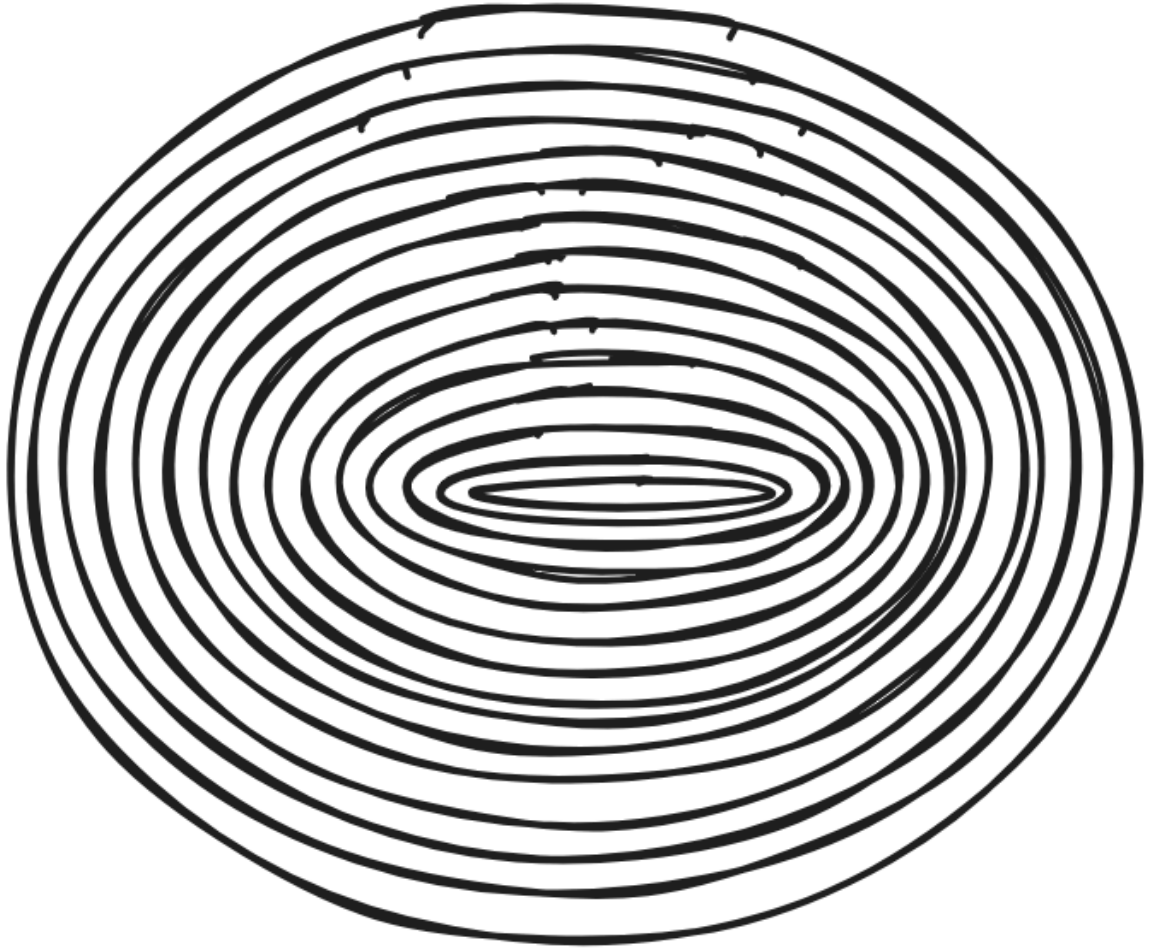
coNP in polinomska hierarhija

Uroš Čibej



Pregled snovi

1. Definicija $coNP$
2. $coNP \cap NP$
3. Osnovni pojmi PH

Preverjanje

- učinkovito preverjanje (dokazovanje) $x \in L$
- učinkovito preverjanje (dokazovanje) $x \notin L$?

UNSAT

$UNSAT = \{\phi \mid \phi \text{ ni izpolnljiva formula } \}$

$UNSAT = \overline{SAT} \in NP$?

