Proof theory and linear logic

Rémi Di Guardia

PhD Seminar, 27 June 2023

Introduction

In Mathematics / Theoretical computer science:

- pose definitions
- write proofs

Introduction

In Mathematics / Theoretical computer science:

- pose definitions
- write proofs

Richard paradox

? the smallest positive integer not definable except if you wrote at least sixty letters [86 letters]

Introduction

In Mathematics / Theoretical computer science:

- pose definitions
- write proofs

Richard paradox

? the smallest positive integer not definable except if you wrote at least sixty letters [86 letters]

? the smallest positive integer not definable in under sixty letters [57 letters]

Introduction

In Mathematics / Theoretical computer science:

- pose definitions
- write proofs

Richard paradox

X the smallest positive integer not definable except if you wrote at least sixty letters [86 letters]

X the smallest positive integer not definable in under sixty letters [57 letters]

Introduction

In Mathematics / Theoretical computer science:

- pose definitions
- write proofs

Richard paradox

- X the smallest positive integer not definable except if you wrote at least sixty letters [86 letters]
- X the smallest positive integer not definable in under sixty letters [57 letters]
- ? the smallest positive integer not definable in under twenty letters [58 letters]

Introduction

In Mathematics / Theoretical computer science:

- pose definitions
- write proofs

Richard paradox

X the smallest positive integer not definable except if you wrote at least sixty letters [86 letters]

X the smallest positive integer not definable in under sixty letters [57 letters]

? the smallest positive integer not definable in under twenty letters [58 letters]

Proof theory: study proofs and their properties

Why studying proofs?

An absolutely true result

$$-1 = 1$$

Proof.

$$-1 = (-1)^{\frac{2}{2}} = ((-1)^2)^{\frac{1}{2}} = 1^{\frac{1}{2}} = 1$$

$\square$

Why studying proofs?

An absolutely true result

$$-1 = 1$$

Proof.

$$-1 = (-1)^{\frac{2}{2}} = ((-1)^2)^{\frac{1}{2}} = 1^{\frac{1}{2}} = 1$$

$\square$

Continuum hypothesis

There is no set whose cardinal is strictly between that of the integers and the real numbers.

Why studying proofs?

An absolutely true result

$$-1 = 1$$

Proof.

$$-1 = (-1)^{\frac{2}{2}} = ((-1)^2)^{\frac{1}{2}} = 1^{\frac{1}{2}} = 1$$

□

Continuum hypothesis

There is no set whose cardinal is strictly between that of the integers and the real numbers.

This hypothesis is not provable.

Why studying proofs?

An absolutely true result

$$-1 = 1$$

Proof.

$$-1 = (-1)^{\frac{2}{2}} = ((-1)^2)^{\frac{1}{2}} = 1^{\frac{1}{2}} = 1$$

$\square$

Continuum hypothesis

There is no set whose cardinal is strictly between that of the integers and the real numbers.

This hypothesis is not provable. But its negation neither is!

A Formal Proof

Lemma

For all integer n, there exists an integer k such that n is equal to $k + 1$.

Proof.

Any n is equal to $(n - 1) + 1$. $\square$

A Formal Proof

Lemma

$$\forall n \in \mathbb{Z}, \exists k \in \mathbb{Z}, n = k + 1$$

Proof.

Any n is equal to $(n - 1) + 1$. $\square$

A Formal Proof

Lemma

$$\forall n \in \mathbb{Z}, \exists k \in \mathbb{Z}, n = k + 1$$

Proof.

