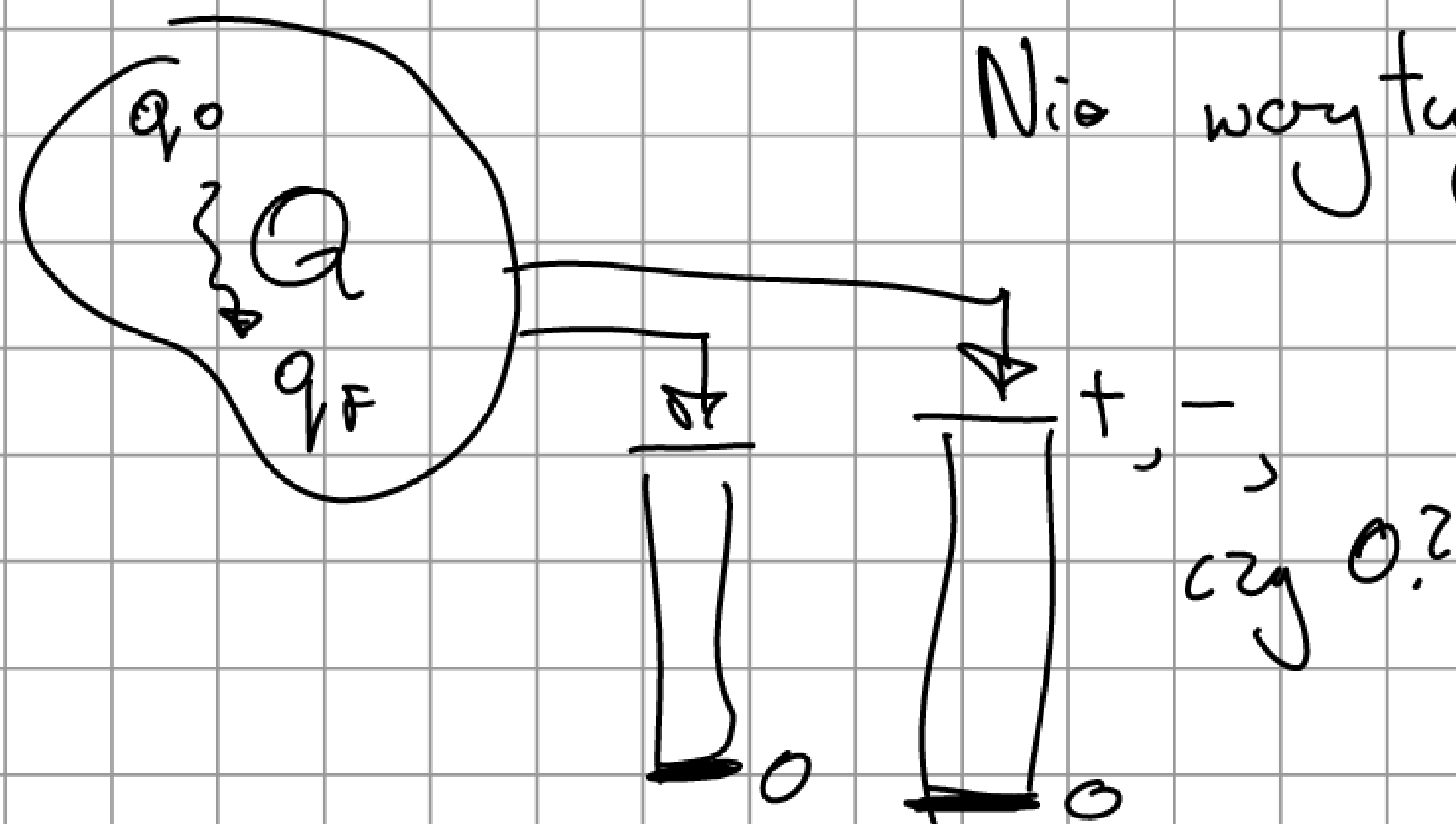
9.05.2022 NIEROZSTRZYGALNOŚĆ ARYTMETYKI

Maszyny Minsky'ego : $\langle Q, q_0, q_F, \delta \rangle$



Nie wczytuje nic – bawi się sam ze sobą.

$$\delta : Q \times \{\text{zero}, \text{nie-zero}\}^2 \longrightarrow Q \times \{+1, 0, -1\}^2$$

TW Problem rozstrzygania czy dana MM zakończy działanie jest nierozstrzygalny. (Problem MM)

