ACCL Lecture 1: Classical Propositional Logic: main notions and results & more

Evgeny Zolin

Department of Mathematical Logic and Theory of Algorithms
Faculty of Mechanics and Mathematics
Moscow State University

Advanced Course in Classical Logic
24.02.2021

Advanced Course in Classical Logic

The Course consists of two parts:

Advanced Course in Classical Logic

The Course consists of two parts:

1. Classical Propositional Logic

Advanced Course in Classical Logic

The Course consists of two parts:

1. Classical Propositional Logic
2. Classical Predicate Logic

Advanced Course in Classical Logic

The Course consists of two parts:

1. Classical Propositional Logic
2. Classical Predicate Logic

It contains topics that are usually not in the standard courses on Mathematical Logic.

Advanced Course in Classical Logic

The Course consists of two parts:

1. Classical Propositional Logic
2. Classical Predicate Logic

It contains topics that are usually not in the standard courses on Mathematical Logic.

This lecture is on **Classical propositional logic**:

- syntax, semantics,
- axiomatization, completeness,
- compactness,
- decidability,
- interpolation,
- peculiar properties.

Classical Propositional Logic: Syntax

Propositional variables: $\mathrm{Var} = \{p_0, p_1, \ldots\}$ — a countable set.

Classical Propositional Logic: Syntax

Propositional variables: $\mathrm{Var} = \{p_0, p_1, \ldots\}$ — a countable set.

Connectives:

Classical Propositional Logic: Syntax

Propositional variables: $\mathsf{Var} = \{p_0, p_1, \ldots\}$ — a countable set.

Connectives:

$\neg$ 'not', *negation*

Classical Propositional Logic: Syntax

Propositional variables: $\mathrm{Var} = \{p_0, p_1, \ldots\}$ — a countable set.

Connectives:

- $\neg$ 'not', *negation*
- $\wedge$ 'and', *conjunction* (sometimes denoted by $\&$)

Classical Propositional Logic: Syntax

Propositional variables: $\mathsf{Var} = \{p_0, p_1, \ldots\}$ — a countable set.

Connectives:

- $\neg$ 'not', *negation*
- $\wedge$ 'and', *conjunction* (sometimes denoted by $\&$)
- $\vee$ 'or', *disjunction*

Classical Propositional Logic: Syntax

Propositional variables: $\mathsf{Var} = \{p_0, p_1, \ldots\}$ — a countable set.

Connectives:

$\neg$	'not', *negation*
$\wedge$	'and', *conjunction* (sometimes denoted by $\&$)
$\vee$	'or', *disjunction*
$\rightarrow$	'if...then...', *implication*

Classical Propositional Logic: Syntax

Propositional variables: $\mathsf{Var} = \{p_0, p_1, \ldots\}$ — a countable set.

Connectives:

$\neg$	'not', *negation*
$\wedge$	'and', *conjunction* (sometimes denoted by $\&$)
$\vee$	'or', *disjunction*
$\rightarrow$	'if...then...', *implication*
$\leftrightarrow$	'if and only if', 'iff', *equivalence* (usually not a primitive symbol)

Classical Propositional Logic: Syntax

Propositional variables: $\mathrm{Var} = \{p_0, p_1, \ldots\}$ — a countable set.

Connectives:

$\neg$	'not', *negation*
$\wedge$	'and', *conjunction* (sometimes denoted by $\&$)
$\vee$	'or', *disjunction*
$\to$	'if...then...', *implication*
$\leftrightarrow$	'if and only if', 'iff', *equivalence* (usually not a primitive symbol)

$\neg$ is a unary connective, $\wedge, \vee, \to, \leftrightarrow$ are binary connectives.

Classical Propositional Logic: Syntax

Propositional variables: $\mathrm{Var} = \{p_0, p_1, \ldots\}$ — a countable set.

Connectives:

$\neg$	'not', *negation*
$\wedge$	'and', *conjunction* (sometimes denoted by $\&$)
$\vee$	'or', *disjunction*
$\to$	'if...then...', *implication*
$\leftrightarrow$	'if and only if', 'iff', *equivalence* (usually not a primitive symbol)

$\neg$ is a unary connective, $\wedge, \vee, \to, \leftrightarrow$ are binary connectives.

Constants (nullary connectives):

- $\top$ (true)
- $\bot$ (false).

Classical Propositional Logic: Syntax

Propositional variables: $\mathrm{Var} = \{p_0, p_1, \ldots\}$ — a countable set.

Connectives:

$\neg$	'not', *negation*
$\wedge$	'and', *conjunction* (sometimes denoted by $\&$)
$\vee$	'or', *disjunction*
$\to$	'if...then...', *implication*
$\leftrightarrow$	'if and only if', 'iff', *equivalence* (usually not a primitive symbol)

$\neg$ is a unary connective, $\wedge, \vee, \to, \leftrightarrow$ are binary connectives.

Constants (nullary connectives):

- $\top$ (true)
- $\bot$ (false).

In formulas, we also use parentheses: (and).

Classical Propositional Logic: Syntax

Definition

Formulas are defined by induction:

Classical Propositional Logic: Syntax

Definition

Formulas are defined by induction:

- the symbols $\bot$ and $\top$ are formulas,

Classical Propositional Logic: Syntax

Definition

Formulas are defined by induction:

- the symbols $\perp$ and $\top$ are formulas,
- every variable p_i is a formula,

Classical Propositional Logic: Syntax

Definition

Formulas are defined by induction:

- the symbols $\perp$ and $\top$ are formulas,
- every variable p_i is a formula,
- if A is a formula, then $\neg A$ is a formula,

Definition

Formulas are defined by induction:

- the symbols $\bot$ and $\top$ are formulas,
- every variable p_i is a formula,
- if A is a formula, then $\neg A$ is a formula,
- if A, B are formulas, then $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ are formulas.

Classical Propositional Logic: Syntax

Definition

Formulas are defined by induction:

- the symbols $\bot$ and $\top$ are formulas,
- every variable p_i is a formula,
- if A is a formula, then $\neg A$ is a formula,
- if A, B are formulas, then $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ are formulas.

This definition can be written concisely:

$$A, B \ ::= \ \bot \ \mid \ \top \ \mid \ p_i \ \mid \ \neg A \ \mid \ (A \wedge B) \ \mid \ (A \vee B) \ \mid \ (A \to B).$$

Classical Propositional Logic: Syntax

Definition

Formulas are defined by induction:

- the symbols $\bot$ and $\top$ are formulas,
- every variable p_i is a formula,
- if A is a formula, then $\neg A$ is a formula,
- if A, B are formulas, then $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ are formulas.

This definition can be written concisely:

$$A, B \ ::= \ \bot \ \mid \ \top \ \mid \ p_i \ \mid \ \neg A \ \mid \ (A \wedge B) \ \mid \ (A \vee B) \ \mid \ (A \to B).$$

Definitions (grammars) like this are in Backus–Naur form.

Classical Propositional Logic: Syntax

Definition

Formulas are defined by induction:

- the symbols $\bot$ and $\top$ are formulas,
- every variable p_i is a formula,
- if A is a formula, then $\neg A$ is a formula,
- if A, B are formulas, then $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ are formulas.

This definition can be written concisely:

$$A, B \ ::= \ \bot \ | \ \top \ | \ p_i \ | \ \neg A \ | \ (A \wedge B) \ | \ (A \vee B) \ | \ (A \to B).$$

Definitions (grammars) like this are in Backus–Naur form.

The set of all formulas is denoted by Fm.

Classical Propositional Logic: Syntax

Definition

Formulas are defined by induction:

- the symbols $\bot$ and $\top$ are formulas,
- every variable p_i is a formula,
- if A is a formula, then $\neg A$ is a formula,
- if A, B are formulas, then $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ are formulas.

This definition can be written concisely:

$$A, B \ ::= \ \bot \ | \ \top \ | \ p_i \ | \ \neg A \ | \ (A \wedge B) \ | \ (A \vee B) \ | \ (A \to B).$$

Definitions (grammars) like this are in Backus–Naur form.

The set of all formulas is denoted by Fm.
Fm is a *countable* set. Why?

Classical Propositional Logic: Semantics

Definition

A valuation is any function $v \colon \mathrm{Var} \to \{0, 1\}$.

So, to every variable p_i the valuation v assigns a digit (bit) 0 or 1.

Classical Propositional Logic: Semantics

Definition

A valuation is any function $v \colon \mathrm{Var} \to \{0, 1\}$.

So, to every variable p_i the valuation v assigns a digit (bit) 0 or 1.
We extend v from Var to all formulas $v \colon \mathrm{Fm} \to \{0, 1\}$ by induction:

Classical Propositional Logic: Semantics

Definition

A valuation is any function $v\colon \mathrm{Var} \to \{0,1\}$.

So, to every variable p_i the valuation v assigns a digit (bit) 0 or 1.
We extend v from Var to all formulas $v\colon \mathrm{Fm} \to \{0,1\}$ by induction:

$$v(\top) = 1, \quad v(\bot) = 0,$$

Classical Propositional Logic: Semantics

Definition

A valuation is any function $v\colon \mathsf{Var} \to \{0,1\}$.

So, to every variable p_i the valuation v assigns a digit (bit) 0 or 1.
We extend v from Var to all formulas $v\colon \mathsf{Fm} \to \{0,1\}$ by induction:

$$v(\top) = 1, \quad v(\bot) = 0, \quad v(\neg A) = 1 - v(A),$$
$$v(A \star B) = \text{ according to the } \textit{truth tables}$$

Definition

A valuation is any function $v\colon \mathrm{Var} \to \{0,1\}$.

So, to every variable p_i the valuation v assigns a digit (bit) 0 or 1.
We extend v from Var to all formulas $v\colon \mathrm{Fm} \to \{0,1\}$ by induction:

$$v(\top) = 1, \quad v(\bot) = 0, \quad v(\neg A) = 1 - v(A),$$
$$v(A \star B) = \text{ according to the } \textit{truth tables}$$

A	B	$A \wedge B$	$A \vee B$	$A \to B$
0	0	0	0	1
0	1	0	1	1
1	0	0	1	0
1	1	1	1	1

Classical Propositional Logic: Semantics

Definition

A valuation is any function $v\colon \mathrm{Var} \to \{0,1\}$.

So, to every variable p_i the valuation v assigns a digit (bit) 0 or 1.
We extend v from Var to all formulas $v\colon \mathrm{Fm} \to \{0,1\}$ by induction:

$$v(\top) = 1, \quad v(\bot) = 0, \quad v(\neg A) = 1 - v(A),$$
$$v(A \star B) = \text{ according to the } \textit{truth tables}$$

A	B	$A \wedge B$	$A \vee B$	$A \to B$
0	0	0	0	1
0	1	0	1	1
1	0	0	1	0
1	1	1	1	1

If $v(A) = 1$, we write $v \models A$ and say: "A is true under the valuation v".

Classical Propositional Logic: Semantics

Definition

A valuation is any function $v\colon \mathrm{Var} \to \{0,1\}$.

So, to every variable p_i the valuation v assigns a digit (bit) 0 or 1.
We extend v from Var to all formulas $v\colon \mathrm{Fm} \to \{0,1\}$ by induction:

$$v(\top) = 1, \quad v(\bot) = 0, \quad v(\neg A) = 1 - v(A),$$
$$v(A \star B) = \text{ according to the } \textit{truth tables}$$

A	B	$A \wedge B$	$A \vee B$	$A \to B$
0	0	0	0	1
0	1	0	1	1
1	0	0	1	0
1	1	1	1	1

If $v(A) = 1$, we write $v \models A$ and say: "A is true under the valuation v".
If $v(A) = 0$, we write $v \not\models A$ and say: "A is false under the valuation v".