We prove $\forall n \in \mathbb{Z}, \exists k \in \mathbb{Z}, n = k + 1$.
It suffices to prove $\exists k \in \mathbb{Z}, n = k + 1$ for arbitrary $n \in \mathbb{Z}$.
Instanciate $k = n - 1 \in \mathbb{Z}$. It holds that $n = (n - 1) + 1$. $\square$

A Formal Proof

Lemma

$$\forall n \in \mathbb{Z}, \exists k \in \mathbb{Z}, n = k + 1$$

Proof.

$$\dfrac{\dfrac{\dfrac{}{n = (n-1) + 1}\ (eq)}{\exists k \in \mathbb{Z}, n = k + 1}\ (\exists)}{\forall n \in \mathbb{Z}, \exists k \in \mathbb{Z}, n = k + 1}\ (\forall)$$

□

Classical Logic

$$\frac{\Gamma \vdash A[y/x], \Sigma}{\Gamma \vdash \exists x\ A, \Sigma}\ (\exists) \qquad \frac{\Gamma \vdash A, \Sigma}{\Gamma \vdash \forall x\ A, \Sigma}\ (\forall)$$

Classical Logic

$$\frac{\Gamma \vdash A[y/x], \Sigma}{\Gamma \vdash \exists x\ A, \Sigma}\ (\exists) \qquad \frac{\Gamma \vdash A, \Sigma}{\Gamma \vdash \forall x\ A, \Sigma}\ (\forall)$$

$$\frac{\Gamma \vdash A, \Sigma \qquad \Gamma \vdash B, \Sigma}{\Gamma \vdash A \wedge B, \Sigma}\ (\wedge) \qquad \frac{\Gamma \vdash A, \Sigma}{\Gamma \vdash A \vee B, \Sigma}\ (\vee) \qquad \frac{\Gamma \vdash B, \Sigma}{\Gamma \vdash A \vee B, \Sigma}\ (\vee)$$

Classical Logic

$$\frac{\Gamma \vdash A[y/x], \Sigma}{\Gamma \vdash \exists x\ A, \Sigma}\ (\exists) \qquad \frac{\Gamma \vdash A, \Sigma}{\Gamma \vdash \forall x\ A, \Sigma}\ (\forall)$$

$$\frac{\Gamma \vdash A, \Sigma \quad \Gamma \vdash B, \Sigma}{\Gamma \vdash A \wedge B, \Sigma}\ (\wedge) \qquad \frac{\Gamma \vdash A, \Sigma}{\Gamma \vdash A \vee B, \Sigma}\ (\vee) \qquad \frac{\Gamma \vdash B, \Sigma}{\Gamma \vdash A \vee B, \Sigma}\ (\vee)$$

$$\frac{\Gamma \vdash A, \Sigma \quad \Delta \vdash B, \Theta}{\Gamma, \Delta \vdash A \wedge B, \Sigma, \Theta}\ (\wedge) \qquad \frac{\Gamma \vdash A, B, \Sigma}{\Gamma \vdash A \vee B, \Sigma}\ (\vee)$$

(and more rules)

Classical Logic

$$\frac{\Gamma \vdash A[y/x], \Sigma}{\Gamma \vdash \exists x\ A, \Sigma}\ (\exists) \qquad \frac{\Gamma \vdash A, \Sigma}{\Gamma \vdash \forall x\ A, \Sigma}\ (\forall)$$

$$\frac{\Gamma \vdash A, \Sigma \qquad \Gamma \vdash B, \Sigma}{\Gamma \vdash A \wedge B, \Sigma}\ (\wedge) \qquad \frac{\Gamma \vdash A, \Sigma}{\Gamma \vdash A \vee B, \Sigma}\ (\vee) \qquad \frac{\Gamma \vdash B, \Sigma}{\Gamma \vdash A \vee B, \Sigma}\ (\vee)$$

$$\frac{\Gamma \vdash A, \Sigma \qquad \Delta \vdash B, \Theta}{\Gamma, \Delta \vdash A \wedge B, \Sigma, \Theta}\ (\wedge) \qquad \frac{\Gamma \vdash A, B, \Sigma}{\Gamma \vdash A \vee B, \Sigma}\ (\vee)$$

(and more rules)

Very symmetric but bad properties: many trees for the same "proof"

Intuitionistic Logic

Cauchy-Lipschitz theorem: unique solution to some differential problems.
Engineer point of view: still no answer :(

