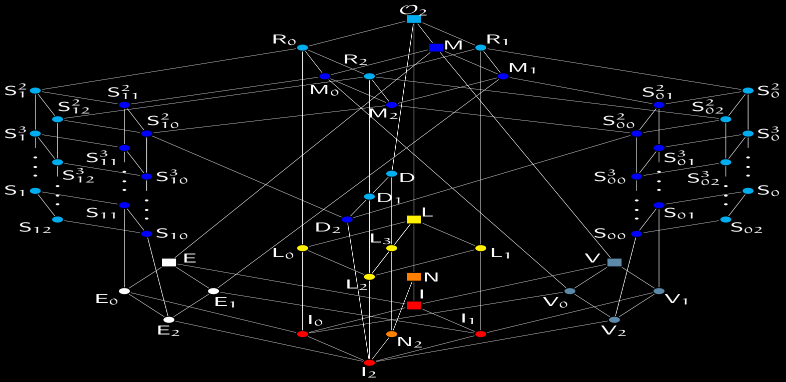
Theorem [Post, 1944]

On the two-element set there are

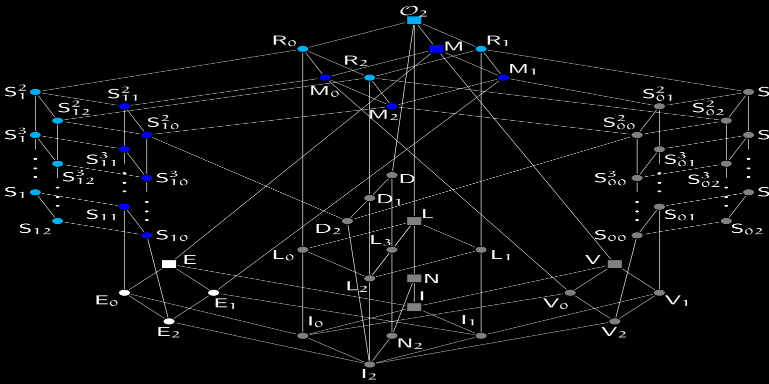
- $\aleph_0$ distinct clones;
- $\aleph_0$ distinct clones that contain $\wedge$;
- 7 distinct clones that contain all constants.

The lattice of clones on the two-element set is called **Post's Lattice**

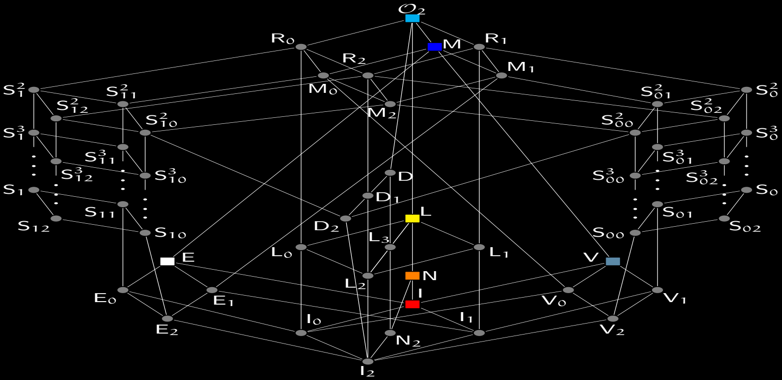
Post's Lattice



Clones that contain the Boolean conjunction



Constantive clones on $\{0, 1\}$



Algebras, terms and polynomials

Algebras

An algebra is a first order structure with only functional symbols.

Algebras

An algebra is a first order structure with only functional symbols.

$$\mathbf{A} = (\underbrace{\boxed{A}}_{\text{universe of } \mathbf{A}}; \{f_i^{\mathbf{A}} \mid i \in I\})$$

Algebras

An algebra is a first order structure with only functional symbols.

$$\mathbf{A} = (\boxed{A}; \boxed{\{f_i^{\mathbf{A}} \mid i \in I\}})$$

universe of $\mathbf{A}$ basic operations of $\mathbf{A}$

Algebras

An algebra is a first order structure with only functional symbols.

$$\mathbf{A} = (\underbrace{\boxed{A}}_{\text{universe of } \mathbf{A}}; \underbrace{\boxed{\{f_i^{\mathbf{A}} \mid i \in I\}}}_{\text{basic operations of } \mathbf{A}})$$

Example The lattice $\mathbf{L} = (\{0, 1\}; \wedge, \vee)$

Algebras

An algebra is a first order structure with only functional symbols.

$$\mathbf{A} = (\underbrace{A}_{\text{universe of } \mathbf{A}}; \underbrace{\{f_i^{\mathbf{A}} \mid i \in I\}}_{\text{basic operations of } \mathbf{A}})$$

Example The lattice $\mathbf{L} = (\underbrace{\{0, 1\}}_{\text{universe}}; \wedge, \vee)$

Algebras

An algebra is a first order structure with only functional symbols.

$$\mathbf{A} = (\underbrace{\boxed{A}}_{\text{universe of } \mathbf{A}}; \underbrace{\boxed{\{f_i^{\mathbf{A}} \mid i \in I\}}}_{\text{basic operations of } \mathbf{A}})$$

Example The lattice $\mathbf{L} = (\{0, 1\}; \underbrace{\boxed{\wedge, \vee}}_{\text{basic operations}})$

Algebras

Example

A group $\mathbf{G} = (G; +, -, 0)$ is an algebra on the language $\{f_+, f_-, f_0\}$.

Algebras

Example

A group $\mathbf{G} = (G; +, -, 0)$ is an algebra on the language $\{f_+, f_-, f_0\}$.

The operation $f_+^{\mathbf{G}} \colon G^2 \to G$ is defined by

$$(g_1, g_2) \mapsto g_1 + g_2.$$

Algebras

Example

A group $\mathbf{G} = (G; +, -, 0)$ is an algebra on the language $\{f_+, f_-, f_0\}$.

The operation $f_+^{\mathbf{G}} \colon G^2 \to G$ is defined by

$$(g_1, g_2) \mapsto g_1 + g_2.$$

The operation $f_-^{\mathbf{G}} \colon G \to G$ is defined by

$$g \mapsto -g.$$

Algebras

Example

A group $\mathbf{G} = (G; +, -, 0)$ is an algebra on the language $\{f_+, f_-, f_0\}$.

The operation $f_+^{\mathbf{G}} \colon G^2 \to G$ is defined by

$$(g_1, g_2) \mapsto g_1 + g_2.$$

The operation $f_-^{\mathbf{G}} \colon G \to G$ is defined by

$$g \mapsto -g.$$

The operation $f_0^{\mathbf{G}} \colon \{\emptyset\} \to G$ is defined by

$$0.$$

Term operations

Let $\mathbf{G} = (G; +, -, 0)$ be a group.

Term operations

Let $\mathbf{G} = (G; +, -, 0)$ be a group.

A term operation is an operation that can be written composing

- $+, -, 0$, i.e. the basic operations of $\mathbf{G}$,

Term operations

Let $\mathbf{G} = (G; +, -, 0)$ be a group.

A term operation is an operation that can be written composing

- $+, -, 0$, i.e. the basic operations of $\mathbf{G}$,
- the projections.

Term operations

Let $\mathbf{G} = (G; +, -, 0)$ be a group.

A term operation is an operation that can be written composing

- $+, -, 0$, i.e. the basic operations of $\mathbf{G}$,
- the projections.

The map $f \colon S_3^2 \to S_3$ given by

$$(x_1, x_2) \mapsto () \circ x_1 \circ () \circ x_2^{-1} \circ x_1$$

is a term operation.

Term operations

Let $\mathbf{G} = (G; +, -, 0)$ be a group.

A term operation is an operation that can be written composing

- $+, -, 0$, i.e. the basic operations of $\mathbf{G}$,
- the projections.