Theorem (Functional completeness)

Every Boolean function $f(x_1, \ldots, x_n)\colon \{0,1\}^n \to \{0,1\}$
is expressed by some propositional formula $A(p_1, \ldots, p_n)$*,*
i.e. the truth table for A *is exactly* f*.*

Theorem (Functional completeness)

Every Boolean function $f(x_1, \dots, x_n)\colon \{0,1\}^n \to \{0,1\}$
is expressed by some propositional formula $A(p_1, \dots, p_n)$*,*
i.e. the truth table for A *is exactly* f*.*

Moreover, $\{\neg, \wedge\}$ are sufficient.

Theorem (Functional completeness)

Every Boolean function $f(x_1, \ldots, x_n)\colon \{0,1\}^n \to \{0,1\}$ *is expressed by some propositional formula* $A(p_1, \ldots, p_n)$, *i.e. the truth table for* A *is exactly* f.

Moreover, $\{\neg, \wedge\}$ are sufficient.

Other complete sets of connectives: $\{\neg, \vee\}$, $\{\bot, \to\}$, $\{1, \&, \oplus\}$, $\{|\}$, $\{\downarrow\}$.

- Sheffer stroke: $A \mid B \ := \ \neg(A \,\&\, B)$. Also called NAND.
- Peirce's arrow: $A \downarrow B \ := \ \neg(A \vee B)$. Also called NOR.

Theorem (Functional completeness)

Every Boolean function $f(x_1, \dots, x_n)\colon \{0,1\}^n \to \{0,1\}$ is expressed by some propositional formula $A(p_1, \dots, p_n)$, i.e. the truth table for A is exactly f.

Moreover, $\{\neg, \wedge\}$ are sufficient.

Other complete sets of connectives: $\{\neg, \vee\}$, $\{\bot, \to\}$, $\{1, \&, \oplus\}$, $\{|\}$, $\{\downarrow\}$.

- Sheffer stroke: $A \mid B \;:=\; \neg(A \,\&\, B)$. Also called NAND.
- Peirce's arrow: $A \downarrow B \;:=\; \neg(A \vee B)$. Also called NOR.

Theorem (Post's criterion)

A system Σ of Boolean functions is functionally complete $\Leftrightarrow$ $\Sigma \not\subseteq$ classes:

Theorem (Functional completeness)

Every Boolean function $f(x_1, \ldots, x_n)\colon \{0,1\}^n \to \{0,1\}$ *is expressed by some propositional formula* $A(p_1, \ldots, p_n)$*, i.e. the truth table for* A *is exactly* f*.*

Moreover, $\{\neg, \wedge\}$ are sufficient.

Other complete sets of connectives: $\{\neg, \vee\}$, $\{\bot, \to\}$, $\{1, \&, \oplus\}$, $\{|\}$, $\{\downarrow\}$.

- Sheffer stroke: $A \mid B \;:=\; \neg(A \,\&\, B)$. Also called NAND.
- Peirce's arrow: $A \downarrow B \;:=\; \neg(A \vee B)$. Also called NOR.

Theorem (Post's criterion)

A system Σ *of Boolean functions is functionally complete* $\Leftrightarrow$ $\Sigma \not\subseteq$ *classes:*

1. T_0 *(false-preserving): functions* f *such that* $f(0, \ldots, 0) = 0$*,*

Theorem (Functional completeness)

Every Boolean function $f(x_1, \ldots, x_n)\colon \{0,1\}^n \to \{0,1\}$ *is expressed by some propositional formula* $A(p_1, \ldots, p_n)$, *i.e. the truth table for* A *is exactly* f.

Moreover, $\{\neg, \wedge\}$ are sufficient.

Other complete sets of connectives: $\{\neg, \vee\}$, $\{\bot, \to\}$, $\{1, \&, \oplus\}$, $\{|\}$, $\{\downarrow\}$.

- Sheffer stroke: $A \mid B \;:=\; \neg(A \,\&\, B)$. Also called NAND.
- Peirce's arrow: $A \downarrow B \;:=\; \neg(A \vee B)$. Also called NOR.

Theorem (Post's criterion)

A system Σ *of Boolean functions is functionally complete* $\Leftrightarrow$ $\Sigma \not\subseteq$ *classes:*

1. T_0 *(false-preserving): functions* f *such that* $f(0, \ldots, 0) = 0$,
2. T_1 *(truth-preserving): functions* f *such that* $f(1, \ldots, 1) = 1$,

Theorem (Functional completeness)

Every Boolean function $f(x_1, \ldots, x_n)\colon \{0,1\}^n \to \{0,1\}$ is expressed by some propositional formula $A(p_1, \ldots, p_n)$, i.e. the truth table for A is exactly f.

Moreover, $\{\neg, \wedge\}$ are sufficient.

Other complete sets of connectives: $\{\neg, \vee\}$, $\{\bot, \to\}$, $\{1, \&, \oplus\}$, $\{|\}$, $\{\downarrow\}$.

- Sheffer stroke: $A \mid B \;:=\; \neg(A \,\&\, B)$. Also called NAND.
- Peirce's arrow: $A \downarrow B \;:=\; \neg(A \vee B)$. Also called NOR.

Theorem (Post's criterion)

A system Σ of Boolean functions is functionally complete $\Leftrightarrow$ $\Sigma \not\subseteq$ classes:

1. *T_0 (false-preserving): functions f such that $f(0, \ldots, 0) = 0$,*
2. *T_1 (truth-preserving): functions f such that $f(1, \ldots, 1) = 1$,*
3. *L (linear): functions f whose polynomial over $\{1, \&, \oplus\}$ is linear,*

Theorem (Functional completeness)

Every Boolean function $f(x_1, \ldots, x_n)\colon \{0,1\}^n \to \{0,1\}$
is expressed by some propositional formula $A(p_1, \ldots, p_n)$*,*
i.e. the truth table for A *is exactly* f*.*

Moreover, $\{\neg, \wedge\}$ are sufficient.
Other complete sets of connectives: $\{\neg, \vee\}$, $\{\bot, \to\}$, $\{1, \&, \oplus\}$, $\{|\}$, $\{\downarrow\}$.

- Sheffer stroke: $A \mid B \;:=\; \neg(A \,\&\, B)$. Also called NAND.
- Peirce's arrow: $A \downarrow B \;:=\; \neg(A \vee B)$. Also called NOR.

Theorem (Post's criterion)

A system Σ *of Boolean functions is functionally complete* $\Leftrightarrow$ $\Sigma \not\subseteq$ *classes:*

1. T_0 (*false-preserving*): *functions* f *such that* $f(0, \ldots, 0) = 0$,
2. T_1 (*truth-preserving*): *functions* f *such that* $f(1, \ldots, 1) = 1$,
3. L (*linear*): *functions* f *whose polynomial over* $\{1, \&, \oplus\}$ *is linear,*
4. M (*monotone*): *functions* f*: if* $x_i \leqslant y_i$ *for all* i*, then* $f(\vec{x}) \leqslant f(\vec{y})$,

Theorem (Functional completeness)

Every Boolean function $f(x_1, \ldots, x_n)\colon \{0,1\}^n \to \{0,1\}$ is expressed by some propositional formula $A(p_1, \ldots, p_n)$, i.e. the truth table for A is exactly f.

Moreover, $\{\neg, \wedge\}$ are sufficient.

Other complete sets of connectives: $\{\neg, \vee\}$, $\{\perp, \to\}$, $\{1, \&, \oplus\}$, $\{|\}$, $\{\downarrow\}$.

- Sheffer stroke: $A \mid B \;:=\; \neg(A \,\&\, B)$. Also called NAND.
- Peirce's arrow: $A \downarrow B \;:=\; \neg(A \vee B)$. Also called NOR.

Theorem (Post's criterion)

A system Σ of Boolean functions is functionally complete $\Leftrightarrow$ $\Sigma \not\subseteq$ classes:

1. *T_0 (false-preserving): functions f such that $f(0, \ldots, 0) = 0$,*
2. *T_1 (truth-preserving): functions f such that $f(1, \ldots, 1) = 1$,*
3. *L (linear): functions f whose polynomial over $\{1, \&, \oplus\}$ is linear,*
4. *M (monotone): functions f: if $x_i \leqslant y_i$ for all i, then $f(\vec{x}) \leqslant f(\vec{y})$,*
5. *S (self-dual): functions f such that $f(\neg x_1, \ldots, \neg x_n) = \neg f(\vec{x})$.*

Definition

A formula A is called valid if $\forall v \; v(A) = 1$.

Valid and Satisfiable formulas / sets

Definition

A formula A is called valid if $\forall v \; v(A) = 1$. Another name: tautology.

Valid and Satisfiable formulas / sets

Definition

A formula A is called valid if $\forall v \; v(A) = 1$. Another name: tautology.

A formula A is called satisfiable if $\exists v \; v(A) = 1$.

Valid and Satisfiable formulas / sets

Definition

A formula A is called valid if $\forall v \; v(A) = 1$. Another name: tautology.

A formula A is called satisfiable if $\exists v \; v(A) = 1$.

Fact. *A is a tautology $\iff$ $\neg A$ is not satisfiable.*

Valid and Satisfiable formulas / sets

Definition

A formula A is called valid if $\forall v\ v(A) = 1$. Another name: tautology.

A formula A is called satisfiable if $\exists v\ v(A) = 1$.

Fact. *A is a tautology $\iff$ $\neg A$ is not satisfiable.*

Let $\Gamma \subseteq \mathrm{Fm}$.

Valid and Satisfiable formulas / sets

Definition

A formula A is called valid if $\forall v\ v(A) = 1$. Another name: tautology.

A formula A is called satisfiable if $\exists v\ v(A) = 1$.

Fact. *A is a tautology $\iff$ $\neg A$ is not satisfiable.*

Let $\Gamma \subseteq \mathrm{Fm}$. We write $v \models \Gamma$ if, for every formula $A \in \Gamma$, we have $v \models A$.

Valid and Satisfiable formulas / sets

Definition

A formula A is called valid if $\forall v \; v(A) = 1$. Another name: tautology.

A formula A is called satisfiable if $\exists v \; v(A) = 1$.

Fact. *A is a tautology $\iff$ $\neg A$ is not satisfiable.*

Let $\Gamma \subseteq \mathrm{Fm}$. We write $v \models \Gamma$ if, for every formula $A \in \Gamma$, we have $v \models A$. In this case we say that Γ is true under the valuation v.

Valid and Satisfiable formulas / sets

Definition

A formula A is called valid if $\forall v\ v(A) = 1$. Another name: tautology.

A formula A is called satisfiable if $\exists v\ v(A) = 1$.

Fact. *A is a tautology $\iff$ $\neg A$ is not satisfiable.*

Let $\Gamma \subseteq \mathrm{Fm}$. We write $v \models \Gamma$ if, for every formula $A \in \Gamma$, we have $v \models A$. In this case we say that Γ is true under the valuation v.

Definition

A set Γ is satisfiable if $\exists v$: $v \models \Gamma$.

Valid and Satisfiable formulas / sets

Definition

A formula A is called valid if $\forall v \ v(A) = 1$. Another name: tautology.

