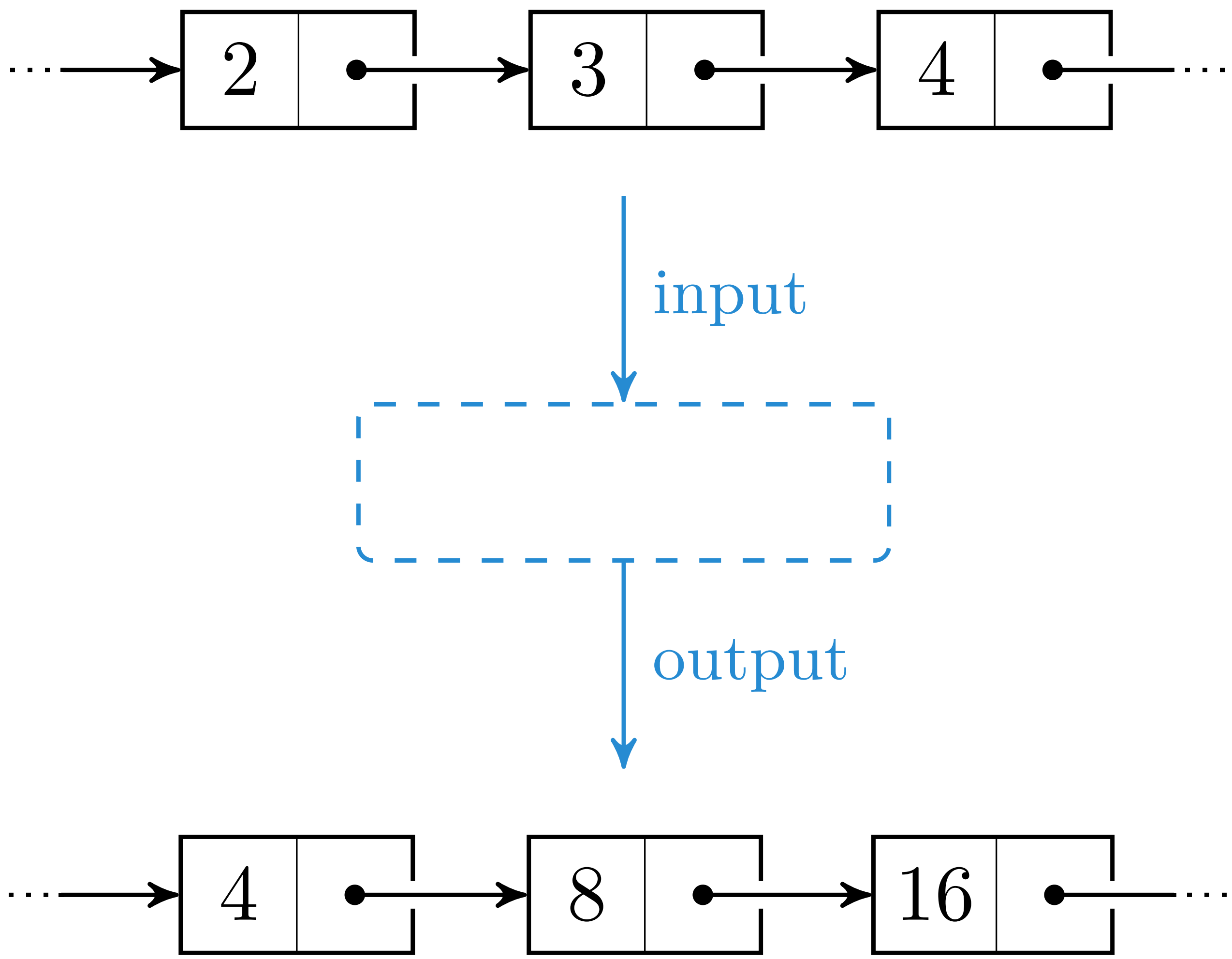
Forelesning 13

NP-kompletthet

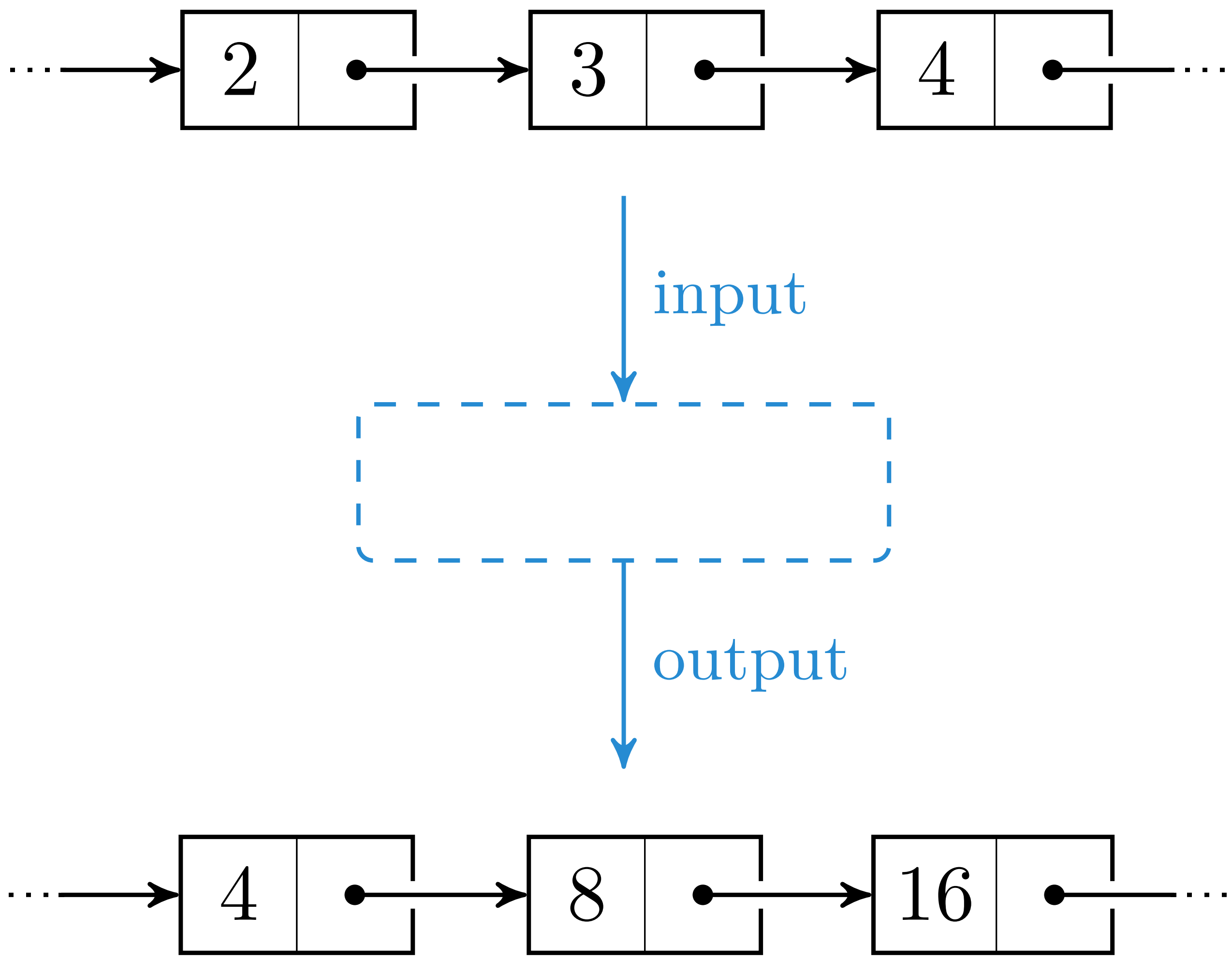
1. **Problemer**
2. **Reduksjoner**
3. **Kompletthet**

