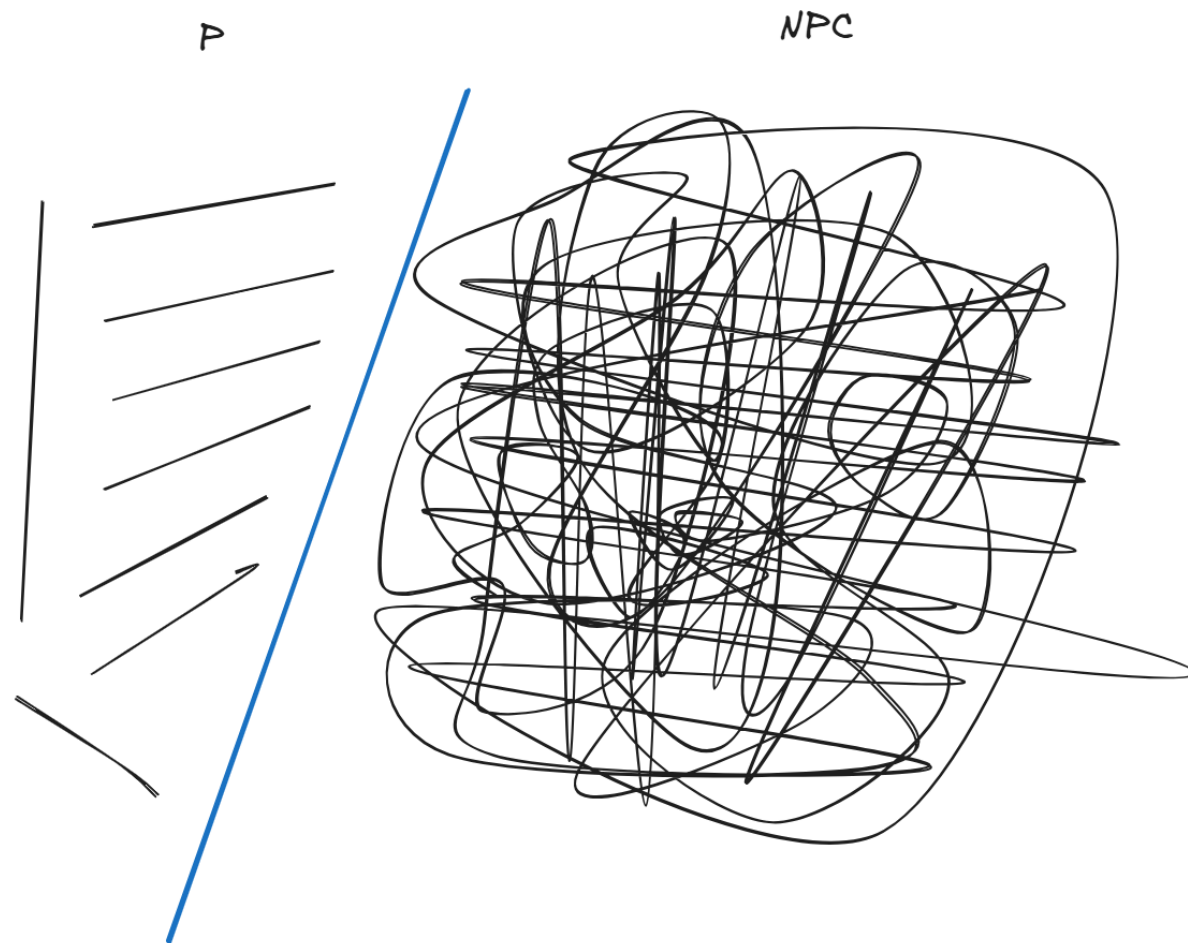


NP, NP-polnost

Uroš Čibej



Literatura

Arora, Barak: poglavje 2

Pregled snovi

1. NP
2. Prevedbe
3. Nedeterministični stroji
4. Cook-Levinov izrek
5. Konkretna prevedbe

Preverjevalnik

Preverjevalnik V je algoritem, ki sprejme dva niza x, c .

- preverjevalnik igra vlogo preverjanja določene lastnosti niza x
- c imenujemo tudi certifikat, oz. priča želene lastnosti

Definicija razreda NP

def. NP je razred problemov (jezikov), ki imajo **polinomski preverjevalnik** V .

$$x \in L \iff \exists c \in \{0, 1\}^* : V(x, c) = 1$$

Problemi v NP

- klika
- vsota podmnožice
- faktorizacija
- grafni izomorfizem
- ...

Kaj so certifikati za te probleme?

SAT

Vhod: Množica logičnih spremenljivk $X = \{x_1, x_2, \dots, x_n\}$ in logični izraz s temi spremenljivkami:

$$\Phi$$

Vprašanje: Ali obstaja dodelitev vrednosti spremenljivkam $\tau : X \rightarrow \{0, 1\}$, da je

$$\Phi[\tau] = 1$$

Predpostavili bomo, da je Φ logični izraz v KNO.

Primer

$$\begin{aligned}\Phi = C_1 : & \quad (x_1 \vee x_2 \vee x_3) \\ \wedge C_2 : & \quad (\neg x_1 \vee x_4) \\ \wedge C_3 : & \quad (\neg x_2 \vee x_4) \\ \wedge C_4 : & \quad (\neg x_3 \vee x_5) \\ \wedge C_5 : & \quad (\neg x_4 \vee \neg x_5) \\ \wedge C_6 : & \quad (x_2 \vee \neg x_3 \vee \neg x_4) \\ \wedge C_7 : & \quad (\neg x_4)\end{aligned}$$

$$P \subseteq NP$$

$L \in P$ in A polinomski algoritem za L .

```
def V(x,c):  
    return A(x)
```

Nedeterministični TS

$$M = \langle Q, \Gamma, \delta, q_0, q_F, q_R \rangle$$

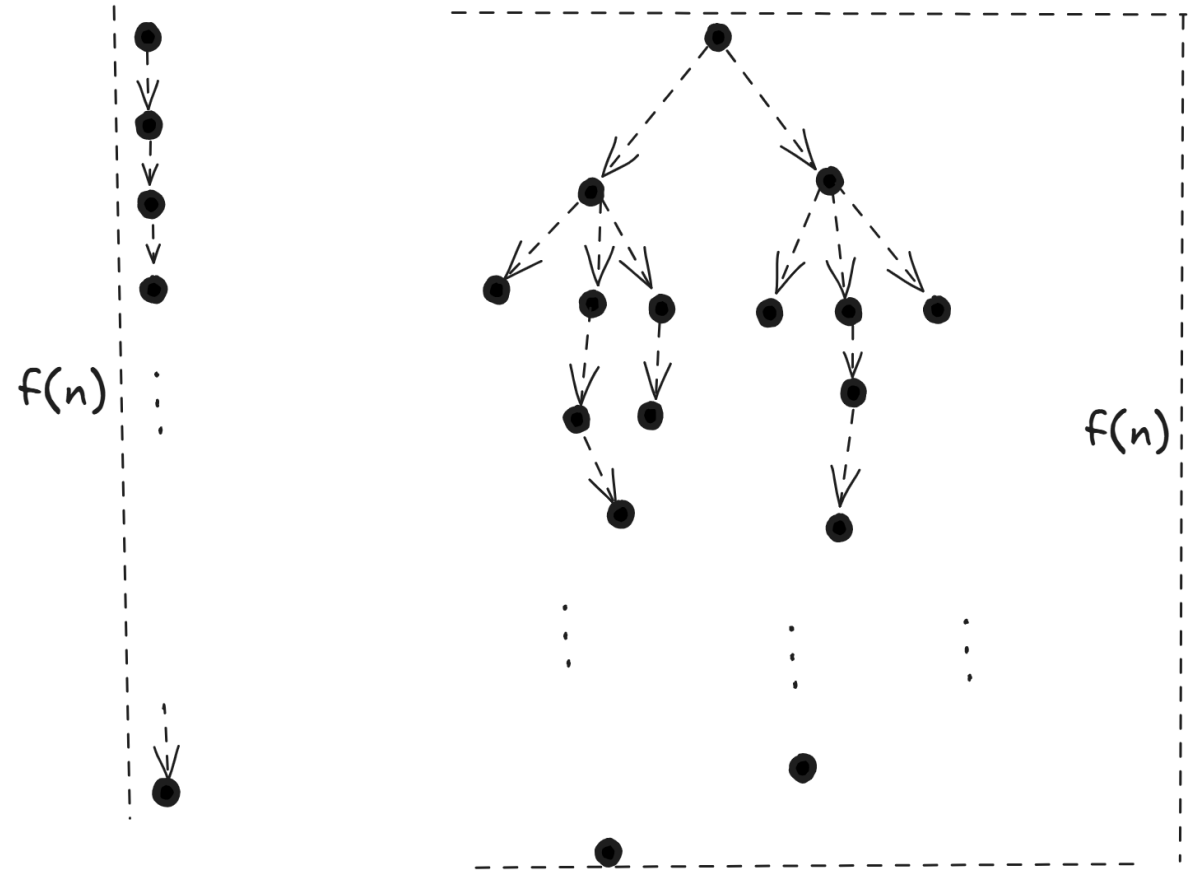
$$\delta : Q \times \Gamma \rightarrow 2^{Q \times \Gamma \times \{L, R\}}$$

