

Hmoto:

$E \dots$ konečná abeceda

$$h \left\{ \begin{array}{c} \rightarrow \\ \rightarrow \\ \rightarrow \end{array} \right| f \rightarrow f: E^h \rightarrow E$$

Lanita

Hmoto sif:

MAJORITY

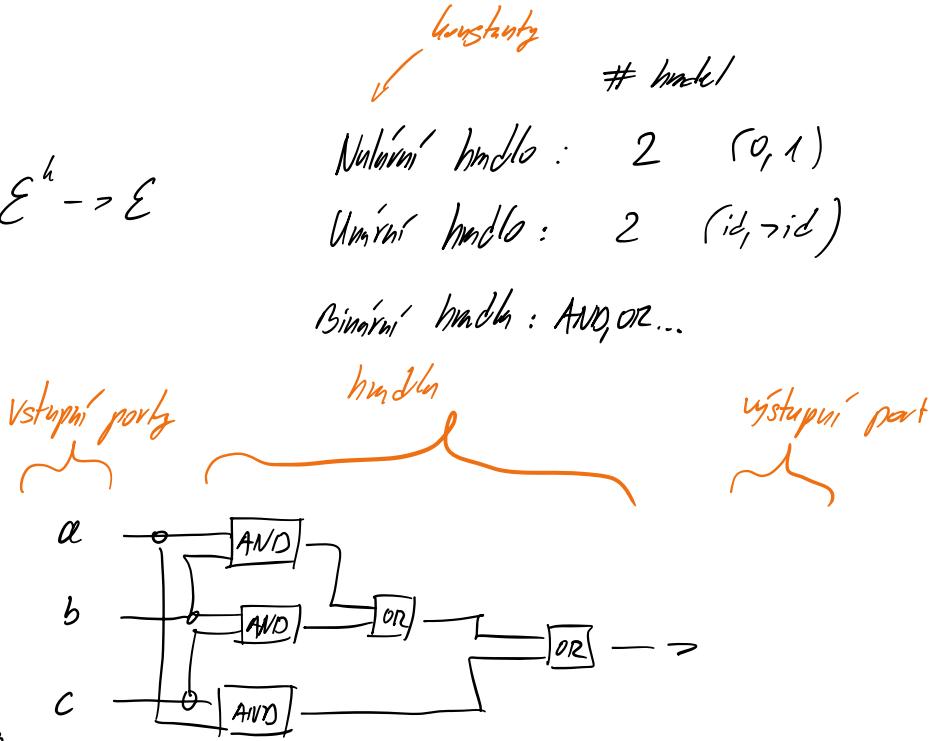
vходы ← въходи
въходи → выходи, анита

hmoto:

въход: $\deg^{in} = 0$

въход: $\deg^{in} = 1$

hmoto: $\deg^{in} = \text{ Lanita}, \deg^{out} > 0$



- každé hmoto má vstupní vystup,

- gmf musí být acyklický

- každé hmoto musí mít funkci

gmf je DAG.

Výpočet:

- běží po fahotech

$t=0$: výstup mají vstupní porty a unív. hmoto

rozdělení na vrstvy $\rightarrow t > 0$: výstup vydají hmoto, co mají všechny vstupy def.

Anita hmoto musí být omezena.

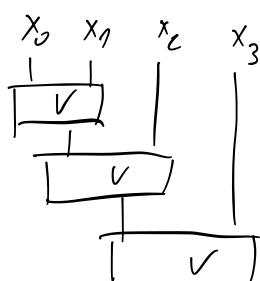
$V_i :=$ vrstvy, co poprvé dají výstup v čase i .

Existence 1 r n-bitovém vystupu.