1:4

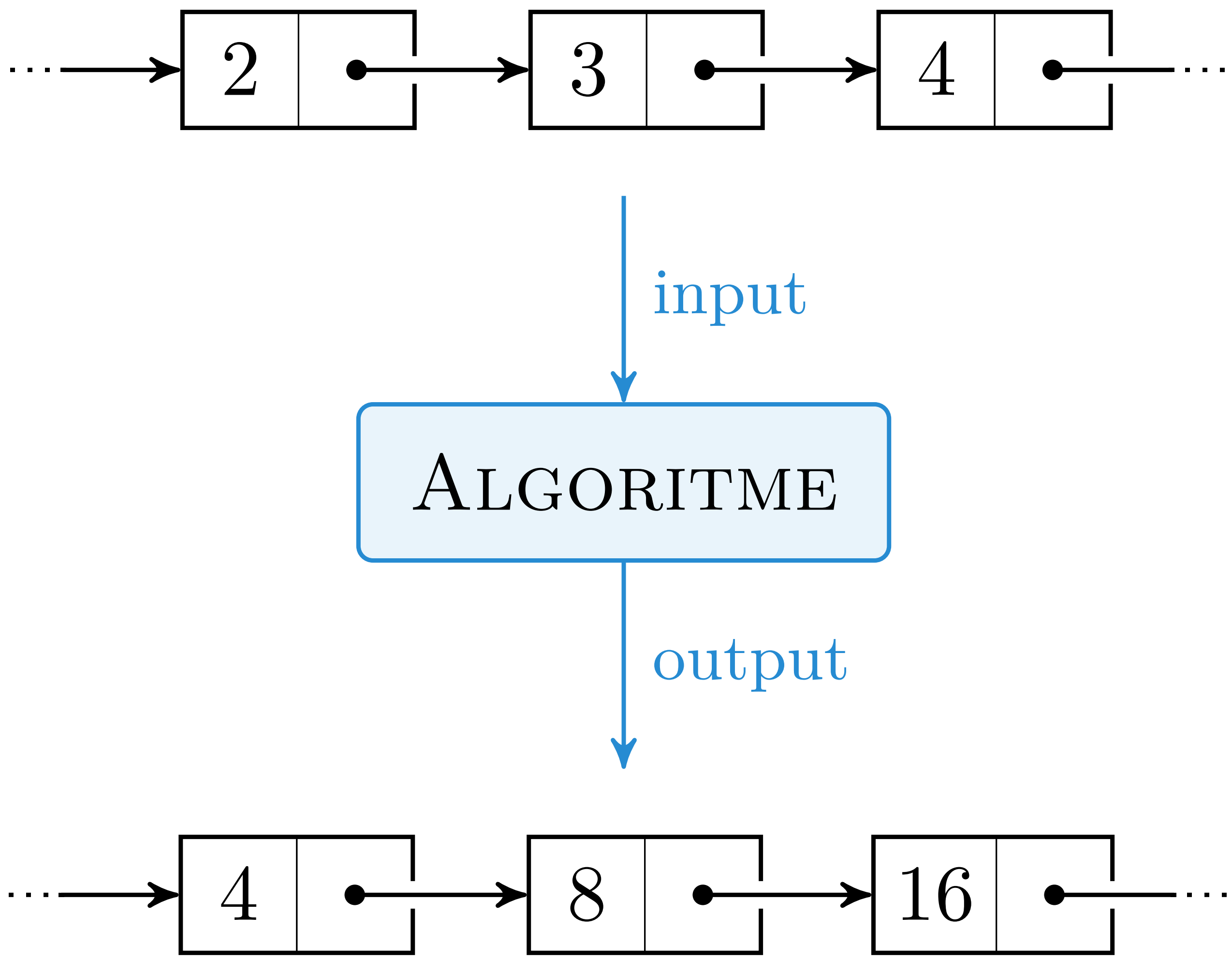
Problemer



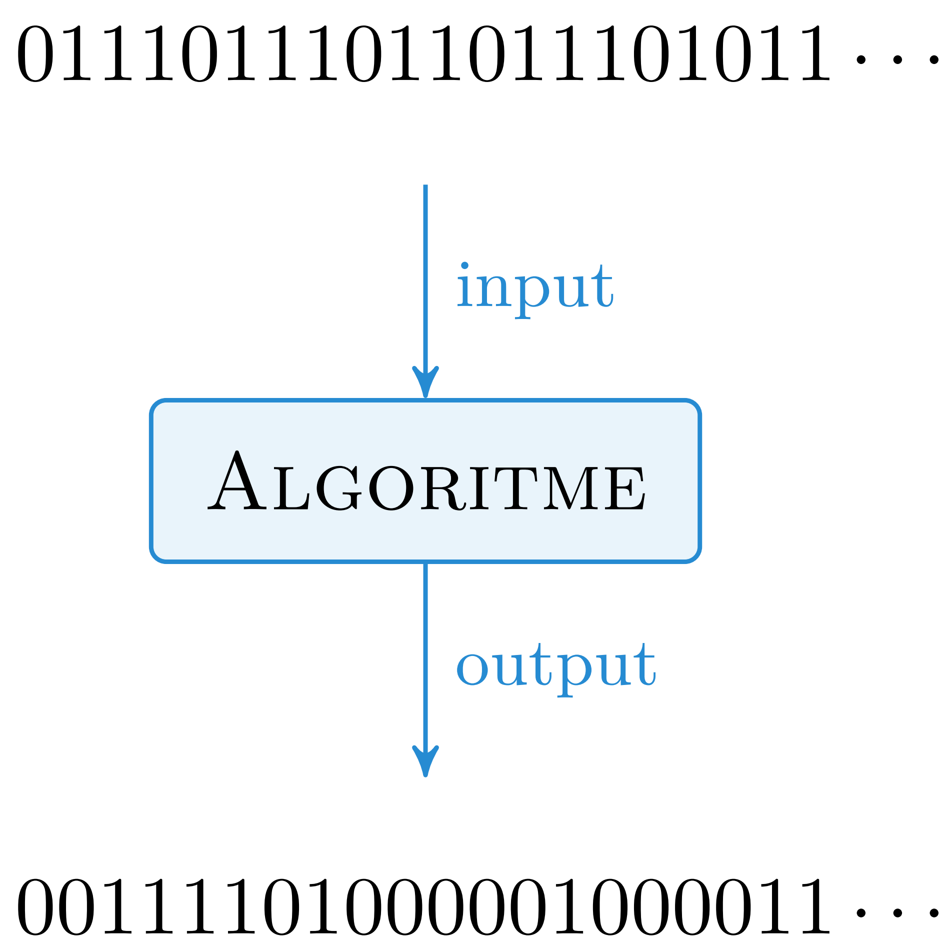
Et problem er en relasjon mellom input og output