Intuitionistic Logic

Cauchy-Lipschitz theorem: unique solution to some differential problems.
Engineer point of view: still no answer :(

Intuitionistic Logic by changing the rules from Classical Logic
Constructive: from a proof of $\exists x\ A$ can recover an algorithm computing x

Intuitionistic Logic

Cauchy-Lipschitz theorem: unique solution to some differential problems.
Engineer point of view: still no answer :(

Intuitionistic Logic by changing the rules from Classical Logic
Constructive: from a proof of $\exists x\ A$ can recover an algorithm computing x

But *weaker* logic (no excluded middle)

Linear Logic

$$\frac{\Gamma \vdash A, \Sigma \quad \Gamma \vdash B, \Sigma}{\Gamma \vdash A \wedge B, \Sigma}\ (\wedge) \qquad \frac{\Gamma \vdash A, \Sigma}{\Gamma \vdash A \vee B, \Sigma}\ (\vee) \qquad \frac{\Gamma \vdash B, \Sigma}{\Gamma \vdash A \vee B, \Sigma}\ (\vee)$$

$$\frac{\Gamma \vdash A, \Sigma \quad \Delta \vdash B, \Theta}{\Gamma, \Delta \vdash A \wedge B, \Sigma, \Theta}\ (\wedge) \qquad \frac{\Gamma \vdash A, B, \Sigma}{\Gamma \vdash A \vee B, \Sigma}\ (\vee)$$

(and more rules)

Linear Logic

$$\frac{\Gamma \vdash A, \Sigma \qquad \Gamma \vdash B, \Sigma}{\Gamma \vdash A \mathbin{\&} B, \Sigma}\ (\&) \qquad \frac{\Gamma \vdash A, \Sigma}{\Gamma \vdash A \oplus B, \Sigma}\ (\oplus) \qquad \frac{\Gamma \vdash B, \Sigma}{\Gamma \vdash A \oplus B, \Sigma}\ (\oplus)$$

$$\frac{\Gamma \vdash A, \Sigma \qquad \Delta \vdash B, \Theta}{\Gamma, \Delta \vdash A \otimes B, \Sigma, \Theta}\ (\otimes) \qquad \frac{\Gamma \vdash A, B, \Sigma}{\Gamma \vdash A \parr B, \Sigma}\ (\parr)$$

(and **even** more rules)

Linear Logic

$$\frac{\Gamma \vdash A, \Sigma \qquad \Gamma \vdash B, \Sigma}{\Gamma \vdash A \,\&\, B, \Sigma}\ (\&) \qquad \frac{\Gamma \vdash A, \Sigma}{\Gamma \vdash A \oplus B, \Sigma}\ (\oplus) \qquad \frac{\Gamma \vdash B, \Sigma}{\Gamma \vdash A \oplus B, \Sigma}\ (\oplus)$$

$$\frac{\Gamma \vdash A, \Sigma \qquad \Delta \vdash B, \Theta}{\Gamma, \Delta \vdash A \otimes B, \Sigma, \Theta}\ (\otimes) \qquad \frac{\Gamma \vdash A, B, \Sigma}{\Gamma \vdash A \parr B, \Sigma}\ (\parr)$$

(and **even** more rules)

- Good properties
- Generalizes both classical and intuitionistic logics
- Linear use of hypotheses: A implies B means A consumed to prove B

Restaurant Menu

Menu	35€
Entree	Quiche or Salmon
Plat	Pasta or Duck
Dessert	Fruit (Banana or Apple according to season) or Cake (Flan or Chocolate according to Chief's mood)
Sides	Water at will

Restaurant Menu

Menu	**35€**
Entree	Quiche or Salmon
Plat	Pasta or Duck
Dessert	Fruit (Banana or Apple according to season) or Cake (Flan or Chocolate according to Chief's mood)
Sides	Water at will

35€ $\multimap$

$\multimap$ linear implication, consume its premise (or as $A \implies B = \neg A \vee B$)

