S1S

kuko

14.4.2021

Pokročilá teória zložitosti

S1S

- $\mathrm{Th}(\mathbb{N}, s, \in)$
- $s : n \mapsto n+1$
- číselné premenné $x, y, z, \ldots$
- množinové premenné $X, Y, Z, \ldots$
- môžeme kvantifikovať cez množiny $(\forall X)(\exists Y)$

Základy

- $A \subseteq B$
- $A = B$
- $\exists 0 : \neg \exists z : sz = 0$
- $3 \equiv s(s(s(0)))$
- $x = y?$
- $x < y?$

Základy

- $A \subseteq B$
- $A = B$
- $\exists 0 : \neg \exists z : sz = 0$
- $3 \equiv s(s(s(0)))$
- $x = y$?
- $x < y$?

Základy

- $A \subseteq B$
- $A = B$
- $\exists 0 : \neg \exists z : sz = 0$
- $3 \equiv s(s(s(0)))$
- $x = y?$
- $x < y?$

Základy

- $A \subseteq B$
- $A = B$
- $\exists 0 : \neg \exists z : sz = 0$
- $3 \equiv s(s(s(0)))$
- $x = y?$
- $x < y?$

Základy

- $A \subseteq B$
- $A = B$
- $\exists 0 : \neg \exists z : sz = 0$
- $3 \equiv s(s(s(0)))$
- $x = y$?
- $x < y$?

Základy

$$x = y \iff \neg(\exists S : x \in S \wedge y \notin S) \quad \iff \forall S : x \in S \leftrightarrow y \in S$$

Základy

- nech $V_x = \{y \mid y > x\}$
- potom $y > x \iff y \in V_x$

$$\Big(\underbrace{s(x) \in V_x}_{\text{obsahuje } x+1}$$

$$\wedge \underbrace{\forall n : n \in V_x \to s(n) \in V_x}_{\text{a je uzavretá na nasledovníka}}\Big)$$

$$\wedge\Big(\forall V' : \underbrace{(s(x) \in V' \wedge \forall n : n \in V' \to s(n) \in V')}_{\text{a každá množina, ktorá toto spĺňa}} \to \underbrace{V_x \subseteq V'}_{\text{je jej nadmnožinou}}\Big)$$

$$\forall X : \Big(s(x) \in X \wedge (\forall n : n \in X \to s(n) \in X)\Big) \to y \in X$$

Základy

- nech $V_x = \{y \mid y > x\}$
- potom $y > x \iff y \in V_x$

$$\Big(\underbrace{s(x) \in V_x}_{\text{obsahuje } x+1}$$

$$\wedge \underbrace{\forall n : n \in V_x \rightarrow s(n) \in V_x}_{\text{a je uzavretá na nasledovníka}} \Big)$$

$$\wedge \Big(\forall V' : \underbrace{(s(x) \in V' \wedge \forall n : n \in V' \rightarrow s(n) \in V')}_{\text{a každá množina, ktorá toto spĺňa}} \rightarrow \underbrace{V_x \subseteq V'}_{\text{je jej nadmnožinou}} \Big)$$

$$\forall X : \Big(s(x) \in X \wedge (\forall n : n \in X \rightarrow s(n) \in X) \Big) \rightarrow y \in X$$

Základy

- nech $V_x = \{y \mid y > x\}$
- potom $y > x \iff y \in V_x$

$$\Big(\underbrace{s(x) \in V_x}_{\text{obsahuje } x+1}$$

$$\wedge \underbrace{\forall n : n \in V_x \rightarrow s(n) \in V_x}_{\text{a je uzavretá na nasledovníka}}\Big)$$

$$\wedge \Big(\forall V' : \underbrace{\big(s(x) \in V' \wedge \forall n : n \in V' \rightarrow s(n) \in V'\big)}_{\text{a každá množina, ktorá toto spĺňa}} \rightarrow \underbrace{V_x \subseteq V'}_{\text{je jej nadmnožinou}}\Big)$$

$$\forall X : \Big(s(x) \in X \wedge \big(\forall n : n \in X \rightarrow s(n) \in X\big)\Big) \rightarrow y \in X$$