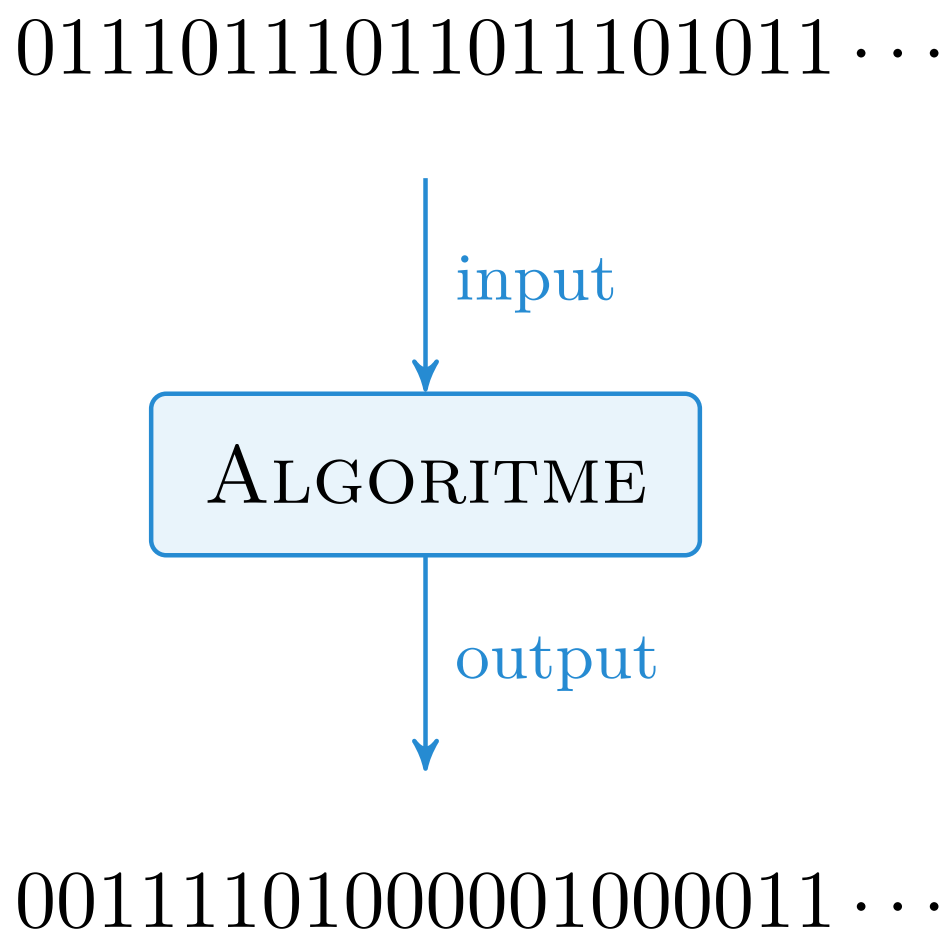
Input og output kan være vilkårlige abstrakte objekter