Nedeterminizem (primer)

$$L = \{a^k \mid k \text{ je sestavljeno število} \}$$

Časovna zahtevnost nedeterminističnega TS

def. Časovna zahtevnost
nedeterminističnega stroja M je
funkcija $f : \mathbb{N} \rightarrow \mathbb{N}$, kjer je $f(n)$
največje število korakov, ki ga naredi
 M pri poljubni veji drevesa izvajanja
pri nekem vhodu dolžine n .



Definicija razreda NP z nedeterminizmom

$$NP = \bigcup_k NTIME(n^k)$$

Relacija $P ? NP$

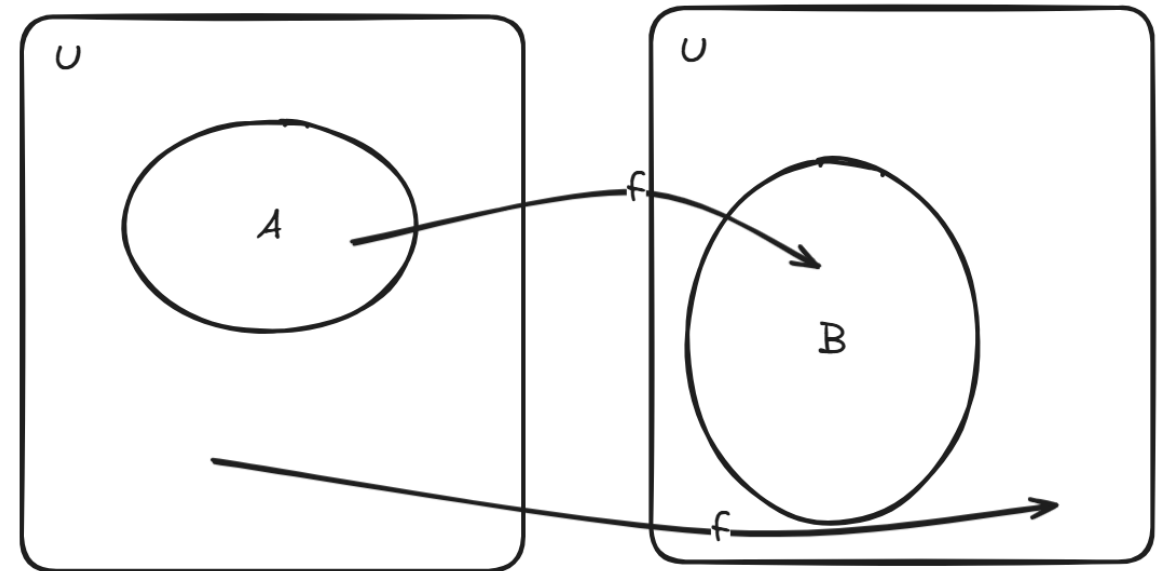
- Ali je preverjanje rešitve enako zahtevno kot generiranje rešitve?
- Ali je izčrpno preiskovanje (eksponentno) edini pristop, ki deluje za določene vrste problemov?
- Se moramo pri določenih problemih zadovoljiti z neoptimalnimi rešitvami?

Prevedbe

- problem A prevedemo na problem B
- funkcija f (izračunljiva) za katero velja

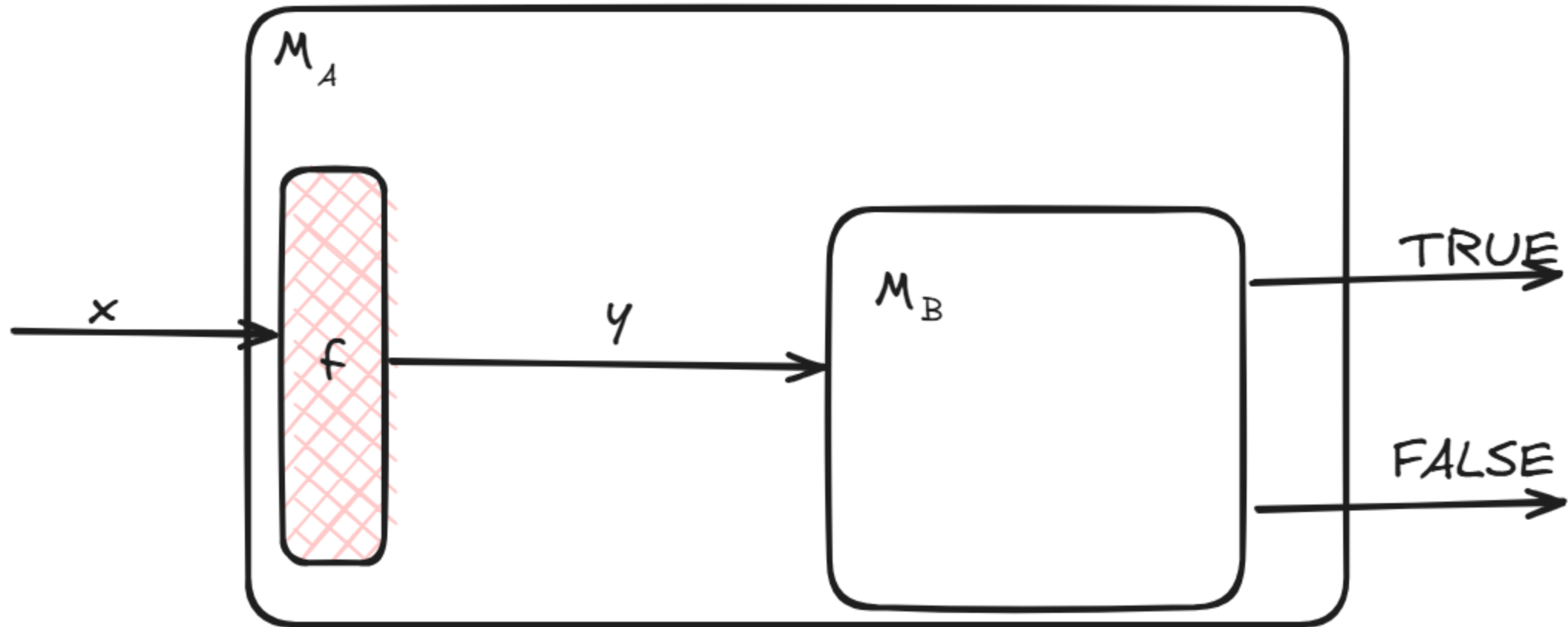
$$x \in A \iff f(x) \in B$$

- $A \leq B$



Polinomske prevedbe (Karpove)