A formula A is called satisfiable if $\exists v \ v(A) = 1$.

Fact. *A is a tautology $\iff$ $\neg A$ is not satisfiable.*

Let $\Gamma \subseteq \mathrm{Fm}$. We write $v \models \Gamma$ if, for every formula $A \in \Gamma$, we have $v \models A$. In this case we say that Γ is true under the valuation v.

Definition

A set Γ is satisfiable if $\exists v$: $v \models \Gamma$.

A set Γ implies (or entails) a formula A, in symbols: $\Gamma \models A$, if

for every valuation v such that $v \models \Gamma$, we have $v \models A$.

Valid and Satisfiable formulas / sets

Definition

A formula A is called valid if $\forall v \; v(A) = 1$. Another name: tautology.

A formula A is called satisfiable if $\exists v \; v(A) = 1$.

Fact. *A is a tautology $\iff$ $\neg A$ is not satisfiable.*

Let $\Gamma \subseteq \mathrm{Fm}$. We write $v \models \Gamma$ if, for every formula $A \in \Gamma$, we have $v \models A$. In this case we say that Γ is true under the valuation v.

Definition

A set Γ is satisfiable if $\exists v$: $v \models \Gamma$.

A set Γ implies (or entails) a formula A, in symbols: $\Gamma \models A$, if

for every valuation v such that $v \models \Gamma$, we have $v \models A$.

Fact. *$\Gamma \models A \iff \Gamma \cup \{\neg A\}$ is not satisfiable.*

Examples

Example 1. Is the formula $(p \to q) \vee (q \to p)$ a tautology?

Examples

Example 1. Is the formula $(p \to q) \vee (q \to p)$ a tautology? Yes.

Examples

Example 1. Is the formula $(p \to q) \vee (q \to p)$ a tautology? Yes.

Example 2. Is the set $\Gamma = \{\, \neg p \vee r, \quad p \vee \neg s, \quad s \to \neg r \,\}$ satisfiable?

Examples

Example 1. Is the formula $(p \to q) \vee (q \to p)$ a tautology? Yes.

Example 2. Is the set $\Gamma = \{\, \neg p \vee r, \quad p \vee \neg s, \quad s \to \neg r \,\}$ satisfiable? Yes.

Examples

Example 1. Is the formula $(p \to q) \vee (q \to p)$ a tautology? Yes.

Example 2. Is the set $\Gamma = \{\, \neg p \vee r, \quad p \vee \neg s, \quad s \to \neg r \,\}$ satisfiable? Yes.

Example 3. Does the same set Γ imply $\neg s$?

Examples

Example 1. Is the formula $(p \to q) \vee (q \to p)$ a tautology? Yes.

Example 2. Is the set $\Gamma = \{\, \neg p \vee r, \quad p \vee \neg s, \quad s \to \neg r \,\}$ satisfiable? Yes.

Example 3. Does the same set Γ imply $\neg s$? Yes.

Examples

Example 1. Is the formula $(p \to q) \vee (q \to p)$ a tautology? Yes.

Example 2. Is the set $\Gamma = \{\, \neg p \vee r, \quad p \vee \neg s, \quad s \to \neg r \,\}$ satisfiable? Yes.

Example 3. Does the same set Γ imply $\neg s$? Yes.

Example 4. Does the same set Γ imply p?

Examples

Example 1. Is the formula $(p \to q) \vee (q \to p)$ a tautology? Yes.

Example 2. Is the set $\Gamma = \{\, \neg p \vee r, \quad p \vee \neg s, \quad s \to \neg r \,\}$ satisfiable? Yes.

Example 3. Does the same set Γ imply $\neg s$? Yes.

Example 4. Does the same set Γ imply p? No: $p, r, s \mapsto 0, 1, 0$.

Examples

Example 1. Is the formula $(p \to q) \vee (q \to p)$ a tautology? Yes.

Example 2. Is the set $\Gamma = \{\, \neg p \vee r, \quad p \vee \neg s, \quad s \to \neg r \,\}$ satisfiable? Yes.

Example 3. Does the same set Γ imply $\neg s$? Yes.

Example 4. Does the same set Γ imply p? No: $p, r, s \mapsto 0, 1, 0$.

There is an algorithm for checking satisfiability of formulas:

Input: a formula A

Output: $\begin{cases} \texttt{Yes}, & \text{if } A \text{ is satisfiable,} \\ \texttt{No}, & \text{otherwise.} \end{cases}$

Examples

Example 1. Is the formula $(p \to q) \vee (q \to p)$ a tautology? Yes.

Example 2. Is the set $\Gamma = \{\, \neg p \vee r, \quad p \vee \neg s, \quad s \to \neg r \,\}$ satisfiable? Yes.

Example 3. Does the same set Γ imply $\neg s$? Yes.

Example 4. Does the same set Γ imply p? No: $p, r, s \mapsto 0, 1, 0$.

There is an algorithm for checking satisfiability of formulas:

Input: a formula A

Output: $\begin{cases} \texttt{Yes}, & \text{if } A \text{ is satisfiable,} \\ \texttt{No}, & \text{otherwise.} \end{cases}$

If you find a polynomial algorithm for this, you'll get \$ 1 000 000.

Examples

Example 1. Is the formula $(p \to q) \vee (q \to p)$ a tautology? Yes.

Example 2. Is the set $\Gamma = \{\, \neg p \vee r, \;\; p \vee \neg s, \;\; s \to \neg r \,\}$ satisfiable? Yes.

Example 3. Does the same set Γ imply $\neg s$? Yes.

Example 4. Does the same set Γ imply p? No: $p, r, s \mapsto 0, 1, 0$.

There is an algorithm for checking satisfiability of formulas:

Input: a formula A

Output: $\begin{cases} \texttt{Yes}, & \text{if } A \text{ is satisfiable,} \\ \texttt{No}, & \text{otherwise.} \end{cases}$

If you find a polynomial algorithm for this, you'll get \$ 1 000 000.
If you prove that no polynomial algorithm exists, you'll get \$ 1 000 000.

Examples

Example 1. Is the formula $(p \to q) \vee (q \to p)$ a tautology? Yes.

Example 2. Is the set $\Gamma = \{\, \neg p \vee r, \quad p \vee \neg s, \quad s \to \neg r \,\}$ satisfiable? Yes.

Example 3. Does the same set Γ imply $\neg s$? Yes.

Example 4. Does the same set Γ imply p? No: $p, r, s \mapsto 0, 1, 0$.

There is an algorithm for checking satisfiability of formulas:

Input: a formula A

Output: $\begin{cases} \texttt{Yes}, & \text{if } A \text{ is satisfiable,} \\ \texttt{No}, & \text{otherwise.} \end{cases}$

If you find a polynomial algorithm for this, you'll get \$ 1 000 000.
If you prove that no polynomial algorithm exists, you'll get \$ 1 000 000.
This is one of the 7 millennium problems: $\boxed{P = NP?}$

Axiomatization

Classical propositional calculus:

Axioms (more exactly: axiom schemata):

1. $A \to (B \to A)$,
2. $[A \to (B \to C)] \;\to\; [(A \to B) \to (A \to C)]$,
3. $(A \wedge B) \to A, \qquad (A \wedge B) \to B$,
4. $A \to (B \to (A \wedge B))$,
5. $A \to (A \vee B), \qquad B \to (A \vee B)$,
6. $(A \to C) \;\to\; [(B \to C) \;\to\; (A \vee B) \to C]$,
7. $(A \to B) \;\to\; [(A \to \neg B) \;\to \neg A]$,
8. $A \to (\neg A \to B)$
9. $A \vee \neg A$ (alternative: $\neg\neg A \to A$)
10. $\top, \qquad \bot \to A$.

Classical propositional calculus:

Axioms (more exactly: axiom schemata):

1. $A \to (B \to A)$,
2. $[A \to (B \to C)] \;\to\; [(A \to B) \to (A \to C)]$,
3. $(A \wedge B) \to A, \qquad (A \wedge B) \to B$,
4. $A \to (B \to (A \wedge B))$,
5. $A \to (A \vee B), \qquad B \to (A \vee B)$,
6. $(A \to C) \;\to\; [(B \to C) \;\to\; (A \vee B) \to C]$,
7. $(A \to B) \;\to\; [(A \to \neg B) \;\to \neg A]$,
8. $A \to (\neg A \to B)$
9. $A \vee \neg A$ (alternative: $\neg\neg A \to A$)
10. $\top, \qquad \bot \to A$.

Rule of inference: *modus ponens* (MP) $\dfrac{A \quad A \to B}{B}$.

Classical propositional calculus:

Axioms (more exactly: axiom schemata):

1. $A \to (B \to A)$,
2. $[A \to (B \to C)] \ \to \ [(A \to B) \to (A \to C)]$,
3. $(A \wedge B) \to A, \qquad (A \wedge B) \to B$,
4. $A \to (B \to (A \wedge B))$,
5. $A \to (A \vee B), \qquad B \to (A \vee B)$,
6. $(A \to C) \ \to \ [(B \to C) \ \to \ (A \vee B) \to C]$,
7. $(A \to B) \ \to \ [(A \to \neg B) \ \to \neg A]$,
8. $A \to (\neg A \to B)$
9. $A \vee \neg A$ (alternative: $\neg\neg A \to A$)
10. $\top, \qquad \bot \to A$.

Rule of inference: *modus ponens* (MP) $\dfrac{A \quad A \to B}{B}$.

Remark. Without $A \vee \neg A$, we obtain the Intuitionistic propositional logic.

Definition

A formula A is called derivable, or provable, or a theorem of the CPC

Derivations

Definition

A formula A is called derivable, or provable, or a theorem of the CPC if there is a derivation, or a proof, or inference in CPC in which A is the last formula.

Notation: $\vdash A$.

Derivations

Definition

A formula A is called derivable, or provable, or a theorem of the CPC if there is a derivation, or a proof, or inference in CPC in which A is the last formula.

Notation: $\vdash A$.

Definition

A derivation, or proof, or inference is a finite sequence (list) of formulas

$$C_1, \ \ldots \ , C_n$$

Derivations

Definition

A formula A is called derivable, or provable, or a theorem of the CPC if there is a derivation, or a proof, or inference in CPC in which A is the last formula.

Notation: $\vdash A$.

Definition

A derivation, or proof, or inference is a finite sequence (list) of formulas

$$C_1, \ \ldots \ , C_n$$

such that each formula C_k

- either is an axiom of CPC,

Derivations

Definition

A formula A is called derivable, or provable, or a theorem of the CPC if there is a derivation, or a proof, or inference in CPC in which A is the last formula.

Notation: $\vdash A$.

Definition

A derivation, or proof, or inference is a finite sequence (list) of formulas

$$C_1, \ \ldots \ , C_n$$

such that each formula C_k

- either is an axiom of CPC,
- or is obtained by the rule MP from some previous formulas C_i and C_j, where $i, j < k$.

Example of a derivation

Here we derive the formula $(A \wedge B) \to (A \vee B)$.

Example of a derivation

Here we derive the formula $(A \wedge B) \to (A \vee B)$.

1. $A \wedge B \to A$ axiom

Example of a derivation

Here we derive the formula $(A \wedge B) \to (A \vee B)$.

1. $A \wedge B \to A$ axiom
2. $A \to A \vee B$ axiom

Example of a derivation

Here we derive the formula $(A \wedge B) \to (A \vee B)$.