(asimetrija v definiciji NP)

Definicija $coNP$

$$coNP = \{L \mid \overline{L} \in NP\}$$

podobno bi lahko definirali coX, kjer je X poljubni razred
$coX = \{L \mid \overline{L} \in X\}$

$$SAT \in P \iff UNSAT \in P$$

$SAT \leq_p UNSAT$?

$$coNP \neq \overline{NP}$$

$$coNP \cap NP \neq \emptyset$$

Primeri:

$$\emptyset$$

$$\Sigma^*$$

coP?

izrek: P je zaprt za komplement

posledica: $P = NP \implies NP = coNP$

$coPSPACE$?

izrek: PSPACE je zaprt za komplement

posledica: $coNP \subseteq PSPACE$

Alternativni definiciji $coNP$

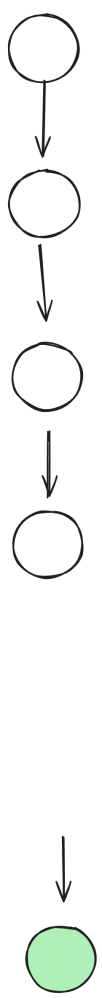
- definicija s preverjevalnikom
- računski model

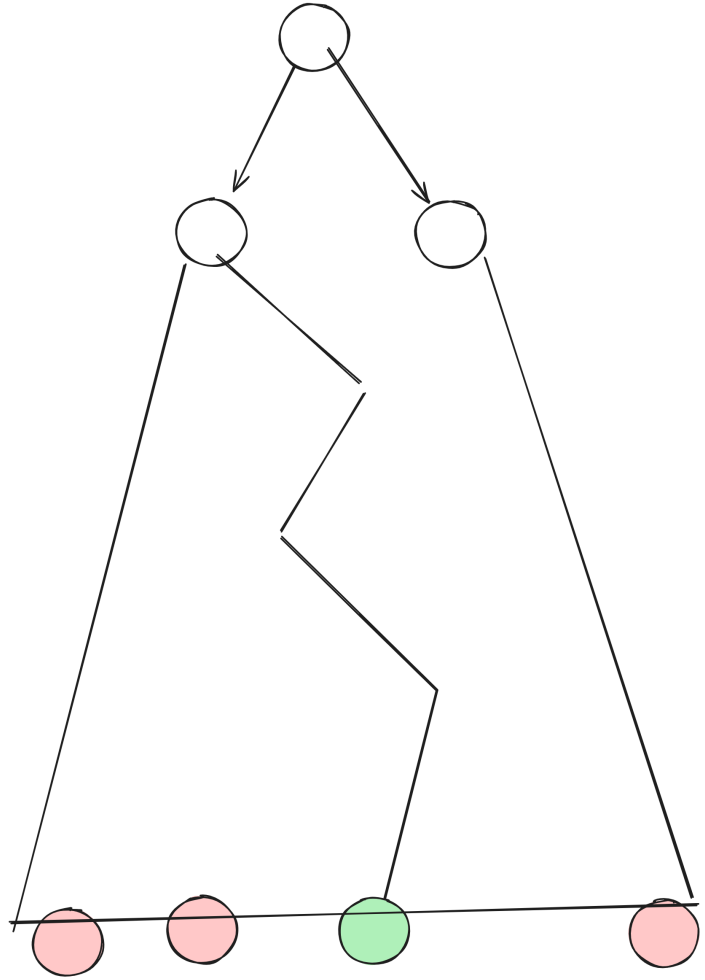
Polinomski preverjevalnik

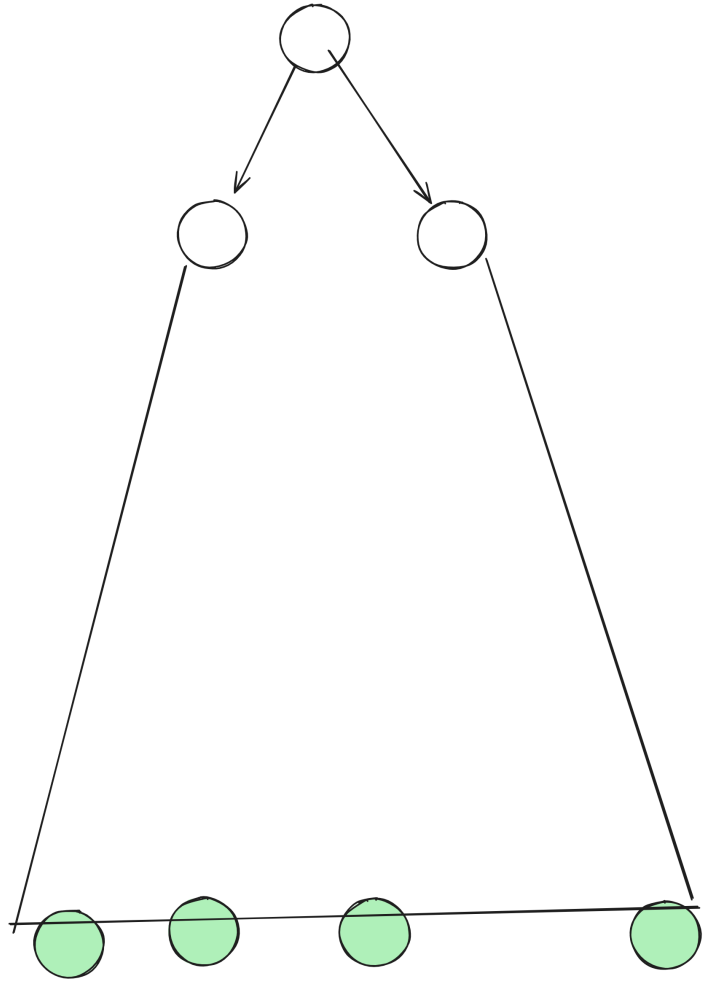
Jezik $L \in coNP$, če obstaja polinomski preverjevalnik V:

