$bit := \{0, 1\}$

$b_1 \dots b_n \in bit^n$

$b_1 \dots b_n = (1 b_n \dots b_1)_2 = 2^n + b_n 2^{n-1} + \dots + b_1$

Relazioni diofantee sulle sequenze

1. $\sigma = \underbrace{0 \dots 0}_{n}$ $\qquad \sigma = 2^n$

2. $n = len(\sigma)$ $\qquad 2^n \le \sigma < 2^{n+1}$

3. $\tau = \sigma_1 \frown \sigma_2$ $\qquad \tau = \sigma_1 + (\sigma_2 - 1)\, 2^{len\, \sigma_1}$

4. $\tau = \sigma << n$ $\qquad \sigma_1 \dots \sigma_m << n = \sigma_n \dots \sigma_{m-n}$

$\tau = \sigma >> n$ $\qquad \sigma_1 \dots \sigma_m >> n = \underbrace{0 \dots 0}_{n} \sigma_1 \dots \sigma_m$

$\sigma << n = \sigma \; div \; 2^n$

$\sigma >> n = \sigma \cdot 2^n$

σ	0	1	1	0	0	
τ	1	0	0	0	0	

Lemma

$dis(\sigma, \tau) \equiv \neg \exists i : \sigma_i = \tau_i = 1$

è diofantea

Dim $dis(\sigma,\tau) \iff \sigma - 2^{\overbrace{\cdots}^{m}}$, $\tau - 2^{\overbrace{\cdots}^{n}}$ non hanno uni incolonnati

$\iff$ sommando m e n in colonna, in binario, non ci sono riporti

1. # riporti nella somma $m+n$ $= v_2 \binom{m+n}{m}$

$\iff \binom{m+n}{m}$ è dispari

2. $x = \binom{y}{z}$ è dispari

$\nu_1(n)$ = n. di 1 nella scrittura binaria di n

(1) $v_2(n!) = n - \#_1(n)$

$v_2(n!) = v_2(1 \cdot 2 \cdot 3 \cdot \ldots \cdot n)$

$= v_2(2 \cdot 4 \cdot 6 \cdot \ldots \cdot 2(n \operatorname{div} 2))$

$= v_2(2^{n \operatorname{div} 2} \cdot 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n \operatorname{div} 2))$

$= (n \operatorname{div} 2) + \underbrace{v_2((n \operatorname{div} 2)!)}$

$(n \operatorname{div} 2) - \#_1(n \operatorname{div} 2)$

$$\nu_2\binom{m+n}{n} = \nu_2((m+n)!) - \nu_2(n!) - \nu_2(m!)$$

$$= m+n - \#_1(m+n) - n + \#_1(n) - m + \#_1(m)$$

$$= \#_1(n) + \#_1(m) - \#_1(m+n)$$

---

(2) $x = \binom{y}{z}$ è dispari.

$$(10001)^2 = 100020001$$

$$(10001)^3 = 1000300030001$$

1 1
1 2 1
1 3 3 1

$$\left((2^y+1)^y \operatorname{div} 2^{yz}\right) \bmod 2^y = \binom{y}{z}$$

∎

Def $f : bit^k \to bit$

$[f] : \mathbb{N}^k \to \mathbb{N}$

seq. seq. con la stessa lungh.

$$\left([f](\sigma_1 \dots \sigma_k)\right)_i = f\left((\sigma_1)_i \dots (\sigma_k)_i\right)$$

	↓	↓	↓				
σ_1	0	1	1	0	0	1	…
⋮	⋮	⋮	⋮				
σ_k	1	0	0	0	1	1	…
	=	=	=				
$[f](\sigma_1 \dots \sigma_k)$	⊓	⊔	⊓				

Lemma Fissata la data $f : bit^k \to bit$ la funzione $[f]$ è discontinua.

