

NP - polnost

Uroš Čibej



Pregled

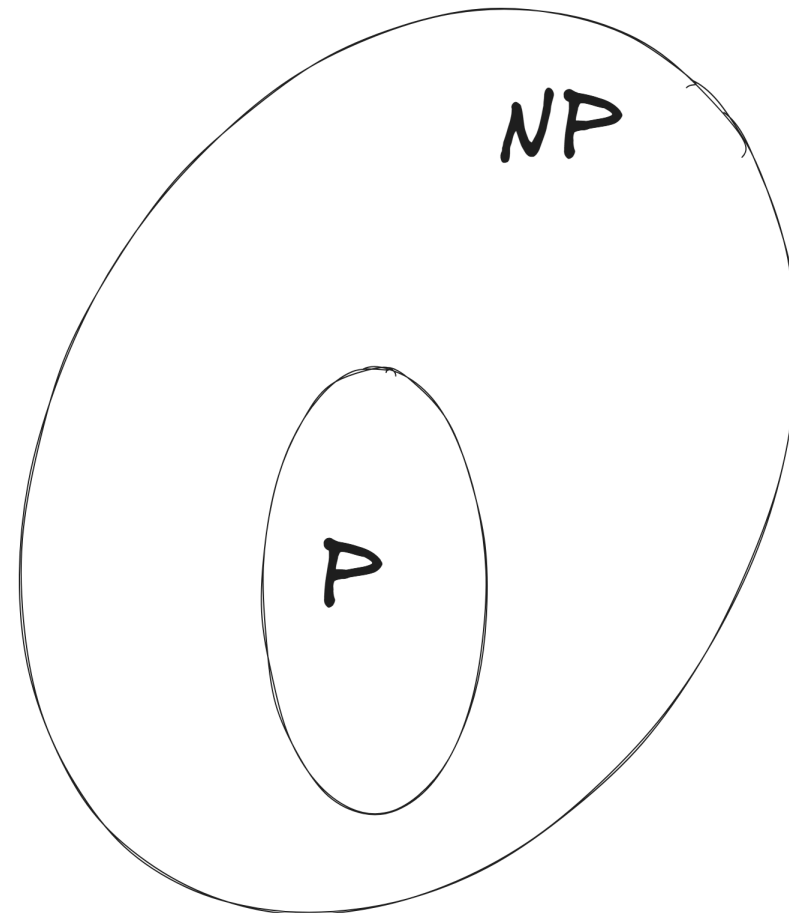
- Polinomske prevedbe
- NP -polnost
- Modeliranje s SAT
- Cook-Levinov izrek

Literatura

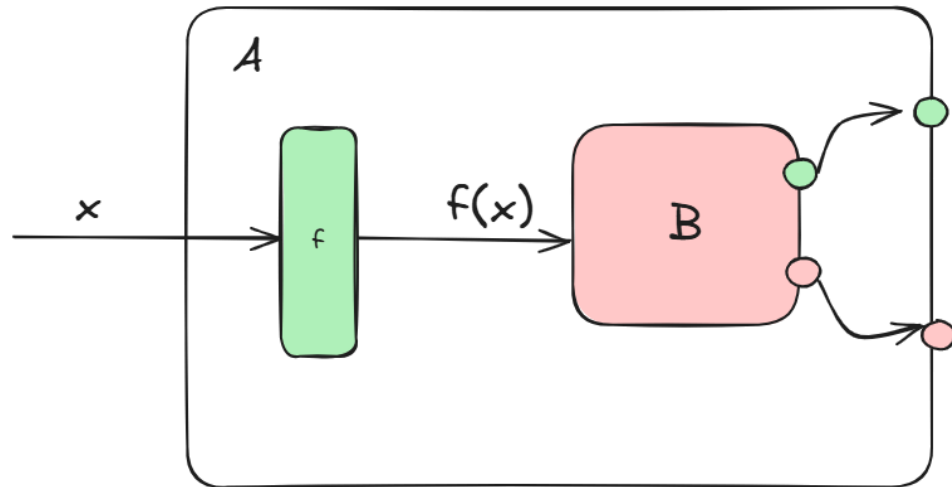
- Sipser razdelek 7

Ponovimo: $P \stackrel{?}{=} NP$

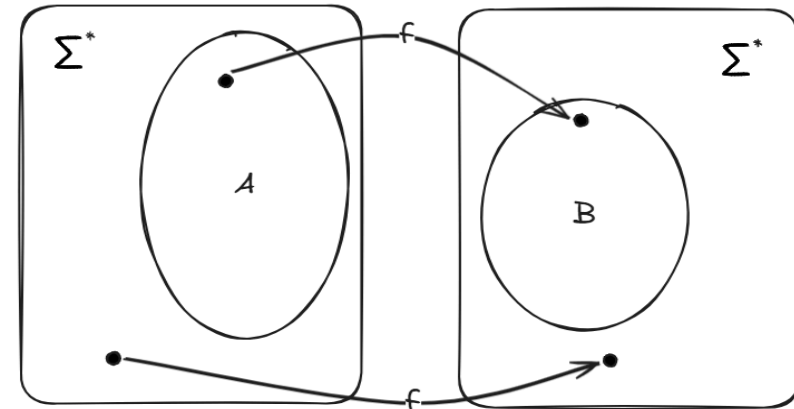
- Ali je preverjanje rešitve enako zahtevno kot generiranje rešitve?
- Ali je izčrpno preiskovanje (eksponentno) edini pristop, ki deluje za določene vrste problemov?
- Se moramo pri določenih problemih zadovoljiti z neoptimalnimi rešitvami?