Základy

- nech $V_x = \{y \mid y > x\}$
- potom $y > x \iff y \in V_x$

$$\Big(\underbrace{s(x) \in V_x}_{\text{obsahuje } x+1}$$

$$\wedge \underbrace{\forall n : n \in V_x \to s(n) \in V_x}_{\text{a je uzavretá na nasledovníka}} \Big)$$

$$\wedge \Big(\forall V' : \underbrace{\big(s(x) \in V' \wedge \forall n : n \in V' \to s(n) \in V'\big)}_{\text{a každá množina, ktorá toto spĺňa}} \to \underbrace{V_x \subseteq V'}_{\text{je jej nadmnožinou}} \Big)$$

$$\forall X : \Big(s(x) \in X \wedge \big(\forall n : n \in X \to s(n) \in X\big) \Big) \to y \in X$$

- X je konečná množina:

$$\exists h : \forall x : x \in X \rightarrow x < h$$

- kódovanie čísel?
- množina $X \longleftrightarrow$ nekonečné slovo $X = x_0 x_1 x_2 \cdots$, kde $x_i = 1 \iff i \in X$

Základy

- X je konečná množina:

$$\exists h : \forall x : x \in X \to x < h$$

- kódovanie čísel?
- množina $X \longleftrightarrow$ nekonečné slovo $X = x_0 x_1 x_2 \cdots$, kde $x_i = 1 \iff i \in X$

Základy

- X je konečná množina:

$$\exists h : \forall x : x \in X \rightarrow x < h$$

- kódovanie čísel?
- množina $X \longleftrightarrow$ nekonečné slovo $X = x_0 x_1 x_2 \cdots$, kde $x_i = 1 \iff i \in X$

S1S je ťažšia ako Presburgerova aritmetika

Sčítanie

- $X \sim n$ – množina X reprezentuje binárny zápis čísla n
- „$X \sim 0$“: $(\forall z)(z \notin X)$
- „$X \sim 1$“: $(\forall z)(z \in X \leftrightarrow z = 0)$
- „$X \sim 11010_2$“: $(\forall z)(z \in X \leftrightarrow (z = 1 \vee z = 3 \vee z = 4))$
- „$X = A + B$“: existuje množina C – prenos do vyššieho rádu
  - 0101101 – A
  - $\underline{0110110}$ – B
  - 111100 – C
  - 1100011 – X
  - $(\exists C)(\forall i)(X_i = A_i \oplus B_i \oplus C_i \wedge C_0 = 0 \wedge C_{i+1} \leftrightarrow A_i + B_i + C_i > 1)$
- „$X \geq Y$“: $(\exists \Delta)(X = Y + \Delta)$

Dôsledok

pomocou množín vieme v S1S reprezentovať $\mathbb{N}$, 0, 1, $+$

$$\Longrightarrow$$

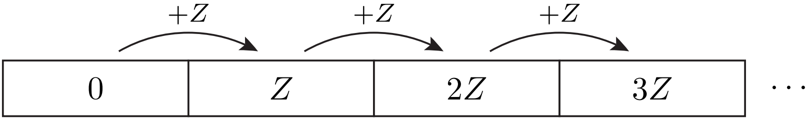
vieme simulovať Pressburgerovu aritmetiku

$$\Longrightarrow$$

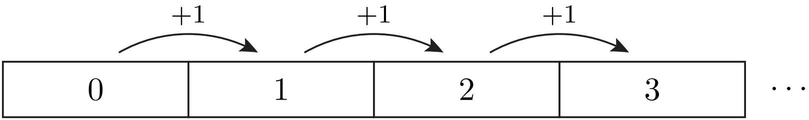
problém rozhodnuteľnosti je aspoň 2NEXP-ťažký

S1S je ešte oveľa zložitejšia

súťaž: zadefinujte v S1S čo najväčšie číslo



- budeme potrebovať $i \equiv j \pmod{n}$ pre veľké n



- „n-bitové počítadlo“ P_n:

  $0, 1, 2, 3, \ldots, 2^n - 1, \quad 0, 1, 2, 3, \ldots, 2^n - 1, \quad 0, 1, 2, 3, \ldots$

mod $n \longrightarrow$ práca s n-bitovými blokmi $\longrightarrow$ n-bitové počítadlo $\longrightarrow$ mod N

(pre $N \gg n$)

$$P_8 = \quad \cdots \quad \underbrace{\boxed{\texttt{11101010}}\boxed{\texttt{00011010}} \quad \cdots \qquad\qquad \cdots}_{\text{vzdialenosť } 2^8 \text{ blokov } \times\ 8 \text{ bitov na blok } = 2048 \text{ (alebo nejaký násobok)}} \boxed{\texttt{11101010}} \quad \cdots$$