The map $f\colon S_3^2 \to S_3$ given by

$$(x_1, x_2) \mapsto () \circ x_1 \circ () \circ x_2^{-1} \circ x_1$$

is a term operation.

The term operations form a clone
$\mathrm{Clo}\,\mathbf{G}$ = the clone generated by the basic operations of $\mathbf{G}$.

Term operations

Is the map f given by

$$\begin{aligned} 0 &\mapsto 1 \\ 1 &\mapsto 0 \end{aligned}$$

a term operation of the two element lattice $(\{0, 1\}; \vee, \wedge)$?

Term operations

Is the map f given by

$$\begin{aligned} 0 &\mapsto 1 \\ 1 &\mapsto 0 \end{aligned}$$

a term operation of the two element lattice $(\{0,1\};\vee,\wedge)$?

No!

The maps $\vee$ and $\wedge$ both preserve the order $0 \leq 1$.

Term operations

Is the map f given by

$$\begin{aligned} 0 &\mapsto 1 \\ 1 &\mapsto 0 \end{aligned}$$

a term operation of the two element lattice $(\{0,1\};\vee,\wedge)$?

No!

The maps $\vee$ and $\wedge$ both preserve the order $0 \leq 1$.
The map f does not:

$$0 \leq 1 \text{ and}$$

Term operations

Is the map f given by

$$\begin{array}{ccc} 0 & \mapsto & 1 \\ 1 & \mapsto & 0 \end{array}$$

a term operation of the two element lattice $(\{0, 1\}; \vee, \wedge)$?

No!

The maps $\vee$ and $\wedge$ both preserve the order $0 \leq 1$.
The map f does not:

$$0 \leq 1 \text{ and } f(0) = 1 \not\leq 0 = f(1).$$

Hence f cannot be a composition of maps that preserve $\leq$.

Terms

How can we formally define a notion of length for a term operation?

Terms

How can we formally define a notion of length for a term operation?

How can we formally define the number of variables needed to represent a term operation?

Terms

Let L be a language with only functional symbols.

Terms

Let L be a language with only functional symbols.
Let X be a set with $\mathrm{X} \cap \mathrm{L} = \emptyset$.

Terms

Let L be a language with only functional symbols.
Let X be a set with $X \cap L = \emptyset$.
$T_L(X)$ is the smallest set of words on $L \cup X$ with

1. $X \cup \{f \in L \mid \text{arity}(f) = 0\} \subseteq T_L(X)$;

Terms

Let L be a language with only functional symbols.
Let X be a set with $X \cap L = \emptyset$.
$T_L(X)$ is the smallest set of words on $L \cup X$ with

1 $X \cup \{f \in L \mid \text{arity}(f) = 0\} \subseteq T_L(X)$;

2 $f \in L$,

Terms

Let L be a language with only functional symbols.
Let X be a set with $X \cap L = \emptyset$.
$T_L(X)$ is the smallest set of words on $L \cup X$ with

1. $X \cup \{f \in L \mid \text{arity}(f) = 0\} \subseteq T_L(X)$;
2. $f \in L$, $\text{arity}(f) = n$, $t_1, \ldots, t_n \in T_L(X)$

Terms

Let L be a language with only functional symbols.
Let X be a set with $X \cap L = \emptyset$.
$T_L(X)$ is the smallest set of words on $L \cup X$ with

1 $X \cup \{f \in L \mid \text{arity}(f) = 0\} \subseteq T_L(X)$;

2 $f \in L$, $\text{arity}(f) = n$, $t_1, \ldots, t_n \in T_L(X) \Rightarrow f t_1 \ldots t_n \in T_L(X)$.

Terms

Let L be a language with only functional symbols.
Let X be a set with $X \cap L = \emptyset$.
$T_L(X)$ is the smallest set of words on $L \cup X$ with

1 $X \cup \{f \in L \mid \text{arity}(f) = 0\} \subseteq T_L(X)$;

2 $f \in L$, $\text{arity}(f) = n$, $t_1, \ldots, t_n \in T_L(X) \Rightarrow ft_1 \ldots t_n \in T_L(X)$.

$T_L(X)$ is called the set of L-terms on X.

Terms

Let L be a language with only functional symbols.
Let X be a set with $X \cap L = \emptyset$.
$T_L(X)$ is the smallest set of words on $L \cup X$ with

1. $X \cup \{f \in L \mid \text{arity}(f) = 0\} \subseteq T_L(X)$;
2. $f \in L$, $\text{arity}(f) = n$, $t_1, \ldots, t_n \in T_L(X) \Rightarrow ft_1 \ldots t_n \in T_L(X)$.

$T_L(X)$ is called the set of L-terms on X.
When $X = \{x_1, \ldots, x_n\}$ we write $T_L(n)$.

Terms

Let L be a language with only functional symbols.
Let X be a set with $X \cap L = \emptyset$.
$T_L(X)$ is the smallest set of words on $L \cup X$ with

1 $X \cup \{f \in L \mid \text{arity}(f) = 0\} \subseteq T_L(X)$;

2 $f \in L$, $\text{arity}(f) = n$, $t_1, \ldots, t_n \in T_L(X) \Rightarrow ft_1 \ldots t_n \in T_L(X)$.

$T_L(X)$ is called the set of L-terms on X.
When $X = \{x_1, \ldots, x_n\}$ we write $T_L(n)$.
When $X = \{x_i \mid i \in \mathbb{N}\}$ we write $T_L(\omega)$.

Terms

Let L be a language with only functional symbols.
Let X be a set with $X \cap L = \emptyset$.
$T_L(X)$ is the smallest set of words on $L \cup X$ with

1 $X \cup \{f \in L \mid \text{arity}(f) = 0\} \subseteq T_L(X)$;

2 $f \in L$, $\text{arity}(f) = n$, $t_1, \ldots, t_n \in T_L(X) \Rightarrow ft_1 \ldots t_n \in T_L(X)$.

$T_L(X)$ is called the set of L-terms on X.
When $X = \{x_1, \ldots, x_n\}$ we write $T_L(n)$.
When $X = \{x_i \mid i \in \mathbb{N}\}$ we write $T_L(\omega)$.

$\mathbf{T}_L(n)$ is a L-algebra with the following interpretation of each $f \in L$

$$f^{\mathbf{T}_L(n)}(\, t_1 \,, \ldots, \, t_{\text{arity}(f)} \,) = ft_1 \ldots t_{\text{arity}(f)} \,.$$

Terms

Let L be a language with only functional symbols.
Let X be a set with $X \cap L = \emptyset$.
$T_L(X)$ is the smallest set of words on $L \cup X$ with

1 $X \cup \{f \in L \mid \text{arity}(f) = 0\} \subseteq T_L(X)$;

2 $f \in L$, $\text{arity}(f) = n$, $t_1, \ldots, t_n \in T_L(X) \Rightarrow ft_1 \ldots t_n \in T_L(X)$.

$T_L(X)$ is called the set of L-terms on X.

When $X = \{x_1, \ldots, x_n\}$ we write $T_L(n)$.

When $X = \{x_i \mid i \in \mathbb{N}\}$ we write $T_L(\omega)$.

$\mathbf{T}_L(n)$ is a L-algebra with the following interpretation of each $f \in L$

$$f^{\mathbf{T}_L(n)}(\underbrace{\boxed{t_1}}_{\in T_L(n)}, \ldots, t_{\text{arity}(f)}) = ft_1 \ldots t_{\text{arity}(f)}.$$

Terms

Let L be a language with only functional symbols.
Let X be a set with $X \cap L = \emptyset$.
$T_L(X)$ is the smallest set of words on $L \cup X$ with

1 $X \cup \{f \in L \mid \text{arity}(f) = 0\} \subseteq T_L(X)$;

2 $f \in L$, $\text{arity}(f) = n$, $t_1, \ldots, t_n \in T_L(X) \Rightarrow ft_1 \ldots t_n \in T_L(X)$.