Jobben vår er å produsere gyldig output

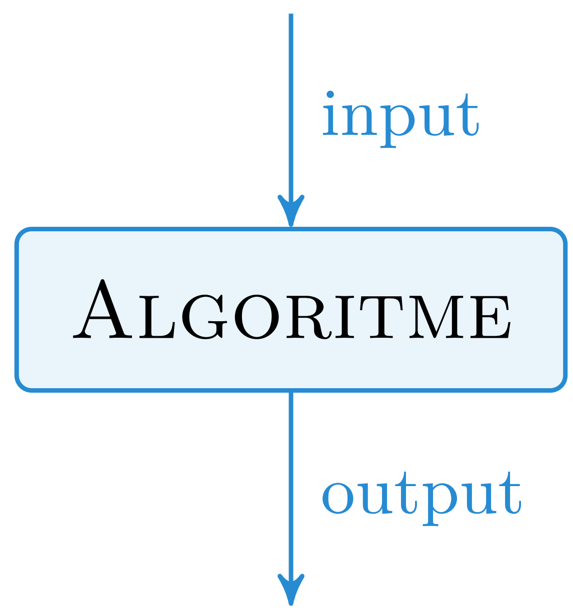


Et problem kalles <u>konkret</u> hvis input og output er bitstrenger



Vi koder instanser og resultater som bits

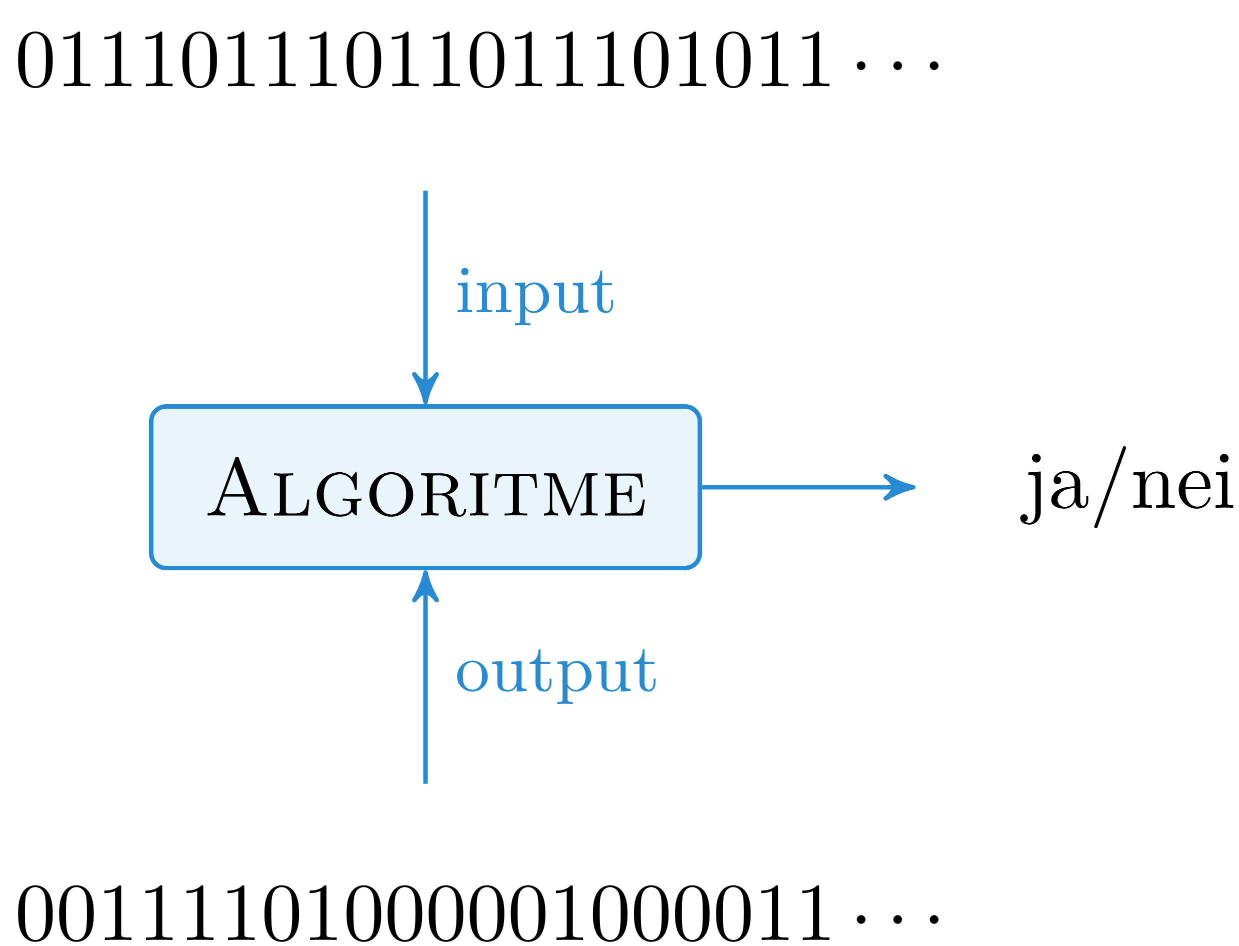
$$0111011101101110\,1011\cdots$$



$$0011110100000100\,0011\cdots$$

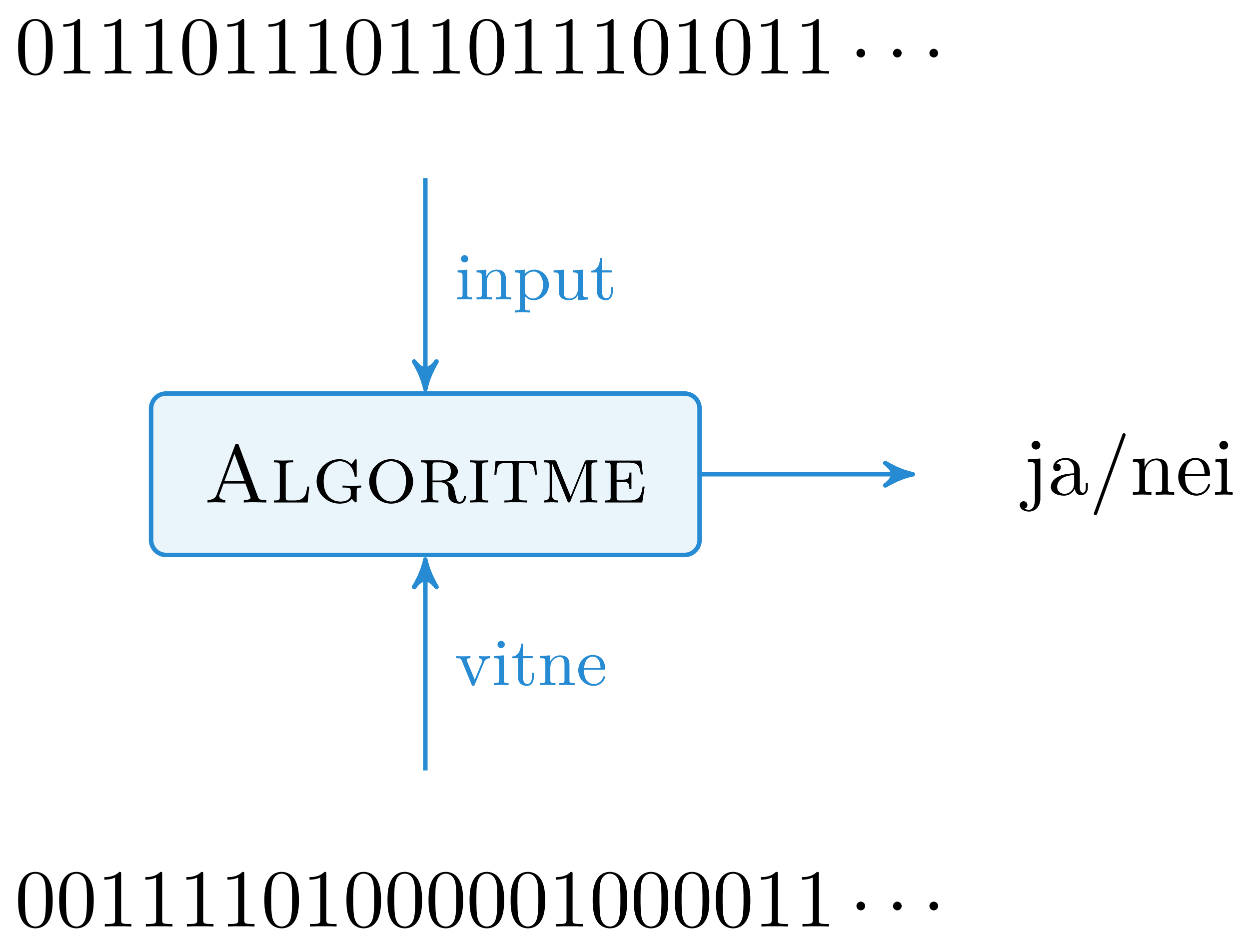
Egentlig ikke så viktig; vi vil bare forenkle «universet» vårt

Og … vi kan da tenke oss at det kanskje ikke *finnes* noen gyldig løsning.