Dim

Oss Ogni funzione $bit^k \to bit$ si scrive come composizione di not e and

- $\sigma = [not](\tau)$ $\quad \sigma + \tau = 3 \cdot 2^{lh(\tau)} - 1$

$$\begin{array}{r} 1001 \\ 0110 \\ \hline 1011 \end{array} \qquad \begin{array}{r} 11001 \\ 10110 \\ \hline 10111 \end{array} = 3 \cdot 2^4 - 1$$

- $\sigma = [and](\tau_1, \tau_2)$

$\Updownarrow$

$\exists\, \varepsilon_1\ \varepsilon_2 \quad dis(\sigma, \varepsilon_1) \wedge dis(\sigma, \varepsilon_2) \wedge dis(\varepsilon_1, \varepsilon_2)$

$\wedge\ lca(\sigma) = lca(\tau_1) = \ldots$

$\wedge\ \tau_1 + 2^{lca\ \tau_1} = \varepsilon_1 + \sigma$

$\wedge\ \tau_2 + 2^{lca\ \tau_2} = \varepsilon_2 + \sigma$

τ_1 1 1 1 0 0 0 0

τ_2 0 1 0 1 1 0 0

0 1 0 0 0 0 0

1 0 1 0 0

1 0 0 1 0

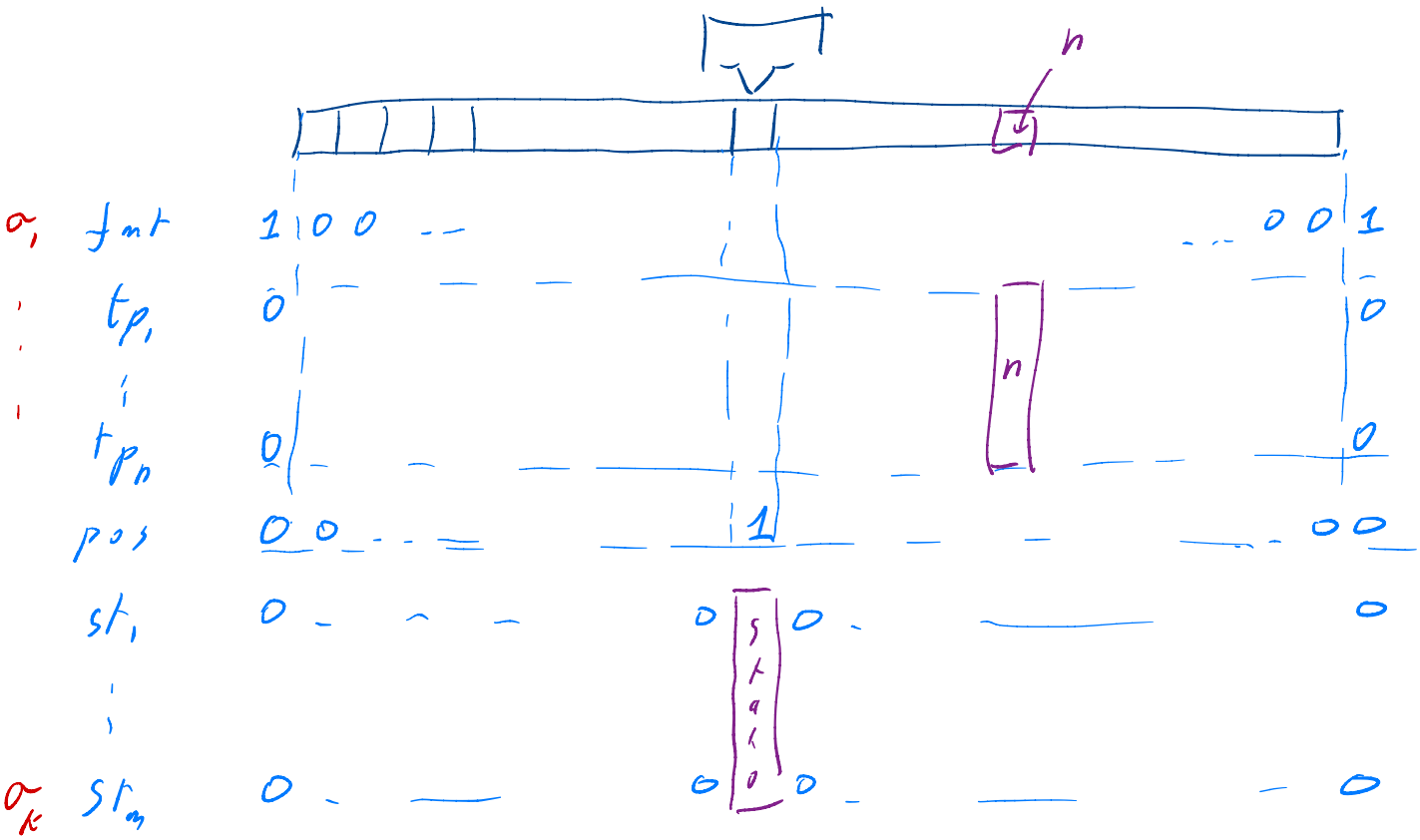
1 0 0 1 1 0

Codifica delle TM

Lavoro con TM su nastri di lung. finita.