$T_L(X)$ is called the set of L-terms on X.

When $X = \{x_1, \ldots, x_n\}$ we write $T_L(n)$.

When $X = \{x_i \mid i \in \mathbb{N}\}$ we write $T_L(\omega)$.

$\mathbf{T}_L(n)$ is a L-algebra with the following interpretation of each $f \in L$

$$f^{\mathbf{T}_L(n)}(t_1, \ldots, \underbrace{\boxed{t_{\text{arity}(f)}}}_{\in T_L(n)}) = ft_1 \ldots t_{\text{arity}(f)}.$$

Terms

Let L be a language with only functional symbols.
Let X be a set with $X \cap L = \emptyset$.
$T_L(X)$ is the smallest set of words on $L \cup X$ with

1 $X \cup \{f \in L \mid \text{arity}(f) = 0\} \subseteq T_L(X)$;

2 $f \in L$, $\text{arity}(f) = n$, $t_1, \ldots, t_n \in T_L(X) \Rightarrow ft_1 \ldots t_n \in T_L(X)$.

$T_L(X)$ is called the set of L-terms on X.

When $X = \{x_1, \ldots, x_n\}$ we write $T_L(n)$.

When $X = \{x_i \mid i \in \mathbb{N}\}$ we write $T_L(\omega)$.

$\mathbf{T}_L(n)$ is a L-algebra with the following interpretation of each $f \in L$

$$f^{\mathbf{T}_L(n)}(\,t_1\,, \ldots,\, t_{\text{arity}(f)}\,) = \underbrace{\boxed{ft_1 \ldots t_{\text{arity}(f)}}}_{\in T_L(n)}.$$

From terms to term operations

Theorem

Let L be a language.

1. The algebra $\mathbf{T}_L(X)$ is generated by X;
2. every mapping ϕ of X into any L-algebra $\mathbf{A}$ uniquely extends to a homomorphism $\overline{\phi}$ of $\mathbf{T}_L(X)$ into $\mathbf{A}$.

From terms to term operations

Theorem

Let L be a language.

1. The algebra $\mathbf{T}_L(X)$ is generated by X;
2. every mapping ϕ of X into any L-algebra $\mathbf{A}$ uniquely extends to a homomorphism $\overline{\phi}$ of $\mathbf{T}_L(X)$ into $\mathbf{A}$.

Let $\mathbf{A}$ be a L-algebra. For $k \in \mathbb{N}$ and $a_1, \ldots, a_k \in A^k$ we let

$$\phi_{\boldsymbol{a}} := \{(x_i, a_i) \mid i \in \{1, \ldots, k\}\}.$$

From terms to term operations

Theorem

Let L be a language.

1. The algebra $\mathbf{T}_L(X)$ is generated by X;
2. every mapping ϕ of X into any L-algebra $\mathbf{A}$ uniquely extends to a homomorphism $\overline{\phi}$ of $\mathbf{T}_L(X)$ into $\mathbf{A}$.

Let $\mathbf{A}$ be a L-algebra. For $k \in \mathbb{N}$ and $a_1, \ldots, a_k \in A^k$ we let

$$\phi_{\boldsymbol{a}} := \{(x_i, a_i) \mid i \in \{1, \ldots, k\}\}.$$

For $t \in T_L(x_1, \ldots, x_k)$, we let $t^{\mathbf{A}} \colon A^k \to A$ be

$$t^{\mathbf{A}}(a_1, \ldots, a_k) = \overline{\phi_{\boldsymbol{a}}}(t).$$

From terms to term operations

Theorem

Let L be a language.

1. The algebra $\mathbf{T}_L(X)$ is generated by X;
2. every mapping ϕ of X into any L-algebra $\mathbf{A}$ uniquely extends to a homomorphism $\overline{\phi}$ of $\mathbf{T}_L(X)$ into $\mathbf{A}$.

Let $\mathbf{A}$ be a L-algebra. For $k \in \mathbb{N}$ and $a_1, \ldots, a_k \in A^k$ we let

$$\phi_{\boldsymbol{a}} := \{(x_i, a_i) \mid i \in \{1, \ldots, k\}\}.$$

For $t \in T_L(x_1, \ldots, x_k)$, we let $t^{\mathbf{A}} \colon A^k \to A$ be

$$t^{\mathbf{A}}(a_1, \ldots, a_k) = \underbrace{\boxed{\overline{\phi_{\boldsymbol{a}}}}}_{T_L(k) \to A}(t).$$

From terms to term operations

Theorem

Let L be a language.

1. The algebra $\mathbf{T}_L(X)$ is generated by X;
2. every mapping ϕ of X into any L-algebra $\mathbf{A}$ uniquely extends to a homomorphism $\overline{\phi}$ of $\mathbf{T}_L(X)$ into $\mathbf{A}$.

Let $\mathbf{A}$ be a L-algebra. For $k \in \mathbb{N}$ and $a_1, \ldots, a_k \in A^k$ we let

$$\phi_{\boldsymbol{a}} := \{(x_i, a_i) \mid i \in \{1, \ldots, k\}\}.$$

For $t \in T_L(x_1, \ldots, x_k)$, we let $t^{\mathbf{A}} \colon A^k \to A$ be

$$t^{\mathbf{A}}(a_1, \ldots, a_k) = \underbrace{\boxed{\overline{\phi_{\boldsymbol{a}}}(t)}}_{\in A}.$$

From terms to term operations

Theorem

Let L be a language.

1. The algebra $\mathbf{T}_L(X)$ is generated by X;
2. every mapping ϕ of X into any L-algebra $\mathbf{A}$ uniquely extends to a homomorphism $\overline{\phi}$ of $\mathbf{T}_L(X)$ into $\mathbf{A}$.

Let $\mathbf{A}$ be a L-algebra. For $k \in \mathbb{N}$ and $a_1, \ldots, a_k \in A^k$ we let

$$\phi_{\boldsymbol{a}} := \{(x_i, a_i) \mid i \in \{1, \ldots, k\}\}.$$

For $t \in T_L(x_1, \ldots, x_k)$, we let $t^{\mathbf{A}} \colon A^k \to A$ be

$$\boxed{t^{\mathbf{A}}}(a_1, \ldots, a_k) = \overline{\phi_{\boldsymbol{a}}}(t).$$

$t \mapsto t^{\mathbf{A}} \colon T_L(k) \to A^{A^k}$

From terms to term operations

Theorem

Let L be a language.

1. The algebra $\mathbf{T}_L(X)$ is generated by X;
2. every mapping ϕ of X into any L-algebra $\mathbf{A}$ uniquely extends to a homomorphism $\overline{\phi}$ of $\mathbf{T}_L(X)$ into $\mathbf{A}$.

Let $\mathbf{A}$ be a L-algebra. For $k \in \mathbb{N}$ and $a_1, \ldots, a_k \in A^k$ we let

$$\phi_{\boldsymbol{a}} := \{(x_i, a_i) \mid i \in \{1, \ldots, k\}\}.$$

For $t \in T_L(x_1, \ldots, x_k)$, we let $t^{\mathbf{A}} \colon A^k \to A$ be

$$t^{\mathbf{A}}(a_1, \ldots, a_k) = \overline{\phi_{\boldsymbol{a}}}(t).$$

We have that

$$\operatorname{Clo} \mathbf{A} = \{\, t^{\mathbf{A}} \mid t \in T_L(n) \,\}.$$

Term operations: Length and number of variables

$\mathrm{L} = \{\mathrm{f}\}$ is a language with a unique functional symbol of arity 4.

