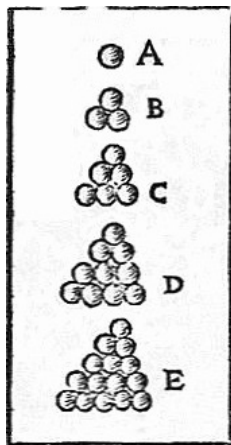


- ▶ **Proof assistant:** software che aiuta nello sviluppo di dimostrazioni formali

- ▶ **Proof assistant:** software che aiuta nello sviluppo di dimostrazioni formali
- ▶ **NON** coincidono con gli automatic theorem prover

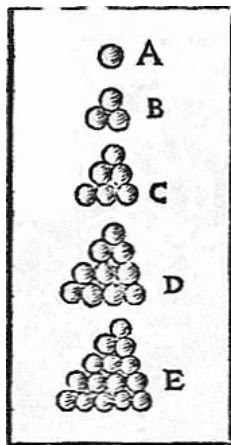
Alcuni traguardi

Alcuni traguardi

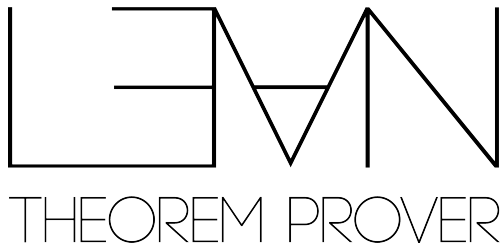


- Congettura di Keplero
(Thomas Hales, 2015)

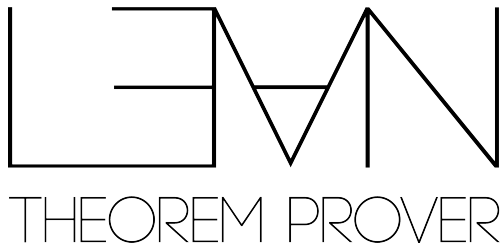
Alcuni traguardi



- Congettura di Keplero
(Thomas Hales, 2015)
- *Liquid Tensor Experiment*
(Peter Scholze, 2021)



- ▶ Un proof assistant: Lean Theorem Prover (Microsoft Research, 2013)



- ▶ Un proof assistant: Lean Theorem Prover (Microsoft Research, 2013)
- ▶ Una libreria digitalizzata di matematica: Mathlib (2017)

Soggetto

Soggetto

- ▶ *A class of Recursive Permutations which is Primitive Recursive complete*
(Luca Paolini, Mauro Piccolo, Luca Roversi, 2019)

Soggetto

- ▶ *A class of Recursive Permutations which is Primitive Recursive complete*

(Luca Paolini, Mauro Piccolo, Luca Roversi, 2019)

- ▶ Computazione reversibile

input

programma

output

Soggetto

- ▶ *A class of Recursive Permutations which is Primitive Recursive complete*

(Luca Paolini, Mauro Piccolo, Luca Roversi, 2019)

- ▶ Computazione reversibile

input

programma

output

Nessuna perdita di informazioni!

- **Reversible Primitive Permutations (RPP)**: una classe di funzioni $\mathbb{Z}^n \rightarrow \mathbb{Z}^n$ calcolabili, reversibili che è PRF-completa

RPP

Appartengono a RPP:

RPP

Appartengono a RPP:

- L'identità n -aria

$$\begin{array}{c} x_1 \\ \vdots \\ x_n \end{array} \quad \text{Id}_n \quad \begin{array}{c} x_1 \\ \vdots \\ x_n \end{array}$$

RPP

Appartengono a RPP:

- L'identità n -aria

$$\begin{array}{ccc} x_1 & & x_1 \\ \vdots & & \vdots \\ x_n & \text{Id}_n & x_n \end{array}$$

- La funzione **negazione**

$$x \quad \text{Ne} \quad -x$$

RPP

Appartengono a RPP:

- L'**identità** n -aria

$$\begin{matrix} x_1 \\ \vdots \\ x_n \end{matrix} \quad \text{Id}_n \quad \begin{matrix} x_1 \\ \vdots \\ x_n \end{matrix}$$

- La funzione **negazione**

$$x \quad \text{Ne} \quad -x$$

- La funzione **successore** e **predecessore**

$$x \quad \text{Su} \quad x + 1 \qquad x \quad \text{Pr} \quad x - 1$$

RPP

Appartengono a RPP:

- L'**identità** n -aria

$$\begin{array}{ccc} x_1 & & x_1 \\ \vdots & & \vdots \\ x_n & \text{Id}_n & x_n \end{array}$$