- f izračunljiva v polinomskem času
- $A \leq_p B$



Lastnosti polinomskih prevedb

$$1. A \leq_p B, B \leq_p C \implies A \leq_p C$$

$$2. A \leq_p B, B \in P \implies A \in P$$

$$3. A \leq_p B, A \notin P \implies B \notin P$$

Definicija NP polnosti

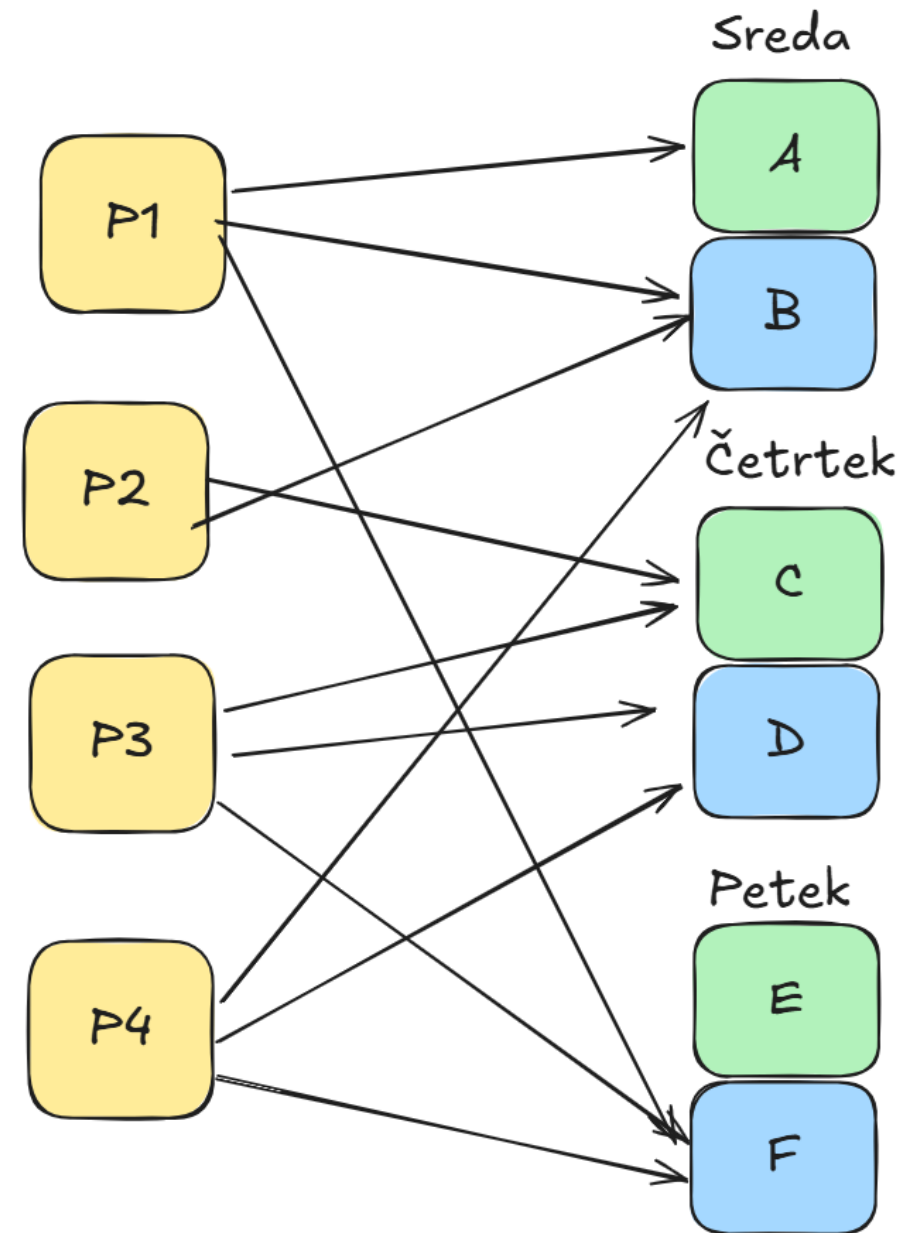
Problem L je NP -poln

1. $L \in NP$
2. $\forall L' \in NP : L' \leq_p L$

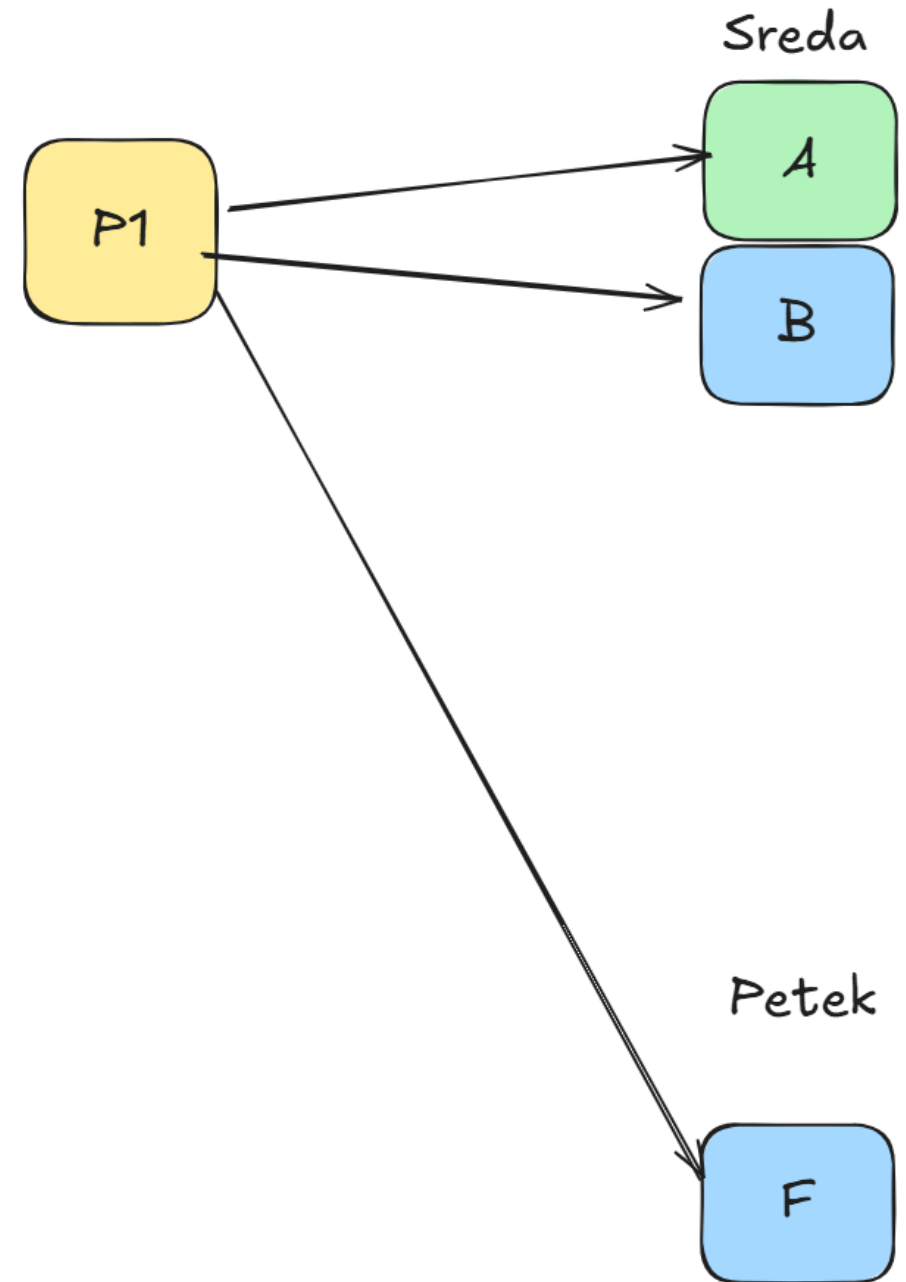
Modeliranje s SAT

"Urnik"

