Introducción a la Realizabilidad Intuicionista

Mauricio GUILLERMO. FIng/UdelaR

Julio 2021
Escuela de Ciencias Informáticas
Exactas/UBA.

Formalismo vs Intuicionismo: Hilbert vs Brouwer...

Programa de Hilbert

- Filosóficamente reduccionista: pretende fundar la matemática en la aritmética.
- Los métodos formales permiten la reducción de las *fórmulas abstractas* a *fórmulas finitistas* (fórmulas aritméticas).
- Plantea la necesidad de codificar las demostraciones en la aritmética (llevada a cabo por Gödel); para poder probar la *consistencia* y la *completitud* de las teorías abstractas mediante pruebas finitistas (refutado por Gödel).
- Plantea el objetivo de probar la propia consistencia de la aritmética dentro de la aritmética (refutado por Gödel).

...Formalismo vs Intuicionismo: Hilbert vs Brouwer

Crítica de Brouwer

- En 1905 publica su manifiesto ▸ *Life, Art and Mysticism*.
- En 1908 publica ▸ *"De onbetrouwbaarheid der logische principes"* (english) (*Los dudosos principios de la lógica*).
- Los objetos matemáticos son construcciones (abstractas) de la mente humana, despegadas del lenguaje y de sus leyes. Las demostraciones son construcciones directas sobre esas nociones abstractas.
- El paradigma reduccionista es incorrecto: La noción de verdad matemática no se puede reducir a ningún procedimiento de verificación finitista.
- Argumenta a favor de la incorrectitud de los métodos formales, explicitando mediante ejemplos que estos métodos no son constructivos (llamados *ejemplos brouwerianos*).

Teoremas no constructivos...

Teorema

Existen irracionales a y b tales que a^b es racional.

Prueba

Primer caso: Si $\sqrt{2}^{\sqrt{2}}$ es racional, está probado eligiendo $a = b = \sqrt{2}$. Segundo caso: Si $\sqrt{2}^{\sqrt{2}}$ es irracional, elegimos $a = \sqrt{2}^{\sqrt{2}}$ y $b = \sqrt{2}$.

- Para aceptar esta prueba por casos, basta con aceptar que $P\left(\sqrt{2}^{\sqrt{2}}\right) \vee \neg P\left(\sqrt{2}^{\sqrt{2}}\right)$ donde $P(x)$ significa *"x es racional"*.
- Pero la prueba no da dos números a y b que cumplan la propiedad, excepto que además podamos discernir si $\sqrt{2}^{\sqrt{2}}$ es racional o irracional.

...teoremas no constructivos...

Teorema de Gelfond-Schneider

"Si $\underline{x}$ e $\underline{y}$ son algebraicos, $\underline{y}$ irracional, $\underline{x} \neq 0$ y $\underline{x} \neq 1$, entonces x^y es trascendente".

Eligiendo $x = y = \sqrt{2}$ tenemos que $a = \sqrt{2}^{\sqrt{2}}$ es trascendente y, por lo tanto, irracional. Eligiendo $b = \sqrt{2}$, tenemos una a, b irracionales con a^b racional.

La prueba basada en el tercero excluído no basta para saberlo.

- El séptimo problema de Hilbert consiste en responder justamente si el teorema de Gelfond-Schneider es cierto o no.
- La primera respuesta a este problema corresponde al matemático soviético Alexsandr Gelfond en 1934 e independientemente en 1935 el matemático alemán Theodor Schneider.

... teoremas no constructivos...

Teorema

Al menos uno de los reales $e + \pi$, $e\pi$ es trascendente.

Prueba

Si ninguno de los dos fuera trascendente, entonces consideramos el polinomio $x^2 - (e + \pi)x + e\pi$, que tiene raíces e y π y probamos que e y π son algebraicos (absurdo).

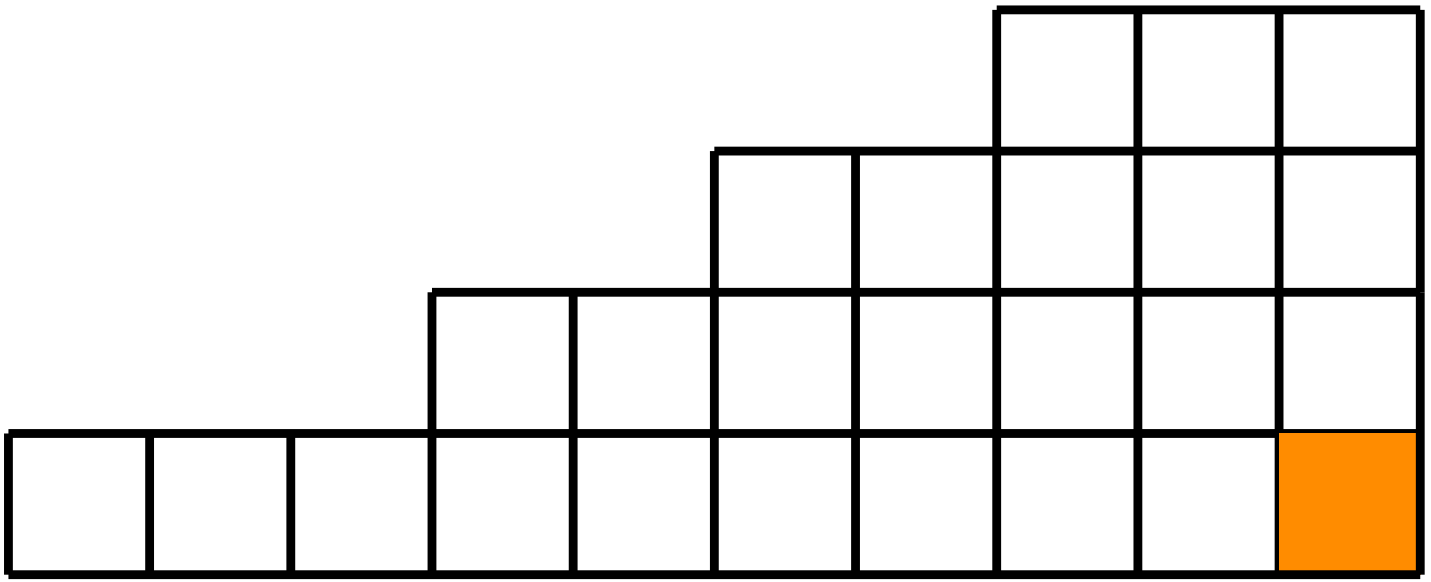
- Para aceptar esta prueba por absurdo, basta con aceptar que $\neg(\neg A \wedge \neg B) \Rightarrow A \vee B$, siendo A la afirmación "$e + \pi$ *es trascendente*" y B la afirmación "$e\pi$ *es trascendente*".
- La prueba no dice cuál de los dos es trascendente.
  De hecho, al día de hoy, saber si $e + \pi$ es trascendente y si $e\pi$ es trascendente son problemas abiertos.

...teoremas no constructivos...

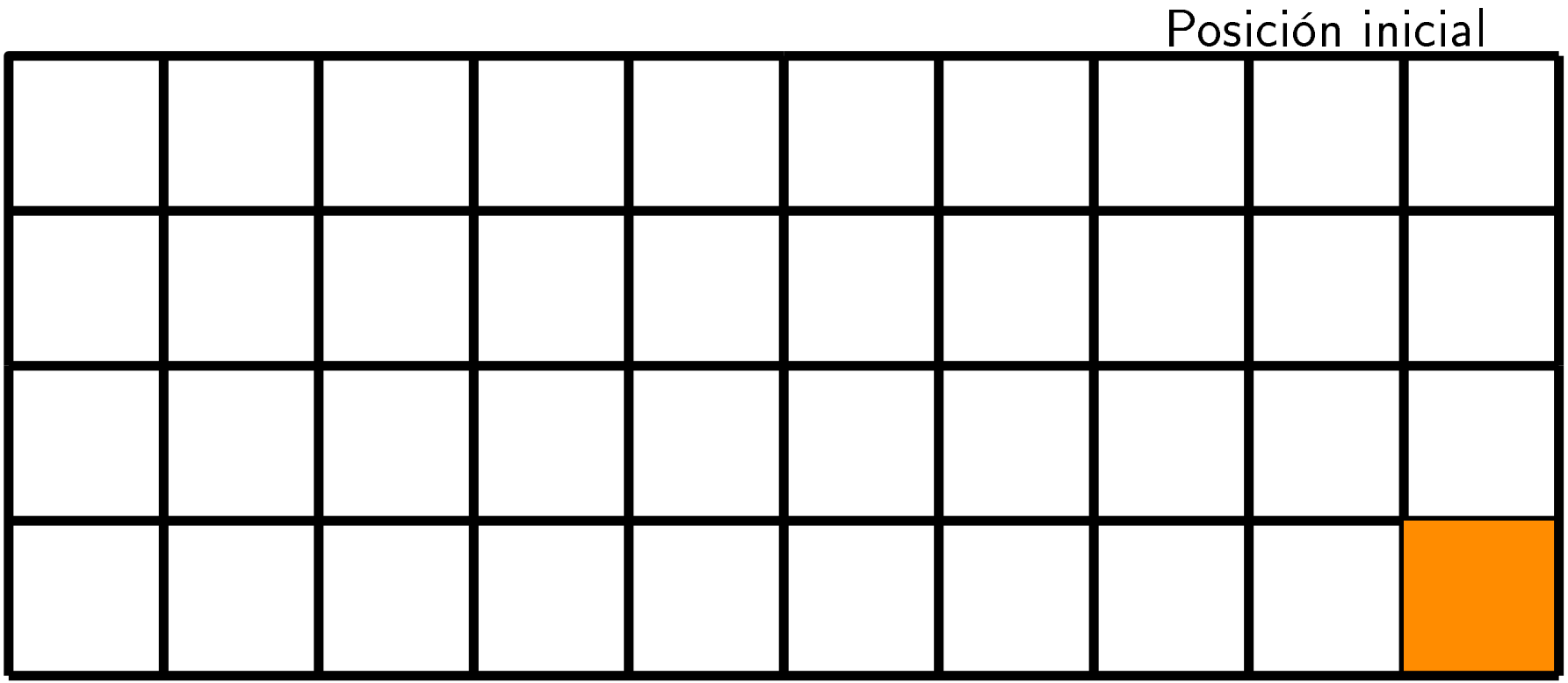
Juego de la tableta de chocolate:

- La tableta tiene la esquina inferior derecha envenenada.
- A cada turno, los jugadores deben comer una porción no vacía de chocolate, cortada del ángulo superior izquierdo.
- Los jugadores juegan hasta que uno se envenena.

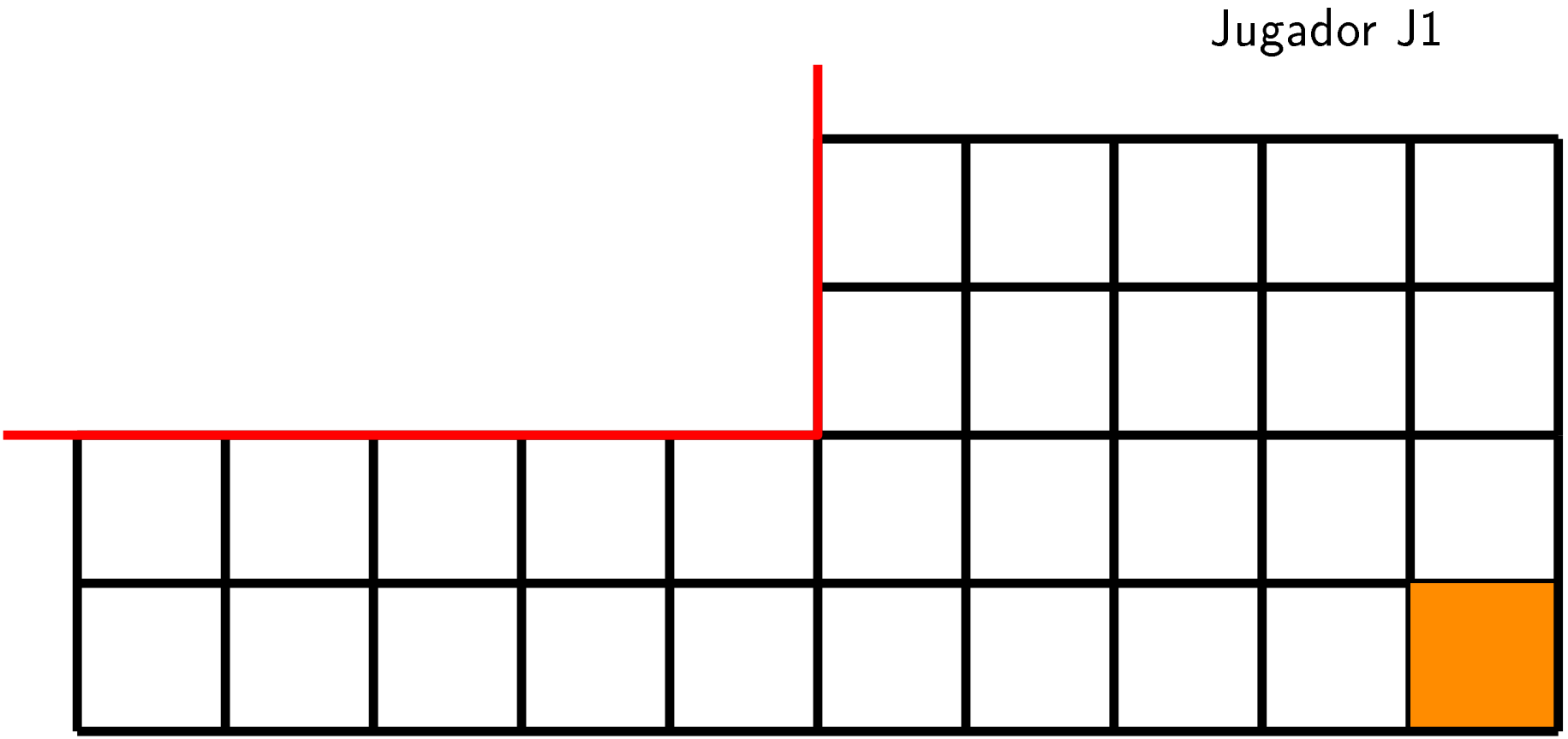
Posición intermedia:



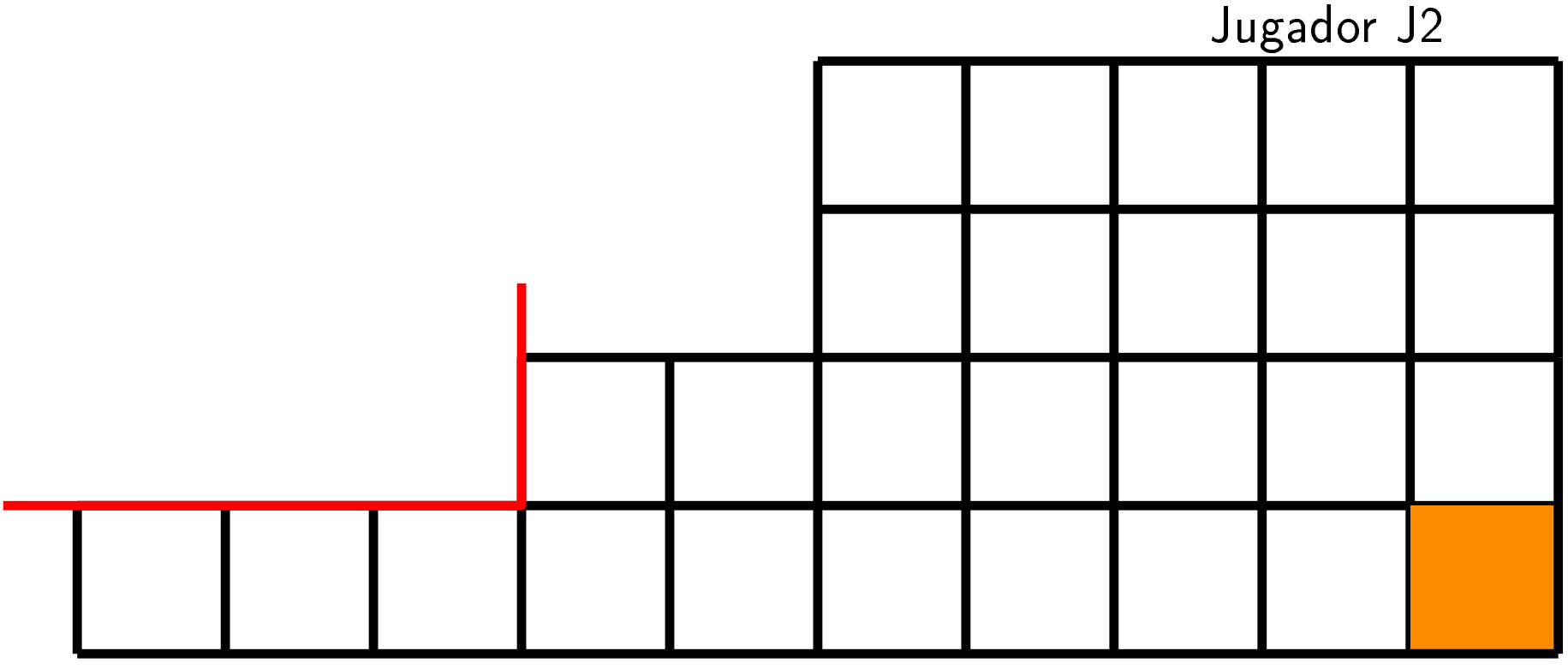
...teoremas no constructivos...