1. $A \wedge B \to A$ axiom
2. $A \to A \vee B$ axiom
3. $[A \to A \vee B] \;\to\; [(A \wedge B) \;\to\; (A \to A \vee B)]$ axiom

Example of a derivation

Here we derive the formula $(A \wedge B) \to (A \vee B)$.

1. $A \wedge B \to A$ axiom
2. $A \to A \vee B$ axiom
3. $[A \to A \vee B] \to [(A \wedge B) \to (A \to A \vee B)]$ axiom
4. $(A \wedge B) \to (A \to A \vee B)$ rule MP

Example of a derivation

Here we derive the formula $(A \wedge B) \to (A \vee B)$.

1. $A \wedge B \to A$ axiom
2. $A \to A \vee B$ axiom
3. $[A \to A \vee B] \;\to\; [(A \wedge B) \;\to\; (A \to A \vee B)]$ axiom
4. $(A \wedge B) \;\to\; (A \to A \vee B)$ rule MP
5. $[(A \wedge B) \;\to\; (A \to A \vee B)] \;\to\; [(A \wedge B \to A) \to (A \wedge B \to A \vee B)]$

Example of a derivation

Here we derive the formula $(A \wedge B) \to (A \vee B)$.

1. $A \wedge B \to A$ axiom
2. $A \to A \vee B$ axiom
3. $[A \to A \vee B] \ \to\ [(A \wedge B) \ \to\ (A \to A \vee B)]$ axiom
4. $(A \wedge B) \ \to\ (A \to A \vee B)$ rule MP
5. $[(A \wedge B) \ \to\ (A \to A \vee B)] \ \to\ [(A \wedge B \to A) \to (A \wedge B \to A \vee B)]$
6. $(A \wedge B \to A) \to (A \wedge B \to A \vee B)$

Example of a derivation

Here we derive the formula $(A \wedge B) \to (A \vee B)$.

1. $A \wedge B \to A$ axiom
2. $A \to A \vee B$ axiom
3. $[A \to A \vee B] \to [(A \wedge B) \to (A \to A \vee B)]$ axiom
4. $(A \wedge B) \to (A \to A \vee B)$ rule MP
5. $[(A \wedge B) \to (A \to A \vee B)] \to [(A \wedge B \to A) \to (A \wedge B \to A \vee B)]$
6. $(A \wedge B \to A) \to (A \wedge B \to A \vee B)$
7. $A \wedge B \to A \vee B$

Completeness of CPC

Theorem (Completeness)

A is a theorem $\iff$ A is a tautology.

$$\vdash A \qquad \iff \qquad \models A$$

Completeness of CPC

Theorem (Completeness)

A is a theorem $\iff$ A is a tautology.

$$\vdash A \qquad \iff \qquad \models A$$

Corollary

CPC is decidable.

Completeness of CPC

Theorem (Completeness)

A is a theorem $\iff$ A is a tautology.

$$\vdash A \qquad \iff \qquad \models A$$

Corollary

CPC is decidable.

This means: there is an algorithm that takes any formula A and returns

$$\begin{cases} \texttt{Yes}, & \text{if } A \text{ is provable in CPC}, \\ \texttt{No}, & \text{otherwise.} \end{cases}$$

Derivation from hypotheses

Let $A \in \mathsf{Fm}$ be a formula and $\Gamma \subseteq \mathsf{Fm}$ some set of formulas.

Derivation from hypotheses

Let $A \in \mathsf{Fm}$ be a formula and $\Gamma \subseteq \mathsf{Fm}$ some set of formulas.

Definition

A formula A is called derivable in CPC from a set of formulas Γ if there is a derivation from Γ in which A is the last formula.

Notation: $\Gamma \vdash A$.

Derivation from hypotheses

Let $A \in \mathrm{Fm}$ be a formula and $\Gamma \subseteq \mathrm{Fm}$ some set of formulas.

Definition

A formula A is called derivable in CPC from a set of formulas Γ if there is a derivation from Γ in which A is the last formula.

Notation: $\Gamma \vdash A$.

Definition

A derivation in CPC from Γ is a finite sequence (list) of formulas

$$C_1, \ \ldots \ , C_n$$

such that each formula C_k

- either is an axiom of CPC,

Derivation from hypotheses

Let $A \in \mathrm{Fm}$ be a formula and $\Gamma \subseteq \mathrm{Fm}$ some set of formulas.

Definition

A formula A is called derivable in CPC from a set of formulas Γ if there is a derivation from Γ in which A is the last formula.

Notation: $\Gamma \vdash A$.

Definition

A derivation in CPC from Γ is a finite sequence (list) of formulas

$$C_1, \ \dots \ , C_n$$

such that each formula C_k

- either is an axiom of CPC,
- or belongs to Γ,

Derivation from hypotheses

Let $A \in \mathrm{Fm}$ be a formula and $\Gamma \subseteq \mathrm{Fm}$ some set of formulas.

Definition

A formula A is called derivable in CPC from a set of formulas Γ if there is a derivation from Γ in which A is the last formula.

Notation: $\Gamma \vdash A$.

Definition

A derivation in CPC from Γ is a finite sequence (list) of formulas

$$C_1, \ \dots \ , C_n$$

such that each formula C_k

- either is an axiom of CPC,
- or belongs to Γ,
- or is obtained by the rule MP from some previous formulas C_i and C_j, where $i, j < k$.

Completeness

Theorem (Completeness of CPC)

A is a theorem $\iff$ A is a tautology:

$$\vdash A \iff \models A$$

Completeness

Theorem (Completeness of CPC)

A is a theorem $\iff$ A is a tautology:

$$\vdash A \iff \models A$$

Theorem (Strong completeness of CPC)

A is derivable from Γ $\iff$ Γ implies A:

$$\Gamma \vdash A \iff \Gamma \models A$$

Compactness

Theorem (Compactness)

If $\Gamma \models A$, then there is a finite subset $\Delta \subseteq \Gamma$ such that $\Delta \models A$.

Proof: $\Gamma \models A$

Compactness

Theorem (Compactness)

If $\Gamma \models A$, then there is a finite subset $\Delta \subseteq \Gamma$ such that $\Delta \models A$.

Proof: $\Gamma \models A \quad \Rightarrow \quad \Gamma \vdash A$.

Compactness

Theorem (Compactness)

If $\Gamma \models A$, then there is a finite subset $\Delta \subseteq \Gamma$ such that $\Delta \models A$.

Proof: $\Gamma \models A \quad \Rightarrow \quad \Gamma \vdash A.$ But proofs are finite!

Compactness

Theorem (Compactness)

If $\Gamma \models A$, then there is a finite subset $\Delta \subseteq \Gamma$ such that $\Delta \models A$.

Proof: $\Gamma \models A \quad \Rightarrow \quad \Gamma \vdash A$. But proofs are finite!
$\Rightarrow \quad \exists$ finite $\Delta \subseteq \Gamma$: $\Delta \vdash A$.

Compactness

Theorem (Compactness)

If $\Gamma \models A$, then there is a finite subset $\Delta \subseteq \Gamma$ such that $\Delta \models A$.

Proof: $\Gamma \models A \quad \Rightarrow \quad \Gamma \vdash A$. But proofs are finite!
$\Rightarrow \quad \exists$ finite $\Delta \subseteq \Gamma$: $\Delta \vdash A. \quad \Rightarrow \quad \Delta \models A$.

Compactness

Theorem (Compactness)

If $\Gamma \models A$, then there is a finite subset $\Delta \subseteq \Gamma$ such that $\Delta \models A$.

Proof: $\Gamma \models A \quad \Rightarrow \quad \Gamma \vdash A$. But proofs are finite!
$\Rightarrow \quad \exists$ finite $\Delta \subseteq \Gamma$: $\Delta \vdash A$. $\quad \Rightarrow \quad \Delta \models A$.

Theorem (Compactness)

If every finite subset $\Delta \subseteq \Gamma$ is satisfiable, then Γ is satisfiable.

Compactness

Theorem (Compactness)

If $\Gamma \models A$, then there is a finite subset $\Delta \subseteq \Gamma$ such that $\Delta \models A$.

Proof: $\Gamma \models A \quad \Rightarrow \quad \Gamma \vdash A$. But proofs are finite!
$\Rightarrow \quad \exists$ finite $\Delta \subseteq \Gamma$: $\Delta \vdash A$. $\quad \Rightarrow \quad \Delta \models A$.

Theorem (Compactness)

If every finite subset $\Delta \subseteq \Gamma$ is satisfiable, then Γ is satisfiable.

Follows from **Theorem 1**. Indeed: Γ is unsatisfiable $\iff$ $\Gamma \models \bot$.

Compactness

Theorem (Compactness)

If $\Gamma \models A$, then there is a finite subset $\Delta \subseteq \Gamma$ such that $\Delta \models A$.

Proof: $\Gamma \models A \quad \Rightarrow \quad \Gamma \vdash A$. But proofs are finite!
$\Rightarrow \quad \exists$ finite $\Delta \subseteq \Gamma$: $\Delta \vdash A. \quad \Rightarrow \quad \Delta \models A$.

Theorem (Compactness)

If every finite subset $\Delta \subseteq \Gamma$ is satisfiable, then Γ is satisfiable.

Follows from **Theorem 1**. Indeed: Γ is unsatisfiable $\iff \Gamma \models \bot$.

Task

Prove Compactness without using axiomatization of CPC.

Compactness

Theorem (Compactness)

If $\Gamma \models A$, then there is a finite subset $\Delta \subseteq \Gamma$ such that $\Delta \models A$.

Proof: $\Gamma \models A \quad \Rightarrow \quad \Gamma \vdash A$. But proofs are finite!
$\Rightarrow \quad \exists$ finite $\Delta \subseteq \Gamma$: $\Delta \vdash A$. $\quad \Rightarrow \quad \Delta \models A$.

Theorem (Compactness)

If every finite subset $\Delta \subseteq \Gamma$ is satisfiable, then Γ is satisfiable.

Follows from **Theorem 1**. Indeed: Γ is unsatisfiable $\iff \Gamma \models \bot$.

Task

Prove Compactness without using axiomatization of CPC.

Let $\Gamma = \{A_0, A_1, \ldots\}$ be an infinite set of formulas.

Compactness

Theorem (Compactness)

If $\Gamma \models A$, then there is a finite subset $\Delta \subseteq \Gamma$ such that $\Delta \models A$.

Proof: $\Gamma \models A \quad \Rightarrow \quad \Gamma \vdash A$. But proofs are finite!
$\Rightarrow \quad \exists$ finite $\Delta \subseteq \Gamma$: $\Delta \vdash A$. $\quad \Rightarrow \quad \Delta \models A$.

Theorem (Compactness)

If every finite subset $\Delta \subseteq \Gamma$ is satisfiable, then Γ is satisfiable.

Follows from **Theorem 1**. Indeed: Γ is unsatisfiable $\iff \Gamma \models \bot$.

Task

Prove Compactness without using axiomatization of CPC.

Let $\Gamma = \{A_0, A_1, \ldots\}$ be an infinite set of formulas.
For each $\Delta_n = \{A_0, \ldots, A_n\}$ there is a valuation $v_n \models \Delta_n$.

Compactness

Theorem (Compactness)

If $\Gamma \models A$, then there is a finite subset $\Delta \subseteq \Gamma$ such that $\Delta \models A$.