Term operations: Length and number of variables

$L = \{f\}$ is a language with a unique functional symbol of arity 4.
Let $\mathbf{A} = (\{0, 1\}; f)$ where

$$f^{\mathbf{A}}(a_1, a_2, a_3, a_4) = \begin{cases} 0 & \text{if } 0 \in \{a_1, a_2, a_3, a_4\} \\ 1 & \text{otherwise.} \end{cases}$$

Term operations: Length and number of variables

$L = \{f\}$ is a language with a unique functional symbol of arity 4.
Let $\mathbf{A} = (\{0, 1\}; f)$ where

$$f^{\mathbf{A}}(a_1, a_2, a_3, a_4) = \begin{cases} 0 & \text{if } 0 \in \{a_1, a_2, a_3, a_4\} \\ 1 & \text{otherwise.} \end{cases}$$

We claim that $\wedge \in \operatorname{Clo} \mathbf{A}$.

Term operations: Length and number of variables

$L = \{f\}$ is a language with a unique functional symbol of arity 4.
Let $\mathbf{A} = (\{0, 1\}; f)$ where

$$f^{\mathbf{A}}(a_1, a_2, a_3, a_4) = \begin{cases} 0 & \text{if } 0 \in \{a_1, a_2, a_3, a_4\} \\ 1 & \text{otherwise.} \end{cases}$$

We claim that $\wedge \in \operatorname{Clo} \mathbf{A}$.

$f x_1 x_2 x_2 x_2 \in T_L(2)$;

Term operations: Length and number of variables

$L = \{f\}$ is a language with a unique functional symbol of arity 4.
Let $\mathbf{A} = (\{0, 1\}; f)$ where

$$f^{\mathbf{A}}(a_1, a_2, a_3, a_4) = \begin{cases} 0 & \text{if } 0 \in \{a_1, a_2, a_3, a_4\} \\ 1 & \text{otherwise.} \end{cases}$$

We claim that $\wedge \in \mathrm{Clo}\,\mathbf{A}$.

$fx_1x_2x_2x_2 \in T_L(2)$;

$\wedge = (fx_1x_2x_2x_2)^{\mathbf{A}}$:

Term operations: Length and number of variables

$L = \{f\}$ is a language with a unique functional symbol of arity 4.
Let $\mathbf{A} = (\{0, 1\}; f)$ where

$$f^{\mathbf{A}}(a_1, a_2, a_3, a_4) = \begin{cases} 0 & \text{if } 0 \in \{a_1, a_2, a_3, a_4\} \\ 1 & \text{otherwise.} \end{cases}$$

We claim that $\wedge \in \operatorname{Clo} \mathbf{A}$.

$fx_1x_2x_2x_2 \in T_L(2)$;

$\wedge = (fx_1x_2x_2x_2)^{\mathbf{A}}$:

$$(fx_1x_2x_2x_2)^{\mathbf{A}}(0, 0) = f^{\mathbf{A}}(0, 0, 0, 0) = 0,$$

Term operations: Length and number of variables

$L = \{f\}$ is a language with a unique functional symbol of arity 4.
Let $\mathbf{A} = (\{0, 1\}; f)$ where

$$f^{\mathbf{A}}(a_1, a_2, a_3, a_4) = \begin{cases} 0 & \text{if } 0 \in \{a_1, a_2, a_3, a_4\} \\ 1 & \text{otherwise.} \end{cases}$$

We claim that $\wedge \in \mathrm{Clo}\,\mathbf{A}$.

$fx_1x_2x_2x_2 \in T_L(2)$;

$\wedge = (fx_1x_2x_2x_2)^{\mathbf{A}}$:

$$(fx_1x_2x_2x_2)^{\mathbf{A}}(1, 0) = f^{\mathbf{A}}(1, 0, 0, 0) = 0,$$

Term operations: Length and number of variables

$L = \{f\}$ is a language with a unique functional symbol of arity 4. Let $\mathbf{A} = (\{0,1\}; f)$ where

$$f^{\mathbf{A}}(a_1, a_2, a_3, a_4) = \begin{cases} 0 & \text{if } 0 \in \{a_1, a_2, a_3, a_4\} \\ 1 & \text{otherwise.} \end{cases}$$

We claim that $\wedge \in \mathrm{Clo}\,\mathbf{A}$.

$fx_1x_2x_2x_2 \in T_L(2)$;

$\wedge = (fx_1x_2x_2x_2)^{\mathbf{A}}$:

$$(fx_1x_2x_2x_2)^{\mathbf{A}}(0,1) = f^{\mathbf{A}}(0,1,1,1) = 0,$$

Term operations: Length and number of variables

$L = \{f\}$ is a language with a unique functional symbol of arity 4.
Let $\mathbf{A} = (\{0, 1\}; f)$ where

$$f^{\mathbf{A}}(a_1, a_2, a_3, a_4) = \begin{cases} 0 & \text{if } 0 \in \{a_1, a_2, a_3, a_4\} \\ 1 & \text{otherwise.} \end{cases}$$

We claim that $\wedge \in \operatorname{Clo} \mathbf{A}$.

$f x_1 x_2 x_2 x_2 \in T_L(2)$;

$\wedge = (f x_1 x_2 x_2 x_2)^{\mathbf{A}}$:

$$(f x_1 x_2 x_2 x_2)^{\mathbf{A}}(1, 1) = f^{\mathbf{A}}(1, 1, 1, 1) = 1.$$

Term operations: Length and number of variables

The term $fx_2x_2x_1x_2$ also induces the function $\wedge$ on $\{0, 1\}$.

Term operations: Length and number of variables

The term $fx_2x_2x_1x_2$ also induces the function $\wedge$ on $\{0, 1\}$.

In general the map $t \mapsto t^{\mathbf{A}}$ is not injective.

Term operations: Length and number of variables

The term $fx_2x_2x_1x_2$ also induces the function $\wedge$ on $\{0, 1\}$.

In general the map $t \mapsto t^{\mathbf{A}}$ is not injective.

For $t \in T_L(\omega)$, $|t|$ is the length of t as a word on $\{x_i \mid i \in \mathbb{N}\} \cup L$.

Term operations: Length and number of variables

The term $fx_2x_2x_1x_2$ also induces the function $\wedge$ on $\{0, 1\}$.

In general the map $t \mapsto t^{\mathbf{A}}$ is not injective.

For $t \in T_L(\omega)$, $|t|$ is the length of t as a word on $\{x_i \mid i \in \mathbb{N}\} \cup L$.

$t \in T_L(n)$ is frugal if t contains exactly one occurrence of each symbol $x_1, \dots, x_n$.

Short conjunctions

Let $\mathbf{A} = (\{0, 1\}; L)$. Is there a frugal $t \in T_L(2)$ such that $t^{\mathbf{A}}$ is the Boolean conjunction?

Polynomials

Let $\mathbf{A}$ be an algebra with language L.
To each $a \in A$ we associate a 0-ary functional symbol c_a.

Polynomials

Let $\mathbf{A}$ be an algebra with language L.
To each $a \in A$ we associate a 0-ary functional symbol c_a.

$$L^* := L \cup \{c_a \mid a \in A\}.$$

Polynomials

Let $\mathbf{A}$ be an algebra with language L.
To each $a \in A$ we associate a 0-ary functional symbol c_a.

$$L^* := L \cup \{c_a \mid a \in A\}.$$

The polynomials of $\mathbf{A}$ on X are the elements of $\mathbf{T}_{L^*}(X)$.

We write $T_{\mathbf{A}}(X)$ for the set of polynomials of $\mathbf{A}$ on X.

Polynomials

Let $\mathbf{A}$ be an algebra with language L.
To each $a \in A$ we associate a 0-ary functional symbol c_a.

$$L^* := L \cup \{c_a \mid a \in A\}.$$

The polynomials of $\mathbf{A}$ on X are the elements of $\mathbf{T}_{L^*}(X)$.

We write $T_{\mathbf{A}}(X)$ for the set of polynomials of $\mathbf{A}$ on X.

The polynomial operations of $\mathbf{A}$ are the operations induced by the elements of $T_{\mathbf{A}}(\omega)$. They form a clone $\mathrm{Pol}\,\mathbf{A}$.