- počet *blokov* medzi i a j je násobok $2^8 = 256$
- oba ukazujú 5-ty bit $\pmod 8$
- $\Longrightarrow i \equiv j \pmod{8 \cdot 2^8 = 2048}$

- $i \equiv j \pmod 1$ je TRUE
- $P_1 = 0101010101 \ \cdots$
  - $0 \notin P_1 \wedge \forall i : i \in P_1 \leftrightarrow s(i) \notin P_1$
- $i \equiv j \pmod 2 \iff i \in P_1 \leftrightarrow j \in P_1$
- $P_2 = 00 \ \ 10 \ \ 01 \ \ 11 \ \ 00 \ \ 10 \ \cdots$
  - $0 \notin P_1 \wedge 1 \notin P_1 \wedge \forall i : i \equiv 0 \pmod 2 \rightarrow [(i+2 \in P_2 \leftrightarrow i \notin P_2) \wedge (i+3 \in P_2 \leftrightarrow i \in P_2 \oplus i+1 \in P_2)]$,
  - $i \equiv j \pmod 8$ ak $i \equiv j \pmod 2$ a nech i_0, j_0 je začiatok bloku a $(i_0 \in P_2 \leftrightarrow j_0 \in P_2) \wedge (i_0+1 \in P_2 \leftrightarrow j_0+1 \in P_2)$.

- $i \equiv j \pmod 1$ je TRUE
- $P_1 = 0101010101\ \cdots$
  - $0 \notin P_1 \wedge \forall i : i \in P_1 \leftrightarrow s(i) \notin P_1$
- $i \equiv j \pmod 2 \iff i \in P_1 \leftrightarrow j \in P_1$
- $P_2 = 00\ \ 10\ \ 01\ \ 11\ \ 00\ \ 10\ \ \cdots$
  - $0 \notin P_1 \wedge 1 \notin P_1 \wedge \forall i : i \equiv 0 \pmod 2 \rightarrow [(i+2 \in P_2 \leftrightarrow i \notin P_2) \wedge (i+3 \in P_2 \leftrightarrow i \in P_2 \oplus i+1 \in P_2)]$,
  - $i \equiv j \pmod 8$ ak $i \equiv j \pmod 2$ a nech i_0, j_0 je začiatok bloku a $(i_0 \in P_2 \leftrightarrow j_0 \in P_2) \wedge (i_0 + 1 \in P_2 \leftrightarrow j_0 + 1 \in P_2)$.

- $i \equiv j \pmod 1$ je $\textsc{True}$
- $P_1 = 0101010101 \ \cdots$
  - $0 \notin P_1 \wedge \forall i : i \in P_1 \leftrightarrow s(i) \notin P_1$
- $i \equiv j \pmod 2 \iff i \in P_1 \leftrightarrow j \in P_1$
- $P_2 = 00 \ \ 10 \ \ 01 \ \ 11 \ \ 00 \ \ 10 \ \ \cdots$
  - $0 \notin P_1 \wedge 1 \notin P_1 \wedge \forall i : i \equiv 0 \pmod 2 \rightarrow [(i+2 \in P_2 \leftrightarrow i \notin P_2) \wedge (i+3 \in P_2 \leftrightarrow i \in P_2 \oplus i+1 \in P_2)],$
  - $i \equiv j \pmod 8$ ak $i \equiv j \pmod 2$ a nech i_0, j_0 je začiatok bloku a $(i_0 \in P_2 \leftrightarrow j_0 \in P_2) \wedge (i_0 + 1 \in P_2 \leftrightarrow j_0 + 1 \in P_2)$.

- $i \equiv j \pmod 1$ je $\textsc{True}$
- $P_1 = 0101010101\ \cdots$
  - $0 \notin P_1 \wedge \forall i : i \in P_1 \leftrightarrow s(i) \notin P_1$
- $i \equiv j \pmod 2 \iff i \in P_1 \leftrightarrow j \in P_1$
- $P_2 = 00\ \ 10\ \ 01\ \ 11\ \ 00\ \ 10\ \ \cdots$
  - $0 \notin P_1 \wedge 1 \notin P_1 \wedge \forall i : i \equiv 0 \pmod 2 \rightarrow [(i+2 \in P_2 \leftrightarrow i \notin P_2) \wedge (i+3 \in P_2 \leftrightarrow i \in P_2 \oplus i+1 \in P_2)]$,
  - $i \equiv j \pmod 8$ ak $i \equiv j \pmod 2$ a nech i_0, j_0 je začiatok bloku a $(i_0 \in P_2 \leftrightarrow j_0 \in P_2) \wedge (i_0 + 1 \in P_2 \leftrightarrow j_0 + 1 \in P_2)$.