Proof: $\Gamma \models A \quad \Rightarrow \quad \Gamma \vdash A$. But proofs are finite!
$\Rightarrow \quad \exists$ finite $\Delta \subseteq \Gamma$: $\Delta \vdash A$. $\quad \Rightarrow \quad \Delta \models A$.

Theorem (Compactness)

If every finite subset $\Delta \subseteq \Gamma$ is satisfiable, then Γ is satisfiable.

Follows from **Theorem 1**. Indeed: Γ is unsatisfiable $\iff$ $\Gamma \models \bot$.

Task

Prove Compactness without using axiomatization of CPC.

Let $\Gamma = \{A_0, A_1, \ldots\}$ be an infinite set of formulas.
For each $\Delta_n = \{A_0, \ldots, A_n\}$ there is a valuation $v_n \models \Delta_n$.
How can we combine all valuations v_n into a single valuation $v \models \Gamma$?

Craig interpolation

Theorem (Craig interpolation theorem)

If $\vdash A \to C$ *then there exists a formula* B *(called an interpolant) such that*

$\textbf{(1)} \vdash A \to B$ *and* $\vdash B \to C$,

Craig interpolation

Theorem (Craig interpolation theorem)

If $\vdash A \to C$ *then there exists a formula* B *(called an* *interpolant**) such that*

$$\textbf{(1)} \vdash A \to B \;\; \textit{and} \;\; \vdash B \to C, \qquad \textbf{(2)}\ \mathrm{Var}(B) \subseteq \mathrm{Var}(A) \cap \mathrm{Var}(C).$$

Craig interpolation

Theorem (Craig interpolation theorem)

If $\vdash A \to C$ then there exists a formula B (called an interpolant) such that

$$\textbf{(1)} \vdash A \to B \text{ and } \vdash B \to C, \qquad \textbf{(2)} \operatorname{Var}(B) \subseteq \operatorname{Var}(A) \cap \operatorname{Var}(C).$$

Proof. Due to Completeness, we prove for $\models$ instead of $\vdash$.

Let $A = A(\vec{p}, \vec{q})$, $C = C(\vec{q}, s)$, where $\vec{p} = (p_1, \ldots, p_k)$, $\vec{q} = (q_1, \ldots, q_\ell)$.
Suppose that $A \to C(\vec{q}, s)$ is a tautology.

Craig interpolation

Theorem (Craig interpolation theorem)

If $\vdash A \to C$ then there exists a formula B (called an interpolant) such that

$$\textbf{(1)} \vdash A \to B \;\; \textit{and} \;\; \vdash B \to C, \qquad \textbf{(2)} \; \mathrm{Var}(B) \subseteq \mathrm{Var}(A) \cap \mathrm{Var}(C).$$

Proof. Due to Completeness, we prove for $\models$ instead of $\vdash$.

Let $A = A(\vec{p}, \vec{q})$, $C = C(\vec{q}, s)$, where $\vec{p} = (p_1, \ldots, p_k)$, $\vec{q} = (q_1, \ldots, q_\ell)$.
Suppose that $A \to C(\vec{q}, s)$ is a tautology. In particular,
$A \to C(\vec{q}, \bot)$ and $A \to C(\vec{q}, \top)$ are tautologies.

Craig interpolation

Theorem (Craig interpolation theorem)

If $\vdash A \to C$ then there exists a formula B (called an interpolant) such that

$$\textbf{(1)} \vdash A \to B \ \textit{ and } \vdash B \to C, \qquad \textbf{(2)} \ \mathrm{Var}(B) \subseteq \mathrm{Var}(A) \cap \mathrm{Var}(C).$$

Proof. Due to Completeness, we prove for $\models$ instead of $\vdash$.

Let $A = A(\vec{p}, \vec{q})$, $C = C(\vec{q}, s)$, where $\vec{p} = (p_1, \ldots, p_k)$, $\vec{q} = (q_1, \ldots, q_\ell)$.
Suppose that $A \to C(\vec{q}, s)$ is a tautology. In particular,
$A \to C(\vec{q}, \bot)$ and $A \to C(\vec{q}, \top)$ are tautologies. Then
$A \to \underbrace{\big[\, C(\vec{q}, \bot) \wedge C(\vec{q}, \top) \,\big]}_{B(\vec{q})}$ is a tautology.
So, $A \to B$ is a tautology.

Craig interpolation

Theorem (Craig interpolation theorem)

If $\vdash A \to C$ then there exists a formula B (called an interpolant) such that

$$\textbf{(1)}\ \vdash A \to B \ \textit{ and } \vdash B \to C, \qquad \textbf{(2)}\ \mathrm{Var}(B) \subseteq \mathrm{Var}(A) \cap \mathrm{Var}(C).$$

Proof. Due to Completeness, we prove for $\models$ instead of $\vdash$.

Let $A = A(\vec{p}, \vec{q})$, $C = C(\vec{q}, s)$, where $\vec{p} = (p_1, \ldots, p_k)$, $\vec{q} = (q_1, \ldots, q_\ell)$.
Suppose that $A \to C(\vec{q}, s)$ is a tautology. In particular,
$A \to C(\vec{q}, \bot)$ and $A \to C(\vec{q}, \top)$ are tautologies. Then
$A \to \underbrace{\big[\, C(\vec{q}, \bot) \wedge C(\vec{q}, \top) \,\big]}_{B(\vec{q})}$ is a tautology.

So, $A \to B$ is a tautology. Why is $B(\vec{q}) \to C(\vec{q}, s)$ a tautology?

Craig interpolation

Theorem (Craig interpolation theorem)

If $\vdash A \to C$ then there exists a formula B (called an interpolant) such that

$$\textbf{(1)} \vdash A \to B \;\; \textit{and} \;\; \vdash B \to C, \qquad \textbf{(2)}\ \mathrm{Var}(B) \subseteq \mathrm{Var}(A) \cap \mathrm{Var}(C).$$

Proof. Due to Completeness, we prove for $\models$ instead of $\vdash$.

Let $A = A(\vec{p}, \vec{q})$, $C = C(\vec{q}, s)$, where $\vec{p} = (p_1, \dots, p_k)$, $\vec{q} = (q_1, \dots, q_\ell)$.
Suppose that $A \to C(\vec{q}, s)$ is a tautology. In particular,
$A \to C(\vec{q}, \bot)$ and $A \to C(\vec{q}, \top)$ are tautologies. Then
$A \to \underbrace{\big[\, C(\vec{q}, \bot) \wedge C(\vec{q}, \top) \,\big]}_{B(\vec{q})}$ is a tautology.

So, $A \to B$ is a tautology. Why is $B(\vec{q}) \to C(\vec{q}, s)$ a tautology?

- for $s := \bot$ we obtain a tautology $[C(\vec{q}, \bot) \wedge C(\vec{q}, \top)] \to C(\vec{q}, \bot)$.

Craig interpolation

Theorem (Craig interpolation theorem)

If $\vdash A \to C$ then there exists a formula B (called an interpolant) such that

$$\textbf{(1)} \vdash A \to B \;\; \textit{and} \; \vdash B \to C, \qquad \textbf{(2)} \; \mathrm{Var}(B) \subseteq \mathrm{Var}(A) \cap \mathrm{Var}(C).$$

Proof. Due to Completeness, we prove for $\models$ instead of $\vdash$.

Let $A = A(\vec{p}, \vec{q})$, $C = C(\vec{q}, s)$, where $\vec{p} = (p_1, \dots, p_k)$, $\vec{q} = (q_1, \dots, q_\ell)$.
Suppose that $A \to C(\vec{q}, s)$ is a tautology. In particular,
$A \to C(\vec{q}, \bot)$ and $A \to C(\vec{q}, \top)$ are tautologies. Then
$A \to \underbrace{\big[\, C(\vec{q}, \bot) \wedge C(\vec{q}, \top) \,\big]}_{B(\vec{q})}$ is a tautology.

So, $A \to B$ is a tautology. Why is $B(\vec{q}) \to C(\vec{q}, s)$ a tautology?

- for $s := \bot$ we obtain a tautology $[C(\vec{q}, \bot) \wedge C(\vec{q}, \top)] \to C(\vec{q}, \bot)$.
- for $s := \top$ we obtain a tautology (similarly). $\square$

Craig interpolation

Theorem (Craig interpolation theorem)

If $\vdash A \to C$ then there exists a formula B (called an interpolant) such that

$$\textbf{(1)} \vdash A \to B \ \ \textit{and} \ \vdash B \to C, \qquad \textbf{(2)} \ \mathrm{Var}(B) \subseteq \mathrm{Var}(A) \cap \mathrm{Var}(C).$$

Proof. Due to Completeness, we prove for $\models$ instead of $\vdash$.

Let $A = A(\vec{p}, \vec{q})$, $C = C(\vec{q}, s)$, where $\vec{p} = (p_1, \dots, p_k)$, $\vec{q} = (q_1, \dots, q_\ell)$.
Suppose that $A \to C(\vec{q}, s)$ is a tautology. In particular,
$A \to C(\vec{q}, \bot)$ and $A \to C(\vec{q}, \top)$ are tautologies. Then
$A \to \underbrace{\big[\, C(\vec{q}, \bot) \wedge C(\vec{q}, \top) \,\big]}_{B(\vec{q})}$ is a tautology.

So, $A \to B$ is a tautology. Why is $B(\vec{q}) \to C(\vec{q}, s)$ a tautology?

- for $s := \bot$ we obtain a tautology $[C(\vec{q}, \bot) \wedge C(\vec{q}, \top)] \to C(\vec{q}, \bot)$.
- for $s := \top$ we obtain a tautology (similarly). □

In general, if $\vec{s} = (s_1, \dots, s_m)$, then $B(\vec{q}) := \bigwedge_{\vec{a} \in \{\bot, \top\}^m} C(\vec{q}, \vec{a})$.

Stronger interpolation theorems

$\boxed{\text{Craig interpolation}}$

Stronger interpolation theorems

$\boxed{\text{Craig interpolation}} \quad \longleftarrow \quad \boxed{\text{Lyndon interpolation}}$

Stronger interpolation theorems

$$\begin{tikzcd}
\boxed{\text{Craig interpolation}} & \boxed{\text{Lyndon interpolation}} \arrow[l] \\
\boxed{\text{Uniform Craig interpolation}} \arrow[u] & \boxed{\text{Uniform Lyndon interpolation}} \arrow[l] \arrow[u]
\end{tikzcd}$$

Lyndon interpolation: Polarity of variables

Recall that $\mathrm{Var}(A)$ is the set of variables in the formula A.

Lyndon interpolation: Polarity of variables

Recall that $\mathrm{Var}(A)$ is the set of variables in the formula A.

Definition (Variables occurring positively and negatively)

The sets $\mathrm{Var}^{+}(A)$ and $\mathrm{Var}^{-}(A)$ are defined by joint induction:

Lyndon interpolation: Polarity of variables

Recall that $\mathsf{Var}(A)$ is the set of variables in the formula A.

Definition (Variables occurring positively and negatively)

The sets $\mathsf{Var}^+(A)$ and $\mathsf{Var}^-(A)$ are defined by joint induction:

- $\mathsf{Var}^+(\bot) = \mathsf{Var}^-(\bot) = \mathsf{Var}^+(\top) = \mathsf{Var}^-(\top) = \varnothing$,

Lyndon interpolation: Polarity of variables

Recall that $\mathsf{Var}(A)$ is the set of variables in the formula A.