Polynomials and polynomial operations

The map $f\colon \mathbb{Z}_2^2 \to \mathbb{Z}_2$ given by

$$(x_1, x_2) \mapsto 1 + x_1 + 0 - x_2 + x_1 + 0$$

is a polynomial operation of the group $\mathbf{G} = (\mathbb{Z}_2; +, -, 0)$.

Short conjunctions

Main result

Theorem [Aichinger, R.]

Let $\mathbf{A} = (\{0,1\}; \mathrm{L})$ and let us assume that $\wedge \in \operatorname{Pol}\mathbf{A}$. Then there exists a frugal $\mathrm{t} \in \mathrm{T}_{\mathbf{A}}(2)$ such that $\mathrm{t}^{\mathbf{A}} = \wedge$.

Main result

Theorem [Aichinger, R.]

Let $\mathbf{A} = (\{0,1\}; L)$ and let us assume that $\wedge \in \operatorname{Pol} \mathbf{A}$.
Then there exists a frugal $t \in T_{\mathbf{A}}(2)$ such that $t^{\mathbf{A}} = \wedge$.

Example

Let $f\colon \{0,1\}^n \to \{0,1\}$ be

$$f(a_1, \dots, a_n) = \begin{cases} 0 & \text{if } 0 \in \{a_1, \dots, a_n\} \\ 1 & \text{otherwise.} \end{cases}$$

Main result

Theorem [Aichinger, R.]

Let $\mathbf{A} = (\{0,1\}; \mathrm{L})$ and let us assume that $\wedge \in \operatorname{Pol} \mathbf{A}$.
Then there exists a frugal $t \in T_{\mathbf{A}}(2)$ such that $t^{\mathbf{A}} = \wedge$.

Example

Let $f \colon \{0,1\}^n \to \{0,1\}$ be

$$f(a_1, \ldots, a_n) = \begin{cases} 0 & \text{if } 0 \in \{a_1, \ldots, a_n\} \\ 1 & \text{otherwise.} \end{cases}$$

Then for all $a_1, a_2 \in \{0,1\}$: $f(a_1, a_2, \ldots, a_2) = a_1 \wedge a_2$

Main result

Theorem [Aichinger, R.]

Let $\mathbf{A} = (\{0,1\}; \mathrm{L})$ and let us assume that $\wedge \in \operatorname{Pol} \mathbf{A}$. Then there exists a frugal $t \in T_{\mathbf{A}}(2)$ such that $t^{\mathbf{A}} = \wedge$.

Example

Let $f \colon \{0,1\}^n \to \{0,1\}$ be

$$f(a_1, \dots, a_n) = \begin{cases} 0 & \text{if } 0 \in \{a_1, \dots, a_n\} \\ 1 & \text{otherwise.} \end{cases}$$

Then for all $a_1, a_2 \in \{0,1\}$: $\boxed{f(a_1, a_2, \dots, a_2)} = a_1 \wedge a_2$

not frugal

Main result

Theorem [Aichinger, R.]

Let $\mathbf{A} = (\{0,1\}; \mathrm{L})$ and let us assume that $\wedge \in \operatorname{Pol} \mathbf{A}$.
Then there exists a frugal $t \in T_{\mathbf{A}}(2)$ such that $t^{\mathbf{A}} = \wedge$.

Example

Let $f\colon \{0,1\}^n \to \{0,1\}$ be

$$f(a_1, \dots, a_n) = \begin{cases} 0 & \text{if } 0 \in \{a_1, \dots, a_n\} \\ 1 & \text{otherwise.} \end{cases}$$

Then for all $a_1, a_2 \in \{0,1\}$: $f(a_1, a_2, \dots, a_2) = a_1 \wedge a_2$ and

$$f(a_1, a_2, 1, \dots, 1) = a_1 \wedge a_2.$$

Main result

Theorem [Aichinger, R.]

Let $\mathbf{A} = (\{0,1\}; L)$ and let us assume that $\wedge \in \operatorname{Pol} \mathbf{A}$.
Then there exists a frugal $t \in T_{\mathbf{A}}(2)$ such that $t^{\mathbf{A}} = \wedge$.

Example

Let $f\colon \{0,1\}^n \to \{0,1\}$ be

$$f(a_1, \dots, a_n) = \begin{cases} 0 & \text{if } 0 \in \{a_1, \dots, a_n\} \\ 1 & \text{otherwise.} \end{cases}$$

Then for all $a_1, a_2 \in \{0,1\}$: $f(a_1, a_2, \dots, a_2) = a_1 \wedge a_2$ and

$$\underbrace{\boxed{f(a_1, a_2, 1, \dots, 1)}}_{\text{frugal}} = a_1 \wedge a_2.$$

Main result

Theorem [Aichinger, R.]

Let $\mathbf{A} = (\{0,1\}; \mathrm{L})$ and let us assume that $\wedge \in \mathrm{Pol}\,\mathbf{A}$. Then there exists a frugal $t \in T_{\mathbf{A}}(2)$ such that $t^{\mathbf{A}} = \wedge$.

Example

Let $\mathbf{A} = \mathrm{GF}(2)$ and let $p \in T_{\mathbf{A}}(4) = \mathrm{GF}(2)[x_1, x_2, x_3, x_4]$ be

$$x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3^2 + x_4^2$$

Main result

Theorem [Aichinger, R.]

Let $\mathbf{A} = (\{0,1\}; L)$ and let us assume that $\wedge \in \operatorname{Pol} \mathbf{A}$. Then there exists a frugal $t \in T_{\mathbf{A}}(2)$ such that $t^{\mathbf{A}} = \wedge$.

Example

Let $\mathbf{A} = GF(2)$ and let $p \in T_{\mathbf{A}}(4) = GF(2)[x_1, x_2, x_3, x_4]$ be

$$x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3^2 + x_4^2$$

Then for all $a_1, a_2 \in \{0,1\}$

$$p^{\mathbf{A}}(a_1, a_2, a_2, a_2) = 3a_1a_2 + 4a_2^2 = a_1 \wedge a_2$$

Main result

Theorem [Aichinger, R.]

Let $\mathbf{A} = (\{0,1\}; L)$ and let us assume that $\wedge \in \operatorname{Pol} \mathbf{A}$.
Then there exists a frugal $t \in T_{\mathbf{A}}(2)$ such that $t^{\mathbf{A}} = \wedge$.

Example

Let $\mathbf{A} = GF(2)$ and let $p \in T_{\mathbf{A}}(4) = GF(2)[x_1, x_2, x_3, x_4]$ be

$$x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3^2 + x_4^2$$

Then for all $a_1, a_2 \in \{0,1\}$

$$\underbrace{\boxed{p^{\mathbf{A}}(a_1, a_2, a_2, a_2)}}_{\text{not frugal}} = 3a_1a_2 + 4a_2^2 = a_1 \wedge a_2$$

Main result

Theorem [Aichinger, R.]

Let $\mathbf{A} = (\{0,1\}; L)$ and let us assume that $\wedge \in \operatorname{Pol}\mathbf{A}$.
Then there exists a frugal $t \in T_{\mathbf{A}}(2)$ such that $t^{\mathbf{A}} = \wedge$.

Example

Let $\mathbf{A} = \mathrm{GF}(2)$ and let $p \in T_{\mathbf{A}}(4) = \mathrm{GF}(2)[x_1, x_2, x_3, x_4]$ be

$$x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3^2 + x_4^2$$

Then for all $a_1, a_2 \in \{0,1\}$

$$p^{\mathbf{A}}(a_1, a_2, a_2, a_2) = 3a_1a_2 + 4a_2^2 = a_1 \wedge a_2$$

and

$$p^{\mathbf{A}}(a_1, a_2, 0, 0) = a_1a_2 + 0 = a_1 \wedge a_2.$$

Main result

Theorem [Aichinger, R.]