$$x \in L \iff \forall c, |c| = poly(|x|) : V(x, c)$$

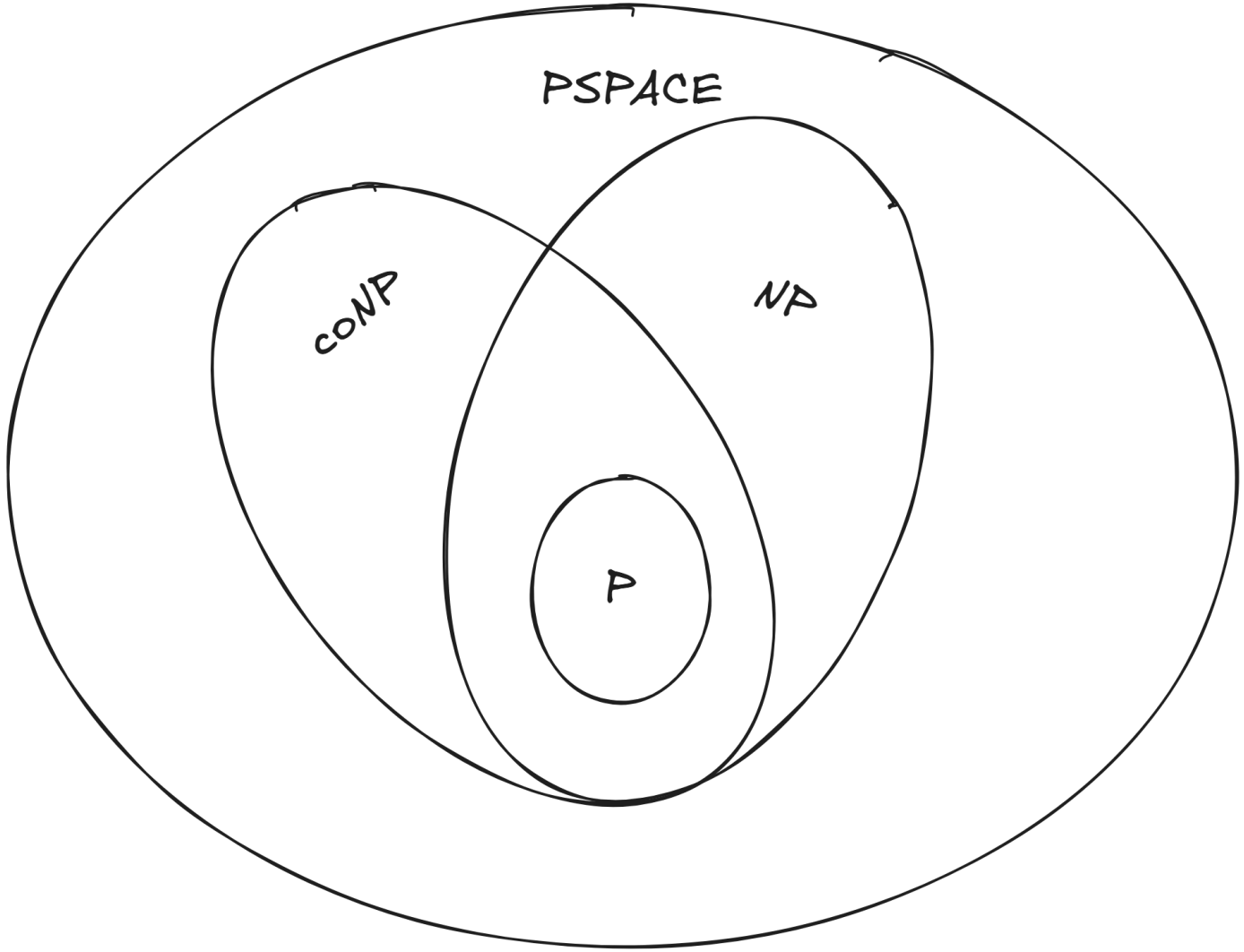
Računski model







Trenutni diagram



$coNP$ polnost

A je $coNP$ poln, če:

1. $A \in coNP$
2. $\forall B \in coNP : B \leq_p A$

Izrek:

$$A \in NPC \implies \overline{A} \in coNPC$$

Dokaz

1. $A \in NP \implies \overline{A} \in coNP$ (po definiciji)
2. obstaja prevedba f iz poljubnega $B \in NP$

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

   $$x \in \overline{B} \iff f(x) \in \overline{A}$$

Tavtologija