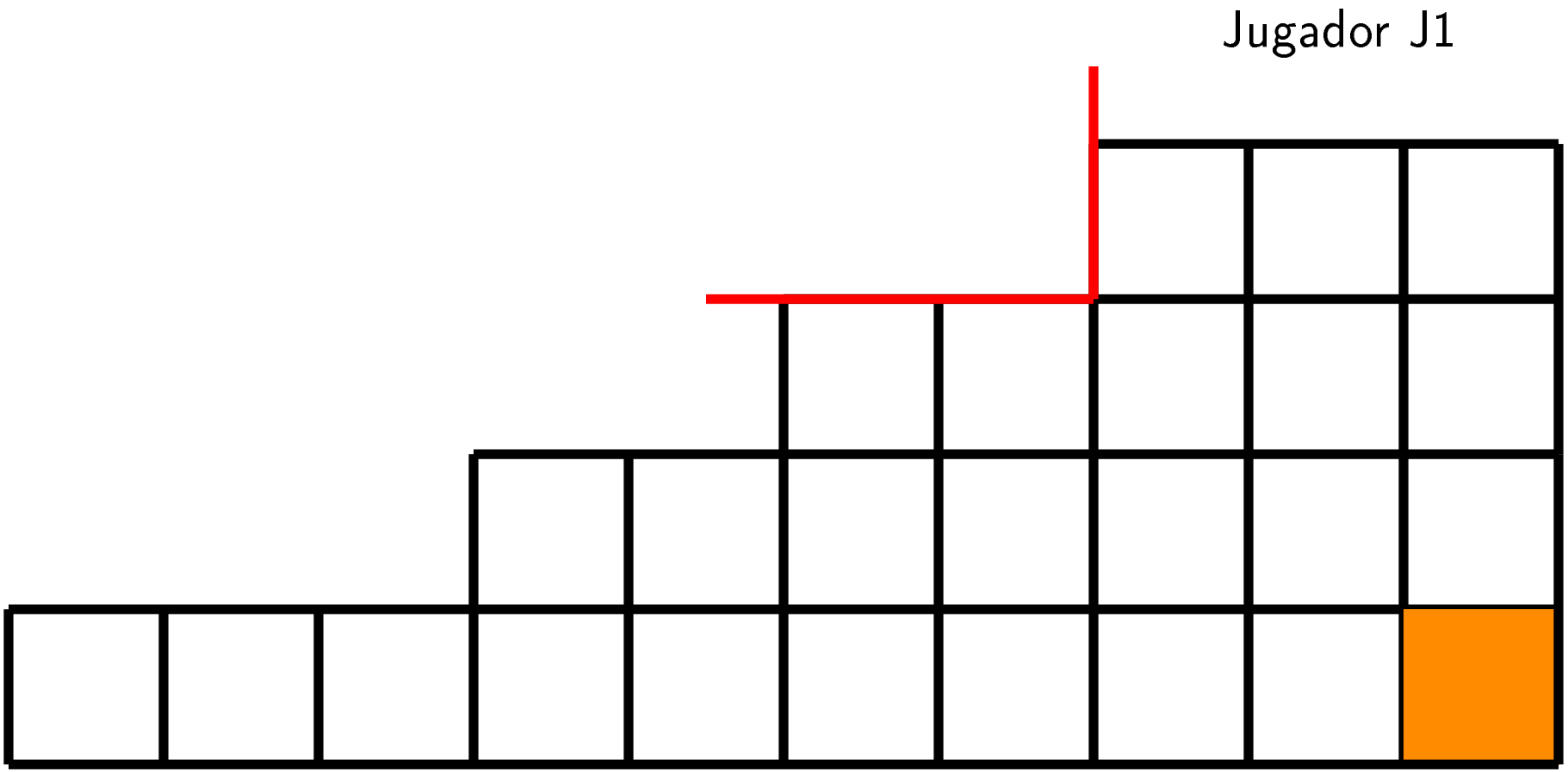
...teoremas no constructivos...



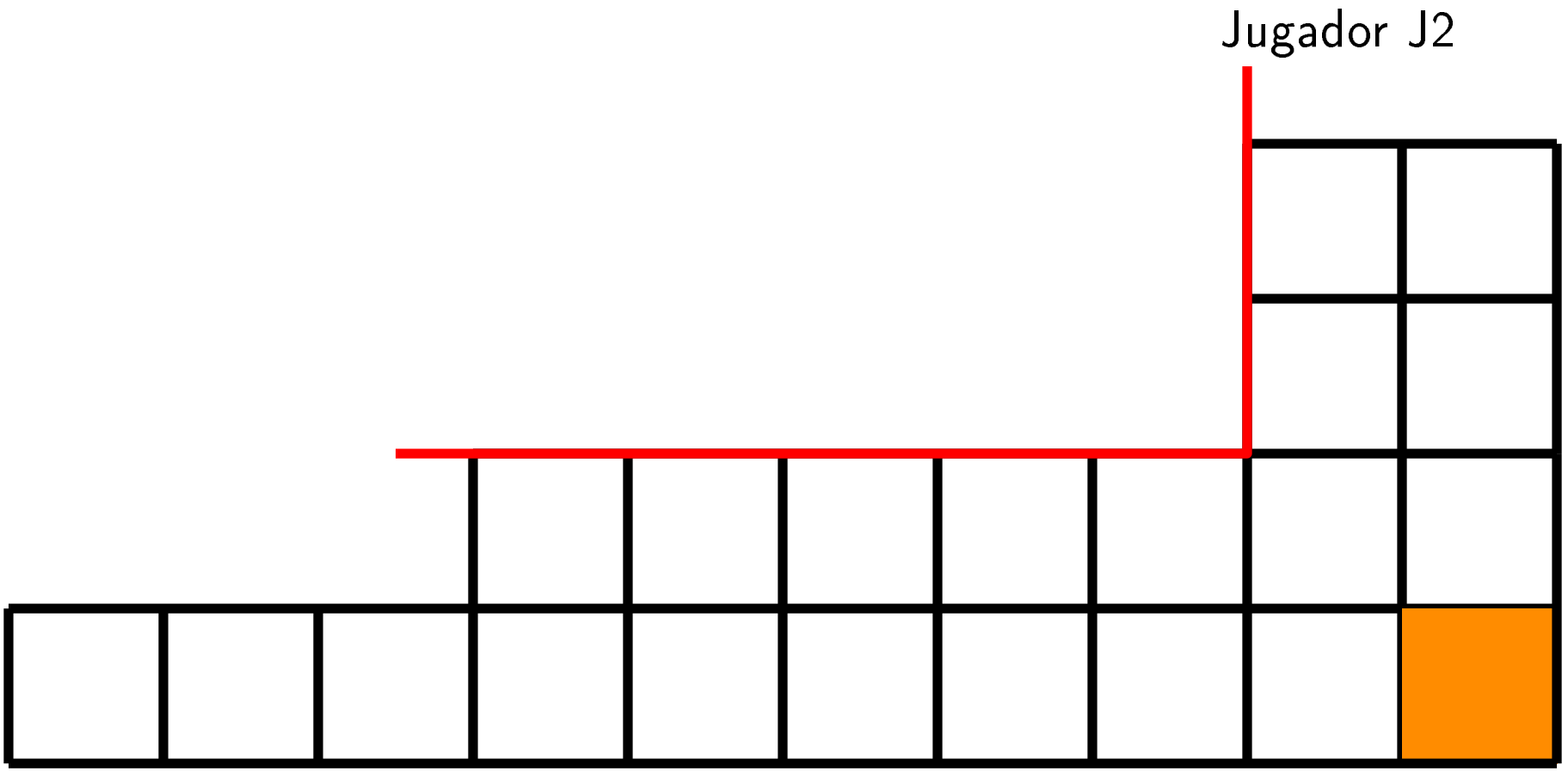
...teoremas no constructivos...