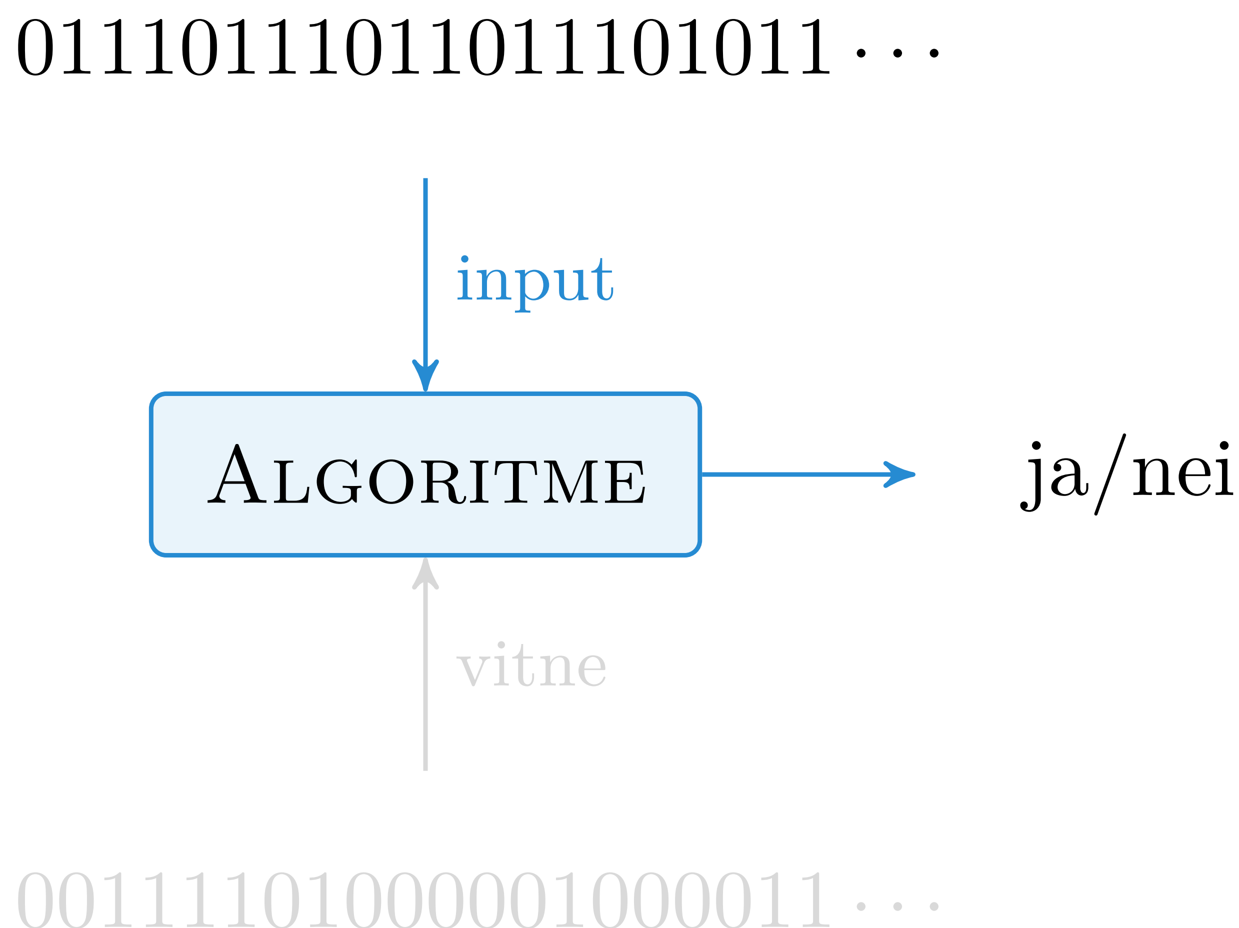


En verifikasjonsalgoritme sjekker om en løsning stemmer

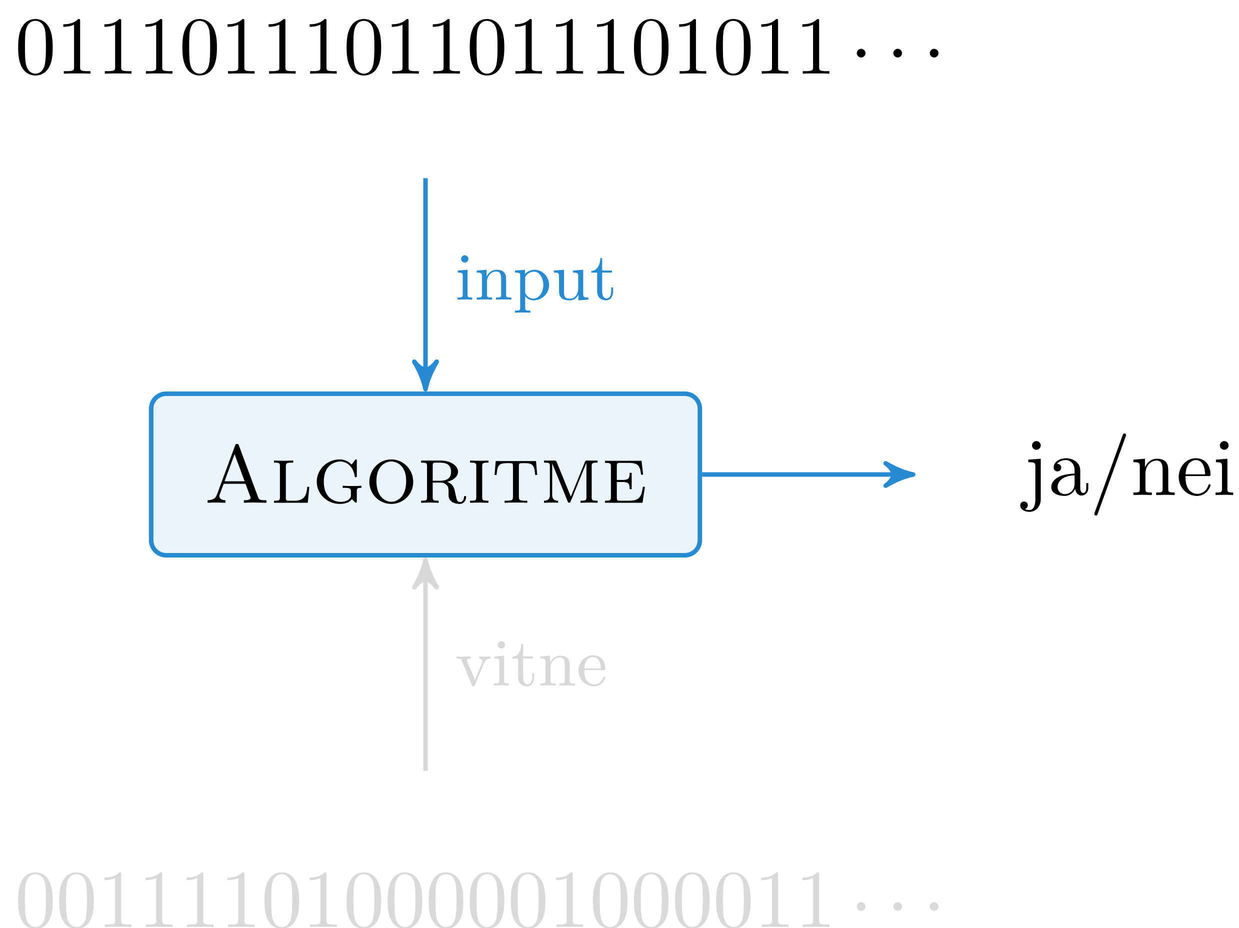
Kanskje vanligere perspektivt: Vi stiller et ja/nei-spørsmål, og hvis svaret er ja, så er sertifikatet et «bevis» for det. (Vi kan også ha sertifikat for nei, eller bare for én av delene.)



Vi kaller da gjerne løsningen et «sertifikat» eller «vitne»



Et beslutningsproblem kan vi tenke på som å stille spørsmålet . . .



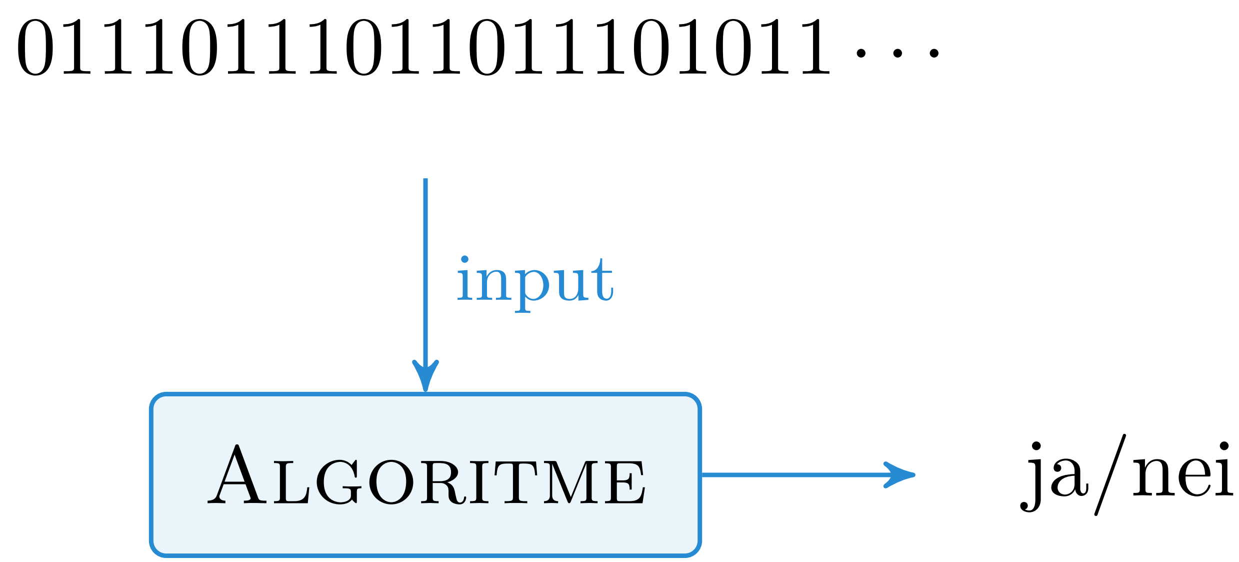
«Finnes det et vitne?»