Let $\mathbf{A} = (\{0,1\}; L)$ and let us assume that $\wedge \in \operatorname{Pol} \mathbf{A}$.
Then there exists a frugal $t \in T_{\mathbf{A}}(2)$ such that $t^{\mathbf{A}} = \wedge$.

Example

Let $\mathbf{A} = GF(2)$ and let $p \in T_{\mathbf{A}}(4) = GF(2)[x_1, x_2, x_3, x_4]$ be

$$x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3^2 + x_4^2$$

Then for all $a_1, a_2 \in \{0,1\}$

$$p^{\mathbf{A}}(a_1, a_2, a_2, a_2) = 3a_1a_2 + 4a_2^2 = a_1 \wedge a_2$$

and

$$\underbrace{\boxed{p^{\mathbf{A}}(a_1, a_2, 0, 0)}}_{\text{frugal}} = a_1a_2 + 0 = a_1 \wedge a_2.$$

Main result

Theorem [Aichinger, R.]

Let $\mathbf{A} = (\{0, 1\}; \mathrm{L})$ and let us assume that $\wedge \in \mathrm{Pol}\,\mathbf{A}$.
Then there exists a frugal $\mathrm{t} \in \mathrm{T}_{\mathbf{A}}(2)$ such that $\mathrm{t}^{\mathbf{A}} = \wedge$.

Proof by example

Main result

Theorem [Aichinger, R.]

Let $\mathbf{A} = (\{0, 1\}; L)$ and let us assume that $\wedge \in \mathrm{Pol}\,\mathbf{A}$. Then there exists a frugal $t \in T_{\mathbf{A}}(2)$ such that $t^{\mathbf{A}} = \wedge$.

Proof by example

$\wedge \in \mathrm{Pol}\,\mathbf{A}$

Main result

Theorem [Aichinger, R.]

Let $\mathbf{A} = (\{0,1\}; L)$ and let us assume that $\wedge \in \mathrm{Pol}\,\mathbf{A}$. Then there exists a frugal $t \in T_{\mathbf{A}}(2)$ such that $t^{\mathbf{A}} = \wedge$.

Proof by example

$$\begin{aligned}\wedge \in \mathrm{Pol}\,\mathbf{A} \Rightarrow &\exists m \in \mathbb{N} \\ &\exists s \in T_{\mathbf{A}}(m) \text{ frugal} \\ &\exists \tau\colon \{1,\ldots,m\} \to \{1,2\} \\ &\forall a_1, a_2 \in \{0,1\}:\end{aligned}$$

Main result

Theorem [Aichinger, R.]

Let $\mathbf{A} = (\{0,1\}; L)$ and let us assume that $\wedge \in \operatorname{Pol}\mathbf{A}$.
Then there exists a frugal $t \in T_{\mathbf{A}}(2)$ such that $t^{\mathbf{A}} = \wedge$.

Proof by example

$$\begin{aligned} \wedge \in \operatorname{Pol}\mathbf{A} \Rightarrow & \exists m \in \mathbb{N} \\ & \exists s \in T_{\mathbf{A}}(m) \text{ frugal} \\ & \exists \tau \colon \{1,\dots,m\} \to \{1,2\} \\ & \forall a_1, a_2 \in \{0,1\}\colon \end{aligned}$$

$$a_1 \wedge a_2 = s^{\mathbf{A}}(a_{\tau(1)},\dots,a_{\tau(m)}) = \left(s^{\mathbf{T_A}(2)}(x_{\tau(1)},\dots,x_{\tau(m)})\right)^{\mathbf{A}}(a_1,a_2)$$

Proof by example

Let $m = 5$, and $\tau = \{(1,1),(2,2),(3,2),(4,1),(5,1)\}$. Then

$$a_1 \wedge a_2 = s^{\mathbf{A}}(a_1, a_2, a_2, a_1, a_1).$$

Proof by example

Let $m = 5$, and $\tau = \{(1,1),(2,2),(3,2),(4,1),(5,1)\}$. Then

$$a_1 \wedge a_2 = s^{\mathbf{A}}(a_1, a_2, a_2, a_1, a_1).$$

Equivalently

$$\begin{aligned} s^{\mathbf{A}}(0,0,0,0,0) &= 0 \\ s^{\mathbf{A}}(0,1,1,0,0) &= 0 \\ s^{\mathbf{A}}(1,0,0,1,1) &= 0 \\ s^{\mathbf{A}}(1,1,1,1,1) &= 1 \end{aligned}$$

Proof by example

Let $m = 5$, and $\tau = \{(1,1),(2,2),(3,2),(4,1),(5,1)\}$. Then

$$a_1 \wedge a_2 = s^{\mathbf{A}}(a_1, a_2, a_2, a_1, a_1).$$

Equivalently

$$\begin{aligned} s^{\mathbf{A}}(0,0,0,0,0) &= 0 \\ s^{\mathbf{A}}(0,1,1,0,0) &= 0 \\ s^{\mathbf{A}}(1,0,0,1,1) &= 0 \\ s^{\mathbf{A}}(1,1,1,1,1) &= 1 \end{aligned}$$

We construct $\tilde{s} \in T_{\mathbf{A}}(\tilde{m})$ frugal and $\tilde{\tau}\colon \{1,\ldots,\tilde{m}\} \to \{1,2\}$ with

$$\begin{aligned} &\tilde{m} < m, \\ &\wedge = \left(\tilde{s}^{\mathbf{T}_{\mathbf{A}}(2)}(x_{\tilde{\tau}(1)},\ldots,x_{\tilde{\tau}(\tilde{m})})\right)^{\mathbf{A}} \end{aligned}$$

Proof by example

Case 1: The negation is induced by a frugal polynomial

Proof by example

Case 1: The negation is induced by a frugal polynomial

$$\exists w \in \mathsf{T}_{\mathbf{A}}(1)\colon w \text{ is frugal, } w^{\mathbf{A}}(0) = 1,\ w^{\mathbf{A}}(1) = 0$$

Proof by example

Case 1: The negation is induced by a frugal polynomial

$$\exists w \in \mathsf{T}_{\mathbf{A}}(1)\colon w \text{ is frugal, } w^{\mathbf{A}}(0) = 1,\ w^{\mathbf{A}}(1) = 0$$

Case 1.1: $s^{\mathbf{A}}(0,1,1,0,\boxed{1}) = 1$ and $s^{\mathbf{A}}(0,0,0,0,1) = 0$:

the last 0 of $(0,1,1,0,0)$

Proof by example

Case 1: The negation is induced by a frugal polynomial

$$\exists w \in \mathsf{T}_{\mathbf{A}}(1)\colon w \text{ is frugal}, w^{\mathbf{A}}(0) = 1, w^{\mathbf{A}}(1) = 0$$

Case 1.1: $s^{\mathbf{A}}(0, 1, 1, 0, 1) = 1$ and $s^{\mathbf{A}}(0, 0, 0, 0, 1) = 0$:

$$\wedge = \left(s^{\mathbf{T}_{\mathbf{A}}(2)}(0, x_1, x_1, 0, x_2)\right)^{\mathbf{A}}$$

Proof by example

Case 1: The negation is induced by a frugal polynomial

$$\exists w \in \mathsf{T}_{\mathbf{A}}(1)\colon w \text{ is frugal, } w^{\mathbf{A}}(0) = 1,\ w^{\mathbf{A}}(1) = 0$$

Case 1.1: $s^{\mathbf{A}}(0,1,1,0,1) = 1$ and $s^{\mathbf{A}}(0,0,0,0,1) = 0$:

$$\wedge = \left(s^{\mathbf{T}_{\mathbf{A}}(2)}(\boxed{0}, x_1, x_1, 0, x_2)\right)^{\mathbf{A}}$$

1^{st} 0 of $(0,1,1,0,0)$

Proof by example

Case 1: The negation is induced by a frugal polynomial

$$\exists w \in \mathsf{T}_{\mathbf{A}}(1)\colon w \text{ is frugal, } w^{\mathbf{A}}(0) = 1,\ w^{\mathbf{A}}(1) = 0$$