Polinomske prevedbe

 \leq_p


$A \leq_p B : w \in A \iff f(w) \in B$
 f mora biti polinomsko izračunljiva funkcija



Posledica polinomske prevedbe

$$A \leq_p B \wedge B \in P \implies A \in P$$

Koncept NP -polnosti

Problem B je NP -poln, če

1. $B \in NP$

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

Izrek. Če B je NP -poln in $B \in P \implies P = NP$

Problem SAT (satisfiability)

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

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

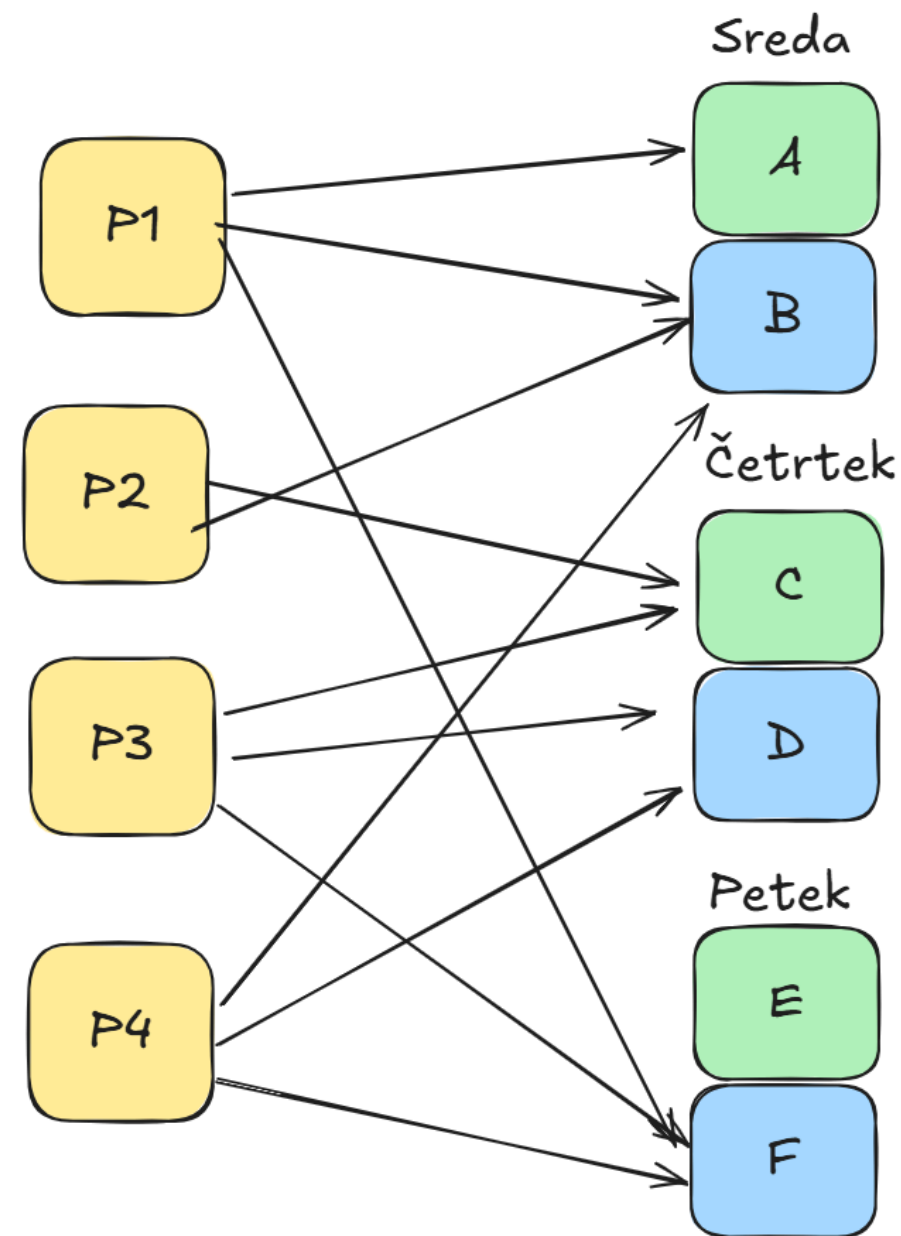
Primer

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

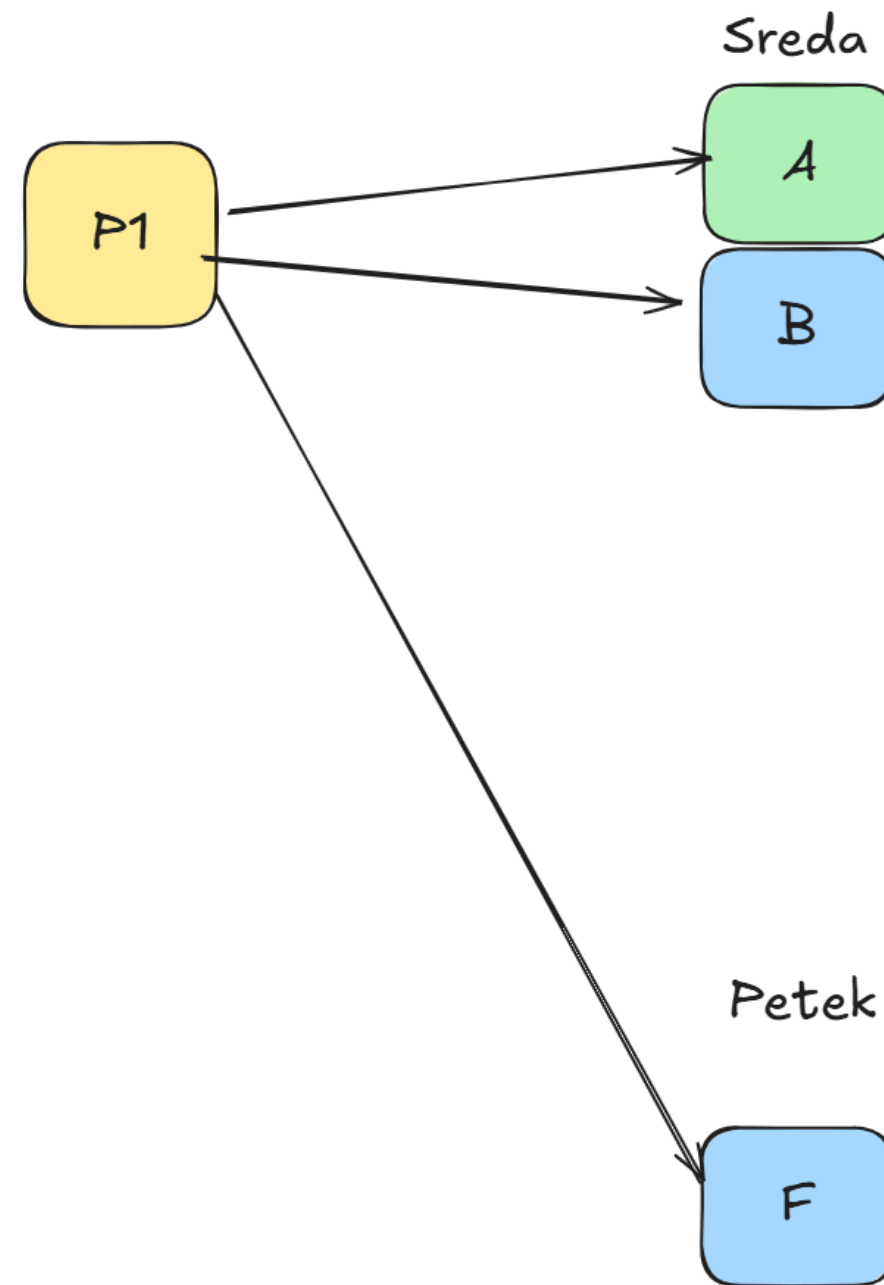
Modeliranje s SAT

"Urnik"

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



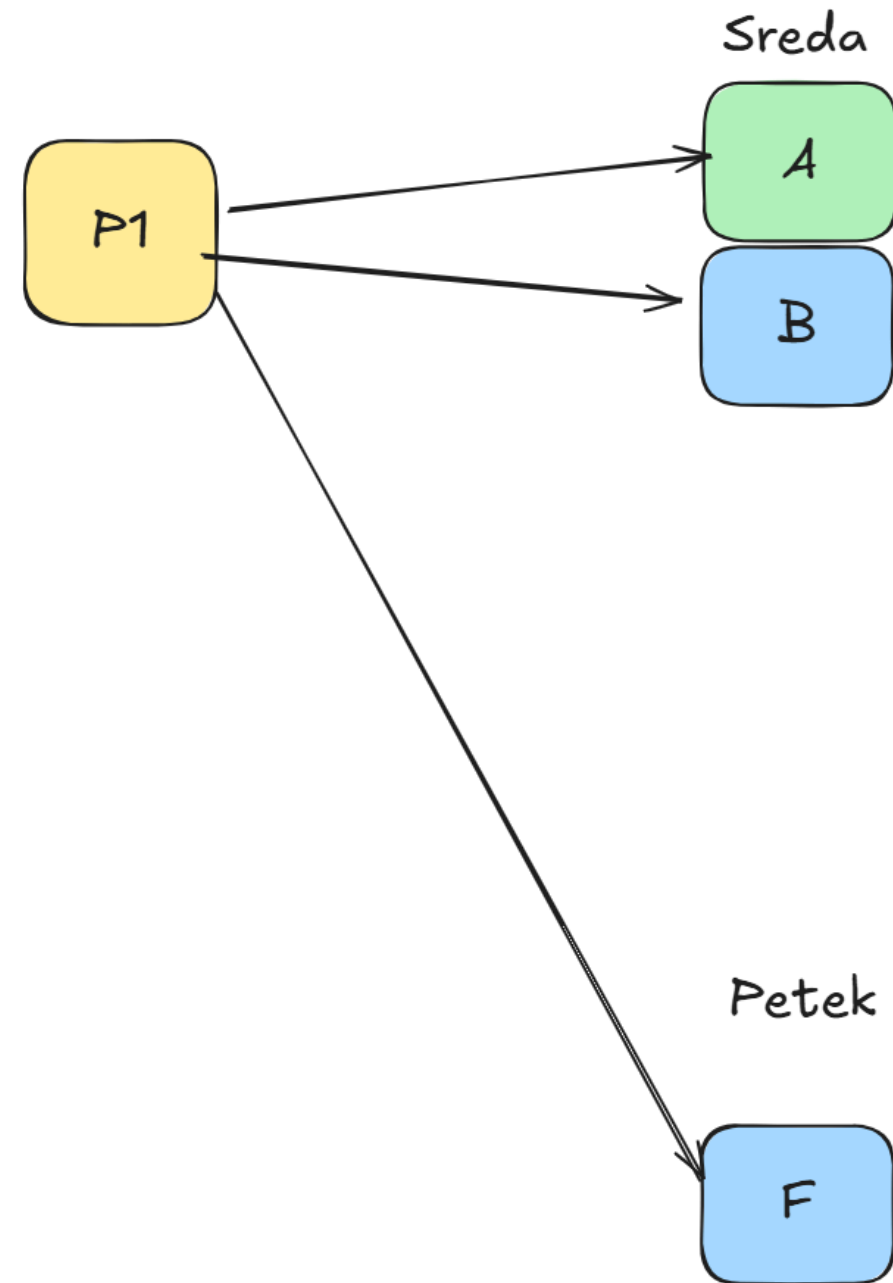
Vsaj ena
(At Least One)