Definition (Variables occurring positively and negatively)

The sets $\mathsf{Var}^+(A)$ and $\mathsf{Var}^-(A)$ are defined by joint induction:

- $\mathsf{Var}^+(\bot) = \mathsf{Var}^-(\bot) = \mathsf{Var}^+(\top) = \mathsf{Var}^-(\top) = \varnothing$,
- $\mathsf{Var}^+(p_i) = \{p_i\}, \quad \mathsf{Var}^-(p_i) = \varnothing$,

Lyndon interpolation: Polarity of variables

Recall that $\mathrm{Var}(A)$ is the set of variables in the formula A.

Definition (Variables occurring positively and negatively)

The sets $\mathrm{Var}^+(A)$ and $\mathrm{Var}^-(A)$ are defined by joint induction:

- $\mathrm{Var}^+(\bot) = \mathrm{Var}^-(\bot) = \mathrm{Var}^+(\top) = \mathrm{Var}^-(\top) = \varnothing$,
- $\mathrm{Var}^+(p_i) = \{p_i\}, \quad \mathrm{Var}^-(p_i) = \varnothing$,
- $\mathrm{Var}^+(\neg A) = \mathrm{Var}^-(A), \quad \mathrm{Var}^-(\neg A) = \mathrm{Var}^+(A)$,

Lyndon interpolation: Polarity of variables

Recall that $\mathsf{Var}(A)$ is the set of variables in the formula A.

Definition (Variables occurring positively and negatively)

The sets $\mathsf{Var}^+(A)$ and $\mathsf{Var}^-(A)$ are defined by joint induction:

- $\mathsf{Var}^+(\bot) = \mathsf{Var}^-(\bot) = \mathsf{Var}^+(\top) = \mathsf{Var}^-(\top) = \varnothing$,
- $\mathsf{Var}^+(p_i) = \{p_i\}, \quad \mathsf{Var}^-(p_i) = \varnothing$,
- $\mathsf{Var}^+(\neg A) = \mathsf{Var}^-(A), \quad \mathsf{Var}^-(\neg A) = \mathsf{Var}^+(A)$,
- $\mathsf{Var}^+(A \wedge B) = \mathsf{Var}^+(A) \cup \mathsf{Var}^+(B)$, similarly for Var^-.

Lyndon interpolation: Polarity of variables

Recall that $\mathrm{Var}(A)$ is the set of variables in the formula A.

Definition (Variables occurring positively and negatively)

The sets $\mathrm{Var}^+(A)$ and $\mathrm{Var}^-(A)$ are defined by joint induction:

- $\mathrm{Var}^+(\bot) = \mathrm{Var}^-(\bot) = \mathrm{Var}^+(\top) = \mathrm{Var}^-(\top) = \varnothing$,
- $\mathrm{Var}^+(p_i) = \{p_i\}, \quad \mathrm{Var}^-(p_i) = \varnothing$,
- $\mathrm{Var}^+(\neg A) = \mathrm{Var}^-(A), \quad \mathrm{Var}^-(\neg A) = \mathrm{Var}^+(A)$,
- $\mathrm{Var}^+(A \wedge B) = \mathrm{Var}^+(A) \cup \mathrm{Var}^+(B)$, similarly for Var^-.
- similarly for $\vee$,

Lyndon interpolation: Polarity of variables

Recall that $\mathrm{Var}(A)$ is the set of variables in the formula A.

Definition (Variables occurring positively and negatively)

The sets $\mathrm{Var}^+(A)$ and $\mathrm{Var}^-(A)$ are defined by joint induction:

- $\mathrm{Var}^+(\bot) = \mathrm{Var}^-(\bot) = \mathrm{Var}^+(\top) = \mathrm{Var}^-(\top) = \varnothing$,
- $\mathrm{Var}^+(p_i) = \{p_i\}, \quad \mathrm{Var}^-(p_i) = \varnothing$,
- $\mathrm{Var}^+(\neg A) = \mathrm{Var}^-(A), \quad \mathrm{Var}^-(\neg A) = \mathrm{Var}^+(A)$,
- $\mathrm{Var}^+(A \wedge B) = \mathrm{Var}^+(A) \cup \mathrm{Var}^+(B)$, similarly for Var^-.
- similarly for $\vee$,
- $\mathrm{Var}^+(A \to B) = \mathrm{Var}^-(A) \cup \mathrm{Var}^+(B)$, similarly for Var^-.

Lyndon interpolation: Polarity of variables

Recall that $\mathsf{Var}(A)$ is the set of variables in the formula A.

Definition (Variables occurring positively and negatively)

The sets $\mathsf{Var}^+(A)$ and $\mathsf{Var}^-(A)$ are defined by joint induction:

- $\mathsf{Var}^+(\bot) = \mathsf{Var}^-(\bot) = \mathsf{Var}^+(\top) = \mathsf{Var}^-(\top) = \varnothing$,
- $\mathsf{Var}^+(p_i) = \{p_i\}, \quad \mathsf{Var}^-(p_i) = \varnothing$,
- $\mathsf{Var}^+(\neg A) = \mathsf{Var}^-(A), \quad \mathsf{Var}^-(\neg A) = \mathsf{Var}^+(A)$,
- $\mathsf{Var}^+(A \wedge B) = \mathsf{Var}^+(A) \cup \mathsf{Var}^+(B)$, similarly for Var^-.
- similarly for $\vee$,
- $\mathsf{Var}^+(A \to B) = \mathsf{Var}^-(A) \cup \mathsf{Var}^+(B)$, similarly for Var^-.

Example. Let A be the formula $(p \to (q \to p)) \to s$. Then
$\mathsf{Var}^+(A) =$

Lyndon interpolation: Polarity of variables

Recall that $\mathrm{Var}(A)$ is the set of variables in the formula A.

Definition (Variables occurring positively and negatively)

The sets $\mathrm{Var}^+(A)$ and $\mathrm{Var}^-(A)$ are defined by joint induction:

- $\mathrm{Var}^+(\bot) = \mathrm{Var}^-(\bot) = \mathrm{Var}^+(\top) = \mathrm{Var}^-(\top) = \varnothing$,
- $\mathrm{Var}^+(p_i) = \{p_i\}$, $\quad \mathrm{Var}^-(p_i) = \varnothing$,
- $\mathrm{Var}^+(\neg A) = \mathrm{Var}^-(A)$, $\quad \mathrm{Var}^-(\neg A) = \mathrm{Var}^+(A)$,
- $\mathrm{Var}^+(A \wedge B) = \mathrm{Var}^+(A) \cup \mathrm{Var}^+(B)$, $\quad$ similarly for Var^-.
- similarly for $\vee$,
- $\mathrm{Var}^+(A \to B) = \mathrm{Var}^-(A) \cup \mathrm{Var}^+(B)$, $\quad$ similarly for Var^-.

Example. Let A be the formula $(p \to (q \to p)) \to s$. Then
$\mathrm{Var}^+(A) = \{p, q, s\}$,

Lyndon interpolation: Polarity of variables

Recall that $\mathsf{Var}(A)$ is the set of variables in the formula A.

Definition (Variables occurring positively and negatively)

The sets $\mathsf{Var}^+(A)$ and $\mathsf{Var}^-(A)$ are defined by joint induction:

- $\mathsf{Var}^+(\bot) = \mathsf{Var}^-(\bot) = \mathsf{Var}^+(\top) = \mathsf{Var}^-(\top) = \varnothing$,
- $\mathsf{Var}^+(p_i) = \{p_i\}$, $\quad \mathsf{Var}^-(p_i) = \varnothing$,
- $\mathsf{Var}^+(\neg A) = \mathsf{Var}^-(A)$, $\quad \mathsf{Var}^-(\neg A) = \mathsf{Var}^+(A)$,
- $\mathsf{Var}^+(A \wedge B) = \mathsf{Var}^+(A) \cup \mathsf{Var}^+(B)$, $\quad$ similarly for Var^-.
- similarly for $\vee$,
- $\mathsf{Var}^+(A \to B) = \mathsf{Var}^-(A) \cup \mathsf{Var}^+(B)$, $\quad$ similarly for Var^-.

Example. Let A be the formula $(p \to (q \to p)) \to s$. Then
$\mathsf{Var}^+(A) = \{p, q, s\}$,
$\mathsf{Var}^-(A) =$

Lyndon interpolation: Polarity of variables

Recall that $\mathrm{Var}(A)$ is the set of variables in the formula A.

Definition (Variables occurring positively and negatively)

The sets $\mathrm{Var}^+(A)$ and $\mathrm{Var}^-(A)$ are defined by joint induction:

- $\mathrm{Var}^+(\bot) = \mathrm{Var}^-(\bot) = \mathrm{Var}^+(\top) = \mathrm{Var}^-(\top) = \varnothing$,
- $\mathrm{Var}^+(p_i) = \{p_i\}, \quad \mathrm{Var}^-(p_i) = \varnothing$,
- $\mathrm{Var}^+(\neg A) = \mathrm{Var}^-(A), \quad \mathrm{Var}^-(\neg A) = \mathrm{Var}^+(A)$,
- $\mathrm{Var}^+(A \wedge B) = \mathrm{Var}^+(A) \cup \mathrm{Var}^+(B)$, similarly for Var^-.
- similarly for $\vee$,
- $\mathrm{Var}^+(A \to B) = \mathrm{Var}^-(A) \cup \mathrm{Var}^+(B)$, similarly for Var^-.

Example. Let A be the formula $(p \to (q \to p)) \to s$. Then
$\mathrm{Var}^+(A) = \{p, q, s\}$,
$\mathrm{Var}^-(A) = \{p\}$.

Lyndon interpolation: Polarity of variables

Recall that $\mathrm{Var}(A)$ is the set of variables in the formula A.

Definition (Variables occurring positively and negatively)

The sets $\mathrm{Var}^+(A)$ and $\mathrm{Var}^-(A)$ are defined by joint induction:

- $\mathrm{Var}^+(\bot) = \mathrm{Var}^-(\bot) = \mathrm{Var}^+(\top) = \mathrm{Var}^-(\top) = \varnothing$,
- $\mathrm{Var}^+(p_i) = \{p_i\}, \quad \mathrm{Var}^-(p_i) = \varnothing$,
- $\mathrm{Var}^+(\neg A) = \mathrm{Var}^-(A), \quad \mathrm{Var}^-(\neg A) = \mathrm{Var}^+(A)$,
- $\mathrm{Var}^+(A \wedge B) = \mathrm{Var}^+(A) \cup \mathrm{Var}^+(B)$, similarly for Var^-.
- similarly for $\vee$,
- $\mathrm{Var}^+(A \to B) = \mathrm{Var}^-(A) \cup \mathrm{Var}^+(B)$, similarly for Var^-.