$$TAVT = \{\phi \mid \phi \text{ je resničen izraz za vse dodelitve vrednosti spremenljivk}\}$$

primer:

$(p \implies q) \implies (\neg p \vee q) \in TAVT$

$TAVT \in NP?$

$TAVT \in coNP?$

Praktična uporaba problema TAVT

- formalna verifikacija
- pravilnost vezij
- ekvivalenca vezij (pri optimizaciji)
- pravilnost protokolov
- varnost

$$NP \cap coNP$$

Popolno ujemanje

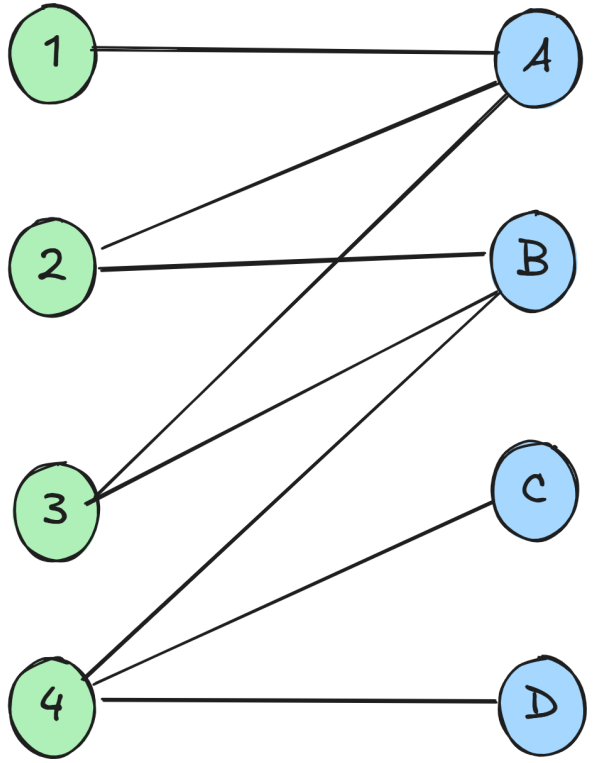
(v dvodelnem grafu)

Problem PM :

vhod: dvodelni graph $G = \langle U, V, E \rangle$

vprašanje: Ali v G obstaja popolno ujemanje?