- Logika I rzędu w $+, \cdot, \uparrow$

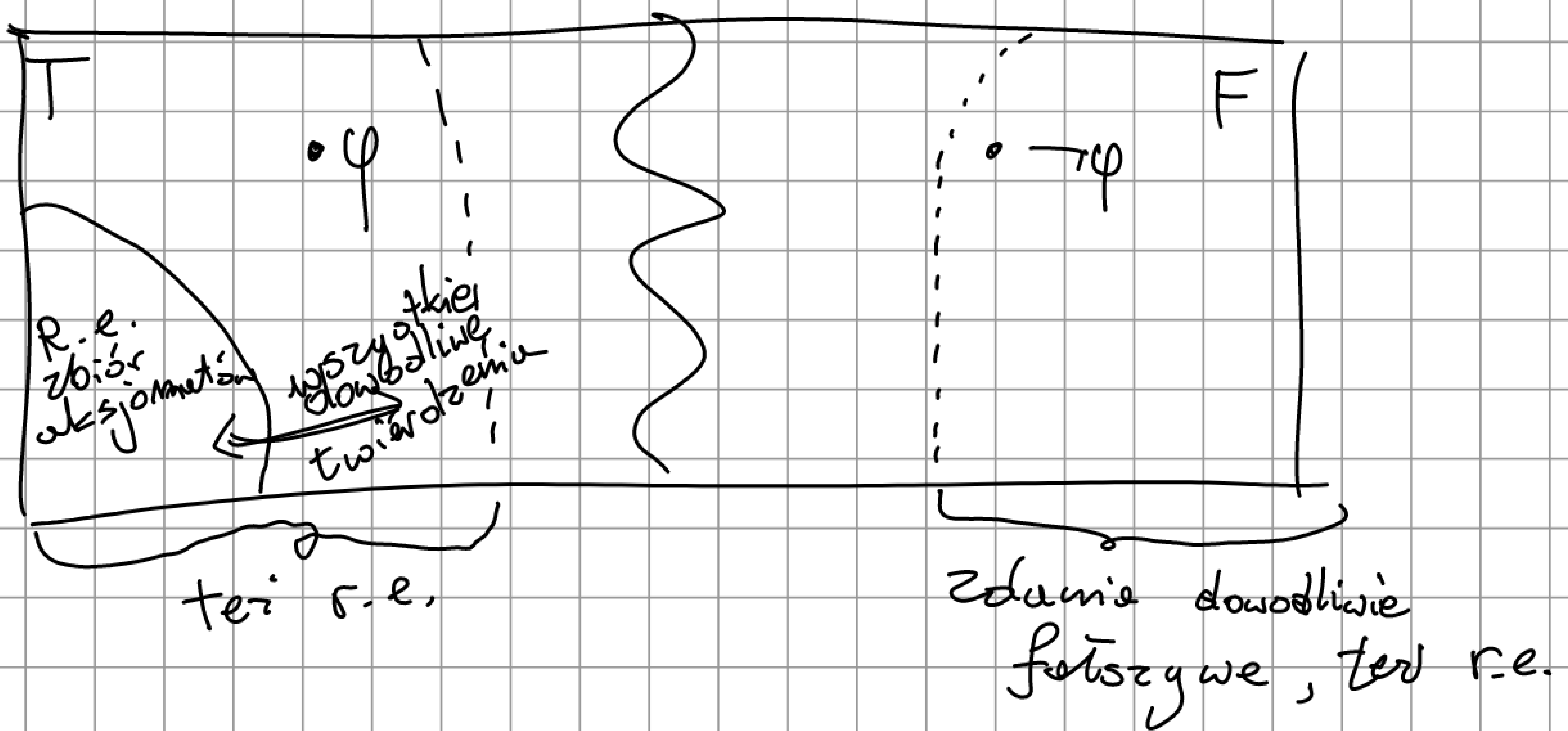
$$\forall n\, \exists m\, \forall k, l\, (m > n \wedge (k \cdot l = m \rightarrow (k = 1 \vee l = 1)))$$

- Aksjomaty arytmetyki Peano $\langle N, +, \cdot \rangle$

Pytanie: czy każde prawdziwe zdanie $Th(N, +, \cdot)$ jest dowodliwe w arytmetyce Peano?

ODP: NIE.

WSZYSTKIE ZDANIA ARYTMETYKI



Gdyby wszystkie zdania arytmetyki dało się udowodnić, to $Th(\mathbb{N}, +, \cdot)$ byłby rozstrzygalny.

<u>Tw.</u> $Th(\mathbb{N}, +, \cdot, \uparrow)$ nie jest rozstrzygalny.

<u>D-d.</u> Pokażemy, że $MM \leq_{rek} Th(\mathbb{N}, \cdot, +, \uparrow)$

Czyli dają nam program M dla MM.

Mamy napisać zdanie Φ_M t. że

$$M \text{ się zatrzymuje} \iff (\mathbb{N}, \cdot, +, \uparrow) \models \Phi_M$$

Potrzebujemy zapamiętać konfigurację M jako trójkę liczb.