- La funzione **negazione**

$$x \quad \text{Ne} \quad -x$$

- La funzione **successore** e **predecessore**

$$x \quad \text{Su} \quad x + 1 \qquad x \quad \text{Pr} \quad x - 1$$

- Lo **swap**

$$\begin{array}{ccc} x & & y \\ y & \text{Sw} & x \end{array}$$

RPP

Appartengono a RPP:

- La **composizione in serie** di due $f, g \in \text{RPP}$

$$\begin{array}{c} x_1 \\ \vdots \\ x_n \end{array} \begin{array}{|c|} \hline f \circ g \\ \hline \end{array} \begin{array}{c} z_1 \\ \vdots \\ z_n \end{array} = \begin{array}{c} x_1 \\ \vdots \\ x_n \end{array} \begin{array}{|c|} \hline f \\ \hline \end{array} \begin{array}{c} y_1 \\ \vdots \\ y_n \end{array} \begin{array}{|c|} \hline g \\ \hline \end{array} \begin{array}{c} z_1 \\ \vdots \\ z_n \end{array}$$

Appartengono a RPP:

- La **composizione in serie** di due $f, g \in \text{RPP}$

$$\begin{array}{c} x_1 \\ \vdots \\ x_n \end{array} \begin{array}{|c|} \hline f \circ g \\ \hline \end{array} \begin{array}{c} z_1 \\ \vdots \\ z_n \end{array} = \begin{array}{c} x_1 \\ \vdots \\ x_n \end{array} \begin{array}{|c|} \hline f \\ \hline \end{array} \begin{array}{c} y_1 \\ \vdots \\ y_n \end{array} \begin{array}{|c|} \hline g \\ \hline \end{array} \begin{array}{c} z_1 \\ \vdots \\ z_n \end{array}$$

- La **composizione parallela** di due $f, g \in \text{RPP}$

$$\begin{array}{c} x_1 \\ \vdots \\ x_n \\ y_1 \\ \vdots \\ y_m \end{array} \begin{array}{|c|} \hline f \parallel g \\ \hline \end{array} \begin{array}{c} z_1 \\ \vdots \\ z_n \\ w_1 \\ \vdots \\ w_m \end{array} = \begin{array}{c} x_1 \\ \vdots \\ x_n \\ y_1 \\ \vdots \\ y_m \end{array} \begin{array}{|c|} \hline f \\ \hline \end{array} \begin{array}{c} z_1 \\ \vdots \\ z_n \end{array} \begin{array}{|c|} \hline g \\ \hline \end{array} \begin{array}{c} w_1 \\ \vdots \\ w_m \end{array}$$

Appartengono a RPP:

- L'iterazione finita di una $f \in \text{RPP}$

$$\begin{array}{ccc}
 \begin{array}{c} x \\ x_1 \\ \vdots \\ x_n \end{array} & \boxed{\text{It}[f]} & \begin{array}{c} x \\ y_1 \\ \vdots \\ y_n \end{array} \\
 & = & \begin{array}{c} x \\ x_1 \\ \vdots \\ x_n \end{array} \underbrace{\boxed{f} \dots \boxed{f}}_{x \text{ volte (se } x > 0)} \begin{array}{c} x \\ y_1 \\ \vdots \\ y_n \end{array}
 \end{array}$$

Appartengono a RPP:

- L'iterazione finita di una $f \in \text{RPP}$

$$\begin{array}{c} x \\ x_1 \\ \vdots \\ x_n \end{array} \boxed{\text{It}[f]} \begin{array}{c} x \\ y_1 \\ \vdots \\ y_n \end{array} = \begin{array}{c} x \\ x_1 \\ \vdots \\ x_n \end{array} \boxed{f} \dots \boxed{f} \begin{array}{c} x \\ y_1 \\ \vdots \\ y_n \end{array}$$

$\underbrace{\hspace{10em}}$
 $x \text{ volte (se } x > 0)$

- La selezione di tre $f, g, h \in \text{RPP}$

$$\begin{array}{c} x \\ x_1 \\ \vdots \\ x_n \end{array} \boxed{\text{If}[f, g, h]} \begin{array}{c} x \\ y_1 \\ \vdots \\ y_n \end{array} \left. \vphantom{\begin{array}{c} x \\ x_1 \\ \vdots \\ x_n \end{array}} \right\} = \begin{cases} f(x_1, \dots, x_n) & \text{if } x > 0 \\ g(x_1, \dots, x_n) & \text{if } x = 0 \\ h(x_1, \dots, x_n) & \text{if } x < 0 \end{cases}$$