Ali je $PM \in NP$?



Hallov izrek

Izrek: V dvodelnem grafu G obstaja popolno ujemanje $\iff \forall S \subseteq U : |S| \leq |N(S)|$

Kjer funkcija N vrne vse sosede vozlišč iz množice S.

Ali je $PM \in coNP$?

Linearno programiranje

$$LP = \{\langle A, b\rangle \mid \exists x \in \mathbb{R}^n : Ax \leq b\}$$

$$LP \in NP?$$

$$LP \in coNP?$$

Farkaseva lema

Sistem nima rešitve, če:

$\exists y \geq 0$

1. $A^T y = 0$
2. $b^T y < 0$

Praštevila

$$PRIMES = \{p \mid p \text{ je praštevilo } \}$$

$$PRIMES \in coNP?$$

$$PRIMES \in NP?$$

Prattov certifikat praštevilskosti

p je praštevilo $\iff \exists a$

1. $a^{p-1} \equiv 1 \pmod{p}$
2. za vsak praštevilski faktor q števila $p-1$ velja $a^{(p-1)/q} \not\equiv 1 \pmod{p}$

(ta dva pogoja lahko izračunamo v polinomskem času)

Faktorizacija

$$FAKT = \{\langle n, a, b\rangle \mid n \text{ ima praštevilski faktor na intervalu } [a, b]\}$$

$FAKT \in NP$? -

$FAKT \in coNP$

certifikat:

$$p_1, p_2, \ldots, p_k$$

praštevilski faktorji števila n

Uvod v polinomsko hierarhijo

Natančna klika

$$ECLIQ = \{\langle G, k\rangle \mid \text{največja klika ima velikost točno } k\}$$

Ali je $ECLIQ \in coNP$

Opis rešitve (dokaza) za $ECLIQ$

$$\exists S \subseteq V : |S| = k \text{ je klika } \wedge \forall S' \subseteq V, |S'| = k+1 \text{ ni klika}$$

Najmanjše vezje

$$SCIRC = \{\langle C \rangle \mid C \text{ je najmanjše vezje, ki računa } f_c\}$$

Opis rešitve (dokaza) za $SCIRC$

$$\forall C' : |C'| < |C|, \exists x : C'(x) \neq C(x)$$

Razred Σ_2^p

def. $L \in \Sigma_2^p$, če obstaja polinomski preverjevalnik V in polinom p, da velja

$$x \in L \iff \exists u_1 \forall u_2 : V(x, u_1, u_2) = 1$$

$|u_1|, |u_2| \leq p(|x|)$

Razred Π_2^p

def. $L \in \Pi_2^p$, če obstaja polinomski preverjevalnik V in polinom p, da velja

$$x \in L \iff \forall u_1 \exists u_2 : V(x, u_1, u_2) = 1$$

$|u_1|, |u_2| \leq p(|x|)$

coX

$$\Pi_2^p = co\Sigma_2^p$$

$ECLIQUE \in \Sigma_2^p$

Preverjevalnik implementiramo tako:

```
def V(x, u1, u2):
  if x!=G,k:
    return False
  if u1 ni k klika v G:
    return False
  if u2 je k+1-klika v G:
    return False
  return True
```

$SCIRC \in \Pi_2^p$

Preverjevalnik implementiramo tako:

```
def V(x, u1, u2):
  if x ni veljavno vezje:
    return False
  if u1 ni veljavno vezje:
    return True
  C = x
  C' = u1
  if C(u2)!=C'(u2):
    return True
  return False
```