Example. Let A be the formula $(p \to (q \to p)) \to s$. Then
$\mathrm{Var}^+(A) = \{p, q, s\}$,
$\mathrm{Var}^-(A) = \{p\}$.

$$(\overset{+}{p} \to (\overset{+}{q} \to \overset{-}{p})) \to \overset{+}{s}$$

Lyndon interpolation

Theorem (Lyndon interpolation theorem)

If $\vdash A \to C$ then there exists a formula B (called an interpolant) such that

$$\textbf{(1)} \vdash A \to B \ \ \textit{and} \ \vdash B \to C,$$

Lyndon interpolation

Theorem (Lyndon interpolation theorem)

If $\vdash A \to C$ then there exists a formula B (called an interpolant) such that

$$\textbf{(1)} \vdash A \to B \ \textit{ and } \vdash B \to C,$$

$$(2^+) \quad \mathrm{Var}^+(B) \subseteq \mathrm{Var}^+(A) \cap \mathrm{Var}^+(C),$$

Lyndon interpolation

Theorem (Lyndon interpolation theorem)

If $\vdash A \to C$ *then there exists a formula* B *(called an interpolant) such that*

$$\textbf{(1)} \vdash A \to B \quad \textit{and} \quad \vdash B \to C,$$

$$(2^+) \quad \mathrm{Var}^+(B) \subseteq \mathrm{Var}^+(A) \cap \mathrm{Var}^+(C),$$

$$(2^-) \quad \mathrm{Var}^-(B) \subseteq \mathrm{Var}^-(A) \cap \mathrm{Var}^-(C).$$

Lyndon interpolation

Theorem (Lyndon interpolation theorem)

If $\vdash A \to C$ then there exists a formula B (called an interpolant) such that

$$\textbf{(1)} \vdash A \to B \;\; \textit{and} \;\; \vdash B \to C,$$

$$(2^{+}) \;\; \mathrm{Var}^{+}(B) \subseteq \mathrm{Var}^{+}(A) \cap \mathrm{Var}^{+}(C),$$

$$(2^{-}) \;\; \mathrm{Var}^{-}(B) \subseteq \mathrm{Var}^{-}(A) \cap \mathrm{Var}^{-}(C).$$

The proof is more subtle.

To prove it, one can use the sequent calculus.

Uniform Craig interpolation

Theorem (Uniform Craig interpolation theorem)

For any formula $A = A(\vec{p}, \vec{q})$ *(and any choice of variables* $\vec{q} \subseteq \mathrm{Var}(A)$*) there is a formula* $B(\vec{q})$ *(a uniform interpolant of* A *w.r.t.* $\vec{q}$*) such that*

Uniform Craig interpolation

Theorem (Uniform Craig interpolation theorem)

For any formula $A = A(\vec{p}, \vec{q})$ *(and any choice of variables* $\vec{q} \subseteq \mathrm{Var}(A)$*) there is a formula* $B(\vec{q})$ *(a uniform interpolant of* A *w.r.t.* $\vec{q}$*) such that*

(1) $\vdash A(\vec{p}, \vec{q}) \to B(\vec{q})$,

Uniform Craig interpolation

Theorem (Uniform Craig interpolation theorem)

For any formula $A = A(\vec{p}, \vec{q})$ *(and any choice of variables* $\vec{q} \subseteq \mathrm{Var}(A)$*) there is a formula* $B(\vec{q})$ *(a uniform interpolant of* A *w.r.t.* $\vec{q}$*) such that*

(1) $\vdash A(\vec{p}, \vec{q}) \to B(\vec{q})$,

(2) *for any formula* $C(\vec{q}, \vec{s})$ *such that* $\vdash A \to C$ *and* $\mathrm{Var}(A) \cap \mathrm{Var}(C) \subseteq \vec{q}$, *we have* $\vdash B \to C$.

Uniform Craig interpolation

Theorem (Uniform Craig interpolation theorem)

For any formula $A = A(\vec{p}, \vec{q})$ *(and any choice of variables* $\vec{q} \subseteq \mathrm{Var}(A)$*) there is a formula* $B(\vec{q})$ *(a uniform interpolant of* A *w.r.t.* $\vec{q}$*) such that*

(1) $\vdash A(\vec{p}, \vec{q}) \to B(\vec{q})$,

(2) *for any formula* $C(\vec{q}, \vec{s})$ *such that* $\vdash A \to C$ *and* $\mathrm{Var}(A) \cap \mathrm{Var}(C) \subseteq \vec{q}$, *we have* $\vdash B \to C$.

Proof.

Take the conjunction of all formulas with variables $\vec{q}$ that follow from A:

$$B(\vec{q}) \;:=\; \bigwedge\{\, D(\vec{q}) \;\mid\; A \to D \text{ is a tautology} \,\}.$$

Uniform Craig interpolation

Theorem (Uniform Craig interpolation theorem)

For any formula $A = A(\vec{p}, \vec{q})$ (and any choice of variables $\vec{q} \subseteq \mathrm{Var}(A)$) there is a formula $B(\vec{q})$ (a uniform interpolant of A w.r.t. $\vec{q}$) such that

(1) $\vdash A(\vec{p}, \vec{q}) \to B(\vec{q})$,

(2) *for any formula $C(\vec{q}, \vec{s})$ such that $\vdash A \to C$ and $\mathrm{Var}(A) \cap \mathrm{Var}(C) \subseteq \vec{q}$, we have $\vdash B \to C$.*

Proof.

Take the conjunction of all formulas with variables $\vec{q}$ that follow from A:

$$B(\vec{q}) \;:=\; \bigwedge\{\, D(\vec{q}) \;\mid\; A \to D \text{ is a tautology} \,\}.$$

There are infinitely many such formulas D!

Uniform Craig interpolation

Theorem (Uniform Craig interpolation theorem)

For any formula $A = A(\vec{p}, \vec{q})$ *(and any choice of variables* $\vec{q} \subseteq \mathrm{Var}(A)$*) there is a formula* $B(\vec{q})$ *(a uniform interpolant of* A *w.r.t.* $\vec{q}$*) such that*

(1) $\vdash A(\vec{p}, \vec{q}) \to B(\vec{q})$,

(2) *for any formula* $C(\vec{q}, \vec{s})$ *such that* $\vdash A \to C$ *and* $\mathrm{Var}(A) \cap \mathrm{Var}(C) \subseteq \vec{q}$, *we have* $\vdash B \to C$.

Proof.

Take the conjunction of all formulas with variables $\vec{q}$ that follow from A:

$$B(\vec{q}) \ := \ \bigwedge \{ \, D(\vec{q}) \ \mid \ A \to D \text{ is a tautology} \, \}.$$

There are infinitely many such formulas D!
But only $\leqslant 2^{2^n}$ pairwise non-equivalent formulas, where $\vec{q} = (q_1, \ldots, q_n)$.

Uniform Craig interpolation

Theorem (Uniform Craig interpolation theorem)

For any formula $A = A(\vec{p}, \vec{q})$ (and any choice of variables $\vec{q} \subseteq \mathrm{Var}(A)$) there is a formula $B(\vec{q})$ (a uniform interpolant of A w.r.t. $\vec{q}$) such that

(1) $\vdash A(\vec{p}, \vec{q}) \to B(\vec{q})$,

(2) *for any formula $C(\vec{q}, \vec{s})$ such that $\vdash A \to C$ and $\mathrm{Var}(A) \cap \mathrm{Var}(C) \subseteq \vec{q}$, we have $\vdash B \to C$.*

Proof.

Take the conjunction of all formulas with variables $\vec{q}$ that follow from A:

$$B(\vec{q}) \;:=\; \bigwedge\{\, D(\vec{q}) \;\mid\; A \to D \text{ is a tautology} \,\}.$$

There are infinitely many such formulas D!
But only $\leqslant 2^{2^n}$ pairwise non-equivalent formulas, where $\vec{q} = (q_1, \ldots, q_n)$.
Please give the remainder of the proof. □

Axiomatization

Classical propositional calculus:

Axioms (more exactly: axiom schemata):

1. $A \to (B \to A)$,
2. $[A \to (B \to C)] \ \to \ [(A \to B) \to (A \to C)]$,
3. $(A \wedge B) \to A, \qquad (A \wedge B) \to B$,
4. $A \to (B \to (A \wedge B))$,
5. $A \to (A \vee B), \qquad B \to (A \vee B)$,
6. $(A \to C) \ \to \ [(B \to C) \ \to \ (A \vee B) \to C]$,
7. $(A \to B) \ \to \ [(A \to \neg B) \ \to \neg A]$,
8. $A \vee \neg A$ (alternative: $\neg\neg A \to A$)
9. $\top, \qquad \bot \to A$.

Rule of inference: *modus ponens* (MP) $\dfrac{A \quad A \to B}{B}$.

Interesting facts

- Without the axiom $A \vee \neg A$ we obtain the Intuitionistic logic.

Interesting facts

- Without the axiom $A \vee \neg A$ we obtain the Intuitionistic logic.
  It is decidable, it has compactness, interpolation.

Interesting facts

- Without the axiom $A \vee \neg A$ we obtain the Intuitionistic logic.
  It is decidable, it has compactness, interpolation.
- The axioms for $\{\neg, \wedge, \rightarrow\}$ axiomatize all tautologies built from $\{\neg, \wedge, \rightarrow\}$.

Interesting facts

- Without the axiom $A \vee \neg A$ we obtain the Intuitionistic logic.
  It is decidable, it has compactness, interpolation.

- The axioms for $\{\neg, \wedge, \rightarrow\}$ axiomatize all tautologies built from $\{\neg, \wedge, \rightarrow\}$.

- The axioms for $\{\neg, \vee, \rightarrow\}$ axiomatize all tautologies built from $\{\neg, \vee, \rightarrow\}$.

Interesting facts

- Without the axiom $A \vee \neg A$ we obtain the Intuitionistic logic. It is decidable, it has compactness, interpolation.
- The axioms for $\{\neg, \wedge, \rightarrow\}$ axiomatize all tautologies built from $\{\neg, \wedge, \rightarrow\}$.
- The axioms for $\{\neg, \vee, \rightarrow\}$ axiomatize all tautologies built from $\{\neg, \vee, \rightarrow\}$.
- The axioms for $\{\neg, \rightarrow\}$ axiomatize all tautologies built from $\{\neg, \rightarrow\}$.

Interesting facts

- Without the axiom $A \vee \neg A$ we obtain the Intuitionistic logic. It is decidable, it has compactness, interpolation.
- The axioms for $\{\neg, \wedge, \to\}$ axiomatize all tautologies built from $\{\neg, \wedge, \to\}$.
- The axioms for $\{\neg, \vee, \to\}$ axiomatize all tautologies built from $\{\neg, \vee, \to\}$.
- The axioms for $\{\neg, \to\}$ axiomatize all tautologies built from $\{\neg, \to\}$.
- What are the axioms for all tautologies over $\{\to\}$?

Interesting facts

- Without the axiom $A \vee \neg A$ we obtain the Intuitionistic logic.
  It is decidable, it has compactness, interpolation.
- The axioms for $\{\neg, \wedge, \to\}$ axiomatize all tautologies built from $\{\neg, \wedge, \to\}$.
- The axioms for $\{\neg, \vee, \to\}$ axiomatize all tautologies built from $\{\neg, \vee, \to\}$.
- The axioms for $\{\neg, \to\}$ axiomatize all tautologies built from $\{\neg, \to\}$.
- What are the axioms for all tautologies over $\{\to\}$?
  Axioms (1) and (2) are not enough!

Interesting facts

- Without the axiom $A \vee \neg A$ we obtain the Intuitionistic logic.
  It is decidable, it has compactness, interpolation.

- The axioms for $\{\neg, \wedge, \to\}$ axiomatize all tautologies built from $\{\neg, \wedge, \to\}$.

- The axioms for $\{\neg, \vee, \to\}$ axiomatize all tautologies built from $\{\neg, \vee, \to\}$.

- The axioms for $\{\neg, \to\}$ axiomatize all tautologies built from $\{\neg, \to\}$.