- X_{pt} - predmet p se izvaja v terminu t



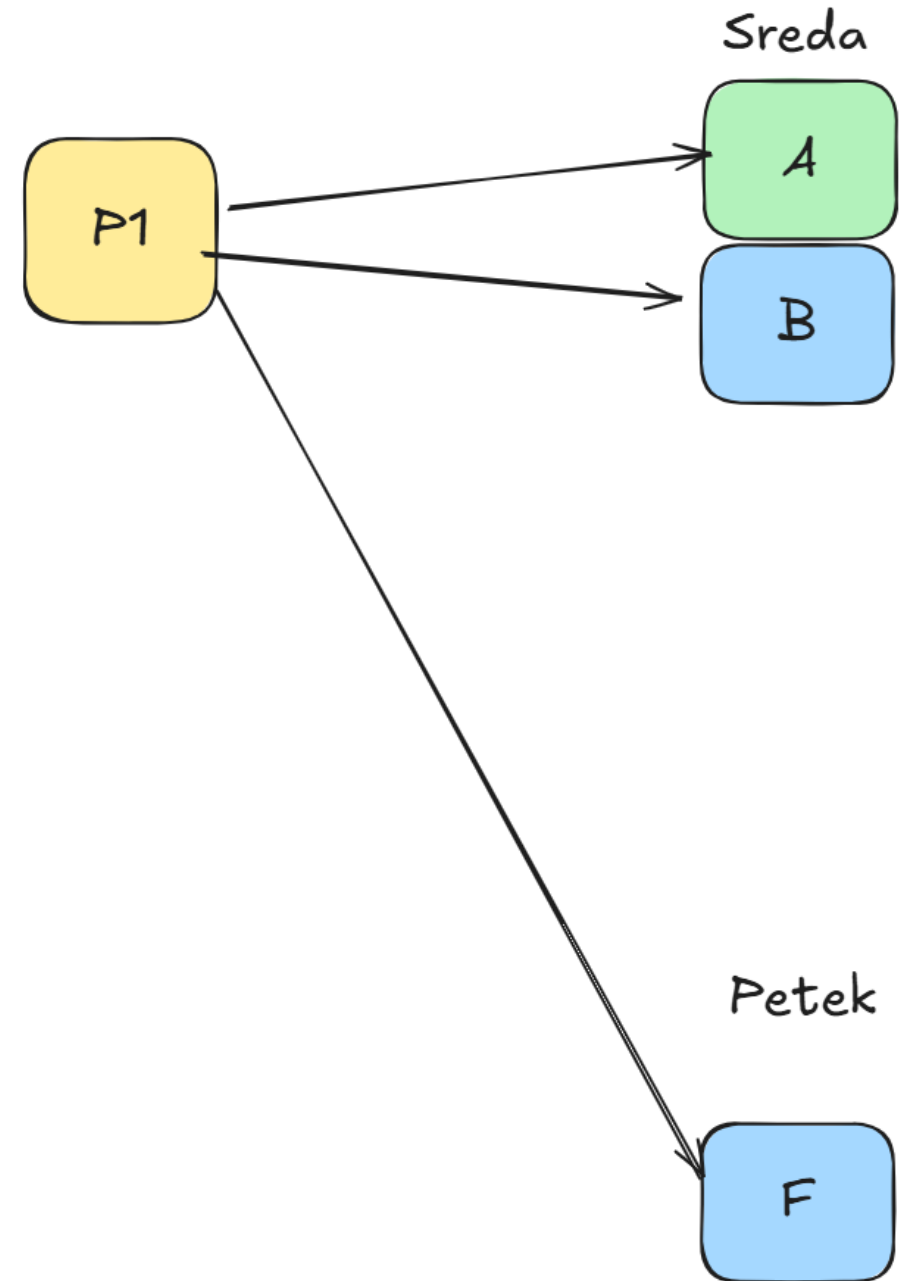
Vsaj ena
(At Least One)



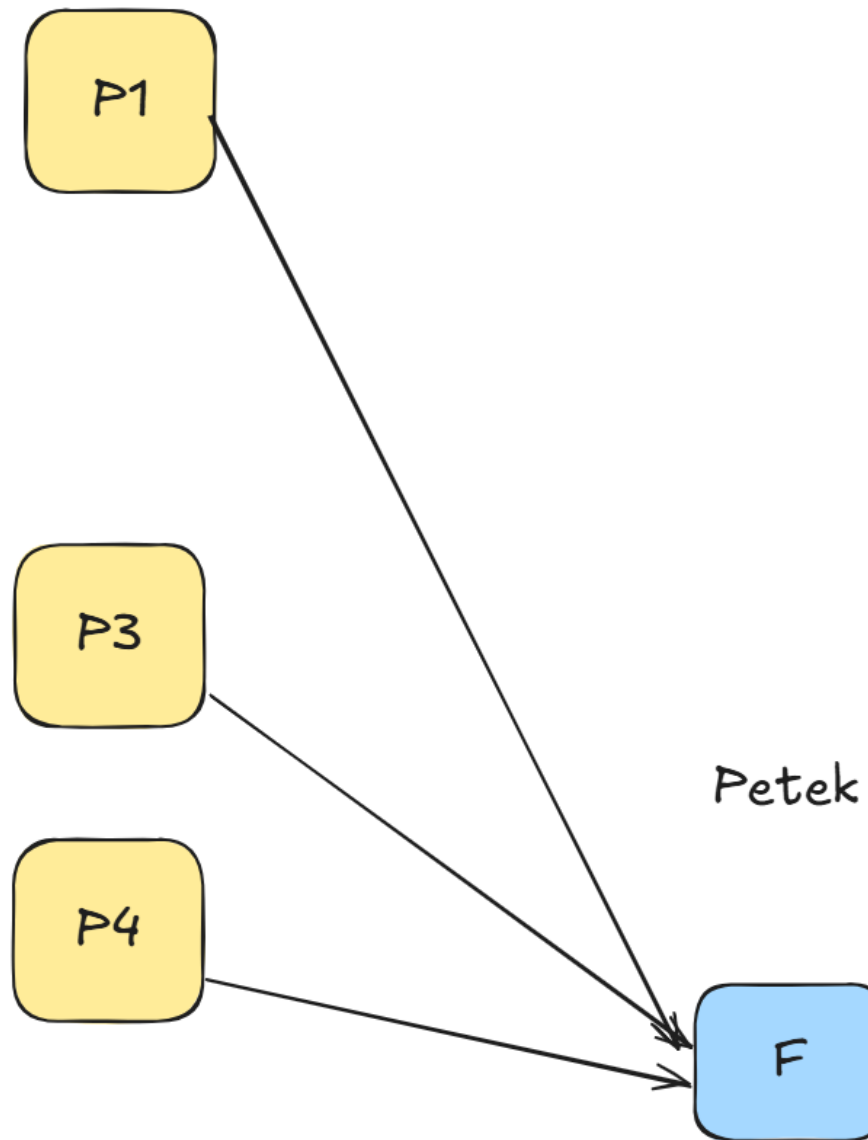
Vsaj ena

(At Least One)

$$X_{1A} \vee X_{1B} \vee X_{1F}$$



Največ ena
(At Most One)