Vsaj ena

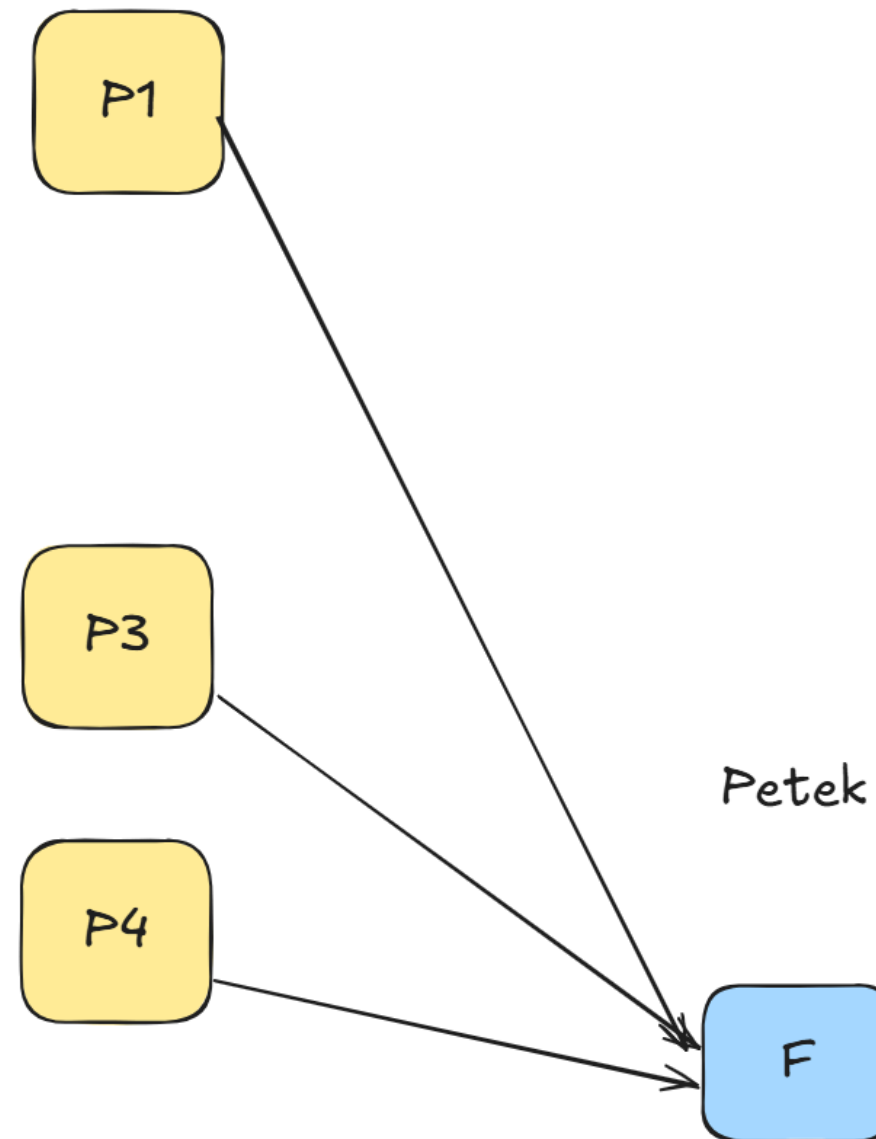
(At Least One)

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



Največ ena

(At Most One)