Case 1.1: $s^{\mathbf{A}}(0, 1, 1, 0, 1) = 1$ and $s^{\mathbf{A}}(0, 0, 0, 0, 1) = 0$:

$$\wedge = \left(s^{\mathbf{T}_{\mathbf{A}}(2)}(0, x_1, x_1, \boxed{0}, x_2)\right)^{\mathbf{A}}$$

last but one 0 of $(0, 1, 1, 0, 0)$

Proof by example

Case 1: The negation is induced by a frugal polynomial

$$\exists w \in \mathsf{T}_{\mathbf{A}}(1)\colon w \text{ is frugal, } w^{\mathbf{A}}(0) = 1,\ w^{\mathbf{A}}(1) = 0$$

Case 1.1: $s^{\mathbf{A}}(0,1,1,0,1) = 1$ and $s^{\mathbf{A}}(0,0,0,0,1) = 0$:

$$\wedge = \left(s^{\mathbf{T}_{\mathbf{A}}(2)}(0, x_1, x_1, 0, \boxed{x_2})\right)^{\mathbf{A}}$$

last 0 of $(0,1,1,0,0)$

Proof by example

Case 1: The negation is induced by a frugal polynomial

$$\exists w \in \mathsf{T}_{\mathbf{A}}(1)\colon w \text{ is frugal}, \ w^{\mathbf{A}}(0) = 1, \ w^{\mathbf{A}}(1) = 0$$

Case 1.1: $s^{\mathbf{A}}(0, 1, 1, 0, 1) = 1$ and $s^{\mathbf{A}}(0, 0, 0, 0, 1) = 0$:

$$\wedge = \big(s^{\mathbf{T_A}(2)}(0, \underbrace{\boxed{x_1, x_1}}_{\text{1s of } (0,1,1,0,0)}, 0, x_2)\big)^{\mathbf{A}}$$

Proof by example

Case 1: The negation is induced by a frugal polynomial

$$\exists w \in \mathrm{T}_{\mathbf{A}}(1) \colon w \text{ is frugal, } w^{\mathbf{A}}(0) = 1,\ w^{\mathbf{A}}(1) = 0$$

Case 1.1: $s^{\mathbf{A}}(0,1,1,0,1) = 1$ and $s^{\mathbf{A}}(0,0,0,0,1) = 0$:

$$\wedge = \left(s^{\mathbf{T}_{\mathbf{A}}(2)}(0, x_1, x_1, 0, x_2)\right)^{\mathbf{A}}$$

Case 1.2: $s^{\mathbf{A}}(0,1,1,0,1) = 0$ and $s^{\mathbf{A}}(0,0,0,0,1) = 1$:

$$\wedge = \left(s^{\mathbf{T}_{\mathbf{A}}(2)}(0, w^{\mathbf{T}_{\mathbf{A}}(1)}(x_1), w^{\mathbf{T}_{\mathbf{A}}(1)}(x_1), 0, x_2)\right)^{\mathbf{A}}$$

Proof by example

Case 1: The negation is induced by a frugal polynomial

$$\exists w \in \mathsf{T}_{\mathbf{A}}(1) \colon w \text{ is frugal}, \ w^{\mathbf{A}}(0) = 1, \ w^{\mathbf{A}}(1) = 0$$

Proof by example

Case 1: The negation is induced by a frugal polynomial

$$\exists w \in \mathsf{T}_{\mathbf{A}}(1) \colon w \text{ is frugal, } w^{\mathbf{A}}(0) = 1,\ w^{\mathbf{A}}(1) = 0$$

Case 1.3: $s^{\mathbf{A}}(0,1,1,0,1) = s^{\mathbf{A}}(0,0,0,0,1) = 0$:

$$\wedge = \left(s^{\mathbf{T}_{\mathbf{A}}(2)}(x_2, x_1, x_1, x_2, \boxed{1})\right)^{\mathbf{A}}$$

last 0 of $(0,1,1,0,0)$

Proof by example

Case 1: The negation is induced by a frugal polynomial

$$\exists w \in \mathsf{T}_{\mathbf{A}}(1)\colon w \text{ is frugal, } w^{\mathbf{A}}(0) = 1,\ w^{\mathbf{A}}(1) = 0$$

Case 1.3: $s^{\mathbf{A}}(0,1,1,0,1) = s^{\mathbf{A}}(0,0,0,0,1) = 0$:

$$\wedge = \left(s^{\mathbf{T}_{\mathbf{A}}(2)}(\boxed{x_2}, x_1, x_1, x_2, 1)\right)^{\mathbf{A}}$$

first 0 of $(0,1,1,0,0)$

Proof by example

Case 1: The negation is induced by a frugal polynomial

$$\exists w \in \mathrm{T}_{\mathbf{A}}(1)\colon w \text{ is frugal}, \; w^{\mathbf{A}}(0) = 1, \; w^{\mathbf{A}}(1) = 0$$

Case 1.3: $s^{\mathbf{A}}(0,1,1,0,1) = s^{\mathbf{A}}(0,0,0,0,1) = 0$:

$$\wedge = \left(s^{\mathbf{T}_{\mathbf{A}}(2)}(\, x_2\,,\, x_1, x_1\,, \boxed{x_2}, \; 1\,)\right)^{\mathbf{A}}$$

last but one 0 of $(0,1,1,0,0)$

Proof by example

Case 1: The negation is induced by a frugal polynomial

$$\exists w \in \mathrm{T}_{\mathbf{A}}(1)\colon w \text{ is frugal, } w^{\mathbf{A}}(0) = 1,\ w^{\mathbf{A}}(1) = 0$$

Case 1.3: $s^{\mathbf{A}}(0,1,1,0,1) = s^{\mathbf{A}}(0,0,0,0,1) = 0$:

$$\wedge = \left(s^{\mathbf{T}_{\mathbf{A}}(2)}(x_2, \boxed{x_1, x_1}, x_2, 1)\right)^{\mathbf{A}}$$

1s of $(0, 1, 1, 0, 0)$

Proof by example

Case 1: The negation is induced by a frugal polynomial

$$\exists w \in \mathrm{T}_{\mathbf{A}}(1) \colon w \text{ is frugal, } w^{\mathbf{A}}(0) = 1,\ w^{\mathbf{A}}(1) = 0$$

Case 1.3: $s^{\mathbf{A}}(0,1,1,0,1) = s^{\mathbf{A}}(0,0,0,0,1) = 0$:

$$\wedge = \left(s^{\mathbf{T_A}(2)}(\,x_2\,,\ x_1, x_1\,,\ x_2\,,\ 1\,)\right)^{\mathbf{A}}$$

Case 1.4: $s^{\mathbf{A}}(0,1,1,0,1) = s^{\mathbf{A}}(0,0,0,0,1) = 1$:

$$\wedge = \left(w^{\mathbf{T_A}(2)}\left(s^{\mathbf{T_A}(2)}(x_2, w^{\mathbf{T_A}(1)}(x_1), w^{\mathbf{T_A}(1)}(x_1), x_2, 1)\right)\right)^{\mathbf{A}}$$

Proof by example

Case 2: The negation is not induced by a frugal polynomial.

Case 2.1: $s^{\mathbf{A}}(0,1,1,1,1) = 1$:

$$\wedge = \left(s^{\mathbf{T}_{\mathbf{A}}(2)}(\,0\,,\ x_2, x_2\,,\ x_1, x_1\,)\right)^{\mathbf{A}}.$$

Proof by example

Case 2: The negation is not induced by a frugal polynomial.

Case 2.1: $s^{\mathbf{A}}(0, 1, 1, 1, 1) = 1$:

$$\wedge = \left(s^{\mathbf{T}_{\mathbf{A}}(2)}(\underbrace{\boxed{0}}_{1^{\text{st}}\text{ component}}, x_2, x_2, x_1, x_1)\right)^{\mathbf{A}}.$$

Proof by example

Case 2: The negation is not induced by a frugal polynomial.