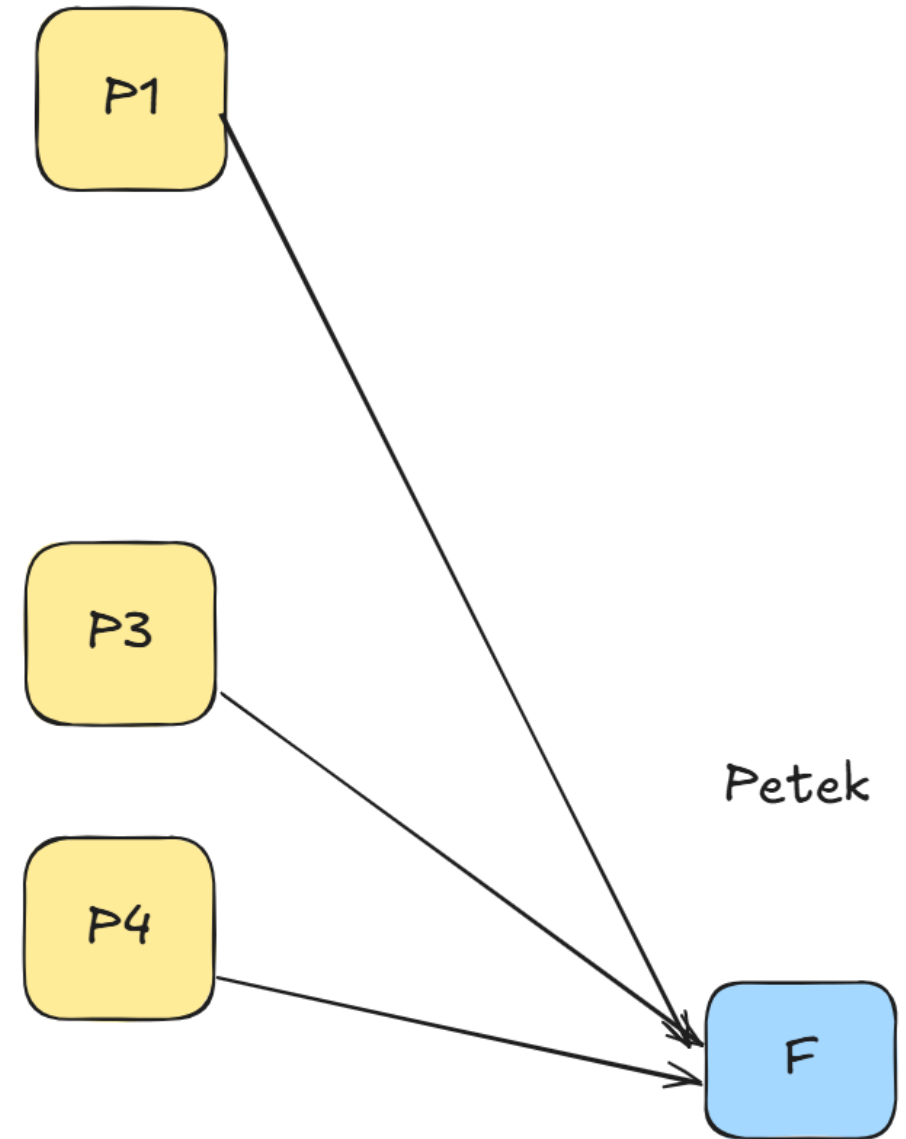
Največ ena

(At Most One)

$$\neg(X_{1F} \wedge X_{3F}) \wedge \neg(X_{1F} \wedge X_{4F}) \wedge \neg(X_{3F} \wedge X_{4F})$$

✓ KNO

$$(\neg X_{1F} \vee \neg X_{3F}) \wedge (\neg X_{1F} \vee \neg X_{4F}) \wedge (\neg X_{3F} \vee \neg X_{4F})$$