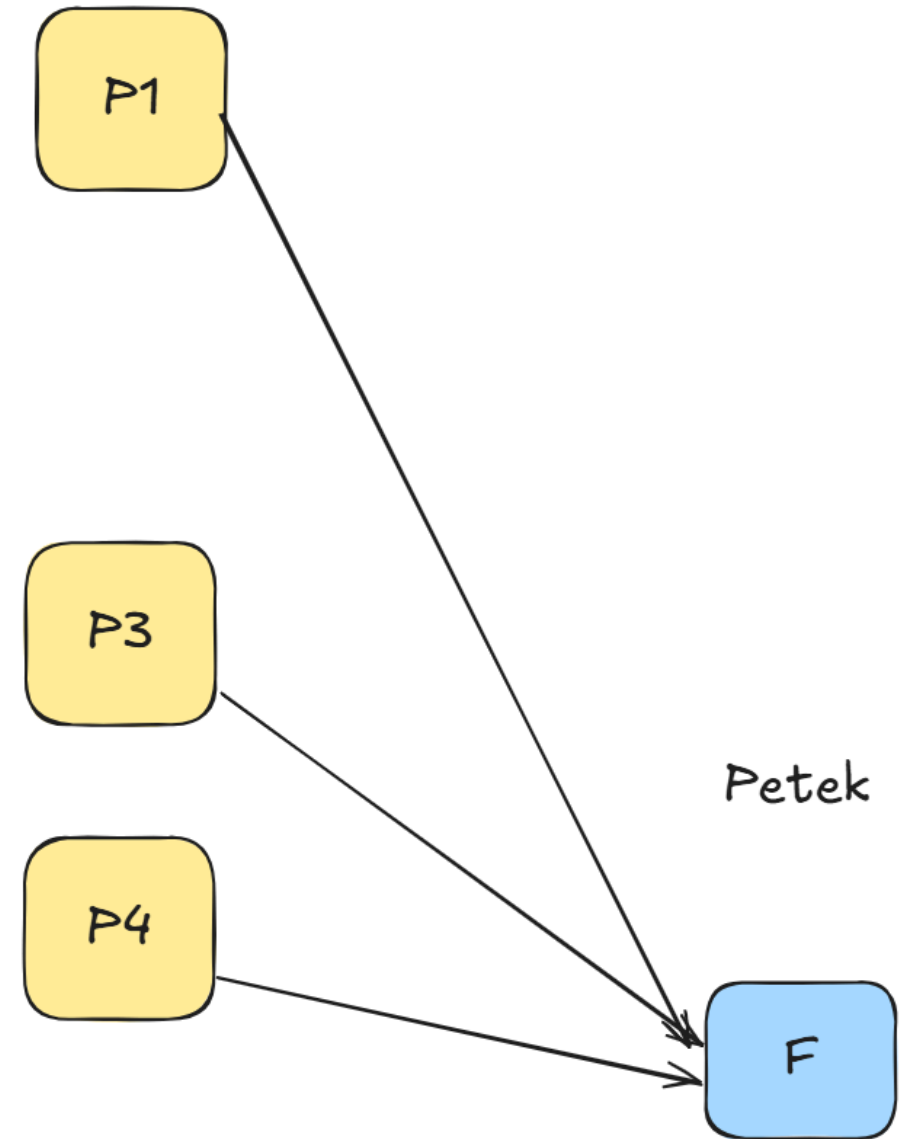
Največ ena

(At Most One)

