

$$\textcircled{7} \text{ Factors} = \{ \langle n \rangle \mid \exists_{x_1 \dots x_n} : x_1^{a_1} * \dots * x_n^{a_n} = n \} \quad \rightarrow x_1 \dots x_n \leq n$$

$$\text{Factorization} = \{ \langle n \rangle \mid \exists p : 1 < p < n \wedge n \% p = 0 \}$$

$$\text{Factorization-D} = \{ \langle n, x \rangle \mid \exists p : 1 < p < x \wedge n \% p = 0 \}$$

\downarrow
 $1 \leq x \leq n$

a) Factorization-D is NP and co-NP

Verificador NP: donat n i x . Verificador co-NP:

input n, x {

Si $n \% x = 0$

return TRUE

else

return FALSE

}

\Rightarrow idem amb $\begin{cases} \text{TRUE} \\ \text{FALSE} \end{cases}$

b) Si $P=NP$, demostra que Factorization $\in FP$ (computable a temps polinomial)

Factorization $\in NP$, si provem que també és NP-hard, llavors com $P=NP$, Factorization és FP, ja que podem reduir en temps P a l'algorisme que resol en temps P .

Factorization \leq_P^P SAT:

Factorization $\xrightarrow{\quad} \text{SAT}$

$N \in \mathbb{Z}$

:

$$F = \bigwedge_{i=1}^{(n)} C_i$$

$$C_i = \{x_2 \dots x_n\}$$

$$C_i = \begin{cases} x_a \vee x_b & \text{si } a * b = N \\ \neg x_a \vee \neg x_b & \text{si } a * b \neq N \end{cases} \quad \begin{matrix} a, b \in \\ [2, n] \end{matrix}$$

Output: p or PRIME

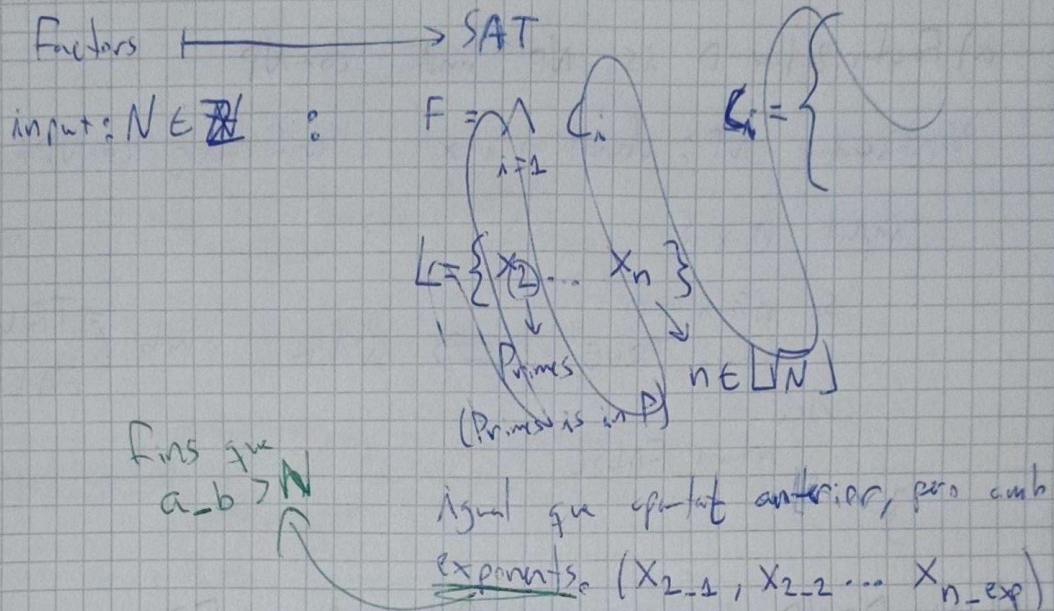
: Output: $X_{min} = 1$ or UNSAT

Cost: $O\left(\binom{n}{2}\right) \approx O(n^2)$, que és P

Correctesa: No se'com demostrar-ho

c) Si $P=NP$, FACTORS \in FP

Razonament similar a apartat b), si reduïm Factors a SAT, que és NP-complet, llavors com $P=NP$, existeix un algoritme polinàmic que redueix NP a P, per tant, redueix ~~SAT~~ a Factors a FP.



Un cop resolt el SAT, l'output és una llista de tots els literals = 1 amb l'exponent més gran