Proprietà delle RPP

- ▶ calcolabili
- ▶ reversibili
- ▶ PRF-completa

Proprietà delle RPP

- ▶ calcolabili
- ▶ reversibili
- ▶ PRF-completa

Possibile arrivare al risultato tramite algoritmo/procedura concreta

Proprietà delle RPP

- ▶ calcolabili
- ▶ **reversibili**
- ▶ PRF-completa

Proprietà delle RPP

- ▶ calcolabili
- ▶ reversibili
- ▶ PRF-completa

Ogni funzione ammette inversa:

- ▶ $\text{Id}_n^{-1} = \text{Id}_n$
- ▶ $\text{Ne}^{-1} = \text{Ne}$
- ▶ $\text{Su}^{-1} = \text{Pr}$
- ▶ $\text{Pr}^{-1} = \text{Su}$
- ▶ $\text{Sw}^{-1} = \text{Sw}$
- ▶ $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$
- ▶ $(f \parallel g)^{-1} = f^{-1} \parallel g^{-1}$
- ▶ $\text{It}[f]^{-1} = \text{It}[f^{-1}]$
- ▶ $\text{If}[f, g, h]^{-1} = \text{If}[f^{-1}, g^{-1}, h^{-1}]$

Proprietà delle RPP

- ▶ calcolabili
- ▶ reversibili
- ▶ PRF-completa

Per esempio, $(\text{Sw} \circ (\text{Ne} \parallel \text{Su}))^{-1} = (\text{Ne} \parallel \text{Pr}) \circ \text{Sw}$:

$$\begin{array}{ccc} x & \boxed{\text{Sw}} & y \\ y & & x \end{array} \quad \begin{array}{cc} \boxed{\text{Ne}} & -y \\ \boxed{\text{Su}} & x + 1 \end{array}$$

Proprietà delle RPP

- ▶ calcolabili
- ▶ reversibili
- ▶ PRF-completa

Per esempio, $(\text{Sw} \circ (\text{Ne} \parallel \text{Su}))^{-1} = (\text{Ne} \parallel \text{Pr}) \circ \text{Sw}$:

$$\begin{array}{ccccc} x & \boxed{\text{Sw}} & y & \boxed{\text{Ne}} & -y \\ y & & x & \boxed{\text{Su}} & x + 1 \end{array}$$

$$\begin{array}{ccccc} -y & \boxed{\text{Ne}} & y & \boxed{\text{Sw}} & x \\ x + 1 & \boxed{\text{Pr}} & x & & y \end{array}$$

Proprietà delle RPP

- ▶ calcolabili
- ▶ reversibili
- ▶ PRF-completa

Proprietà delle RPP

- ▶ calcolabili
- ▶ reversibili
- ▶ PRF-completa

Sia $F \in \text{PRF}$.

Allora, esiste $g \in \text{RPP}$ che **codifica** F :

$$\begin{array}{ccc} z & g & z + F(x) \\ x & & x \\ 0 & & 0 \end{array}$$

Formalizzazione in Lean

Formalizzazione in Lean

La definizione: divisione in **sintassi** e **semantica**.

Formalizzazione in Lean

La definizione: divisione in **sintassi** e **semantica**.

► Sintassi: RPP

```
def f := Sw ;; (Ne || Su) : RPP
```

Formalizzazione in Lean

La definizione: divisione in **sintassi** e **semantica**.

- Sintassi: RPP

```
def f := Sw ;; (Ne || Su) : RPP
```

- Semantica: $\text{ev} : \text{RPP} \rightarrow (\text{list } \mathbb{Z} \rightarrow \text{list } \mathbb{Z})$

Formalizzazione in Lean

La definizione: divisione in **sintassi** e **semantica**.

- Sintassi: RPP

```
def f := Sw ;; (Ne || Su) : RPP
```

- Semantica: $ev : RPP \rightarrow (list \mathbb{Z} \rightarrow list \mathbb{Z})$

$\langle f \rangle : list \mathbb{Z} \rightarrow list \mathbb{Z}$

$\langle f \rangle [x, y] = [-y, x+1]$

Formalizzazione in Lean

Principali teoremi:

Formalizzazione in Lean

Principali teoremi:

- ▶ Ogni RPP è invertibile:

```
theorem inv_iff (f : RPP) (X Y : list  $\mathbb{Z}$ ) :  
   $\langle f^{-1} \rangle X = Y \leftrightarrow \langle f \rangle Y = X$ 
```

- ▶ PRF-completezza:

```
theorem completeness (F :  $\mathbb{N} \rightarrow \mathbb{N}$ ) :  
  nat.primrec F  $\rightarrow \exists$  f : RPP, encode F f
```