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

V KNO

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

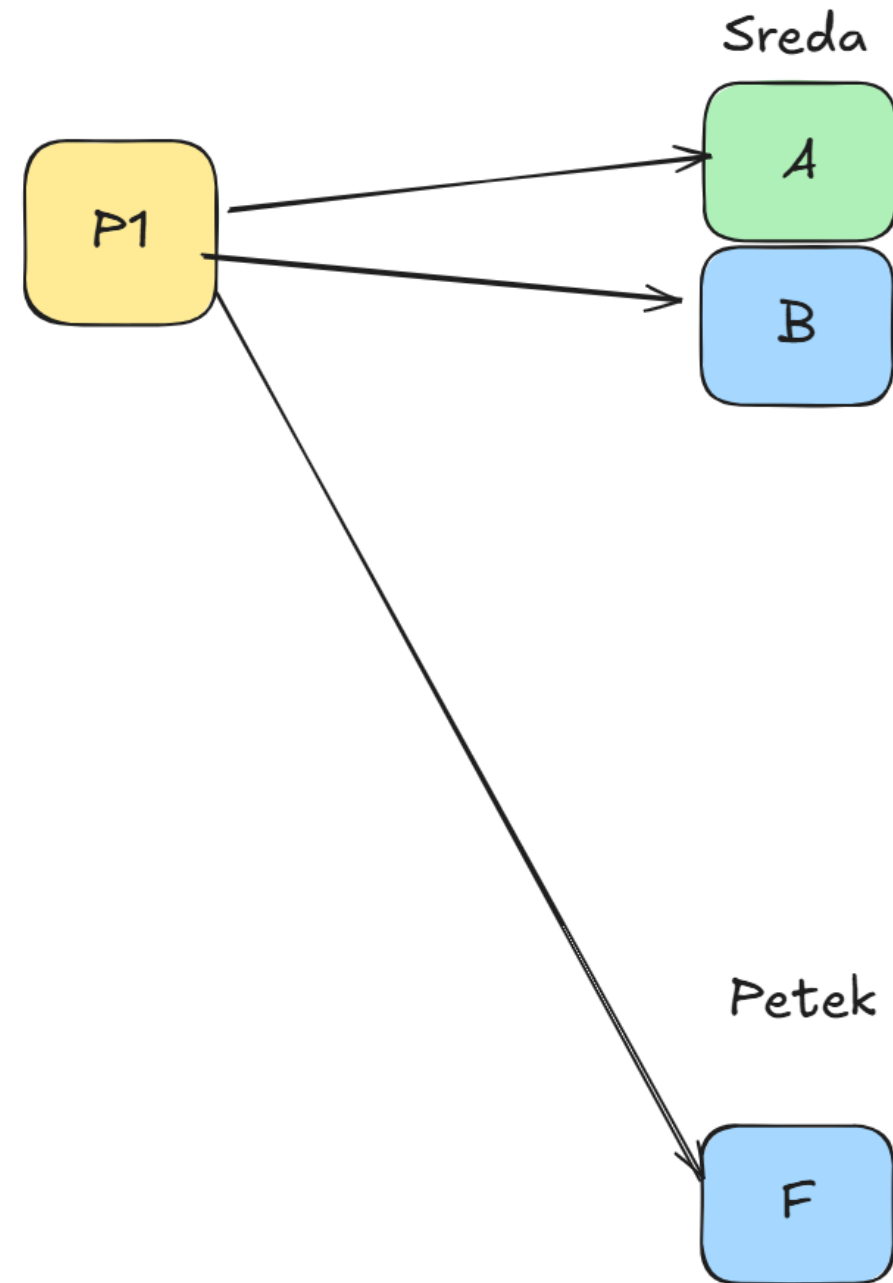


Natanko ena

vsaj ena in največ ena

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

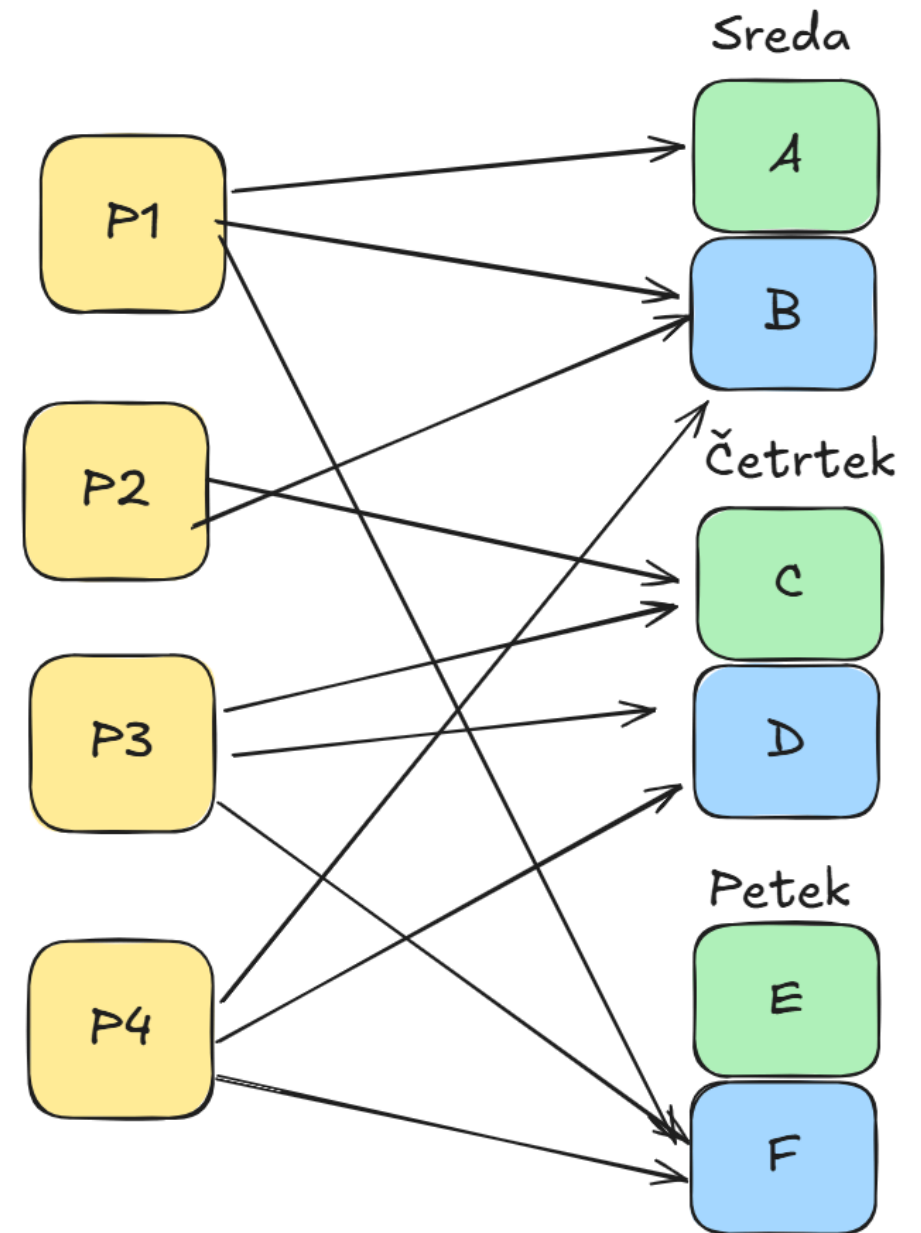
$$(\neg X_{1A} \vee \neg X_{1B}) \wedge (\neg X_{1A} \vee \neg X_{1F}) \wedge (\neg X_{1B} \vee \neg X_{1F})$$