Posplošitev

Σ	Π
$\Sigma_0^p = P$	$\Pi_0^p = P$
$\Sigma_1^p = NP$	$\Pi_1^p = coNP$
$\Sigma_2^p = \exists\forall P$	$\Pi_2^p = \forall\exists P$
$\Sigma_3^p = \exists\forall\exists P$	$\Pi_3^p = \forall\exists\forall P$

$$\Sigma_i^p = \exists\Pi_{i-1}^p$$
$$\Pi_i^p = \forall\Sigma_{i-1}^p$$

Osnovna dejstva

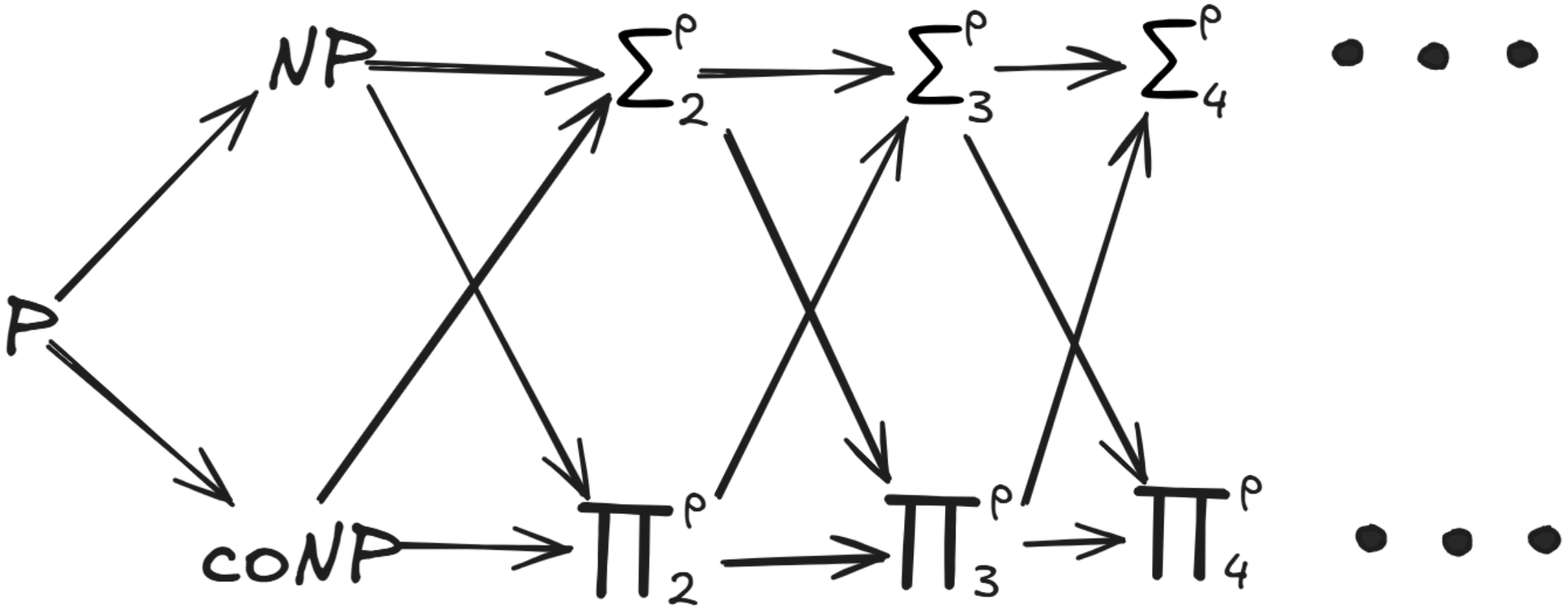
$$\Sigma_i^p \subseteq \Sigma_{i+1}^p$$
$$\Sigma_i^p \subseteq \Pi_{i+1}^p$$
$$\Pi_i^p \subseteq \Sigma_{i+1}^p$$
$$\Pi_i^p \subseteq \Pi_{i+1}^p$$

(ker en kvantifikator vedno lahko ignoriramo)