- $i \equiv j \pmod 1$ je $\textsc{True}$
- $P_1 = 0101010101\ \cdots$
  - $0 \notin P_1 \wedge \forall i : i \in P_1 \leftrightarrow s(i) \notin P_1$
- $i \equiv j \pmod 2 \iff i \in P_1 \leftrightarrow j \in P_1$
- $P_2 = 00\ \ 10\ \ 01\ \ 11\ \ 00\ \ 10\ \ \cdots$
  - $0 \notin P_1 \wedge 1 \notin P_1 \wedge \forall i : i \equiv 0 \pmod 2 \rightarrow [(i+2 \in P_2 \leftrightarrow i \notin P_2) \wedge (i+3 \in P_2 \leftrightarrow i \in P_2 \oplus i+1 \in P_2)]$,
  - $i \equiv j \pmod 8$ ak $i \equiv j \pmod 2$ a nech i_0, j_0 je začiatok bloku a $(i_0 \in P_2 \leftrightarrow j_0 \in P_2) \wedge (i_0 + 1 \in P_2 \leftrightarrow j_0 + 1 \in P_2)$.

- majme
    - $i \equiv j \pmod{n}$
    - P_n
- ukážme, ako definovať
    - $i \equiv j \pmod{N}$
    - P_N
    - pre $N = n \cdot 2^n$

- zb(i) – začiatok bloku i:

$$z = \mathrm{zb}(i) \iff z \leq i \land z \equiv 0 \pmod{n} \land \forall j : z < j < i : j \not\equiv 0 \pmod{n}.$$

- i, j ukazujú na ten istý blok $\iff \mathrm{zb}(i) = \mathrm{zb}(j)$
- „pre všetky indexy z jedného bloku platí …“
- „$A[x] = B[y]$“ („blok, kam ukazuje x v A, je rovnaký ako blok, kam ukazuje y v B“):

$$\forall i, j : i \equiv j \pmod{n} \land \mathrm{zb}(i) = \mathrm{zb}(x) \land \mathrm{zb}(j) = \mathrm{zb}(y) \to (i \in A \leftrightarrow j \in B)$$

- $x \equiv y \pmod{N}$:

$$x \equiv y \pmod{n} \land P_n[x] = P_n[y].$$

- $\mathrm{zb}(i)$ – začiatok bloku i:

$$z = \mathrm{zb}(i) \iff z \leq i \wedge z \equiv 0 \pmod{n} \wedge \forall j : z < j < i : j \not\equiv 0 \pmod{n}.$$

- i, j ukazujú na ten istý blok $\iff \mathrm{zb}(i) = \mathrm{zb}(j)$
- „pre všetky indexy z jedného bloku platí …“
- „$A[x] = B[y]$“ („blok, kam ukazuje x v A, je rovnaký ako blok, kam ukazuje y v B“):

$$\forall i, j : i \equiv j \pmod{n} \wedge \mathrm{zb}(i) = \mathrm{zb}(x) \wedge \mathrm{zb}(j) = \mathrm{zb}(y) \rightarrow (i \in A \leftrightarrow j \in B)$$

- $x \equiv y \pmod{N}$:

$$x \equiv y \pmod{n} \wedge P_n[x] = P_n[y].$$

- $\mathrm{zb}(i)$ – začiatok bloku i:

$$z = \mathrm{zb}(i) \iff z \leq i \wedge z \equiv 0 \pmod{n} \wedge \forall j : z < j < i : j \not\equiv 0 \pmod{n}.$$

- i, j ukazujú na ten istý blok $\iff \mathrm{zb}(i) = \mathrm{zb}(j)$
- „pre všetky indexy z jedného bloku platí . . . "
- „$A[x] = B[y]$" („blok, kam ukazuje x v A, je rovnaký ako blok, kam ukazuje y v B"):

$$\forall i, j : i \equiv j \pmod{n} \wedge \mathrm{zb}(i) = \mathrm{zb}(x) \wedge \mathrm{zb}(j) = \mathrm{zb}(y) \to (i \in A \leftrightarrow j \in B)$$