Celotna formula

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

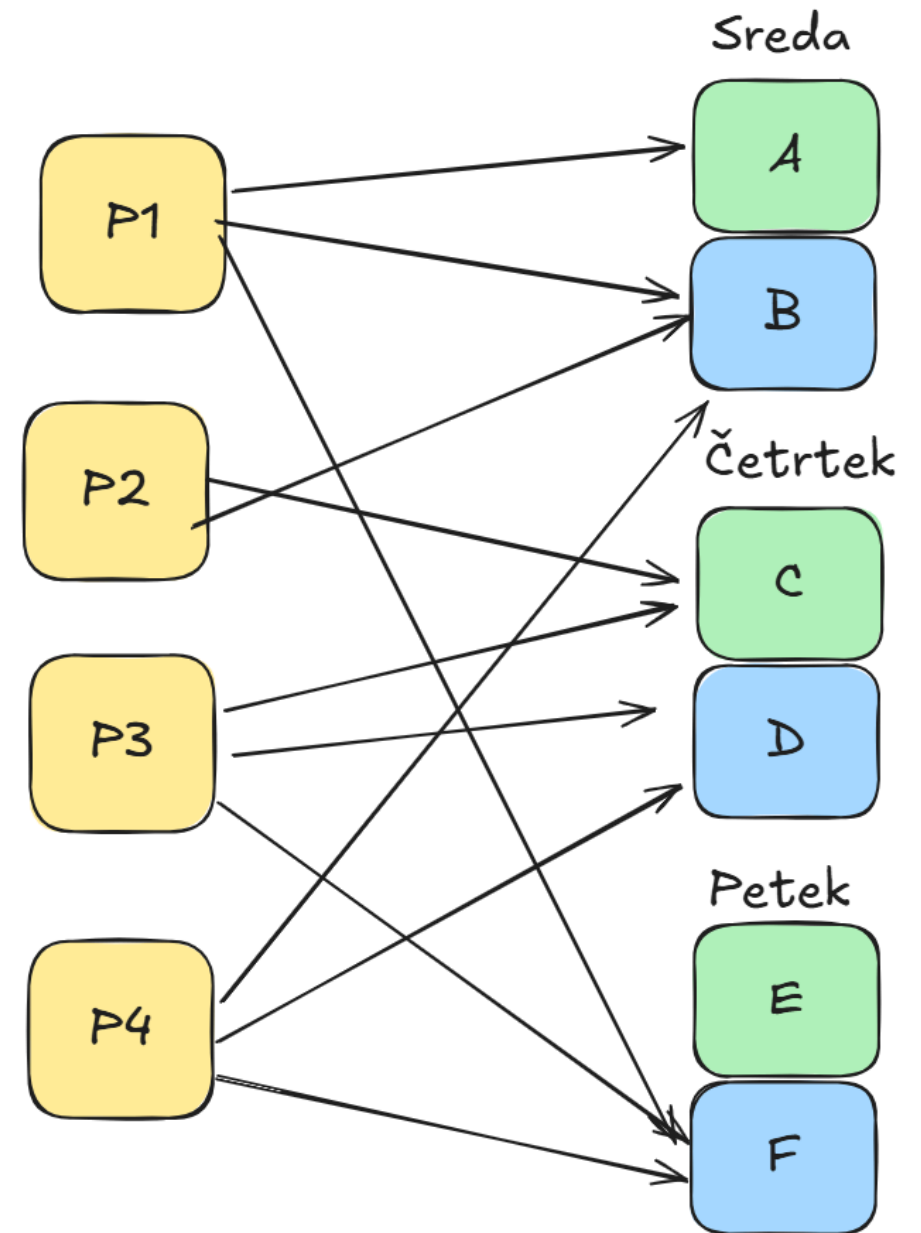
| P_i | vsaj eden |
|-------|-------------------------------------|
| P_1 | $X_{1,A} \vee X_{1,B} \vee X_{1,F}$ |
| P_2 | $X_{2,B} \vee X_{2,C}$ |
| P_3 | $X_{3,C} \vee X_{3,D} \vee X_{3,F}$ |
| P_4 | $X_{4,B} \vee X_{4,D} \vee X_{4,F}$ |



Celotna formula

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

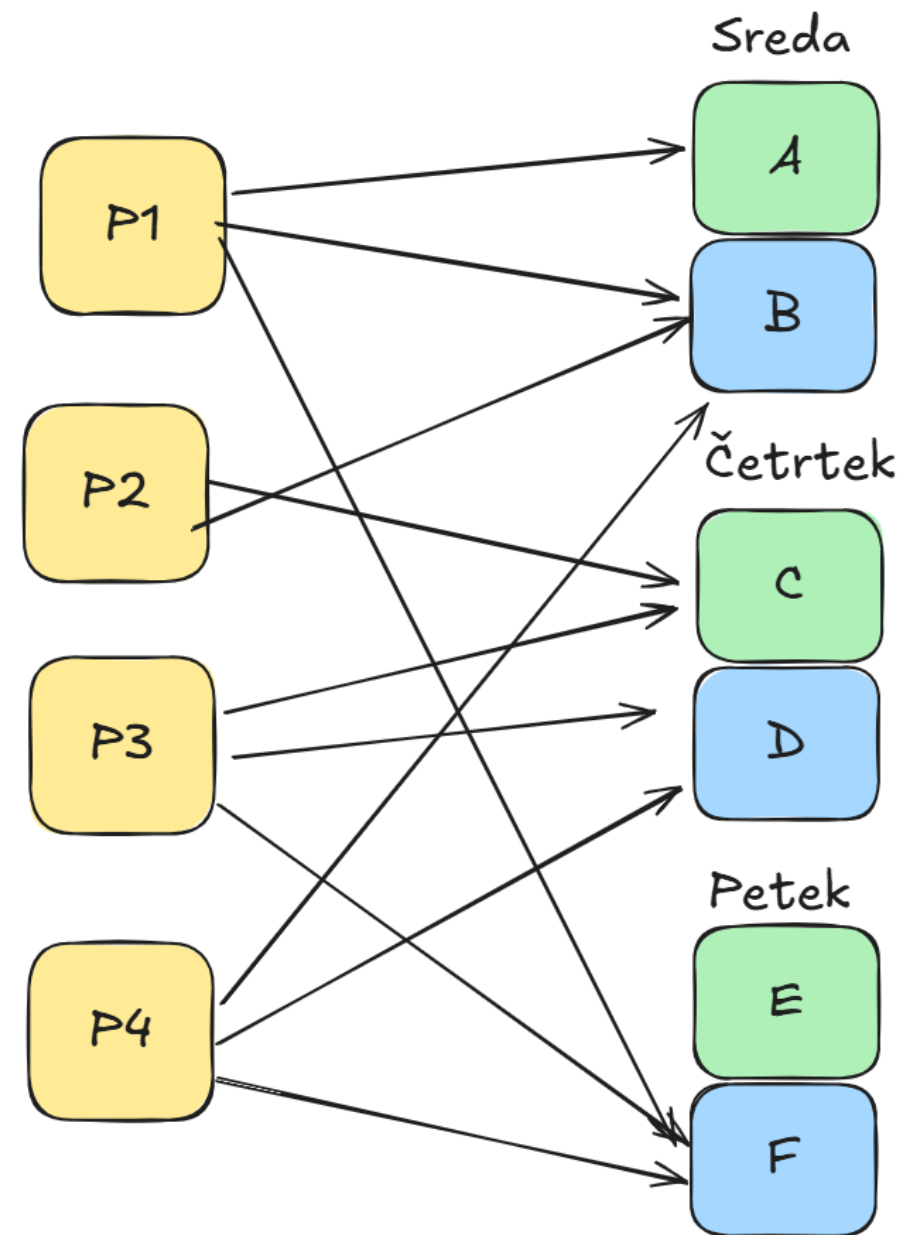
| P_i | <i>Največ en</i> |
|-------|--|
| P_1 | $(\neg X_{1,A} \vee \neg X_{1,B}) \wedge (\neg X_{1,A} \vee \neg X_{1,F}) \wedge (\neg X_{1,B} \vee \neg X_{1,F})$ |
| P_2 | $(\neg X_{2,B} \vee \neg X_{2,C})$ |
| P_3 | $(\neg X_{3,C} \vee \neg X_{3,D}) \wedge (\neg X_{3,C} \vee \neg X_{3,F}) \wedge (\neg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