Polinomska hierarhija

$$PH = \bigcup_{i \geq 1} \Sigma_i^p = \bigcup_{i \geq 1} \Pi_i^p$$

Shema vsebovanosti

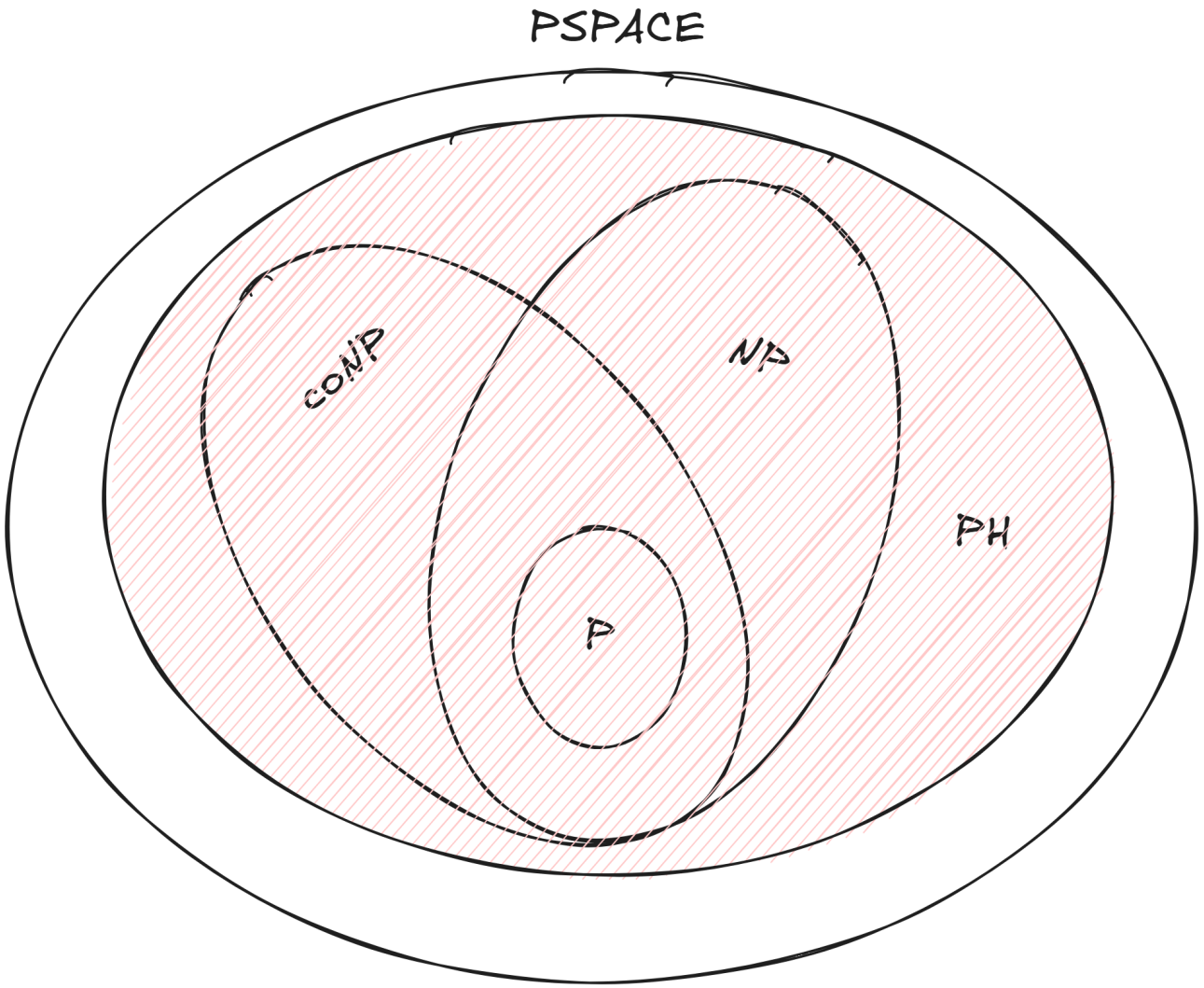


Relacija s prostorom

$$PH \subseteq PSPACE$$

"Dokaz": Preizkusimo vse možnosti za certifikate - poženemo preverjevalnik V. Prostor je ponovno uporabljen, zato ga porabimo samo polinomsko mnogo.

Nov diagram



Kolaps polinomske hierarhije

Izrek:

$$P = NP \implies P = PH$$

Kolaps do nivoja i

Izrek:

$$\Sigma_i^p = \Pi_i^p \implies PH = \Sigma_i^p$$