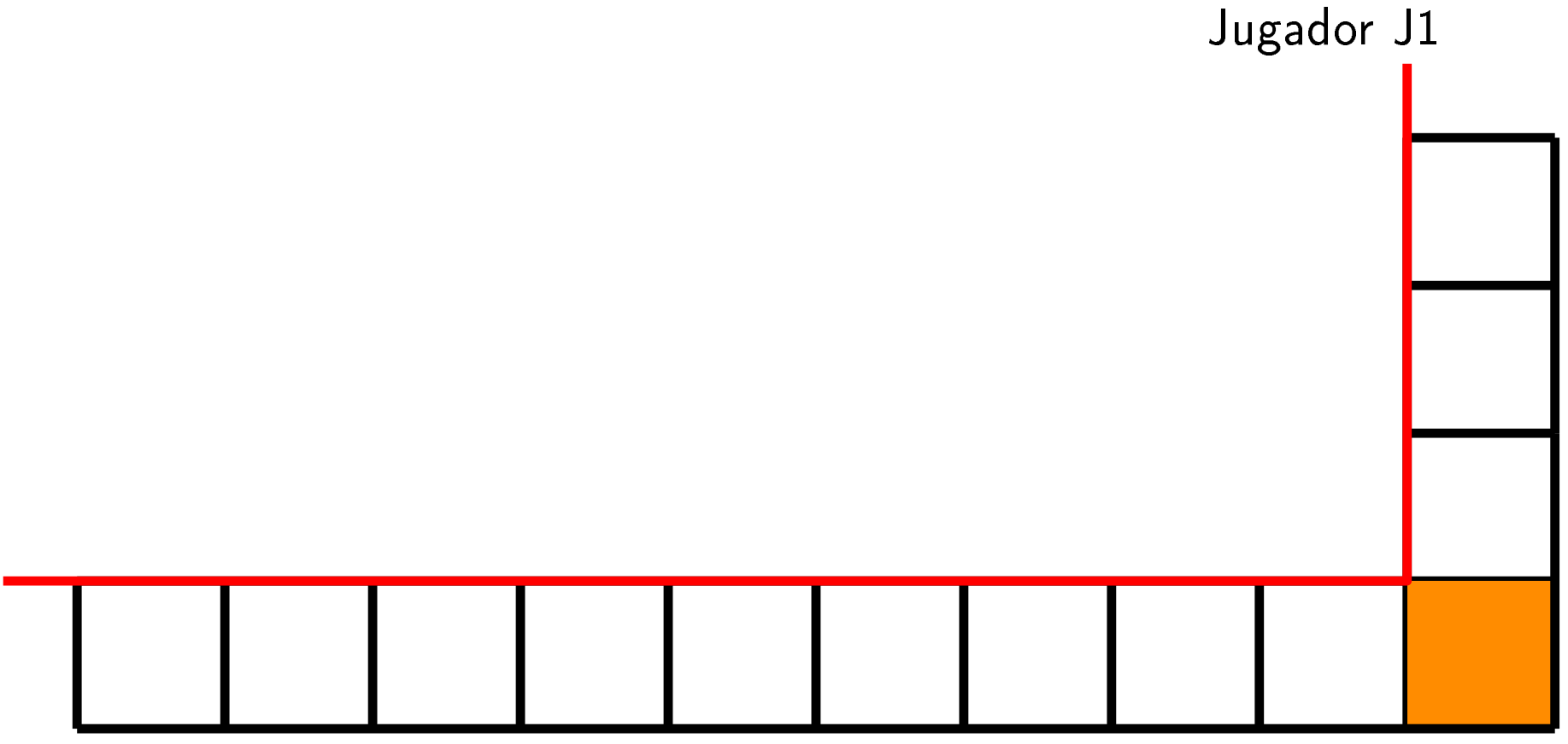
...teoremas no constructivos...



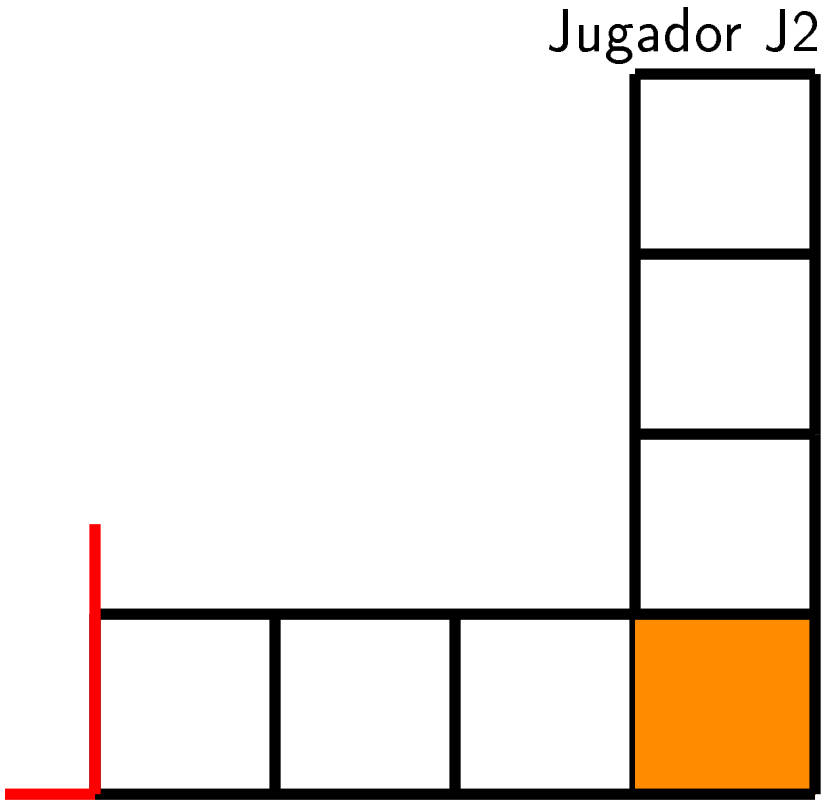
...teoremas no constructivos...



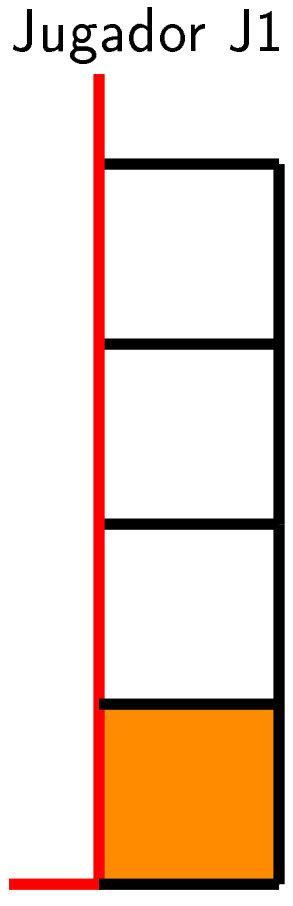
...teoremas no constructivos...



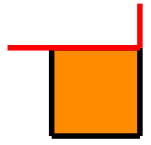
...teoremas no constructivos...

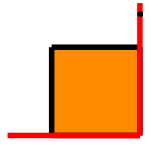


...teoremas no constructivos...



...teoremas no constructivos...

Jugador J2 

Jugador J1 

El jugador J1 **Muere** y el jugador J2 **Sobrevive**.

...teoremas no constructivos...

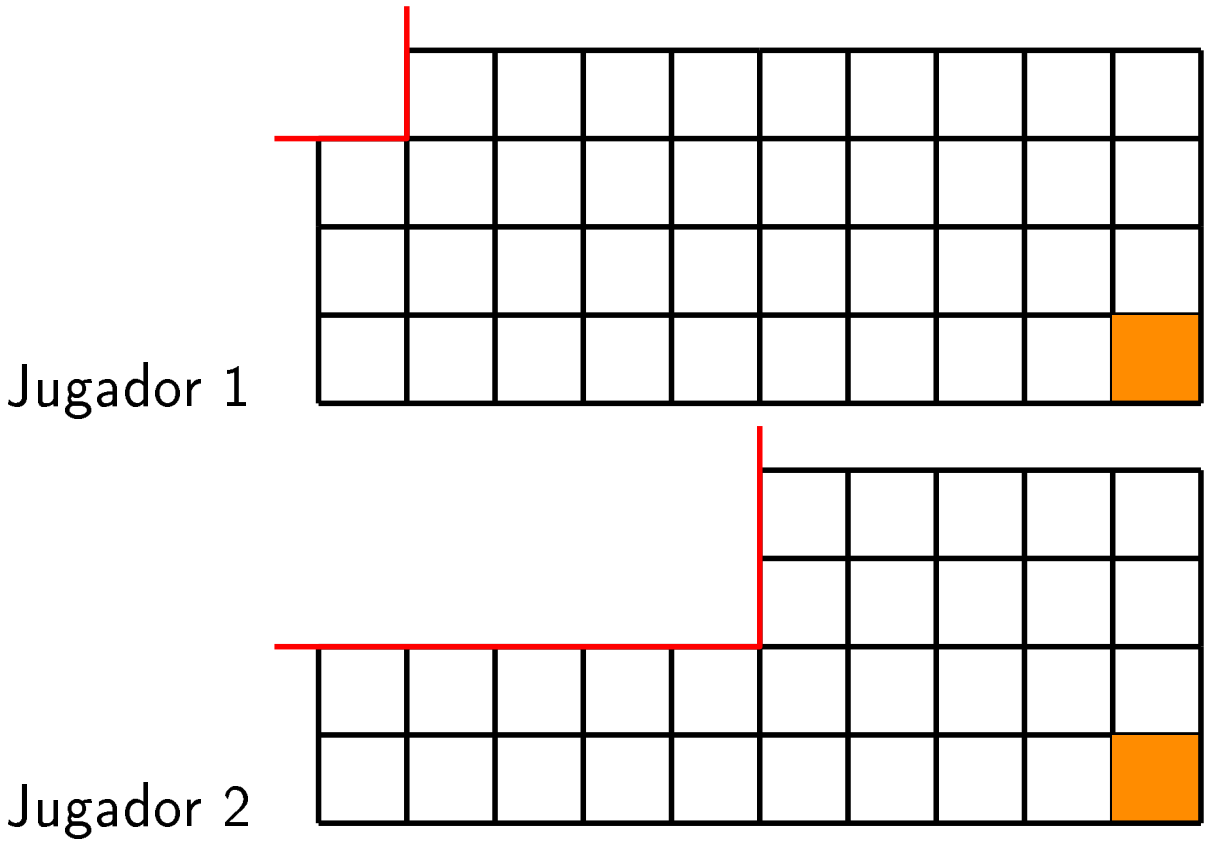
Teorema

El primer jugador tiene una estrategia ganadora para el juego de la tableta de chocolate.