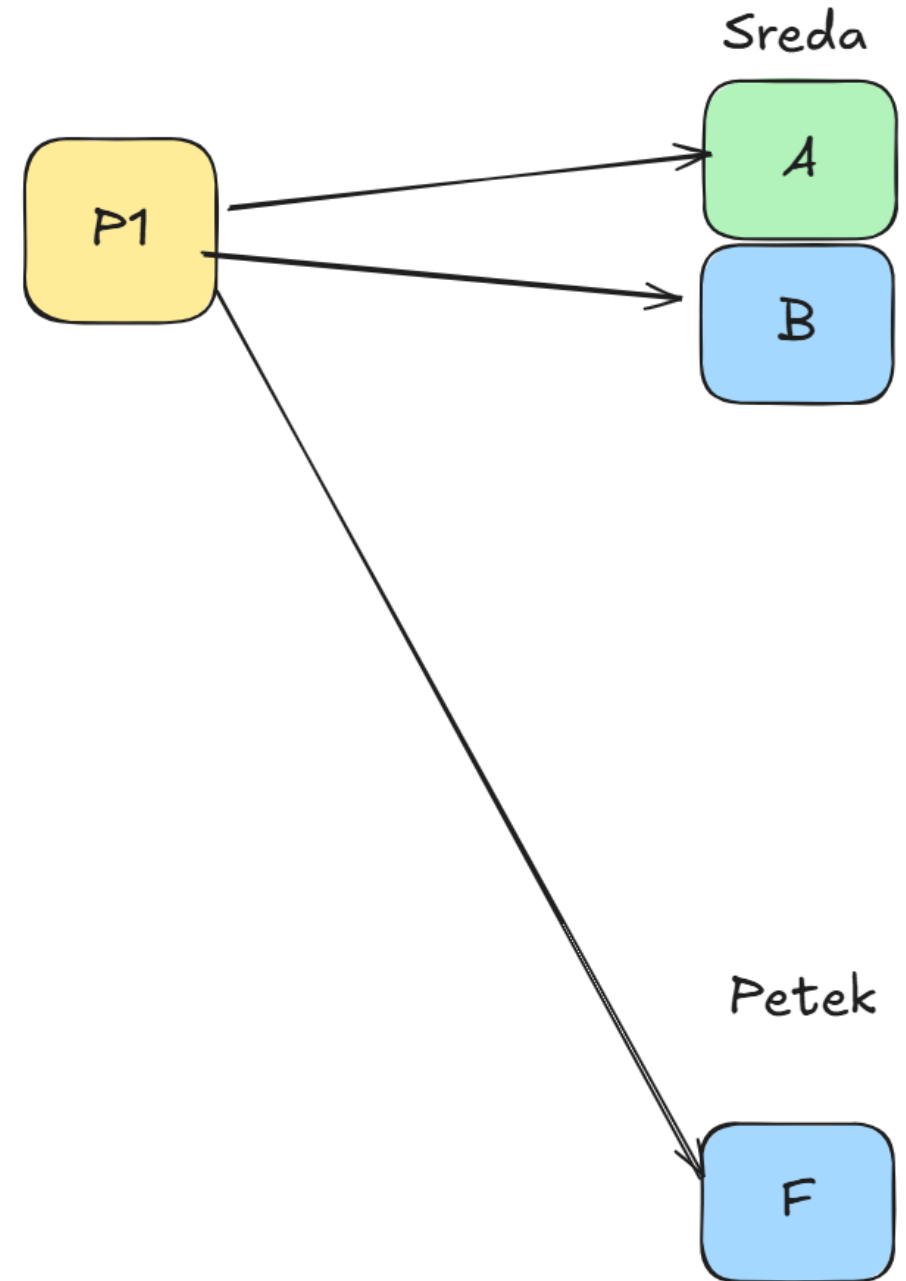


Natanko ena

vsaj ena in največ ena

$$X_{1A} \vee X_{1B} \vee X_{1F}$$

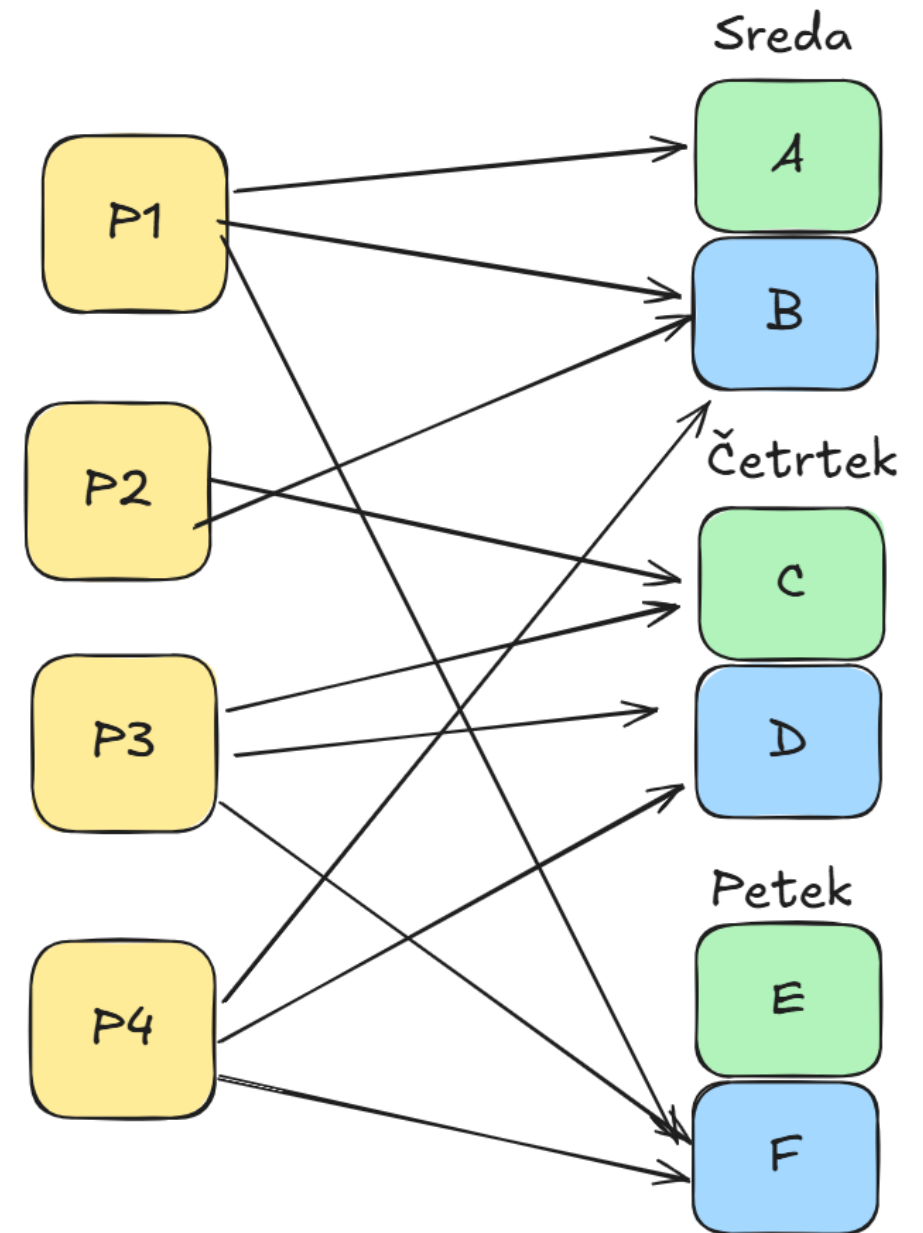
$$(\neg X_{1A} \vee \neg X_{1B}) \wedge (\neg X_{1A} \vee \neg X_{1F}) \wedge (\neg X_{1B} \vee \neg X_{1F})$$



Celotna formula

$$\Phi_{\text{SAT}} = \mathbf{ALO}_P \wedge \mathbf{AMO}_P \wedge \mathbf{AMO}_T$$

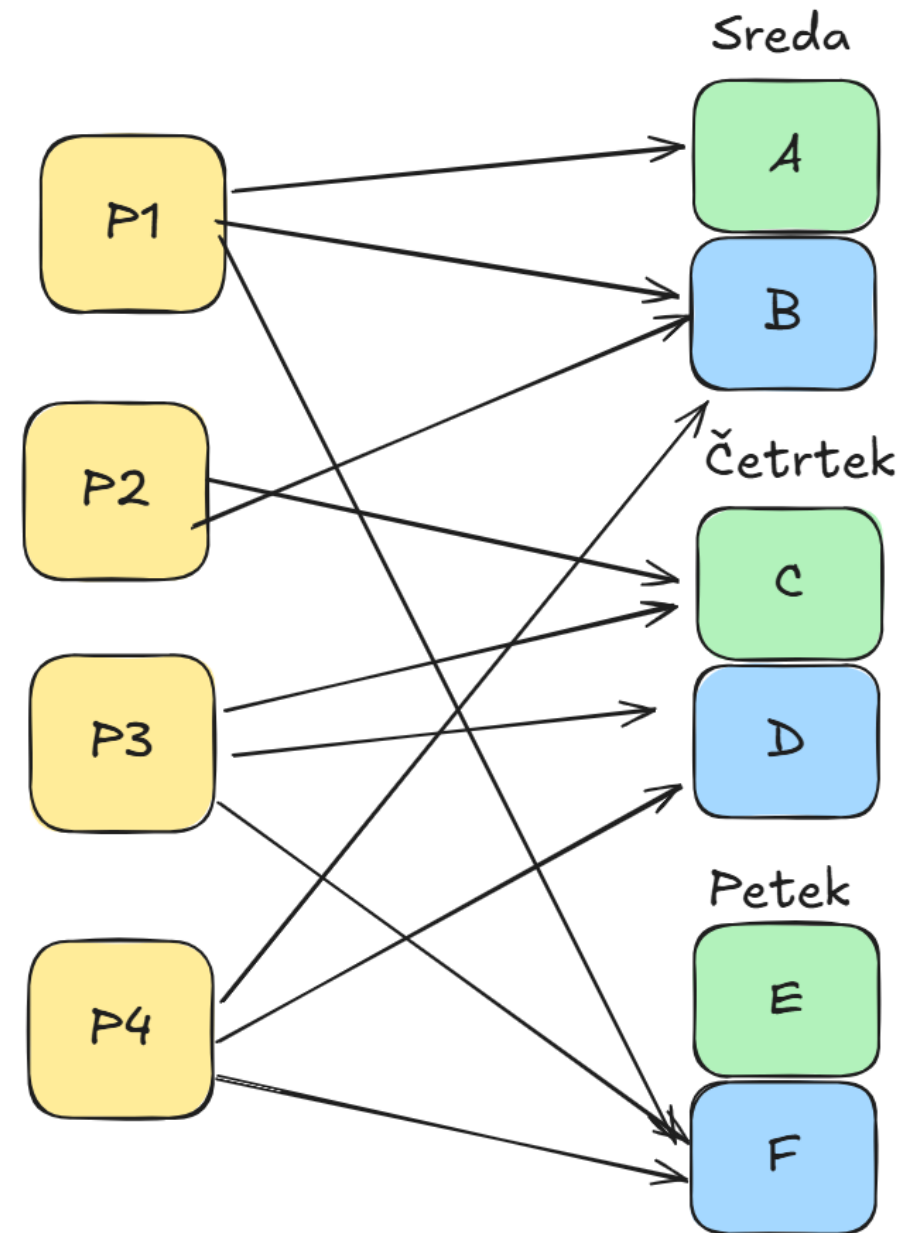
P_i	vsaj eden
P_1	$X_{1,A} \vee X_{1,B} \vee X_{1,F}$
P_2	$X_{2,B} \vee X_{2,C}$
P_3	$X_{3,C} \vee X_{3,D} \vee X_{3,F}$
P_4	$X_{4,B} \vee X_{4,D} \vee X_{4,F}$



Celotna formula

$$\Phi_{\text{SAT}} = \mathbf{ALO}_P \wedge \mathbf{AMO}_P \wedge \mathbf{AMO}_T$$