Restaurant Menu

Menu	35€
Entree	Quiche or Salmon
Plat	Pasta or Duck
Dessert	Fruit (Banana or Apple according to season) or Cake (Flan or Chocolate according to Chief's mood)
Sides	Water at will

$$35€ \multimap [(Q \,\&\, S)$$

$\multimap$ linear implication, consume its premise (or as $A \implies B = \neg A \vee B$)

$\&$ and where we (the client) choose between two options

Restaurant Menu

Menu	35€
Entree	Quiche or Salmon
Plat	Pasta or Duck
Dessert	Fruit (Banana or Apple according to season) or Cake (Flan or Chocolate according to Chief's mood)
Sides	Water at will

$$35€ \multimap [(Q \,\&\, S) \otimes (P \,\&\, D)]$$

- $\multimap$ linear implication, consume its premise (or as $A \implies B = \neg A \vee B$)
- $\&$ and where we (the client) choose between two options
- $\otimes$ and where we get both options

Restaurant Menu

Menu	35€
Entree	Quiche or Salmon
Plat	Pasta or Duck
Dessert	Fruit (Banana or Apple according to season) or Cake (Flan or Chocolate according to Chief's mood)
Sides	Water at will

$$35€ \multimap [(Q \,\&\, S) \otimes (P \,\&\, D) \otimes ((B \oplus A) \,\&\, (F \oplus C))$$

- $\multimap$ linear implication, consume its premise (or as $A \implies B = \neg A \vee B$)
- $\&$ and where we (the client) choose between two options
- $\otimes$ and where we get both options
- $\oplus$ or where we (the client) do not choose between two options

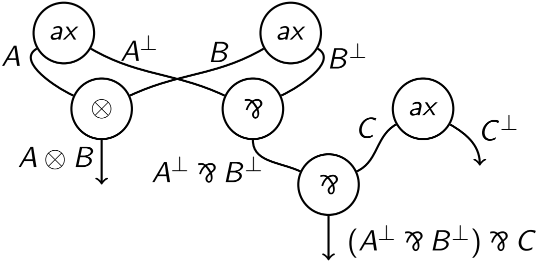
Restaurant Menu

Menu	35€
Entree	Quiche or Salmon
Plat	Pasta or Duck
Dessert	Fruit (Banana or Apple according to season) or Cake (Flan or Chocolate according to Chief's mood)
Sides	Water at will

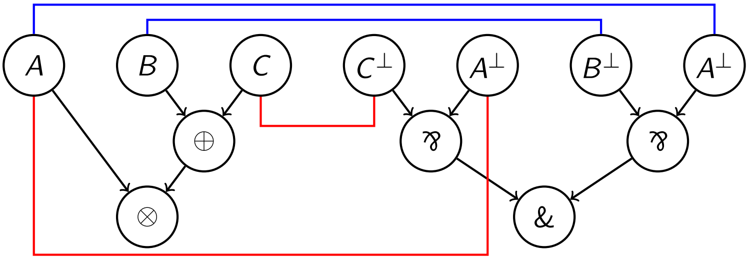
$$35€ \multimap [(Q \,\&\, S) \otimes (P \,\&\, D) \otimes ((B \oplus A) \,\&\, (F \oplus C)) \otimes !W]$$

- $\multimap$ linear implication, consume its premise (or as $A \implies B = \neg A \vee B$)
- $\&$ and where we (the client) choose between two options
- $\otimes$ and where we get both options
- $\oplus$ or where we (the client) do not choose between two options
- $!$ unlimited resource

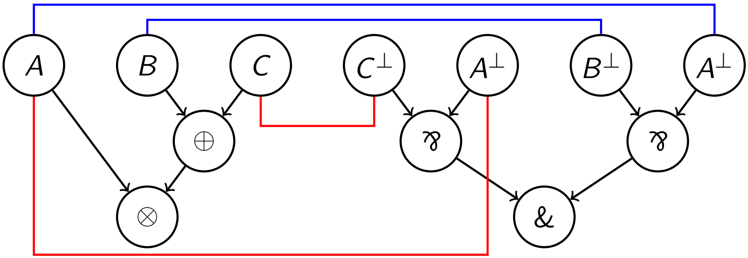
Proof Nets: graphs as proofs



Proof Nets: graphs as proofs



Proof Nets: graphs as proofs



Even better properties: one graph for one “proof”!
But does not work for the full logic.