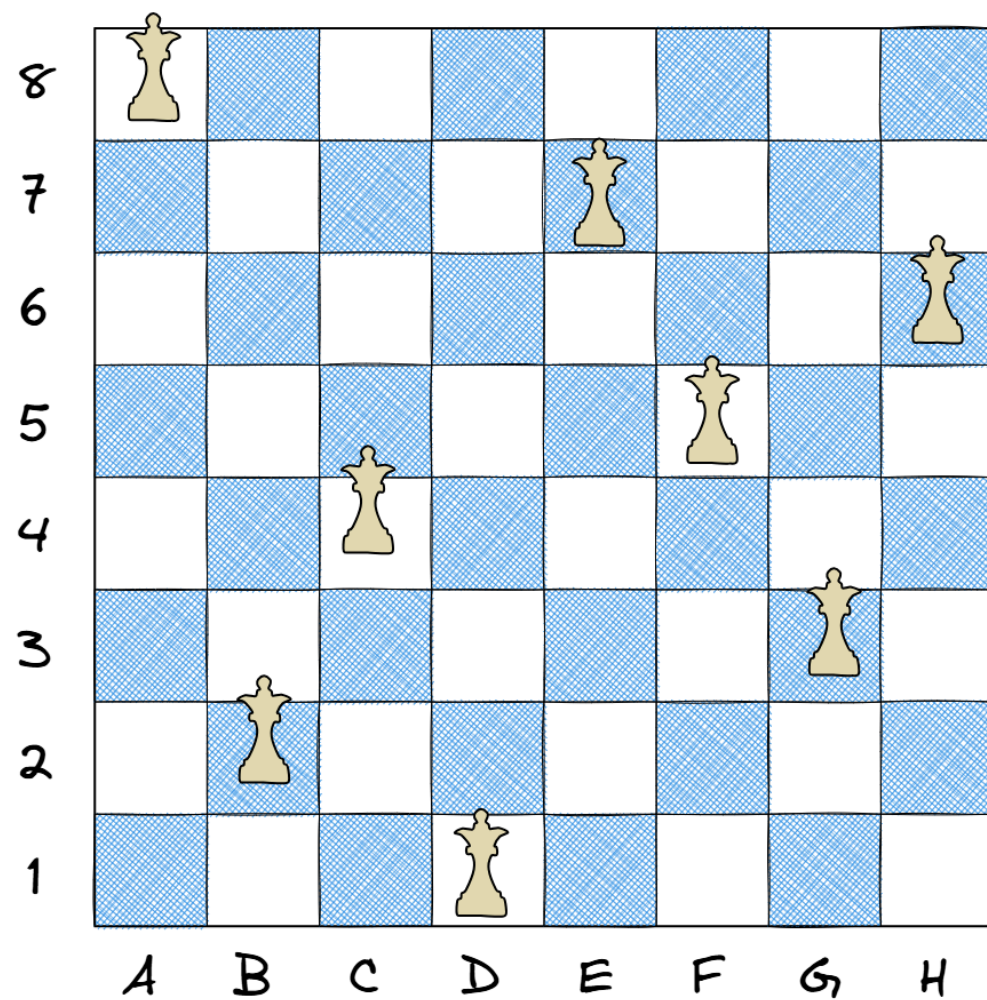
Celotna formula

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

| 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

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

Veljavna okna

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

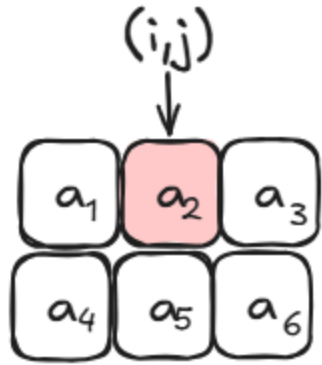
| | | |
|---|---|---|
| x | q | a |
| x | b | r |

| | | |
|---|---|---|
| x | y | q |
| x | y | b |

| | | |
|---|---|---|
| a | y | x |
| r | y | x |

| | | |
|---|---|---|
| x | y | z |
| x | y | z |

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



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

Končni 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 $\Phi_{move} = O(n^{2k})$

Stanje vprašanje $P = NP$?

- večina problemov $p \in (NP \setminus P)$ je tudi NP -polnih (naslednjič)
- **ogromno** poskusov za razreševanje tega vprašanja (naključnost, aproksimacija, vezja, preroki, ...)
- seveda je trenutni konsenz $P \neq NP$, ampak nekaj optimizma kljub temu ostaja