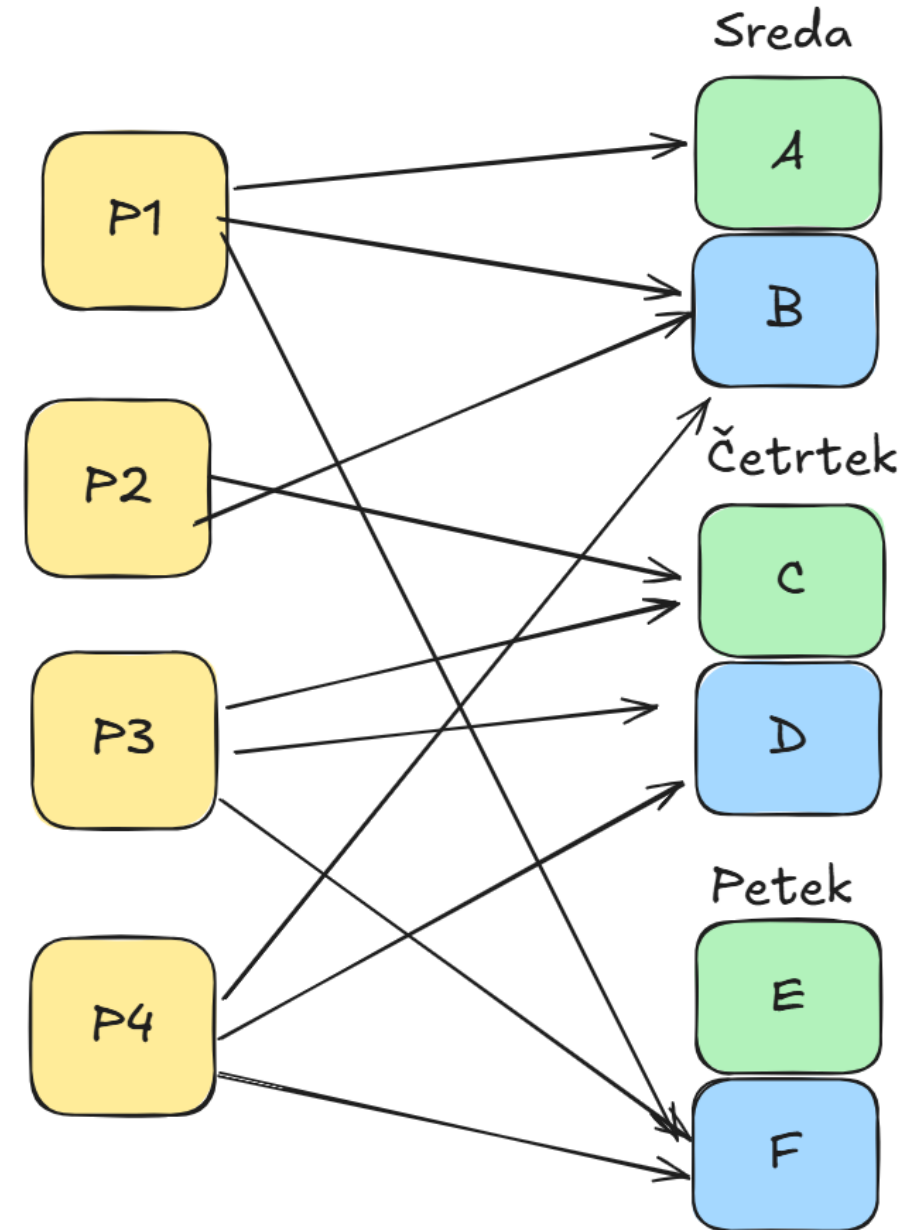
P_i	<i>Največ en</i>
P_1	$(\neg X_{1,A} \vee \neg X_{1,B}) \wedge (\neg X_{1,A} \vee \neg X_{1,F}) \wedge (\neg X_{1,B} \vee \neg X_{1,F})$
P_2	$(\neg X_{2,B} \vee \neg X_{2,C})$
P_3	$(\neg X_{3,C} \vee \neg X_{3,D}) \wedge (\neg X_{3,C} \vee \neg X_{3,F}) \wedge (\neg X_{3,D} \vee \neg X_{3,F})$
P_4	$(\neg X_{4,B} \vee \neg X_{4,D}) \wedge (\neg X_{4,B} \vee \neg X_{4,F}) \wedge (\neg X_{4,D} \vee \neg X_{4,F})$



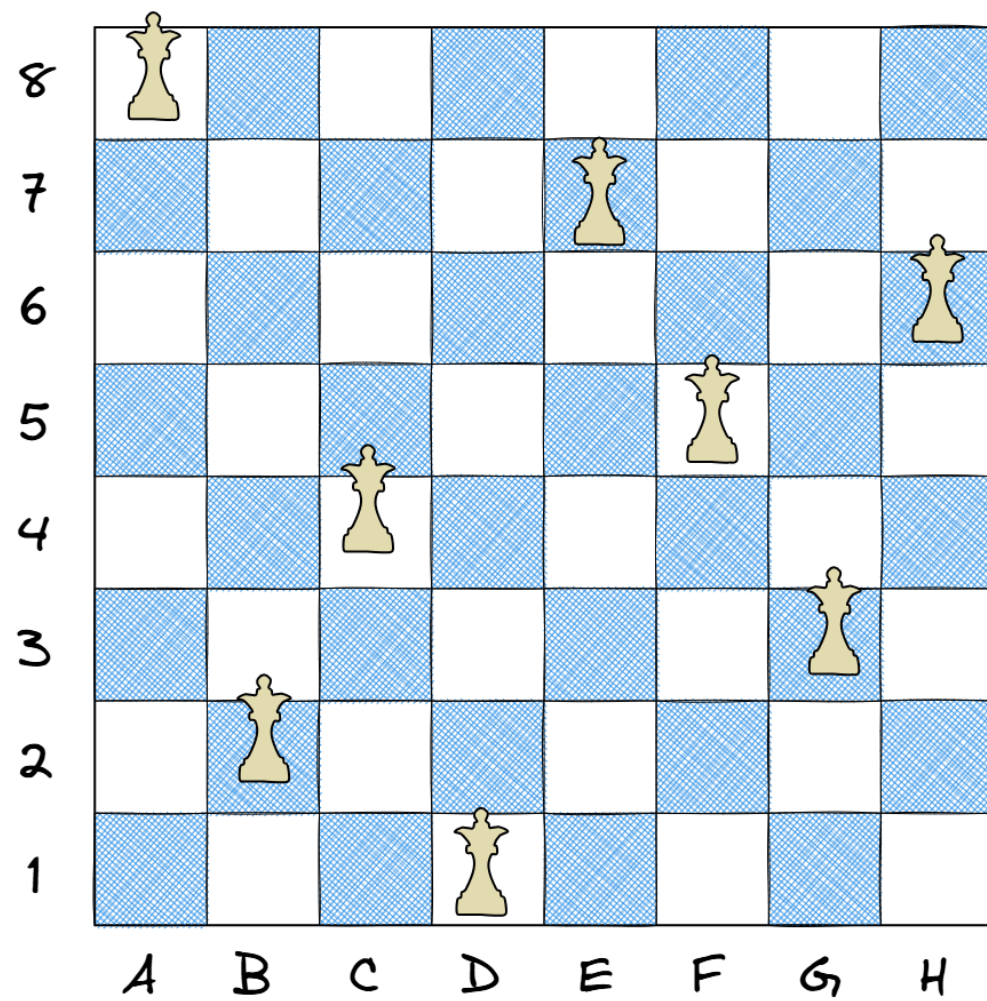
Celotna formula

$$\Phi_{\text{SAT}} = \mathbf{ALO_P} \wedge \mathbf{AMO_P} \wedge \mathbf{AMO_T}$$

Termin t	Največ ena
B	$(\neg X_{1,B} \vee \neg X_{2,B}) \wedge (\neg X_{1,B} \vee \neg X_{4,B}) \wedge (\neg X_{2,B} \vee \neg X_{4,B})$
C	$(\neg X_{2,C} \vee \neg X_{3,C})$
D	$(\neg X_{3,D} \vee \neg X_{4,D})$
F	$(\neg X_{1,F} \vee \neg X_{3,F}) \wedge (\neg X_{1,F} \vee \neg X_{4,F}) \wedge (\neg X_{3,F} \vee \neg X_{4,F})$



N-kraljic



SAT kraljice

1. spremenljivke q_{ij} (kraljica je na polju ij)
2. vsaka vrstica $ALO \wedge AMO$
3. vsak stolpec $ALO \wedge AMO$
4. vsaka diagonalna AMO

Cook-Levinov izrek

- Stephen Cook (1971): The complexity of theorem proving procedures
- Leonid Levin (1973):
Универсальные задачи перебора



Izrek. SAT je NP -poln

Obstaja veliko formulacij tega izreka, ta je verjetno najbolj kompaktna.