My thesis

- Use proof nets to find results, e.g. isomorphisms

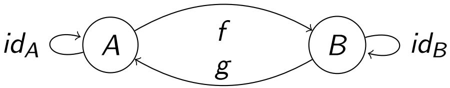
$$\begin{tikzcd} A \arrow[loop left, "id_A"] \arrow[r, bend left, "f"] & B \arrow[l, bend left, "g"] \arrow[loop right, "id_B"] \end{tikzcd}$$

$$(A \times B) \to C \simeq A \to (B \to C)$$

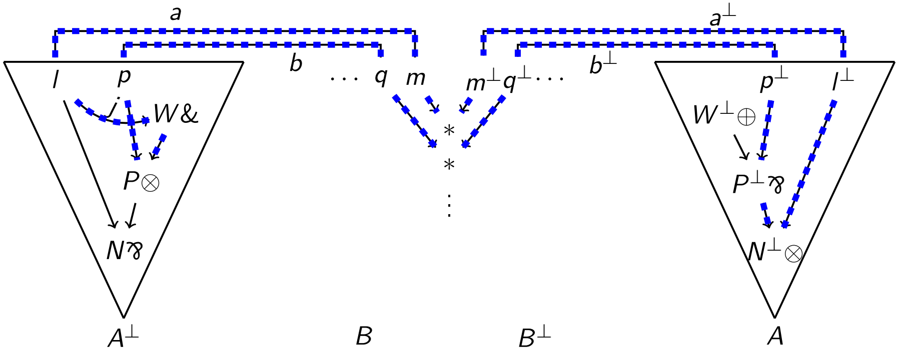
Associativity	$A \otimes (B \otimes C) = (A \otimes B) \otimes C$		$A \parr (B \parr C) = (A \parr B) \parr C$	
	$A \oplus (B \oplus C) = (A \oplus B) \oplus C$		$A \& (B \& C) = (A \& B) \& C$	
Commutativity	$A \otimes B = B \otimes A$	$A \parr B = B \parr A$	$A \oplus B = B \oplus A$	$A \& B = B \& A$
Neutrality	$A \otimes 1 = A$	$A \parr \bot = A$	$A \oplus 0 = A$	$A \& \top = A$
Distributivity	$A \otimes (B \oplus C) = (A \otimes B) \oplus (A \otimes C)$		$A \parr (B \& C) = (A \parr B) \& (A \parr C)$	
Annihilation	$A \otimes 0 = 0$	$A \parr \top = \top$		

My thesis

- Use proof nets to find results, e.g. isomorphisms



$$(A \times B) \to C \simeq A \to (B \to C)$$



My thesis

- Use proof nets to find results, e.g. isomorphisms

$$\begin{tikzcd} A \arrow[loop left, "id_A"] \arrow[r, bend left, "f"] & B \arrow[l, bend left, "g"] \arrow[loop right, "id_B"] \end{tikzcd}$$

$$(A \times B) \to C \simeq A \to (B \to C)$$

- Proof nets on more parts of the logic

My thesis

- Use proof nets to find results, e.g. isomorphisms

$$\begin{tikzcd} A \arrow[loop left, "id_A"] \arrow[rr, bend left, "f"] & & B \arrow[loop right, "id_B"] \arrow[ll, bend left, "g"] \end{tikzcd}$$

$$(A \times B) \to C \simeq A \to (B \to C)$$

- Proof nets on more parts of the logic
- Formalization in Coq

Thank you!