- $x \equiv y \pmod{N}$:

$$x \equiv y \pmod{n} \wedge P_n[x] = P_n[y].$$

- $\mathrm{zb}(i)$ – začiatok bloku i:

$$z = \mathrm{zb}(i) \iff z \leq i \wedge z \equiv 0 \pmod{n} \wedge \forall j : z < j < i : j \not\equiv 0 \pmod{n}.$$

- i, j ukazujú na ten istý blok $\iff \mathrm{zb}(i) = \mathrm{zb}(j)$
- „pre všetky indexy z jedného bloku platí …“
- „$A[x] = B[y]$“ („blok, kam ukazuje x v A, je rovnaký ako blok, kam ukazuje y v B“):

$$\forall i, j : i \equiv j \pmod{n} \wedge \mathrm{zb}(i) = \mathrm{zb}(x) \wedge \mathrm{zb}(j) = \mathrm{zb}(y) \to (i \in A \leftrightarrow j \in B)$$

- $x \equiv y \pmod{N}$:

$$x \equiv y \pmod{n} \wedge P_n[x] = P_n[y].$$

- $\mathrm{zb}(i)$ – začiatok bloku i:

$$z = \mathrm{zb}(i) \iff z \leq i \land z \equiv 0 \pmod{n} \land \forall j : z < j < i : j \not\equiv 0 \pmod{n}.$$

- i, j ukazujú na ten istý blok $\iff \mathrm{zb}(i) = \mathrm{zb}(j)$
- „pre všetky indexy z jedného bloku platí …“
- „$A[x] = B[y]$“ („blok, kam ukazuje x v A, je rovnaký ako blok, kam ukazuje y v B“):

$$\forall i, j : i \equiv j \pmod{n} \land \mathrm{zb}(i) = \mathrm{zb}(x) \land \mathrm{zb}(j) = \mathrm{zb}(y) \to (i \in A \leftrightarrow j \in B)$$

- $x \equiv y \pmod{N}$:

$$x \equiv y \pmod{n} \land P_n[x] = P_n[y].$$

- číslo N
- $y = x + N$
- „A je N-bitové číslo“:

$$\forall i : i \geq N \to i \notin A \qquad \text{alebo} \qquad \forall i : i \in A \to \mathrm{zb}(i) = 0.$$

- sčítanie N-bitových čísel modulo 2^N:

$$X = A + B \bmod 2^N \iff \exists X' = A + B \land \underbrace{\forall i : i < N : i \in X \leftrightarrow i \in X'}_{\text{prvých } N \text{ bitov sa zhoduje}}$$

$$\land \qquad \underbrace{\forall i : i \geq N : i \notin X}_{\text{zvyšné bity sú nulové – } X \text{ je } N\text{-bitové}}$$

- P_N: $(\forall i : i < N \to i \notin P_N) \land \forall i : P_N[i+N] = P_N[i] + 1 \bmod 2^N$.

- číslo N
- $y = x + N$
- „A je N-bitové číslo“:

$$\forall i : i \geq N \to i \notin A \qquad \text{alebo} \qquad \forall i : i \in A \to \mathrm{zb}(i) = 0.$$

- sčítanie N-bitových čísel modulo 2^N:

$$X = A + B \bmod 2^N \iff \exists X' = A + B \wedge \underbrace{\forall i : i < N : i \in X \leftrightarrow i \in X'}_{\text{prvých } N \text{ bitov sa zhoduje}}$$
$$\wedge \quad \underbrace{\forall i : i \geq N : i \notin X}_{\text{zvyšné bity sú nulové – } X \text{ je } N\text{-bitové}}$$

- P_N: $(\forall i : i < N \to i \notin P_N) \wedge \forall i : P_N[i+N] = P_N[i] + 1 \bmod 2^N$.

- číslo N
- $y = x + N$
- „A je N-bitové číslo“:

$$\forall i : i \geq N \to i \notin A \qquad \text{alebo} \qquad \forall i : i \in A \to \mathrm{zb}(i) = 0.$$

- sčítanie N-bitových čísel modulo 2^N:

$$X = A + B \bmod 2^N \iff \exists X' = A + B \wedge \underbrace{\forall i : i < N : i \in X \leftrightarrow i \in X'}_{\text{prvých } N \text{ bitov sa zhoduje}}$$
$$\wedge \quad \underbrace{\forall i : i \geq N : i \notin X}_{\text{zvyšné bity sú nulové} - X \text{ je } N\text{-bitové}}$$

- P_N: $(\forall i : i < N \to i \notin P_N) \wedge \forall i : P_N[i+N] = P_N[i] + 1 \bmod 2^N$.