Niech $k = |Q|$, $Q = \{q_1, \dots, q_k\}$ gdzie $q_1 = q_0$, $q_2 = q_F$. Konfiguracja C: Maszyna jest w stanie q_i, a na licznikach jest m_1 oraz m_2, będzie oznaczona przez trójkę $t(C) = \langle i, k+1+m_1, k+1+m_2 \rangle$

Def. Fajna szóstka to szóstka liczb $\langle a_1, a_2, a_3, a_4, a_5, a_6 \rangle$ która:

- $a_1 > k$ lub
- $a_1 \leq k$; $a_2, a_3 > k$; $a_4 \leq k$; $a_5, a_6 > k$ oraz istnieją konfiguracje C oraz C' maszyny M t.że C' wynika z C w jednym kroku obliczenia M oraz że $t(C) = \langle a_1, a_2, a_3 \rangle$ i $t(C') = \langle a_4, a_5, a_6 \rangle$

Def Ciąg $a_1, \ldots, a_N$ jest ~~fajny~~ gdy

- $\langle a_1, a_2, a_3 \rangle = t(C_0)$, początkowa konfiguracja M
- $\langle a_{n-2}, a_{n-1}, a_n \rangle = t(C_F)$, końcowa konfiguracja M
- $\langle a_l, a_{l+1}, \ldots, a_{l+5} \rangle$ jest fajną szóstką dla $1 \leq l \leq N-5$

Obserwacja Istnieje formuła arytmetyki ψ z 6 zm. wolnymi taka, że

$(\mathbb{N}, +, \cdot, \uparrow) \models \psi(x_1, \ldots, x_6)$ w.t.w. gdy $x_1, \ldots, x_6$ są fajne.

$\psi(x_1, \ldots, x_6)$: $x_1 > k \ \vee$

sprawdza czy x_2 jest w stanie opisanym przez j

$$\bigwedge_{\substack{i \in \{1 \ldots k\} \\ j, j' \in \{0,1\}}} \Big[\big(x_1 = i \wedge \chi(x_2, j) \wedge \chi(x_3, j)\big) \rightarrow$$

$$x_4 = \Pi_1(\delta(q_i, j, j')) \wedge x_5 = x_2 + \Pi_2(\delta(q_i, j, j'))$$

$$\wedge\ x_6 = x_3 + \Pi_3(\delta(q_i, j, j')) \Big]$$

gdzie te Π_1, Π_2, Π_3 działają jak trzeba

Teraz chcemy formułę, która sprawdza czy ciąg jest fajny. Musimy kodować ciągi jako liczby: $a_1, \dots, a_N \longrightarrow 2^{a_1} 3^{a_2} \dots p_N^{a_N}$

"Makra":

- pierwsza(x): $\forall y,z \ (yz = x \rightarrow y=1 \vee z=1) \wedge x>1$
- kolejne_pierwsze(x,y): $\forall z \ (x<z<y \rightarrow \neg$pierwsza$(z))$ $\wedge$ pierwsza$(x) \wedge$ pierwsza$(y) \wedge x<y$
- w_rozkładzie(x,y,z):

  $\exists m \ x^y m = z \wedge \forall m \ x^{y+1} m \neq z \wedge$ pierwsza(x)
- największa_pierwsza(x,y):

  $\exists s \forall z,t$ pierwsza$(x) \wedge sx=y \wedge ($pierwsza$(z) \wedge z>x \rightarrow zt \neq y)$

Φ_M: $\exists m \ \forall x,x',y,y' ($kolejne_pierwsze$(x,x')$ $\wedge$ w_rozkladzie$(x,y,m) \wedge y'>0$ $\wedge$ w_rozkladzie$(x',y',m) \longrightarrow y>0)$

$\land$ w_rozkładzie$(2, 1, m)$ $\land$ w_rozkładzie$(3, k+1, m)$

$\land$ w_rozkładzie$(5, k+1, m)$

$\land \forall_{p, p', p''} \big($ najw_pierwsza(p'', m) $\land$ kolejne_pierwsze(p, p')

$\land$ kolejne_pierwsze(p', p'') $\rightarrow$ w_rozkładzie$(p, 2, m)$

$\land$ w_rozkładzie$(p', k+1, m)$ $\land$ w_rozkładzie$(p'', k+1, m)\big)$

$$\land \forall_{\substack{x_1, x_2, \dots, x_6, x \\ y_1, \dots, y_6}} \Big[\bigwedge_{i=1}^{5} \text{kolejne\_pierwsze}(x_i, x_{i+1}) \land \text{najw\_pierwsza}(x, m)$$

$$\land\ x_6 \leq x \land \bigwedge_{i=1}^{6} \text{w\_rozkładzie}(x_i, y_i, m) \rightarrow \varphi(y_1, \dots, y_6) \Big]$$

$\blacksquare$

X PROBLEM HILBERTA

Czy jest algorytm rozwiązujący układ równań diofantycznych?

ODP: Nie, to jest nierozstrzygalne (trudne)