Fisso una macchina M con $\leq 2^m$ stati e

$\leq 2^n$ simboli



$step_1(\sigma_1 \dots \sigma_K) = \sigma_1'$

$\vdots$

$step_K(\sigma_1 \dots \sigma_K) = \sigma_K'$

$\overline{step}(\bar{\sigma}) = \bar{\sigma}'$

$(\sigma_1 \dots \sigma_K) \xrightarrow{M} (\sigma_1' \dots \sigma_K')$

Lemma step i disjunction.

$$\left(step_i(\bar{\sigma})\right)_j = f\begin{pmatrix} (\sigma_1)_{j-1} & \cdots & (\sigma_k)_{j-1} \\ (\sigma_1)_j & - & (\sigma_k)_j \\ (\sigma_1)_{j+1} & \cdots & (\sigma_k)_{j+1} \end{pmatrix}$$

$$= f\begin{pmatrix} (\sigma_1 >> 1)_j & \cdots & (\sigma_k >> 1)_j \\ (\sigma_1)_j & - & (\sigma_k)_j \\ (\sigma_1 << 1)_j & \cdots & (\sigma_k << 1)_j \end{pmatrix}$$

$$step_i(\bar{\sigma}) = [f]\begin{pmatrix} (\sigma_1 >> 1) & \cdots & (\sigma_k >> 1) \\ (\sigma_1) & - & (\sigma_k) \\ (\sigma_1 << 1) & \cdots & (\sigma_k << 1) \end{pmatrix}$$

Lem $\bar{\sigma} \xrightarrow{M^*} \bar{\tau}$ è diagonale.

Dim

$$stop(\bar{\sigma}_1 \wedge \bar{\sigma}_2 \wedge \dots \wedge \bar{\sigma}_n) =$$

$$= \overline{stop}(\bar{\sigma}_1) \wedge \overline{stop}(\bar{\sigma}_2) \wedge \dots \wedge \overline{stop}(\bar{\sigma}_n)$$

$\bar{\sigma} \xrightarrow{M^*} \bar{\tau}$

$\Leftrightarrow$

$\exists n \quad \exists \bar{\sigma}_1 \dots \bar{\sigma}_n$ tali che

$$\begin{cases} \overline{stop}(\bar{\sigma}) = \bar{\sigma}_1 \\ \overline{stop}(\bar{\sigma}_i) = \bar{\sigma}_{i+1} \\ \overline{stop}(\bar{\sigma}_n) = \bar{\tau} \end{cases}$$

$\Leftrightarrow$

$\exists n \quad \exists \bar{\sigma}_1 \dots \bar{\sigma}_n \quad \overline{stop}(\bar{\sigma} \wedge \underbrace{\bar{\sigma}_1 \wedge \dots \wedge \bar{\sigma}_n}_{\alpha}) = \underbrace{\bar{\sigma}_1 \wedge \dots \wedge \bar{\sigma}_n}_{\alpha} \wedge \bar{\tau}$

$\Leftrightarrow$

$\exists \alpha \quad \overline{stop}(\bar{\sigma} \wedge \bar{\alpha}) = \bar{\alpha} \wedge \bar{\tau}$

□

Teo Se $X \subseteq \mathbb{N}$ è r.e. allora X è diofanteo.

Dim Fisso una TM M t.c.

M su input $\underbrace{1\,1\,\dots\,1}_{n}$ entra nello stato o se e solo se $n \in X$.

$n \in X \iff \exists m$ $\underbrace{1\,1\,1\,1}_{n}\,0\,\underbrace{\dots}_{m}\,0$ $\xrightarrow{M^*}$ $\underbrace{_\;_\;_\;_\;_}_{p}$

p è diofanteo perché lo stato è o.

n è diof. costruisco questa configurazione iniziale

□