0111011101101110101 1 · · ·

input

Algoritme → ja/nei

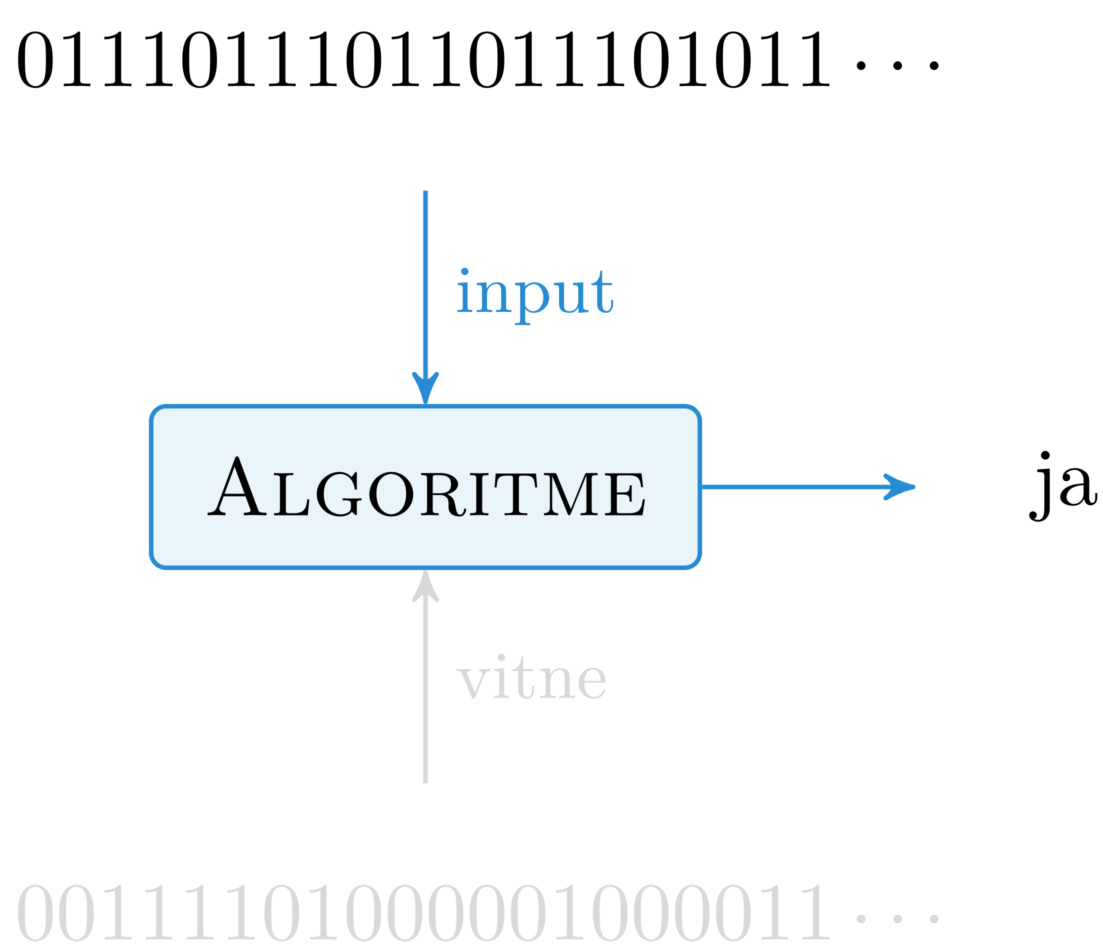
Mer generelt: Egentlig et r … som helst ja/nei-spørsmål



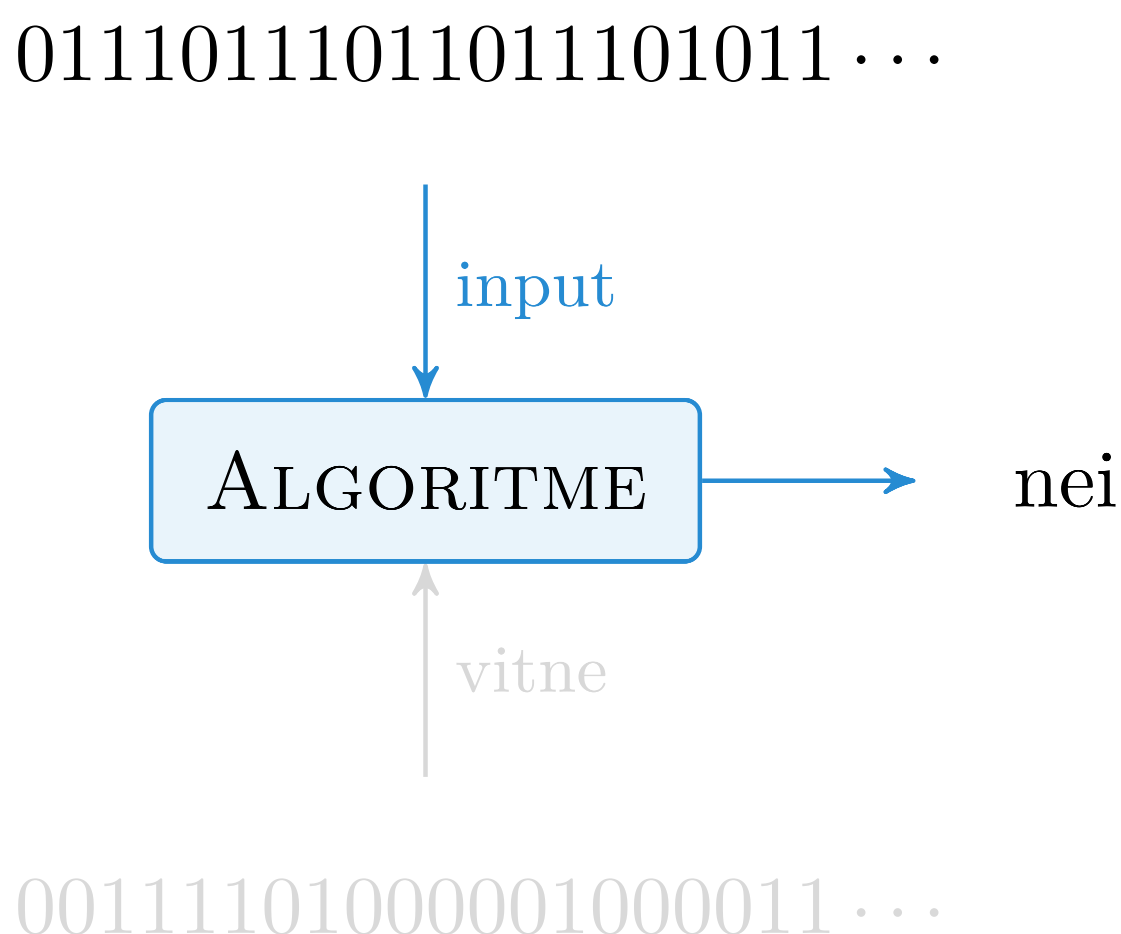
Pussig nok: Ekvivalent med å kunne løse bare ja-instanser i polynomisk tid. (Tilsvarer distinksjonen mellom decide og accept for språk; se teorem 34.2.)

Klassen **P** er slike problemer som kan løses i polynomisk tid

NP står for «non-deterministic polynomial time» – om vi på magisk vis kan gjette svaret (ikke-deterministisk), så kan vi altså løse problemet i polynomisk tid.



NP: Ja-svar har vitner som kan sjekkes i pol. tid



co-NP: Nei-svar har vitner som kan sjekkes i pol. tid

- **Optimering: Ikke nødvendigvis noe vitne**
- **Lag beslutningsproblem med terskling**
- **Avgjøres vha. optimering, som da er minst like vanskelig**
- **Hvis P = NP kan vi finne optimum vha. binærsøk med terskelen**

- **Problem som språk:**
  Konkrete beslutningsproblemer tilsvarer formelle språk (mengder av strenger). Ja-instanser er med, nei-instanser er ikke
- **Accept, reject, decide:**
  En algoritme A *aksepterer* x dersom $\mathrm{A}(x) = 1$.
  Den *avviser* x dersom $\mathrm{A}(x) = 0$.
  Den *avgjør* et språk L dersom …
  - $x \in \mathrm{L} \rightarrow \mathrm{A}(x) = 1$
  - $x \notin \mathrm{L} \rightarrow \mathrm{A}(x) = 0$.
- **Accept vs decide:**
  Selv om L er språket som *aksepteres* av A, så trenger ikke A *avgjøre* L, siden den kan la være å svare for nei-instanser (ved å aldri terminere)

- **Kompleksitetsklasse:** En mengde språk
- **P:** Språkene som kan avgjøres i polynomisk tid

Pussig nok, også språkene som aksepteres i pol. tid! (Thm. 34.2)

- **Kompleksitetsklasse:** En mengde språk
- **P:** Språkene som kan avgjøres i polynomisk tid
- **Cobham's tese:**
  Det er disse problemene vi kan løse i praksis