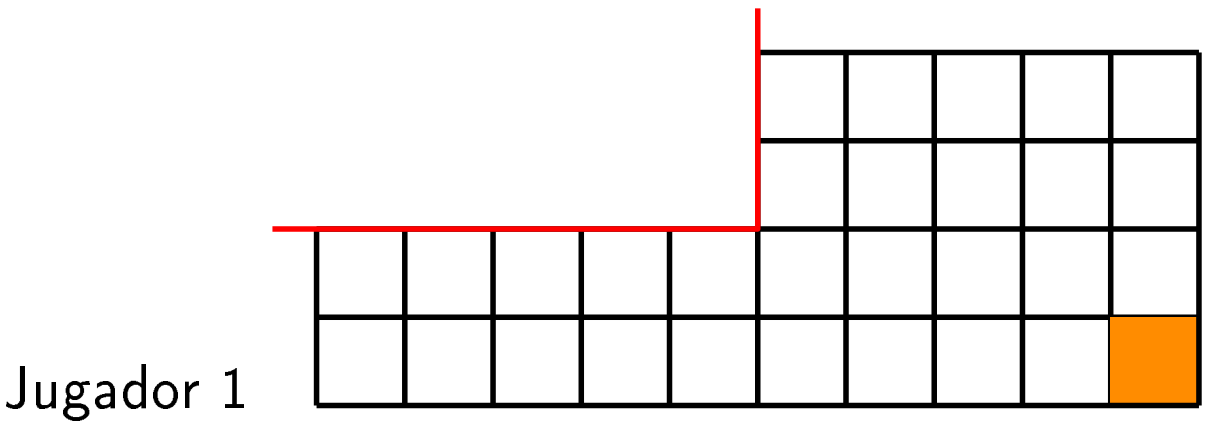
Prueba

El juego es finito $\Rightarrow$ tiene una estrategia ganadora (para alguno de los dos jugadores).
Si el segundo jugador tiene una estrategia ganadora, podemos usarla para definir una para el primer jugador (lo cual es absurdo): El primer jugador come la esquina superior izquierda. El segundo juega y, por la forma como se corta la tableta, el primer jugador podría haber comenzado la partida de modo de emplear la estrategia del oponente.

...teoremas no constructivos...



...teoremas no constructivos...



Haga lo que haga el jugador 2, el jugador 1 continúa con la estrategia ganadora para el jugador 2.

...teoremas no constructivos...

- Para aceptar esta prueba por absurdo, basta con aceptar que $(\neg\forall x \quad \neg P(x)) \Rightarrow (\exists x \quad P(x))$, donde $P(x)$ significa *"La estrategia x es ganadora para el jugador 1"*.
- Pero la prueba no da una estrategia para jugar primero y no morir envenenado.
  La prueba de la existencia de la estrategia para el jugador 1 depende de suponer que existe una estrategia ganadora para el jugador 2, ¡estrategia que estamos probando que no existe!.

Si buscamos que las demostraciones nos den cálculos efectivos, es preciso ser más exigentes para demostrar una disjunción o un cuantificador existencial.

...teoremas no constructivos...

Este juego fue publicado por David Gale (Un. de California, Berkeley).
Gale fue matemático y economista, especialista en la teoría de juegos.

Para convencerse de que en un tablero de 7×4 la estrategia ganadora de J1 no es para nada evidente, uno puede divertirse jugando aquí: ▸ Chomp! (Thomas S. Ferguson's homepage at UCLA's University)
El programa siempre deja el rol de J1 al adversario, así que tenemos estrategia ganadora 😉

un ejemplo *brouweriano*.

- Definimos la fórmula:
  $G(n) := n > 2 \wedge n$ par $\Rightarrow \exists p\ q$ primos $\quad n = p + q$.
  Conjetura de Goldbach: $\forall n \in \mathbb{N} \quad G(n)$.
- definimos la sucesión: $a_n := \begin{cases} 0 \Leftarrow \forall k \leq n & G(k) \\ 1 \Leftarrow \exists k \leq n & \neg G(k) \end{cases}$
- a_n define un real α dado por el desarrollo $0, a_0 a_1 a_2 \ldots$ en base 2.
- Si pudiéramos probar (de forma constructiva) $\alpha = 0 \vee \alpha \neq 0$, tendríamos un proceso de decisión para resolver la conjetura de Goldbach.
- Dada cualquier fórmula $G(x)$ decidir si $\forall x \in \mathbb{N} \quad G(x)$ es equivalente a decidir si el real $(a_n)_{n \in \mathbb{N}}$ asociado es 0 o no.

... un ejemplo *brouweriano*

- Cambiando G por un enunciado indecidible, concluímos:

En análisis constructivo, $\forall x \quad x = 0 \vee x \neq 0$ no es un teorema.
Ídem para la tricotomía $\forall x \quad x < 0 \vee x = 0 \vee x > 0$.

- En $\mathbb{N}, \mathbb{Z}$ y $\mathbb{Q}$, en cambio, $\forall x \quad x = 0 \vee x \neq 0$ y $\forall x \quad x < 0 \vee x = 0 \vee x > 0$ son teoremas.
- Esto se debe a que los números de $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ tienen una cantidad finita de información.
- En cambio, averiguar si un real es 0 implica poder averiguar en tiempo finito si todas sus cifras son cero o no.

Brouwer como matemático clásico.

"Even though his most important research contributions were in topology, Brouwer never gave courses in topology, but always on –and only on– the foundations of his intuitionism. It seemed that he was no longer convinced of his results in topology because they were not correct from the point of view of intuitionism, and he judged everything he had done before, his greatest output, false according to his philosophy. He was a very strange person, crazy in love with his philosophy."

Interview with Bartel Leendert van der Waerden MARCH 1997 NOTICES OF THE AMS 313–Yvonne Dold-Samplonius.

▸ Entrevista en las Notices de la AMS

Semántica de Brouwer/Heyting/Kolmogorov:

- Una prueba de $P \wedge Q$ es un par (a, b) donde a es una prueba de P y b es una prueba de q.
- Una prueba de $P \vee Q$ es un par (a, b) donde o bien $a = 0$ y b es una prueba de P, o bien $a = 1$ y b es una prueba de Q.
- Una prueba de $P \Rightarrow Q$ es un cálculo que transforma pruebas de P en pruebas de Q.
- Una prueba de $\exists x \in D \quad P(x)$ es un par (a, b) donde a es un elemento de D y b es una prueba de que b satisface P.
- Una prueba de $\forall x \in D \quad P(x)$ es un cálculo que transforma todo elemento $d \in D$ en una prueba de que d satisface P.
- $\perp$ no tiene demostraciones.

La fórmula $\neg P$ es una abreviación de $P \Rightarrow \perp$.

Semántica de Brouwer/Heyting/Kolmogorov

¿Cuál es la semántica de la negación de una fórmula?
Son funciones de codominio vacío...

- Si P tiene al menos una prueba, entonces $\neg P \equiv P \Rightarrow \bot$ no tiene pruebas.
- Si P no tiene pruebas, entonces cualquier transformación de pruebas es una prueba de $\neg P \equiv P \Rightarrow \bot$.

Conclusión: $\neg\neg$ destruye información sobre la fórmula:

Si A admite una prueba, entonces $A \Rightarrow \bot$ no tiene pruebas y entonces cualquier transformación de pruebas es una prueba de $\neg\neg A = (A \Rightarrow \bot) \Rightarrow \bot$ (funciones de $\emptyset \to \emptyset$).
Si A es probable, $\neg\neg A$ es trivialmente probable.

Semántica de Brouwer/Heyting/Kolmogorov

$\neg\neg$ destruye información sobre la fórmula:

- Construir una prueba de $\neg\neg A$ a partir de una de A es directo: $f(a) := \mathrm{id}$ lo hace. Podemos probar *uniformemente* $A \Rightarrow \neg\neg A$.
- En cambio, una prueba de $\neg\neg A$ no tiene información sobre A, de modo que no es posible probar $\neg\neg A \Rightarrow A$ sin conocer una prueba de A.

¿Cuál es la semántica de la disjunción $\vee$ y del existencial?