Výstup: $x_0 \vee x_1 \dots x_{n-1}$

Obeení checeme časy $O(\log^k n)$

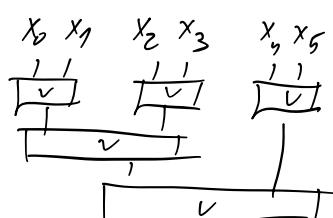
Trivium:



$h: O(n)$

$v: O(n)$

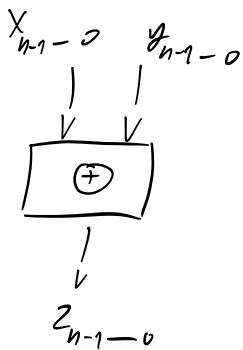
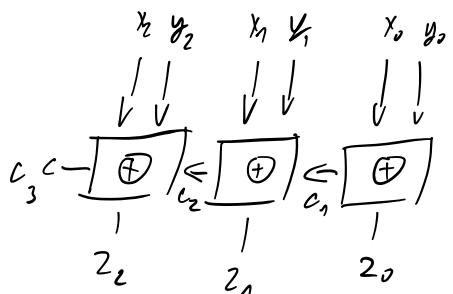
Příklad:



$h: O(\log n)$

$v: O(n)$

Binární sčítací řetězec:



$$c_0 = 0$$

$$z_i = x_i \oplus y_i \oplus c_i$$

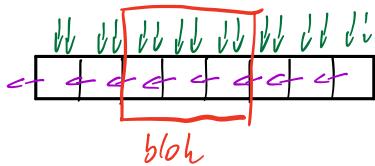
$$c_{i+1} = \text{maj}(x_i, y_i, c_i) = (x_i \wedge y_i) \vee (x_i \wedge c_i) \vee (y_i \wedge c_i)$$

$$h: \Theta(n)$$

To je ale schvázení

Dohudl bych většinu přenosů dopředu, může být výpočet v konstantním čase.

- Můžu uvažovat obě možnosti pro carry bit zespoda.



charakter bloku: $f: C_m \rightarrow \text{Cont}$

- identity = <

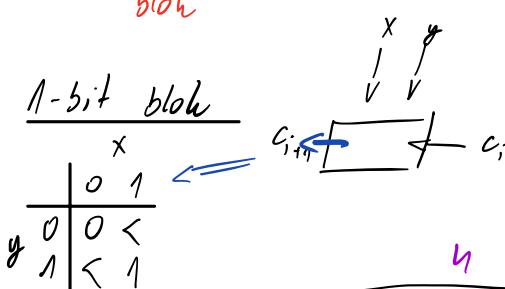
- negace = nikdy nezmění

- konst 0 = 0

- konst 1 = 1

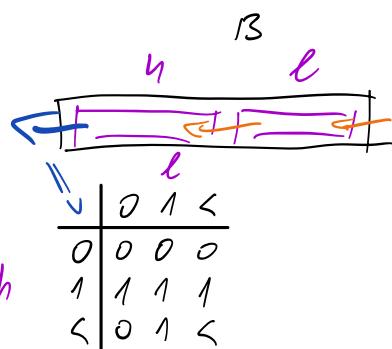
\hookrightarrow jednobitový blok nezmění,

schichování takových bloků nezmění negaci



$$p = x \oplus y$$

$$q = x$$



$$< (1, *)$$

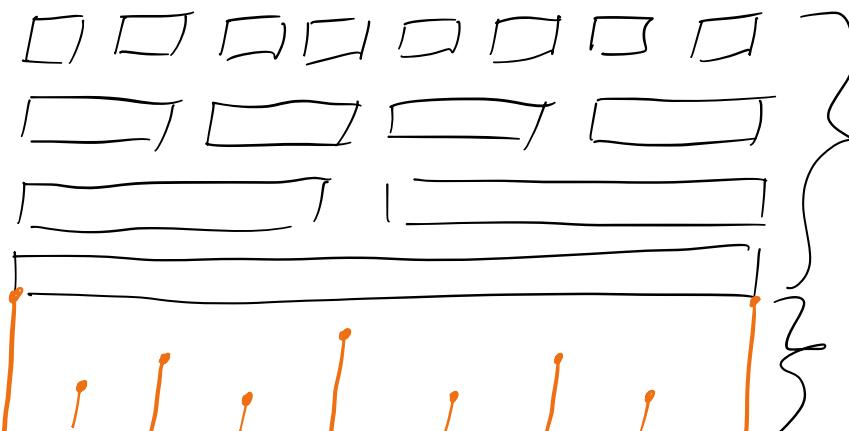
$$0 (0, 0)$$

$$1 (0, 1)$$

$$P_B = P_h \wedge P_e$$

$$q_B = (P_h \wedge q_e) \vee (\neg P_h \wedge q_h)$$

Jak udělat binární sčítací řetězec? První charakteristické bloky:



charakteristické bloky

$$h: \Theta(\log n)$$

$$v: \Theta(n)$$

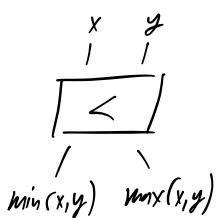
zahrnující bloky

$$h: \Theta(\log n)$$

$$v: \Theta(n)$$

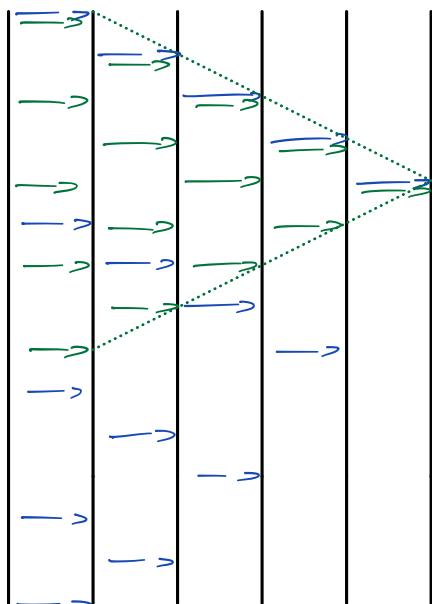
Třídíci sít:

Komparátor:



SUMO: Sít se nechá.

Bubble Sort:



Tahle ale nemá paralelní způsob.

Tahle je paralelní způsob.

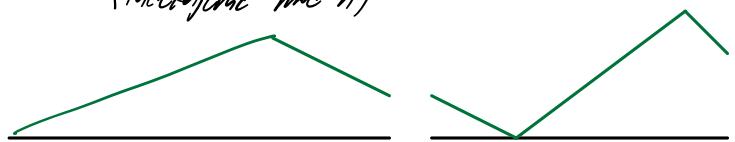
Hlavní $\Theta(n)$ → lineární paralelní čas
Velikost $\Theta(n^2)$ kde vzdálost $\Theta(\log^2 n)$

Merge Sort:

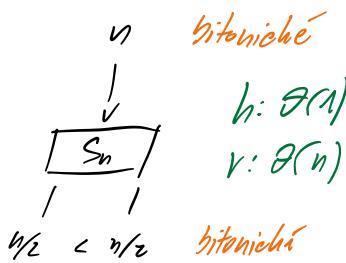
Df: Post. $x_0 - x_{n-1}$ je bitomický \equiv

$\exists i: x_i < x_{i+1} < \dots < x_{i+j} > x_{i+j+1} > \dots > x_{i+n-1}$

(indexujeme mod n)



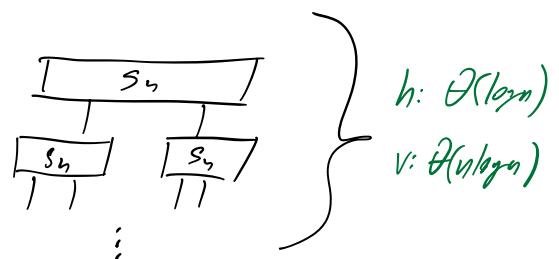
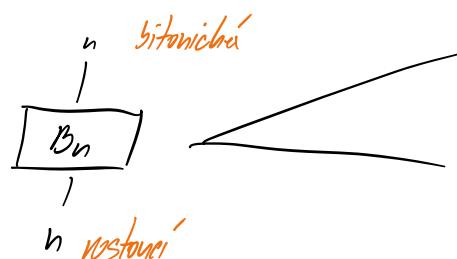
Separátor:



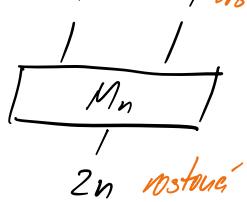
✓ můžete dílčí postupnosti, které jsou bitomické, ale hlavní věci jsou souběžně.

Pokud budu opakovat za sebou reťaz, dostanu seřazené jednoznačně → princip bitomického třídění.

(Bitomické) třídění:



Slévaček:



→ rozděluji jednu, spojuji oběma otáčením a posléze bitomickou třídění.

h: $\Theta(\log n)$

v: $\Theta(n \log n)$