Case 2.1: $s^{\mathbf{A}}(0,1,1,1,1) = 1$:

$$\wedge = \left(s^{\mathbf{T}_{\mathbf{A}}(2)}(\,0\,,\underbrace{\boxed{x_2, x_2}}_{\text{1s of } (0,1,1,0,0)}, x_1, x_1\,)\right)^{\mathbf{A}}.$$

Proof by example

Case 2: The negation is not induced by a frugal polynomial.

Case 2.1: $s^{\mathbf{A}}(0,1,1,1,1) = 1$:

$$\wedge = \left(s^{\mathbf{T}_{\mathbf{A}}(2)}(0, x_2, x_2, \boxed{x_1, x_1})\right)^{\mathbf{A}}.$$

0s of $(0,1,1,0,0)$

Proof by example

Case 2: The negation is not induced by a frugal polynomial.

Case 2.1: $s^{\mathbf{A}}(0,1,1,1,1) = 1$:

$$\wedge = \left(s^{\mathbf{T}_{\mathbf{A}}(2)}(\,0\,,\,x_2,x_2\,,\,x_1,x_1\,)\right)^{\mathbf{A}}.$$

In fact $s^{\mathbf{A}}(0,0,0,1,1) = 0$. Since, if $s^{\mathbf{A}}(0,0,0,1,1) = 1$, then $s^{\mathbf{T}_{\mathbf{A}}(1)}(x_1,0,0,1,1)$ would induce the negation and be frugal.

Proof by example

Case 2: The negation is not induced by a frugal polynomial.

Case 2.2: $s^{\mathbf{A}}(1,0,1,1,1) = 1$:

$$\wedge = \left(s^{\mathbf{T_A}(2)}(x_2, 0, x_1, x_2, x_2)\right)^{\mathbf{A}}.$$

Proof by example

Case 2: The negation is not induced by a frugal polynomial.

Case 2.2: $s^{\mathbf{A}}(1,0,1,1,1) = 1$:

$$\wedge = \left(s^{\mathbf{T_A}(2)}(x_2, 0, x_1, x_2, x_2)\right)^{\mathbf{A}}.$$

In fact $s^{\mathbf{A}}(0,0,1,0,0) = 0$. Since, if $s^{\mathbf{A}}(0,0,1,0,0) = 1$, then $s^{\mathbf{T_A}(1)}(0, x_1, 1, 0, 0)$ would induce the negation and be frugal.

Proof by example

Case 2: The negation is not induced by a frugal polynomial.

Case 2.3: $s^{\mathbf{A}}(0,1,1,1,1) = s^{\mathbf{A}}(1,0,1,1,1) = 0$:

Proof by example

Case 2: The negation is not induced by a frugal polynomial.

Case 2.3: $s^{\mathbf{A}}(0,1,1,1,1) = s^{\mathbf{A}}(1,0,1,1,1) = 0$:

$$\wedge = \left(s^{\mathbf{T_A}(2)}(x_1, x_2, 1, 1, 1)\right)^{\mathbf{A}}.$$

Proof by example

Case 2: The negation is not induced by a frugal polynomial.

Case 2.3: $s^{\mathbf{A}}(0,1,1,1,1) = s^{\mathbf{A}}(1,0,1,1,1) = 0$:

$$\wedge = \left(s^{\mathbf{T}_{\mathbf{A}}(2)}(x_1, x_2, 1, 1, 1)\right)^{\mathbf{A}}.$$

Note that if $s^{\mathbf{A}}(0,0,1,1,1) = 1$, then $s^{\mathbf{T}_{\mathbf{A}}(1)}(x_1, 0, 1, 1, 1)$ would induce the negation and be frugal.

Applications to the study of the complexity of $\textsc{PolSat}\ \mathbf{A}$

The polynomial satifiability problem

The problem $\textsc{PolSat}(\mathbf{A})$ is the following search problem:

The polynomial satifiability problem

The problem $\textsc{PolSat}(\mathbf{A})$ is the following search problem:

$$\text{Given } p, q \in T_{\mathbf{A}}(n)$$
$$\text{find } \boldsymbol{a} \in A^n \text{ such that}$$
$$p^{\mathbf{A}}(\boldsymbol{a}) = q^{\mathbf{A}}(\boldsymbol{a}).$$

The polynomial satifiability problem

The problem $\textsc{PolSat}(\mathbf{A})$ is the following search problem:

$$\begin{gathered}\text{Given } p, q \in T_{\mathbf{A}}(n) \\ \text{find } \boldsymbol{a} \in A^n \text{ such that} \\ p^{\mathbf{A}}(\boldsymbol{a}) = q^{\mathbf{A}}(\boldsymbol{a}).\end{gathered}$$

The complexity parameter of $\textsc{PolSat}(\mathbf{A})$ is $|p| + |q|$.

The Exponential Time Hypothesis

The exponential time hypothesis implies that there exists no sub-exponential time algorithm that solves $3\mathrm{SAT}$.

When is PolSat($\mathbf{A}$) not solvable in sub-exponential time

Theorem
[Gorazd, Krzaczkowski, 2011]

Let $\mathbf{A}$ be an algebra on $\{0, 1\}$.

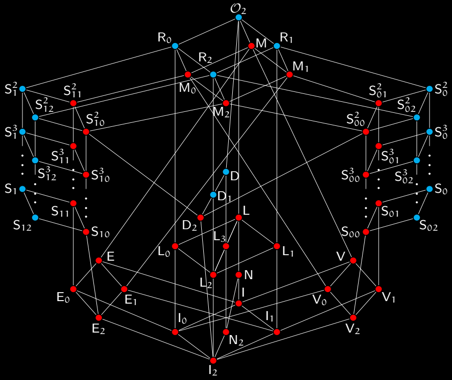
When is PolSat$(\mathbf{A})$ not solvable in sub-exponential time

Theorem

[Gorazd, Krzaczkowski, 2011]

Let $\mathbf{A}$ be an algebra on $\{0, 1\}$.

$\text{Clo}\,\mathbf{A} \Rightarrow \textsc{PolSat}(\mathbf{A})$ in P.



When is PolSat$(\mathbf{A})$ not solvable in sub-exponential time

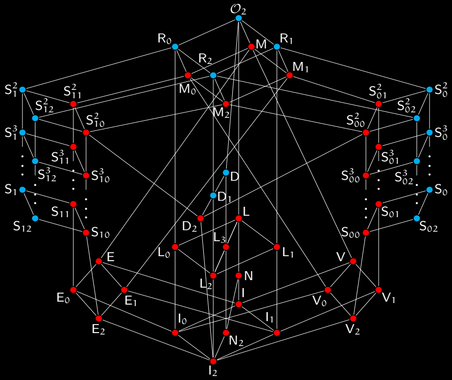
Theorem

[Gorazd, Krzaczkowski, 2011]

Let $\mathbf{A}$ be an algebra on $\{0,1\}$.

$\mathrm{Clo}\,\mathbf{A} \Rightarrow \textsc{PolSat}(\mathbf{A})$ in P.

$\mathrm{Clo}\,\mathbf{A} \Rightarrow$
$\textsc{PolSat}(\mathbf{A})$ NP-complete.



When is PolSat$(\mathbf{A})$ not solvable in sub-exponential time

Theorem
[Aichinger, R.]

Let $\mathbf{A}$ be an algebra on $\{0, 1\}$.

$\mathrm{Clo}\,\mathbf{A} \Rightarrow \textsc{PolSat}(\mathbf{A})$ in P.

$\mathrm{Clo}\,\mathbf{A} \Rightarrow$
no sub-exponential time algorithm that solves $\textsc{PolSat}(\mathbf{A})$ under ETH.