- What are the axioms for all tautologies over $\{\to\}$?
  Axioms (1) and (2) are not enough!
  We also need Peirce's Law: $((A \to B) \to A) \to A$.

Interesting facts

- Without the axiom $A \vee \neg A$ we obtain the Intuitionistic logic.
  It is decidable, it has compactness, interpolation.
- The axioms for $\{\neg, \wedge, \to\}$ axiomatize all tautologies built from $\{\neg, \wedge, \to\}$.
- The axioms for $\{\neg, \vee, \to\}$ axiomatize all tautologies built from $\{\neg, \vee, \to\}$.
- The axioms for $\{\neg, \to\}$ axiomatize all tautologies built from $\{\neg, \to\}$.
- What are the axioms for all tautologies over $\{\to\}$?
  Axioms (1) and (2) are not enough!
  We also need Peirce's Law: $((A \to B) \to A) \to A$.
  Without it we obtain all $\{\to\}$-theorems of Intuitionistic logic.

Axiomatizations with just one axiom

- Can we axiomatize all $\{\to\}$-tautologies with just *one axiom*?

Axiomatizations with just one axiom

- Can we axiomatize all $\{\to\}$-tautologies with just *one axiom*?
  $[(A \to B) \to C] \to [(C \to A) \to (D \to A)]$ (Łukasiewicz, 1948)

Axiomatizations with just one axiom

- Can we axiomatize all $\{\to\}$-tautologies with just *one axiom*?
  $[(A \to B) \to C] \to [(C \to A) \to (D \to A)]$ (Łukasiewicz, 1948)
- Meredith (1953) did the same for all Intuitionistic $\{\to\}$-theorems:

Axiomatizations with just one axiom

- Can we axiomatize all $\{\to\}$-tautologies with just *one axiom*?
  $[(A \to B) \to C] \to [(C \to A) \to (D \to A)]$ (Łukasiewicz, 1948)
- Meredith (1953) did the same for all Intuitionistic $\{\to\}$-theorems:
  $[(A \to B) \to C] \to [D \to \big((B \to (C \to E)) \to (B \to E)\big)]$

Axiomatizations with just one axiom

- Can we axiomatize all $\{\to\}$-tautologies with just *one axiom*?
  $[(A \to B) \to C] \to [(C \to A) \to (D \to A)]$ (Łukasiewicz, 1948)
- Meredith (1953) did the same for all Intuitionistic $\{\to\}$-theorems:
  $[(A \to B) \to C] \to [D \to \big((B \to (C \to E)) \to (B \to E)\big)]$
- We can also find a single axiom for $\{\neg, \to\}$, for $\{\neg, \wedge, \to\}$, etc.

Axiomatizations with just one axiom

- Can we axiomatize all $\{\to\}$-tautologies with just *one axiom*?
  $[(A \to B) \to C] \to [(C \to A) \to (D \to A)]$ (Łukasiewicz, 1948)
- Meredith (1953) did the same for all Intuitionistic $\{\to\}$-theorems:
  $[(A \to B) \to C] \to [D \to \big((B \to (C \to E)) \to (B \to E)\big)]$
- We can also find a single axiom for $\{\neg, \to\}$, for $\{\neg, \wedge, \to\}$, etc.
- Can we do the same for Sheffer stroke $|$ in the Classical logic?

Axiomatizations with just one axiom

- Can we axiomatize all $\{\to\}$-tautologies with just *one axiom*?
  $[(A \to B) \to C] \to [(C \to A) \to (D \to A)]$ (Łukasiewicz, 1948)
- Meredith (1953) did the same for all Intuitionistic $\{\to\}$-theorems:
  $[(A \to B) \to C] \to [D \to \big((B \to (C \to E)) \to (B \to E)\big)]$
- We can also find a single axiom for $\{\neg, \to\}$, for $\{\neg, \wedge, \to\}$, etc.
- Can we do the same for Sheffer stroke $|$ in the Classical logic? Yes:
  Axiom: $(A \mid (B \mid C)) \mid \{[D \mid (D \mid D)] \mid [(E \mid B) \mid ((A \mid E) \mid (A \mid E))]\}$
  Rule: $\dfrac{A \quad A \mid (B \mid C)}{C}$

Axiomatizations with just one axiom

- Can we axiomatize all $\{\to\}$-tautologies with just *one axiom*?
  $[(A \to B) \to C] \to [(C \to A) \to (D \to A)]$ (Łukasiewicz, 1948)
- Meredith (1953) did the same for all Intuitionistic $\{\to\}$-theorems:
  $[(A \to B) \to C] \to [D \to \big((B \to (C \to E)) \to (B \to E)\big)]$
- We can also find a single axiom for $\{\neg, \to\}$, for $\{\neg, \wedge, \to\}$, etc.
- Can we do the same for Sheffer stroke $\mid$ in the Classical logic? Yes:
  Axiom: $(A \mid (B \mid C)) \mid \{[D \mid (D \mid D)] \mid [(E \mid B) \mid ((A \mid E) \mid (A \mid E))]\}$
  Rule: $\dfrac{A \quad A \mid (B \mid C)}{C}$
  The same can be done for Peirce's arrow $\downarrow$, too!

Axiomatizations with just one axiom

- Can we axiomatize all $\{\to\}$-tautologies with just *one axiom*?
  $[(A \to B) \to C] \to [(C \to A) \to (D \to A)]$ (Łukasiewicz, 1948)
- Meredith (1953) did the same for all Intuitionistic $\{\to\}$-theorems:
  $[(A \to B) \to C] \to [D \to \big((B \to (C \to E)) \to (B \to E)\big)]$
- We can also find a single axiom for $\{\neg, \to\}$, for $\{\neg, \wedge, \to\}$, etc.
- Can we do the same for Sheffer stroke $|$ in the Classical logic? Yes:
  Axiom: $(A \mid (B \mid C)) \mid \{[D \mid (D \mid D)] \mid [(E \mid B) \mid ((A \mid E) \mid (A \mid E))]\}$
  Rule: $\dfrac{A \quad A \mid (B \mid C)}{C}$
  The same can be done for Peirce's arrow $\downarrow$, too!
- Alfred Tarski gave a **sufficient condition** under which a calculus can be axiomatized by just **one axiom**.

Axiomatizations with just one axiom

- Can we axiomatize all $\{\to\}$-tautologies with just *one axiom*?
  $[(A \to B) \to C] \to [(C \to A) \to (D \to A)]$ (Łukasiewicz, 1948)
- Meredith (1953) did the same for all Intuitionistic $\{\to\}$-theorems:
  $[(A \to B) \to C] \to [D \to \big((B \to (C \to E)) \to (B \to E)\big)]$
- We can also find a single axiom for $\{\neg, \to\}$, for $\{\neg, \wedge, \to\}$, etc.
- Can we do the same for Sheffer stroke $\mid$ in the Classical logic? Yes:
  Axiom: $(A \mid (B \mid C)) \mid \{[D \mid (D \mid D)] \mid [(E \mid B) \mid ((A \mid E) \mid (A \mid E))]\}$
  Rule: $\dfrac{A \quad A \mid (B \mid C)}{C}$
  The same can be done for Peirce's arrow $\downarrow$, too!
- Alfred Tarski gave a **sufficient condition** under which a calculus can be axiomatized by just **one axiom**.
- **Ted Ulrich** — collects shortest single axioms for many logics with only $\{\to\}$ or $\{\leftrightarrow\}$.
  `https://web.ics.purdue.edu/~dulrich/Home-page.htm`

Questions for further thinking

- Try to build an algorithm such that

Questions for further thinking

- Try to build an algorithm such that

  Input: finitely many tautologies $A_1, \ldots, A_k$

Questions for further thinking

- Try to build an algorithm such that

  Input: finitely many tautologies $A_1, \ldots, A_k$
  Output: Yes $\iff$ the formulas $A_1, \ldots, A_k$
  axiomatize all tautologies (with the rule MP).

Questions for further thinking

- Try to build an algorithm such that

  Input: finitely many tautologies $A_1, \ldots, A_k$
  Output: Yes $\iff$ the formulas $A_1, \ldots, A_k$
  axiomatize all tautologies (with the rule MP).

- The same question for just one tautology A.

Questions for further thinking

- Try to build an algorithm such that

  Input: finitely many tautologies $A_1, \ldots, A_k$
  Output: Yes $\iff$ the formulas $A_1, \ldots, A_k$
  axiomatize all tautologies (with the rule MP).
- The same question for just one tautology A.

- Imagine that we can write countable conjunctions: $(A_1 \wedge A_2 \wedge \ldots)$.

Questions for further thinking

- Try to build an algorithm such that

  Input: finitely many tautologies $A_1, \ldots, A_k$
  Output: Yes $\iff$ the formulas $A_1, \ldots, A_k$
  axiomatize all tautologies (with the rule MP).

- The same question for just one tautology A.

- Imagine that we can write countable conjunctions: $(A_1 \wedge A_2 \wedge \ldots)$.
  - How many formulas do we get then?

Questions for further thinking

- Try to build an algorithm such that

  Input: finitely many tautologies $A_1, \ldots, A_k$
  Output: Yes $\iff$ the formulas $A_1, \ldots, A_k$
  axiomatize all tautologies (with the rule MP).
- The same question for just one tautology A.

- Imagine that we can write countable conjunctions: $(A_1 \wedge A_2 \wedge \ldots)$.
  - How many formulas do we get then?
    Countably many? Continuum? Hyper-continuum?

Questions for further thinking

- Try to build an algorithm such that

  Input: finitely many tautologies $A_1, \ldots, A_k$
  Output: Yes $\Longleftrightarrow$ the formulas $A_1, \ldots, A_k$
  axiomatize all tautologies (with the rule MP).
- The same question for just one tautology A.

- Imagine that we can write countable conjunctions: $(A_1 \wedge A_2 \wedge \ldots)$.
  - How many formulas do we get then?
    Countably many? Continuum? Hyper-continuum?
  - Can we express every function $f(x_1, x_2, \ldots)\colon \{0,1\}^\omega \to \{0,1\}$?

Questions for further thinking

- Try to build an algorithm such that

  Input: finitely many tautologies $A_1, \ldots, A_k$
  Output: Yes $\iff$ the formulas $A_1, \ldots, A_k$
  axiomatize all tautologies (with the rule MP).

- The same question for just one tautology A.

- Imagine that we can write countable conjunctions: $(A_1 \wedge A_2 \wedge \ldots)$.
  - How many formulas do we get then?
    Countably many? Continuum? Hyper-continuum?
  - Can we express every function $f(x_1, x_2, \ldots)\colon \{0,1\}^\omega \to \{0,1\}$?
  - What are the axioms and rules for tautologies?

Questions for further thinking

- Try to build an algorithm such that

  Input: finitely many tautologies $A_1, \ldots, A_k$
  Output: Yes $\iff$ the formulas $A_1, \ldots, A_k$
  axiomatize all tautologies (with the rule MP).

- The same question for just one tautology A.

- Imagine that we can write countable conjunctions: $(A_1 \wedge A_2 \wedge \ldots)$.
  - How many formulas do we get then?
    Countably many? Continuum? Hyper-continuum?
  - Can we express every function $f(x_1, x_2, \ldots)\colon \{0,1\}^\omega \to \{0,1\}$?
  - What are the axioms and rules for tautologies?

The end of lecture 1. Thank you!