- **Sertifikat:**
  En streng y som brukes som «bevis» for et ja-svar
- **Verifikasjonsalgoritme:**
  Tar inn sertifikat y i tillegg til instans x
- En algoritme A **verifiserer** x hvis det eksisterer et sertifikat y slik at $\mathrm{A}(x, y) = 1$
- **Intuitivt:**
  Algoritmen «sjekker svaret». Om en graf har en Hamilton-sykel, kan sertifikatet være noderekkefølgen i sykelen.
- **Asymmetrisk:**
  Det finnes ikke «motbevis» eller «anti-sertifikater»

- **NP:** Språkene som kan verifiseres i polynomisk tid
- **HAM-CYCLE**
  Språket for Hamilton-sykel-problemet
- HAM-CYCLE $\in$ **NP**
  Lett å verifisere i polynomisk tid
  Merk: Ikke nødvendigvis lett å *falsifisere*
- **co-NP:**
  Språkene som kan *falsifiseres* i polynomisk tid

$$\mathrm{L} \in \textbf{co-NP} \iff \bar{\mathrm{L}} \in \textbf{NP}$$

$\bar{\mathrm{L}}$ er *komplementet* til L: $x \in \bar{\mathrm{L}} \iff x \notin \mathrm{L}$

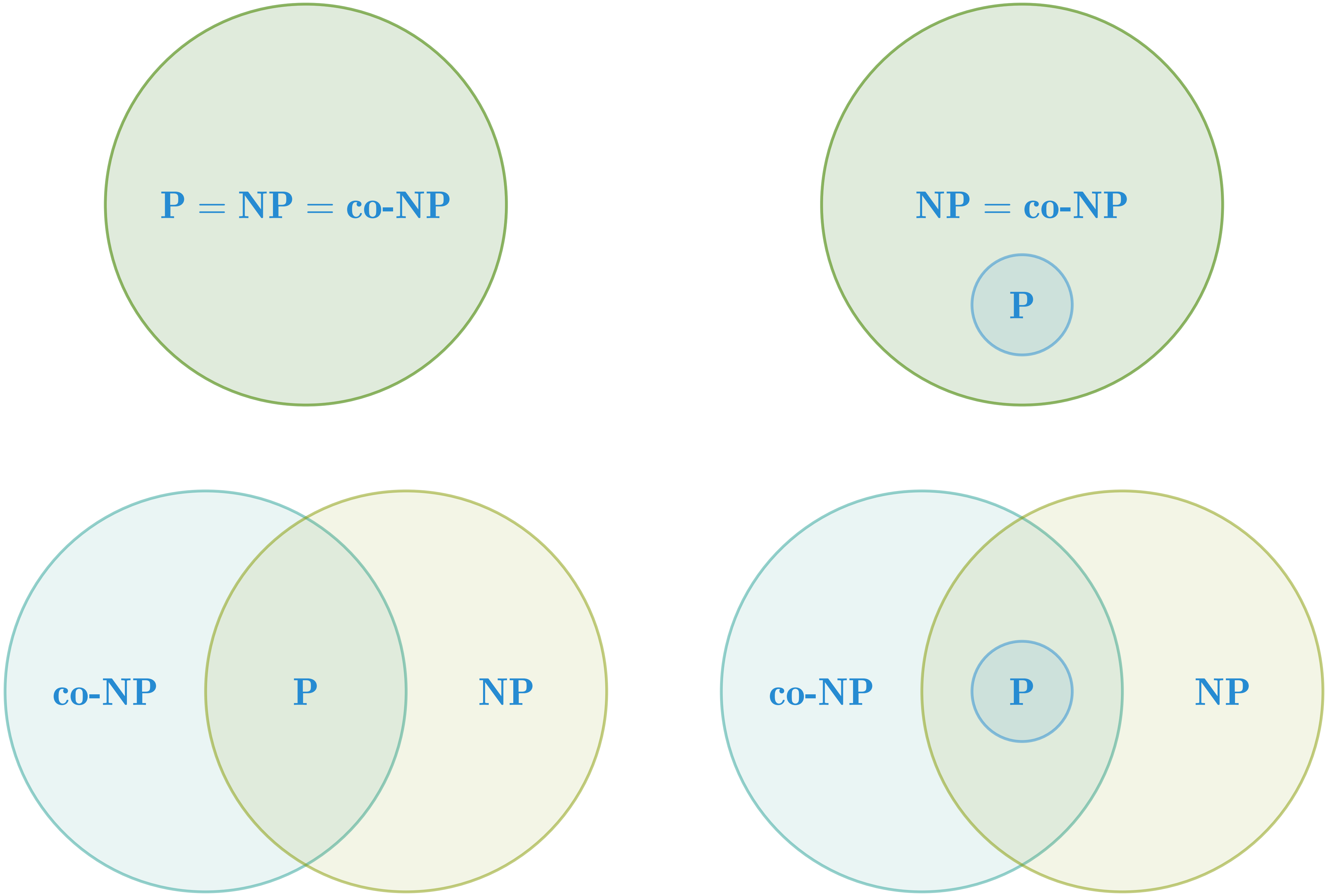
- **NP:** Språkene som kan verifiseres i polynomisk tid
- **HAM-CYCLE**
  Språket for Hamilton-sykel-problemet
- HAM-CYCLE $\in$ **NP**
  Lett å verifisere i polynomisk tid
  Merk: Ikke nødvendigvis lett å *falsifisere*
- **co-NP:**
  Språkene som kan *falsifiseres* i polynomisk tid

$$\mathrm{L} \in \textbf{co-NP} \iff \bar{\mathrm{L}} \in \textbf{NP}$$

F.eks.: TAUTOLOGY

(Det er komplementet til negasjonen av SAT … som vi ser igjen siden)

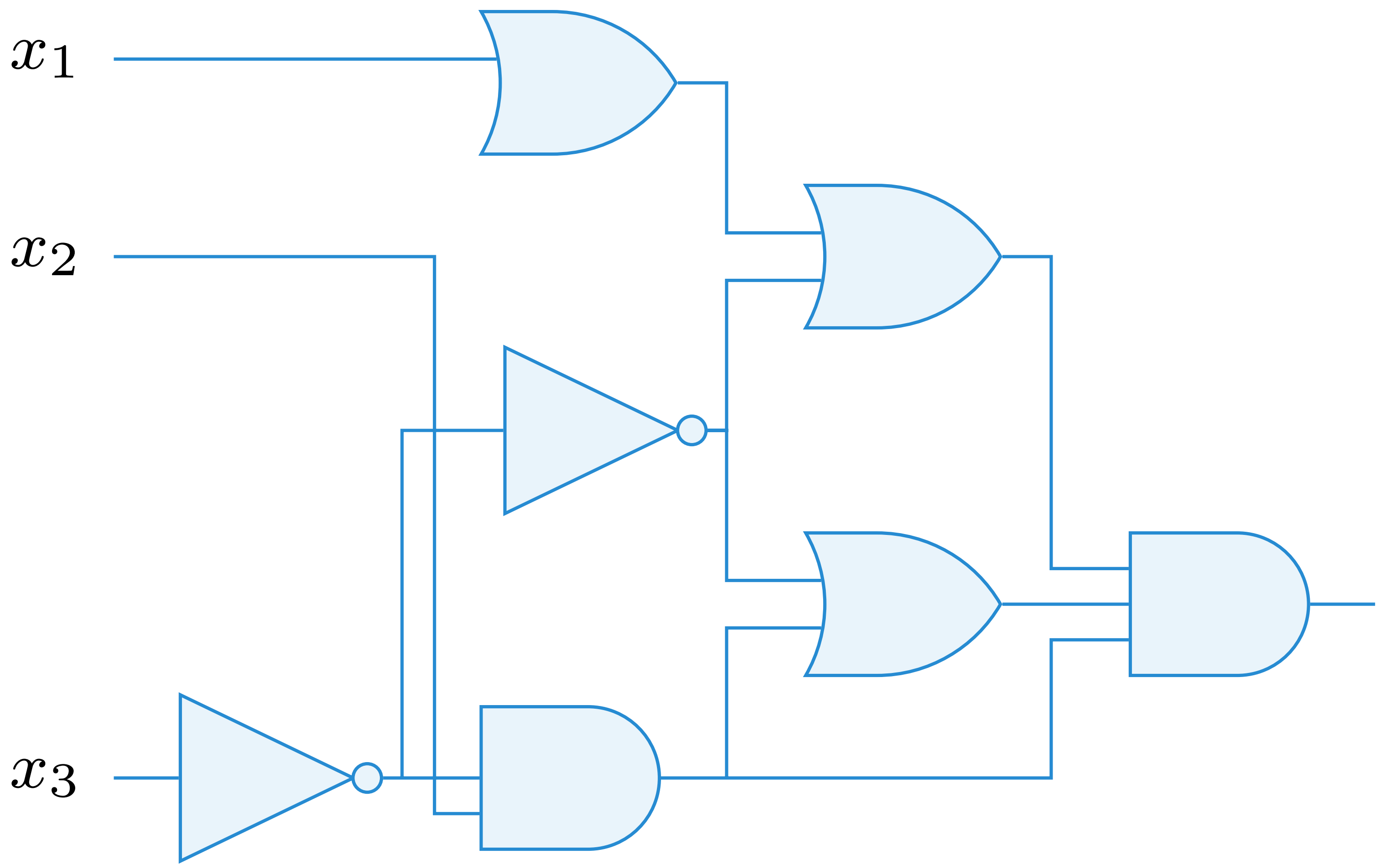
- **P vs NP**
  Om vi kan *løse* problemet, så kan vi *verifisere* det med samme algoritme, og bare ignorere sertifikatet
  Dvs.: $\mathbf{P} \subseteq \mathbf{NP}$ og $\mathbf{P} \subseteq \mathbf{co\text{-}NP}$
- **Vi vet ikke** om $\mathbf{P} = \mathbf{NP} \cap \mathbf{co\text{-}NP}$