- A partir de una prueba de $A \vee B$ es posible computar una prueba de una de las dos fórmulas A o B. Entonces: probar $A \vee B$ equivale a probar A o probar B. ¿Existe una prueba uniforme de $A \vee \neg A$?
- El existencial es como una disjunción infinita: probar $\exists x{\in}D \quad P(x)$ equivale a poder probar alguna de las instancias de $(P(x))_{x\in D}$.

¿Qué es un cálculo?

Es una noción a priori intuitiva que fué formalizada a posteriori. Diversas nociones teóricas dan lugar a diferentes teorías matemáticas que definen la misma clase de funciones calculables:

- Funciones recursivas: clase de funciones naturales parciales (1923 Skolem, 1931 Gödel).
- Cálculo λ. Funciones λ-calculables (1930, Church). Es la base de la programación funcional (LISP, Haskell, Caml, ...).
- Máquinas de Turing (1936, Turing). Una máquina universal, pero teórica (y sus variantes: registros, Post, ábacos, ...). Base teórica de la arquitectura de Von Neumann.
- Lógica combinatoria (1942, Fitch). Presentación algebraica del cálculo lambda. Se evita el problema de la substitución sintáctica.

Lógica intuicionista (LJ)

- Heyting, alumno de Brouwer, formaliza la noción de prueba intuicionista (LJ). Esto va en contra del paradigma intuicionista de Brouwer.
- Formalmente LJ $\subseteq$ LK.
- Publicación: Heyting, A. (1930) Die formalen Regeln der intuitionistischen Logik. (German) 3 parts, In: Sitzungsberichte der preußischen Akademie der Wissenschaften. phys.-math. Klasse, 1930, 42-65, 57-71, 158-169.

Lógica intuicionista en deducción natural (NJ)

$$\frac{}{\Gamma \vdash A}\ A \in \Gamma$$

Intro	Elim
$\dfrac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}$	$\dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \qquad \dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$
$\dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \qquad \dfrac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$	$\dfrac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}$
$\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}$	$\dfrac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B}$
$\dfrac{}{\Gamma \vdash \top}$	$\dfrac{\Gamma \vdash \bot}{\Gamma \vdash A}$

...lógica intuicionista (NJ)...

Intro	Elim
$\dfrac{\Gamma \vdash A}{\Gamma \vdash \forall x\ A}\ x \notin \mathsf{free}(\Gamma)$	$\dfrac{\Gamma \vdash \forall x\ A}{\Gamma \vdash A\{x := t\}}$
$\dfrac{\Gamma \vdash A\{x := t\}}{\Gamma \vdash \exists x\ A}$	$\dfrac{\Gamma \vdash \exists x\ A, \quad \Gamma, A \vdash B}{\Gamma \vdash B}\ x \notin \mathsf{free}(\Gamma, B)$

Observación:

Intuitivamente, estas reglas son correctas con la semántica BHK.

...lógica intuicionista (NJ).

$$\begin{array}{rcrcr} A & \Rightarrow & \neg\neg A & \not\Rightarrow & A \\ (A \Rightarrow B) & \Rightarrow & \neg B \Rightarrow \neg A & \not\Rightarrow & (A \Rightarrow B) \\ (\neg A \vee B) & \Rightarrow & (A \Rightarrow B) & \not\Rightarrow & (\neg A \vee B) \\ (\neg A \vee \neg B) & \Rightarrow & \neg(A \wedge B) & \not\Rightarrow & (\neg A \vee \neg B) \\ \exists x \quad \neg A(x) & \Rightarrow & \neg(\forall x \quad A(x)) & \not\Rightarrow & \exists x \quad \neg A(x) \end{array}$$

$$\begin{array}{rcr} \neg A & \Leftrightarrow & \neg\neg\neg A \\ \neg(A \vee B) & \Leftrightarrow & \neg A \wedge \neg B \\ \neg(\exists x \quad A(x)) & \Leftrightarrow & \forall x \quad \neg A(x) \end{array}$$

Lógica clásica (LK)

Se obtiene cambiando la regla $\dfrac{\Gamma \vdash \bot}{\Gamma \vdash A}$ por la regla $\dfrac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}$.

Realizabilidad de Kleene

- $0 \Vdash t = u$ si y sólo si $t = u$ (verificable por métodos finitistas).
- $n \Vdash A \wedge B$ si y sólo si n codifica un par (p, q) tal que $p \Vdash A$ y $q \Vdash B$.
- $n \Vdash A \vee B$ si y sólo si n codifica un par (p, q) tal que $p = 0$ y $q \Vdash A$ o $p = 1$ y $q \Vdash B$.
- $n \Vdash \forall x \quad A(x)$ si y sólo si n es el código de Gödel de una función recursiva (total) $f : \mathbb{N} \to \mathbb{N}$ tal que para todo $m \in \mathbb{N}$, $f(n) = p$ y $p \Vdash A(m)$.
- $n \Vdash \exists x \quad A(x)$ si y sólo si n codifica un par (p, q) tal que $q \Vdash A(p)$.
- $n \Vdash A \Rightarrow B$ si y sólo si n es el código de Gödel de una función recursiva (parcial) $f : \mathbb{N} \to \mathbb{N}$ tal que para todo m, si $m \Vdash A$, entonces $f(m) \downarrow p$ y $p \Vdash B$.
- $\bot$ no tiene realizadores.

Realizabilidad de Kleene

Teorema (Kleene)

Si $HA \vdash A$ entonces A es realizable.

Demostración:

Cada prueba construye un realizador. Para eso es necesario probar la adecuación de la semántica respecto al sistema (NJ).

¿Qué es la adecuación? Es afirmar que el sistema formal (NJ) prueba secuentes que *son verdaderos* en la semántica.
¿Qué significa que un secuente sea verdadero para la realizabilidad? Un secuente $G_1, \ldots, G_k \vdash A$ es verdadero si existe una función recursiva $f : \mathbb{N}^k \to \mathbb{N}$ tal que:

- Para cualquier instanciación de las variables libres del secuente.
- Para cualquier k-upla $g_1, \ldots, g_k$ de realizadores de $G_1, \ldots, G_k$.

$f(\vec{g})$ converge a un realizador de A.

Realizabilidad de Kleene

¿Cómo probar la adecuación de (NJ) respecto a la realizabilidad? Probando que a partir de premisas verdaderas, las reglas producen conclusiones verdaderas.

Ejemplo: adecuación de $\vee$-elim

Supongamos que $\Gamma \vdash A \vee B$; $\Gamma, A \vdash C$ y $\Gamma, B \vdash C$ son verdaderos. Estos secuentes tienen asociadas funciones recursivas u, v, w respectivamente. Queremos probar que $\Gamma \vdash C$ es verdadero.
Objetivo: construir una función recursiva que lleve realizadores de Γ en realizadores de C. Consideremos $\vec{g} \Vdash \Gamma$

- Computamos $u(\vec{g}) = \ulcorner (m, n) \urcorner \Vdash A \vee B$.
- Computamos la proyección $p_1(\ulcorner (m, n) \urcorner)$ y obtenemos m.
- Si $m = 0$, entonces $n \Vdash A$ y $v(n) \Vdash C$.
- Si $m = 1$, entonces $n \Vdash B$ y $w(n) \Vdash C$.

Entonces: $\Gamma \vdash C$ es verdadero.

Realizabilidad de Kleene

Corolarios:

- Las ecuaciones de la forma $\forall \vec{x} \quad t(\vec{x}) = u(\vec{x})$ que son verdaderas, son trivialmente realizables por el código $\ulcorner (n \mapsto 0) \urcorner$.
- La fórmula del teorema de Fermat tiene un realizador trivial.

$$\forall xyzn \Big(x \neq 0 \Rightarrow y \neq 0 \Rightarrow n \dot{-} 2 \neq 0 \Rightarrow x^n + y^n \neq z^n \Big)$$

que es el código $\ulcorner (a, b, c \mapsto \ulcorner \mathrm{id} \urcorner) \urcorner$.

- $\forall x(P(x) \vee \neg P(x))$ es realizable si y sólo si P es decidible.

Aritmética de Heyting

Hay varias presentaciones posibles. Presentamos una versión minimal basada en el sucesor y el principio de inducción. El lenguaje en el que se escriben es el primer orden con una constante 0 y una función s de aridad 1.

- $\forall x \quad \mathsf{s}(x) \neq 0$.
- $\forall x, y \quad \mathsf{s}(x) = \mathsf{s}(y) \Rightarrow x = y$.
- Para toda fórmula de primer orden $A(x)$ tenemos $\forall x(A(x) \Rightarrow A(\mathsf{s}\, x)) \Rightarrow A(0) \Rightarrow \forall x A(x)$.

Las siguientes ecuaciones definen recursivamente la suma y el producto en la aritmética de Heyting:

- $\forall x \quad x + 0 = x$.
- $\forall x, y \quad x + \mathsf{s}(y) = \mathsf{s}(x + y)$.
- $\forall x \quad x \times 0 = 0$.
- $\forall x, y \quad x \times \mathsf{s}(y) = (x \times y) + x$.