Oris dokaza

1. $SAT \in NP$

2. $\forall A \in NP : A \leq_p SAT$

◦ $(M_A, w) \rightarrow \Phi$, če stroj M_A sprejme w , $\Phi \in SAT$

Znaki v tabeli

$$\Phi_{cell}$$

- $C = \Gamma \cup Q \cup \{\#\}$
- spremenljivke $x_{i,j,c}$: na poziji i, j v tabeli je znak $c \in C$
- v vsaki celici je natanko en znak iz C

$$ALO \wedge AMO$$

Začetni trenutni opis

$$\Phi_{start} = x_{1,1,\#} \wedge x_{1,2,q_0} \wedge x_{1,3,w_1} \wedge x_{1,4,w_2} \wedge \dots \wedge x_{1,n+2,w_n} \wedge x_{1,n+3,\#}$$

Detekcija sprejetja besede

$$\Phi_{accept} = \bigvee_{i,j} x_{i,j,q_F}$$

Veljavna okna

$$\delta(q, a) = \{(r, b, R)\}$$

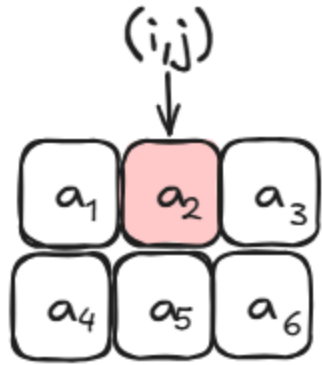
x	q	a
x	b	r

x	y	q
x	y	b

a	y	x
r	y	x

x	y	z
x	y	z

$$\Phi_{move} = \bigwedge_{(i,j)} (i, j) \text{ je eno izmed veljavnih oken}$$



$$\bigvee_{a \text{ je veljavno okno}} x_{i,j-1,a_1} \wedge x_{i,j,a_2} \wedge x_{i,j+1,a_3} \wedge x_{i+1,j-1,a_4} \wedge x_{i+1,j,a_5} \wedge x_{i+1,j+1,a_6}$$

Konční izraz

$$\Phi_{cell} \wedge \Phi_{start} \wedge \Phi_{accept} \wedge \Phi_{move}$$

Analiza pravilnosti

1. Prva vrstica je veljaven trenutni opis
2. vrstica i je veljaven trenutni opis $\implies$ vrstica $i + 1$ je veljaven **naslednji** trenutni opis

Analiza časovne zahtevnosti

$$t(n) = n^k, |C| = l$$

1. Število spremenljivk $(n^k)^2 \times l = O(n^{2k})$
2. velikost $\Phi_{cell} = O(n^{2k})$
3. velikost $\Phi_{start} = O(n^k)$
4. velikost $\Phi_{accept} = O(n^{2k})$
5. velikost $\Phi_{move} = O(n^{2k})$

3SAT (koliko lahko problem poenostavimo)

1. Oblika KNO

$$\bigwedge c_i, c_i = l_1 \vee l_2 \vee \dots \vee l_k$$

2. Oblika 3-KNO

$$\bigwedge c_i, c_i = l_1 \vee l_2 \vee l_3$$

Prevedba

$$\Phi \rightarrow \Phi'$$

- Φ je v KNO
- Φ' je v 3-KNO

$$c_i = l_1 \vee l_2 \vee \dots \vee l_k$$

1. $k = 1$

2. $k = 2$

3. $k > 3$

$$k = 1$$

$$c_i = l_1$$

vpeljemo dve novi spremenljivki s_1 in s_2 n c_i nadomestimo z

$$c'_i = (l_1 \vee s_1 \vee s_2) \wedge (l_1 \vee s_1 \vee \overline{s_2}) \wedge (l_1 \vee \overline{s_1} \vee s_2) \wedge (l_1 \vee \overline{s_1} \vee \overline{s_2})$$

$$k = 2$$

$$c_i = l_1 \vee l_2$$

vpeljemo eno novo spremenljivko s_1 in c_i nadomestimo z

$$(l_1 \vee l_2 \vee s_1) \wedge (l_1 \vee l_2 \vee \overline{s_1})$$

$$k > 3$$

$$c_i = l_1 \vee l_2 \vee \dots \vee l_k$$

vpeljemo $k - 3$ novih spremenljivk $s_1, \dots, s_{k-3}$

$$c'_i = (l_1 \vee l_2 \vee s_1) \wedge (\overline{s_1} \vee l_3 \vee s_2) \wedge (\overline{s_2} \vee l_3 \vee s_3) \wedge \dots \wedge (\overline{s_{k-4}} \vee l_{k-2} \vee s_{k-3}) \wedge (\overline{s_{k-3}} \vee l_{k-1} \vee l_k)$$

Primer

$$\Phi = (x \vee y \vee z \vee w) \wedge (\overline{x} \vee y)$$

Zakaj ne 2-SAT?

Problem neodvisne množice

$$INDSET = \{\langle G, k \rangle, G \text{ ima neodvisno množico velikosti } k\}$$

INDSET je *NP*-poln problem

Prevedba

$$3SAT \leq_p INDSET$$

Vhod je Φ z m klavzulami, izhod je $\langle G, k \rangle$.

1. za vsako klavzulo naredimo 7 vozlišč v G (vsak)
2. vozlišča iz iste klavzule povežemo med sabo (7 klika)
3. med klavzulami povežemo vozlišča, ki predstavljajo protislovne dodelitve
4. iščemo neodvisno množico velikosti m

Vhod: $G = \langle E, V \rangle, k$

Vprašanje: Ali obstaja $V' \subseteq V, |V'| \geq k,$

$$\forall u, v \in V' : v \neq u, (u, v) \in E$$

Prevedba $3SAT$ na $Clique$

Vhod: $\Phi = C_1 \wedge C_2 \wedge \dots \wedge C_m$

$$C_i = (\ell_{i1} \vee \ell_{i2} \vee \ell_{i3})$$

Izhod: $G = (V, E), m$

$$V = \{v_{ij} \mid \ell_{ij} \text{ j-ti literal klavzule } C_i\}$$

$$E = \{ \{v_{ij}, v_{pq}\} \mid i \neq p \text{ in } \ell_{ij} \neq \neg \ell_{pq} \}.$$

Primer

$$\varphi = (x_1 \vee \neg x_2 \vee x_3) \wedge (\neg x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee x_2 \vee \neg x_3)$$

Izrek

$$\Phi \in 3SAT \iff \langle G, k \rangle \in Clique$$



Formula ima dodelitev spremenljivkam, da je vrednost formule 1.

1. V vsaki klavzuli je vsaj en literal 1, v klico izberemo pripadajoče vozlišče grafa (imamo torej m vozlišč)
2. Vsa vozlišča so povezana med sabo, ker vsa pripadajo različnim klavzulam in noben par ni $(x, \neg x)$

Imamo torej klico velikosti m



Graf ima kliko velikosti m

1. vsak par vozlišč pripada različnim klavzulam (vsaka klavzula ima natanko eno vozlišče v kliku)
2. x in $\neg x$ nista istočasno v nobeni kliku, zato lahko dodelimo vrednost 1 vsem vozliščem (literalom)

Vrednost izraza pri tej dodelitvi je 1