- číslo N
- $y = x + N$
- „A je N-bitové číslo“:

$$\forall i : i \geq N \to i \notin A \qquad \text{alebo} \qquad \forall i : i \in A \to \mathrm{zb}(i) = 0.$$

- sčítanie N-bitových čísel modulo 2^N:

$$X = A + B \bmod 2^N \iff \exists X' = A + B \wedge \underbrace{\forall i : i < N : i \in X \leftrightarrow i \in X'}_{\text{prvých } N \text{ bitov sa zhoduje}}$$
$$\wedge \underbrace{\forall i : i \geq N : i \notin X}_{\text{zvyšné bity sú nulové – } X \text{ je } N\text{-bitové}}$$

- P_N: $(\forall i : i < N \to i \notin P_N) \wedge \forall i : P_N[i + N] = P_N[i] + 1 \bmod 2^N$.

- číslo N
- $y = x + N$
- „A je N-bitové číslo“:

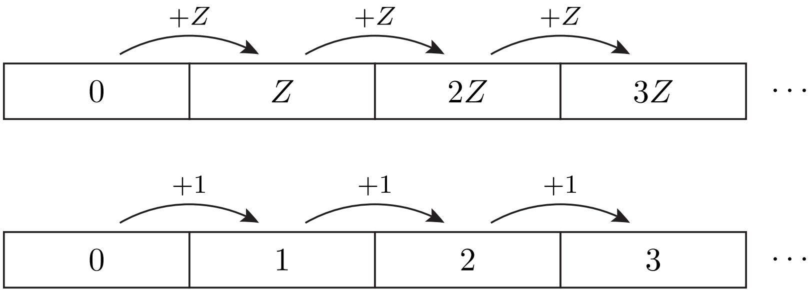
$$\forall i : i \geq N \to i \notin A \qquad \text{alebo} \qquad \forall i : i \in A \to \mathrm{zb}(i) = 0.$$

- sčítanie N-bitových čísel modulo 2^N:

$$X = A + B \bmod 2^N \iff \exists X' = A + B \wedge \underbrace{\forall i : i < N : i \in X \leftrightarrow i \in X'}_{\text{prvých } N \text{ bitov sa zhoduje}}$$
$$\wedge \quad \underbrace{\forall i : i \geq N : i \notin X}_{\text{zvyšné bity sú nulové – } X \text{ je } N\text{-bitové}}$$

- P_N: $(\forall i : i < N \to i \notin P_N) \wedge \forall i : P_N[i+N] = P_N[i] + 1 \bmod 2^N$.

Násobenie



Násobenie $X = K \times Z \bmod 2^M$:

$$\exists T : T[0] = 0 \wedge \forall i : T[i+M] = T[i] + Z \bmod 2^M \wedge T[K] = X,$$

kde $T[K] = X$ je skratka pre

$$\exists j : P_M[j] = K \wedge j \text{ je najmenšie také} \wedge T[j] = X.$$

Dôsledok

- takto vieme po k iteráciach definovať $> \underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{k}$-bitové čísla
- násobenie veľkých čísel
- $\implies$ v S1S vieme sformulovať, že „TS zastaví na $\underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{n}$ krokov“
- $\implies$ rozhodnuteľnosť S1S $\notin$ ELEMENTARY, kde
  - $\mathsf{ELEMENTARY} = \mathsf{EXP} \cup \mathsf{2EXP} \cup \mathsf{3EXP} \cup \cdots$
  - $\mathsf{ELEMENTARY} =$
    $\mathsf{DTIME}(2^n) \cup \mathsf{DTIME}(2^{2^n}) \cup \mathsf{DTIME}(2^{2^{2^n}}) \cup \cdots$

Konkrétna zložitosť

- Stockmeyer, Meyer '02: Cosmological lower bound on the circuit complexity of a small problem in logic
  - na rozhodnuteľnosť ≤ 610-znakových formúl EWS1S treba obvod s $> 10^{125}$ hradlami
  - na rozhodnuteľnosť ≤ 614-znakových formúl s úspešnosťou $\geq 2/3$ treba obvod s $> 10^{125}$ hradlami
  - odhadovaný #atómov v pozorovateľnom vesmíre: 10^{78}–10^{82}