Aritmética de Heyting

Los axiomas de la aritmética son realizables *à la Kleene*:

- $\ulcorner x \mapsto \mathrm{id} \urcorner \Vdash \forall x \quad \mathsf{s}(x) = 0 \Rightarrow \bot$.
- $\ulcorner x, y \mapsto \mathrm{id} \urcorner \Vdash \forall x, y \quad \mathsf{s}(x) = \mathsf{s}(y) \Rightarrow x = y$.
- $\ulcorner \mathrm{Rec} \urcorner \Vdash \forall x(A(x) \Rightarrow A(\mathsf{s}\, x)) \Rightarrow A(0) \Rightarrow \forall x A(x)$.
- Las ecuaciones que definen $+$ y $\times$ se realizan con códigos de funciones constantes iguales a 0.

¿Qué es Rec? Es un iterador: $\mathrm{Rec}(p, o, n)$ computa $\underbrace{\{p\} \ldots \{p\}}_{n-\text{ veces}} o$.

En la teoría de las funciones recursivas se prueba que $\{p\}(m) = \mathrm{eval}(p, m)$ es una función recursiva en p y m (es el sentido de tener una *máquina universal*).

Realizabilidad de Kleene (adecuación de (HA))

Retomando el teorema de adecuación:

Puesto que los axiomas de (HA) son realizables y las reglas de inferencia de (NJ) son realizables, tenemos la adecuación de (HA).

Corolarios:

- Todo realizador de $\forall x_1, x_2 \exists y \quad x_1 + x_2 = y$ computa la suma y toda función recursiva que computa la suma realiza esta fórmula: Decimos que la fórmula $\forall x_1, x_2 \exists y \quad x_1 + x_2 = y$ *especifica el comportamiento de los programas que computan la suma*. Lo mismo vale para cualquier función recursiva en lugar de $+$.

Realizabilidad de Kleene (adecuación de (HA))

Corolarios:

- Si $HA \vdash \forall \vec{x} \exists y \quad A(\vec{x}, y)$, donde $|\vec{x}| = k$ y A es una ecuación de la forma $t = u$; entonces existe una función recursiva $f : \mathbb{N}^k \to \mathbb{N}$ tal que para toda k-upla $\vec{n}$ se cumple $A(\vec{n}, f(\vec{n}))$: $f = \{m\}$ es la función codificada por cualquier realizador $m \Vdash \forall \vec{x} \exists y \quad A(\vec{x}, y)$.
- $\forall x(\mathrm{Halt}(x) \vee \neg\, \mathrm{Halt}(x))$ no es realizable y entonces $HA \nvdash \forall x(\mathrm{Halt}(x) \vee \neg\, \mathrm{Halt}(x))$.
- $\neg\forall x(\mathrm{Halt}(x) \vee \neg\, \mathrm{Halt}(x))$ es realizable (por cualquier natural). Sin embargo, $HA \nvdash \neg\forall x(\mathrm{Halt}(x) \vee \neg\, \mathrm{Halt}(x))$ puesto que $PA \vdash \forall x \quad (H(x) \vee \neg H(x))$.

Realizabilidad y consistencia relativa:

- La noción de modelo fue sistematizada por el matemático polaco Alfred Tarski a partir de los años 30's, si bien existen antecedentes previos de trabajos que usan estas ideas (Lövenheim, Skolem).
- La idea general es separar la noción de verdad de la noción de demostración.
- Para eso hay que formalizar el lenguaje en el que se escribe una teoría y dar una noción de verdad relativa a una estructura. Un modelo de una teoría es una estructura matemática en la que se pueden interpretar todos los símbolos del lenguaje y la cual satisface todos los axiomas de la teoría. Esta noción de satisfacción es metateórica e informal aunque es formalizable:
  a. Formalizando la metateoría en alguna teoría de conjuntos.
  b. Definiendo en la teoría una noción de modelo interno.

Realizabilidad y consistencia relativa:

- Implícitamente la verdad en un modelo es completa: toda afirmación es verdadera o bien su negación es verdadera.
- La noción de demostración vive en el lenguaje: una prueba es un objeto sintáctico. Las nociones de verdad y demostrabilidad están relacionadas: Si una afirmación es demostrable, es cierta en todos los modelos (adecuación) y si una afirmación es cierta en todos los modelos, entonces es demostrable (Teorema de completitud de Gödel).
- Una consecuencia de la completitud es que todo conjunto consistente de fórmulas admite un modelo. Se trata de un modelo sintánctico definido por el método de agregar constantes para tener testigos de todos los existenciales demostrables (testigos de Henkin)[1].

[1] Y entonces tratamos a los objetos del lenguaje como conjuntos... 

Realizabilidad y consistencia relativa:

- Las teorías matemáticas son en general incompletas (Teorema de incompletitud de Gödel), i.e.: **siempre existe una sentencia tal que no se puede probar ni ella ni su negación** (se dice que es *independiente* de la teoría).
- Recíprocamente: si a una teoría consistente se le agrega cualquier sentencia independiente se obtiene una nueva teoría también consistente.
- Si en una teoría $\mathfrak{T}$ una sentencia A es independiente, entonces por completitud existe un modelo de $\mathfrak{T} \cup \{A\}$ y otro de $\mathfrak{T} \cup \{\neg A\}$.
- Recíprocamente si $\mathfrak{T} \cup \{A\}$ admite un modelo, entonces por adecuación la teoría $\mathfrak{T}$ no puede demostrar $\neg A$. Análogamente, si existe un modelo de $\mathfrak{T} \cup \{\neg A\}$ entonces $\mathfrak{T}$ no puede demostrar A.

Realizabilidad y consistencia relativa:

- El teorema de Gödel además establece que no es posible probar la consitencia de una teoría matemática *"suficientemente interesante"* dentro de la propia teoría (lo que refuta parte del programa de Hilbert).
- Entonces, las únicas pruebas de consitencia a las que podemos aspirar son de consitencia relativa: suponiendo que una teoría es consistente se prueba que otra teoría es consistente.
- ¿Dónde vive la realizabilidad de Kleene? Es posible formalizarla en la aritmética de Peano (PA).
- Entonces, si suponemos que (PA) es consistente, la teoría de las fórmulas realizables es también consistente (porque $\perp$ no es realizable).

- El **primer teorema de incompletitud de Gödel** establece que todo sistema formal de **primer orden**, **decidible** y **consistente** cuya teoría **contenga** a la **aritmética** Q **de Robinson** es **incompleto**.
- La artimética de Robinson axiomatiza al sucesor, a la suma y al producto, pero carece del principio de inducción. La clausura universal de los siguientes enunciados son los axiomas de la teoría:
  - $\mathsf{s}\,0 \neq x$.
  - $\mathsf{s}\,x = \mathsf{s}\,y \longrightarrow x = y$.
  - $y = 0 \vee \exists x(\mathsf{s}\,x = y)$.
  - $x + 0 = x$.
  - $x + \mathsf{s}\,y = \mathsf{s}(x + y)$.
  - $x.0 = 0$.
  - $x.(\mathsf{s}(y)) = x.y + x$.

- Si cambiamos el axioma $y = 0 \vee \exists x(\mathrm{s}\, x = y)$ por el esquema de inducción:
  $(IS_A)A(0) \longrightarrow \forall y(A(y) \longrightarrow A(\mathrm{s}\, y)) \longrightarrow \forall x.A(x)$ tenemos la aritmética de Heyting (o Peano si la lógica es clásica).
- En la metateoría podemos hablar de naturales estándar: son aquellos que se escriben como $\underbrace{\mathrm{s} \ldots \mathrm{s}}_{\text{finitos}}\ 0$.
- La aritmética de Robinson permite probar para cada par de naturales m, n que $m + n = n + m$, pero no permite probar $\forall x \forall y(x + y = y + x)$.
- Un modelo no estándar de la aritmética de Robinson consiste en agregar a los naturales estándar un punto ∞ y definir las operaciones $\mathrm{s}\, \infty = \infty$, $n + \infty = \infty$ para todo natural estándar n, $\infty + \infty = \infty$, $0.\infty = \infty.0 = 0$, $n.\infty = \infty$ para $n \neq 0$
- Si bien para todo natural estándar $\mathrm{s}\, n \neq n$, eso no implica que $\forall x.\, \mathrm{s}\, x \neq x$ porque ∞ no lo cumple.

- Intuición: La aritmética de Robinson es un fragmento *muy débil* de la aritmética de Peano.
- Sin embargo: es suficiente para codificar las **demostraciones formales** de una **teoría de primer** orden cuyo **lenguaje** es **decidible**.
- Toda teoría decidible de primer orden y consistente que implique a la aritmética Q es incompleta, esto es: **contiene fórmulas que no se pueden ni probar ni refutar**.
- La fórmula de Gödel expresa en la teoría la afirmación

"Yo soy una fórmula no demostrable"  .