Rýchlo rastúce funkcie

- $2 \times n = \underbrace{2 + (2 + (\cdots + 2))}_{n}$
- $2^n = 2 \uparrow n = \underbrace{2 \times (2 \times (\cdots \times 2))}_{n}$
- $2 \uparrow\uparrow n = \underbrace{2 \uparrow (2 \uparrow (\cdots \uparrow 2))}_{n}$
- $2 \uparrow\uparrow\uparrow n = \underbrace{2 \uparrow\uparrow (2 \uparrow\uparrow (\cdots \uparrow\uparrow 2))}_{n}$
- $\cdots$
- $2 \uparrow^k n = \underbrace{2 \uparrow^{k-1} (2 \uparrow^{k-1} (\cdots \uparrow^{k-1} 2))}_{n}$
- Ackermann $\sim 2 \uparrow^n n$

Dyadická S1S

Veta

Teória dyadickej S1S je nerozhodnuteľná.

PKP:

typ 1: $\boxed{\dfrac{\texttt{a}}{\texttt{baa}}}$ typ 2: $\boxed{\dfrac{\texttt{ab}}{\texttt{aa}}}$ typ 3: $\boxed{\dfrac{\texttt{bba}}{\texttt{bb}}}$,

bba	ab	bba	a
bb	aa	bb	baa

dominá typu 3, 2, 3, 1

<table>
<tr><td colspan="3">b b a</td><td colspan="2">a b</td><td colspan="3">b b a</td><td colspan="1">a</td></tr>
<tr><td colspan="2">b b</td><td colspan="2">a a</td><td colspan="2">b b</td><td colspan="3">b a a</td></tr>
</table>

$$
\begin{array}{lcccccccccc}
 & \downarrow & & & \downarrow & & \downarrow & & & \downarrow & \downarrow \\
\textit{pozície} & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
s = & \mathtt{b} & \mathtt{b} & \mathtt{a} & \mathtt{a} & \mathtt{b} & \mathtt{b} & \mathtt{b} & \mathtt{a} & \mathtt{a} & \\
 & \uparrow & & \uparrow & & \uparrow & & \uparrow & & & \uparrow
\end{array}
$$

- $S = \{0,1,4,5,6\}$
- S: spoločný text hore aj dolu (presnejšie pozície béčok)
- H_i, D_i, T_i: pozícia, kde začína i-te domino hore/dolu; typ i-teho domina

$$\begin{array}{lcccccccccc}
 & \downarrow & & & \downarrow & & \downarrow & & & \downarrow & \downarrow \\
\textit{pozície} & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
s = & \mathtt{b} & \mathtt{b} & \mathtt{a} & \mathtt{a} & \mathtt{b} & \mathtt{b} & \mathtt{b} & \mathtt{a} & \mathtt{a} & \\
 & \uparrow & & \uparrow & & \uparrow & & \uparrow & & & \uparrow
\end{array}$$

- $S = \{0, 1, 4, 5, 6\}$
- S: spoločný text hore aj dolu (presnejšie pozície béčok)
- H_i, D_i, T_i: pozícia, kde začína i-te domino hore/dolu; typ i-teho domina

$$
\begin{aligned}
&\exists \text{množina } S : \exists \text{funkcie } H, D, T : H_0 = 0 \land D_0 = 0 \\
&\quad \land \forall i : \big((T_i = 1 \rightarrow [\psi_{\mathtt{a}}(H_i) \land \psi_{\mathtt{baa}}(D_i) \land H_{i+1} = H_i + 1 \land D_{i+1} = D_i + 3]) \\
&\qquad\quad (T_i = 2 \rightarrow [\psi_{\mathtt{ab}}(H_i) \land \psi_{\mathtt{aa}}(D_i) \land H_{i+1} = H_i + 2 \land D_{i+1} = D_i + 2]) \\
&\qquad\quad (T_i = 3 \rightarrow [\psi_{\mathtt{bba}}(H_i) \land \psi_{\mathtt{bb}}(D_i) \land H_{i+1} = H_i + 3 \land D_{i+1} = D_i + 2] \\
&\quad \land \exists i : i \neq 0 \land H_i = D_i
\end{aligned}
$$

$\square$