- La aritmética Q permite además expresar la propia consistencia de una teoría T de primer orden cuyo lenguaje es decidible: escribiendo la fórmula

(Con(T))

"Existe n que es el código de una fórmula que no se puede probar en T"

- El **segundo teorema de incompletitud de Gödel** dice que (Con(T)) **no es demostrable en** T si T es una **teoría de primer orden, consistente** y **decidible** que **implica a la aritmética** Q.
- Este resultado echa por tierra con el objetivo del programa de Hilbert de fundar la aritmética en una teoría que pruebe su propia consistencia.
- Nos condena a dar pruebas de consistencia relativa para (casi) cualquier teoría matemática interesante.

Ppio. de Markov (MP)

$$(\forall x \quad A(x) \vee \neg A(x)) \Rightarrow (\neg\forall x \quad \neg A(x)) \Rightarrow \exists x \quad A(x).$$

Teorema

El principio de Markov es realizable.

Bosquejo de la prueba

Conociendo un realizador m de $\forall x \quad A(x) \vee \neg A(x)$ y otro n de $\neg\forall x \ \neg A(x)$ tenemos que hallar un *testigo* p y un realizador q tales que $q \Vdash A(p)$.

- m nos permite hallar un programa de decisión para A.
  Enumeramos los naturales y buscamos el primero que satisfaga A con ayuda del programa de decisión.
  Como $n \Vdash \neg\forall x \quad \neg A(x)$, entonces *"debe"*[a] existir un p tal que el programa de búsqueda pare.

[a] ¡Razonando de manera clásica en la metateoría!

Realizabilidad modificada (Kreisel)...

Teorema

$HA \nvdash$ Principio de Markov

Bosquejo de la prueba...

Tipos: Hay un tipo especial N (números naturales). Los demás se construyen recursivamente mediante las operaciones $\to$ y $,\times$:
$\sigma \to \tau$, $\sigma \times \tau$ son tipos si σ y τ lo son.
Realizadores: Cálculo lambda tipado *"à la Church"*.

- Infinitas variables de cada tipo: x^σ
- Constantes $0 : N$ y $S : N \to N$.
- Para cada tipo σ existe un *recursor primitivo* $\mathrm{Rec}_\sigma : (\sigma \to \sigma) \to \sigma \to N \to \sigma$

...Realizabilidad modificada (Kreisel)...

Teorema

$HA \nvdash$ Principio de Markov

Bosquejo de la prueba...

...Realizadores:

- y se agregan proyecciones para todos los productos: $\pi_1^{\sigma,\tau} : \sigma \times \tau \to \sigma$, $\pi_2^{\sigma,\tau} : \sigma \times \tau \to \tau$ y pares: $\langle \cdot, \cdot \rangle^{\sigma,\tau} : \sigma \to \tau \to \sigma \times \tau$.
- Se agregan las construcciones del λ-cálculo: si $t : \tau$ entonces $\lambda x^{\sigma}.t : \sigma \to \tau$. Si $s : \tau \to \sigma$ y $t : \tau$, entonces $st : \sigma$.

...Realizabilidad modificada (Kreisel)...

...Teorema...

$HA \nvdash$ Principio de Markov.

...Bosquejo de la prueba...

Se ponen reglas de cálculo (reducción), para que los realizadores calculen. Se define el tipado de las fórmulas:

- Las fórmulas atómicas (igualdades, $\bot$, $\top$) tienen tipo N: $\mathrm{Type}(\bot) = \mathrm{Type}(t = u) = \mathrm{Type}(\top) = N$
- $\mathrm{Type}(A \Rightarrow B) = \mathrm{Type}(A) \to \mathrm{Type}(B)$.
- $\mathrm{Type}(A \wedge B) = \mathrm{Type}(A) \times \mathrm{Type}(B)$.
- $\mathrm{Type}(\forall x \quad A(x)) = N \to \mathrm{Type}(A)$.
- $\mathrm{Type}(\exists x \quad A(x)) = N \times \mathrm{Type}(A)$.

...Realizabilidad modificada (Kreisel)...

...Teorema...

$HA \nvdash$ Principio de Markov.

...Bosquejo de la prueba...

Tenemos un sistema de tipos asociado a este cálculo:

$$\frac{}{x_1 : A_1, \ldots, x_k : A_k \vdash x_i : A_i} \qquad \frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x.t : A \Rightarrow B}$$

$$\frac{\Gamma \vdash s : A \Rightarrow B \quad \Gamma \vdash t : A}{\Gamma \vdash st : B} \qquad \frac{}{\vdash \langle \cdot, \cdot \rangle : A \Rightarrow B \Rightarrow A \times B}$$

$$\frac{}{\vdash \pi_1 : A \times B \Rightarrow A :} \qquad \frac{}{\vdash \pi_2 : A \times B \Rightarrow B}$$

...Realizabilidad modificada (Kreisel)...

...Teorema...

$HA \nvdash$ Principio de Markov.

...Bosquejo de la prueba...

Se define la realizabilidad:

- $n \Vdash t = u$ sii $t = u$ (decidible).
- $n \Vdash A \wedge B$ sii $\pi_1 n \Vdash A$ y $\pi_2 n \Vdash B$.
- $n \Vdash A \Rightarrow B$ sii para todo s : Type(A), si $s \Vdash A$ entonces $ns \Vdash B$.
- $n \Vdash \forall x \ \ A$ sii para todo $m : N$ $nm \Vdash A([\![m]\!])$.
- $n \Vdash \exists x \ \ A$ sii $\pi_1 n \Vdash A([\![\pi_2 n]\!])$.

...Realizabilidad modificada (Kreisel)...

...Teorema...

$HA \nvdash$ Principio de Markov.

...Bosquejo de la prueba...

Un secuente $x_1 : A_1, \ldots, x_k : A_k \vdash t : B$ es verdadero si y sólo si para todo $u_1 : \mathrm{Type}(A_1), \ldots, u_k : \mathrm{Type}(A_k)$ tales que $u_1 \Vdash A_1, \ldots, u_k \Vdash A_k$, entonces $t\{x_i := u_i\}_{i=1}^k : \mathrm{Type}(B)$ y $t\{x_i := u_i\}_{i=1}^k \Vdash B$.

Teorema:

Las reglas de tipado son adecuadas.

Teorema:

Los términos tipados son fuertemente normalizables: si $\vdash t : A$ y $t : \mathrm{Type}(A)$, entonces t es fuertemente normalizable.

...Realizabilidad modificada (Kreisel)...

...Teorema...

$HA \nvdash$ Principio de Markov.

...Bosquejo de la prueba...

Si (MP) fuera demostrable, sería realizable. Vamos a resolver el problema de la parada usando un hipotético realizador $t \Vdash$(MP):
Caso particular: $t \Vdash \neg\forall x \overline{T}(n,n,x) \Rightarrow \exists x T(n,n,x)$, donde $T(m,n,x)$ significa *"la máquina de Turing m con entrada n termina luego de x pasos"*. (predicado de Kleene).
$d := \lambda x^{N\to N}.0 : (N \to N) \to N$. Entonces
$u := td : \text{Type}(\exists x.T(n,n,x)) = N \times N$.
El cálculo que definimos para los realizadores es fuertemente normalizable, de modo que u reduce a $\langle p, q\rangle$ (forma normal de los términos de tipo $N \times N$).

...Realizabilidad modificada (Kreisel)...

...Teorema...

$HA \nvdash$ Principio de Markov.

...Bosquejo de la prueba...

- Si $T(n, n, q)$ es verdadero, se deduce que *La máquina de Turing n con entrada n para*.
- Si $T(n, n, q)$ es falso, (Claim): *La máquina de Turing n con entrada n no para*.

Conclusión: Resolvimos el problema de la parada (absurdo).

...Realizabilidad modificada (Kreisel)...

...Teorema...

$HA \nvdash$ Principio de Markov.

...Bosquejo de la prueba...

Probamos el claim:

Si $T(n, n, q)$ es falso y suponemos que la máquina de Turing n con entrada n para, tenemos que:

1. $\overline{T}(n, n, q)$ es verdadera.
2. $\forall x \quad \overline{T}(n, n, x)$ es falsa.

De 2 deducimos que $\neg\forall x \quad \overline{T}(n, n, x)$ es realizada por cualquier término, en particular por d. Por definición de la realizabilidad para $\Rightarrow$, tenemos que $u = td \Vdash \exists x \quad T(n, n, x)$, de donde $T(n, n, q)$ debe ser cierto (absurdo).

...Realizabilidad modificada (Kreisel).

...Teorema

$HA \nvdash$ Principio de Markov.

Nota: ¡Hemos usado extensivamente la reducción al absurdo en la metateoría! Tenemos entonces tres niveles:

- La metateoría: la asumimos clásica para hacer la prueba.
- El cálculo: asumimos que tenemos la teoría clásica de las funciones primitivo-recursivas.
- La teoría: asumimos HA, que es la teoría para la que queremos probar que (MP) no es demostrable.

¿Hay un problema en esto?
¡PA y HA son equiconsistentes!