Mulige scenarier; ingen vet hvilket som stemmer!

Disse problemene er NP-komplette; vi kommer til hva det betyr.

Noen (vanskelige) problemer



CIRCUIT-SAT

Instans: En krets med logiske porter og én utverdi

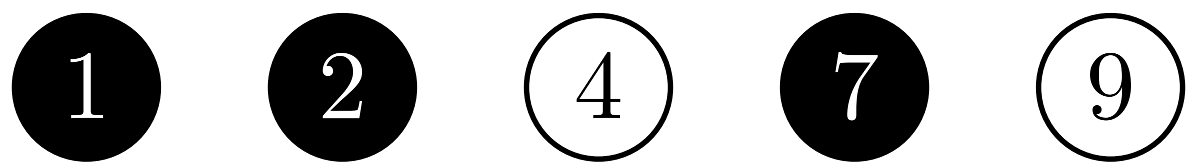
Spørsmål: Kan utverdien bli 1?

$$\phi = ((x_1 \to x_2) \vee \neg((\neg x_1 \leftrightarrow x_3) \vee x_4)) \wedge \neg x_2$$

SAT
Instans: En logisk formel
Spørsmål: Kan formelen være sann?

$$\begin{aligned}\phi = {} & (\ \ x_1 \vee \neg x_2 \vee \neg x_3) \wedge \\ & (\neg x_1 \vee \ \ x_2 \vee \ \ x_3) \wedge \\ & (\ \ x_1 \vee \ \ x_2 \vee \ \ x_3)\end{aligned}$$

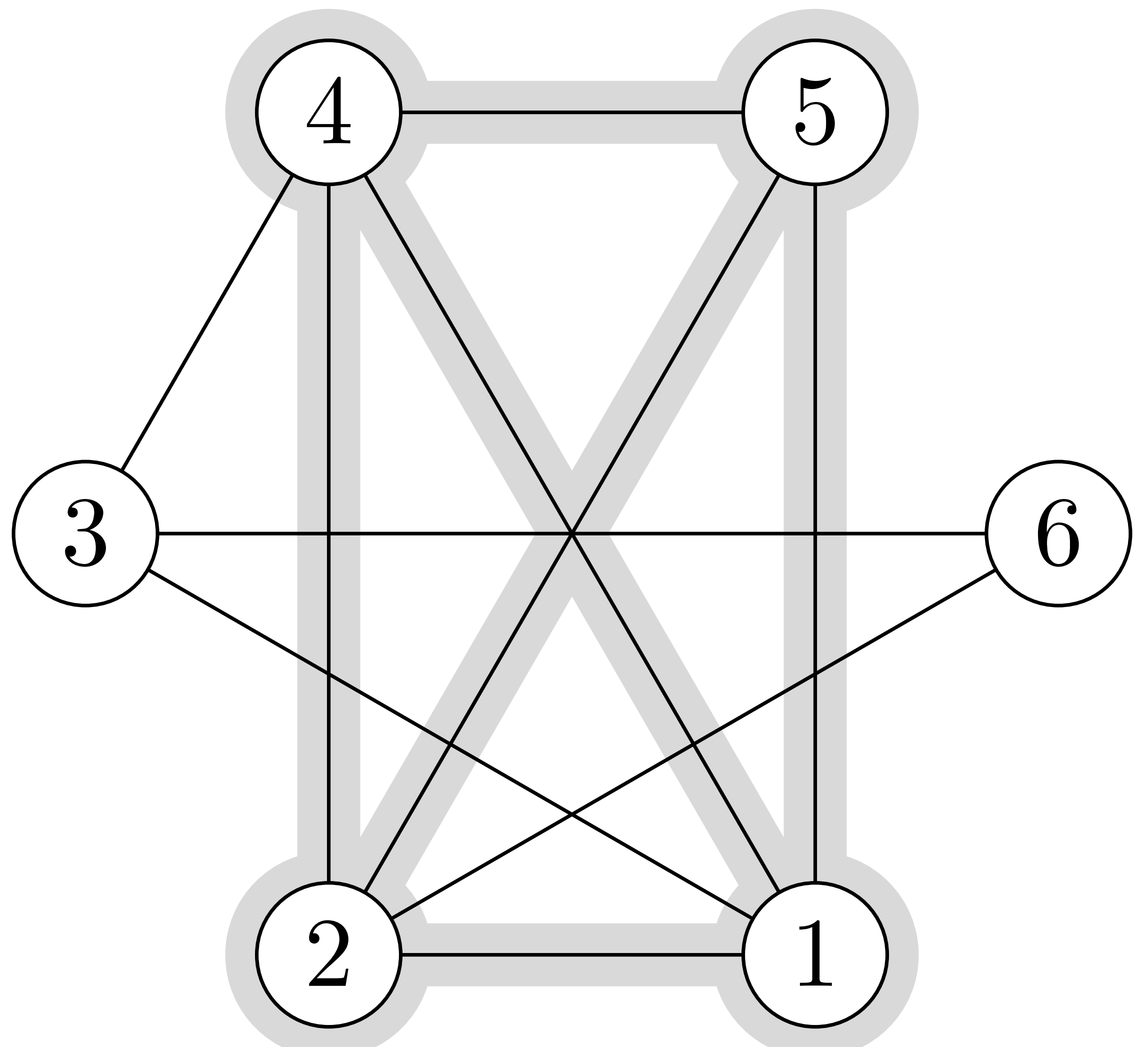
3-CNF-SAT
Instans: En logisk formel på 3-CNF-form
Spørsmål: Kan formelen være sann?



SUBSET-SUM

Instans: Mengde positive heltall S og positivt heltall t

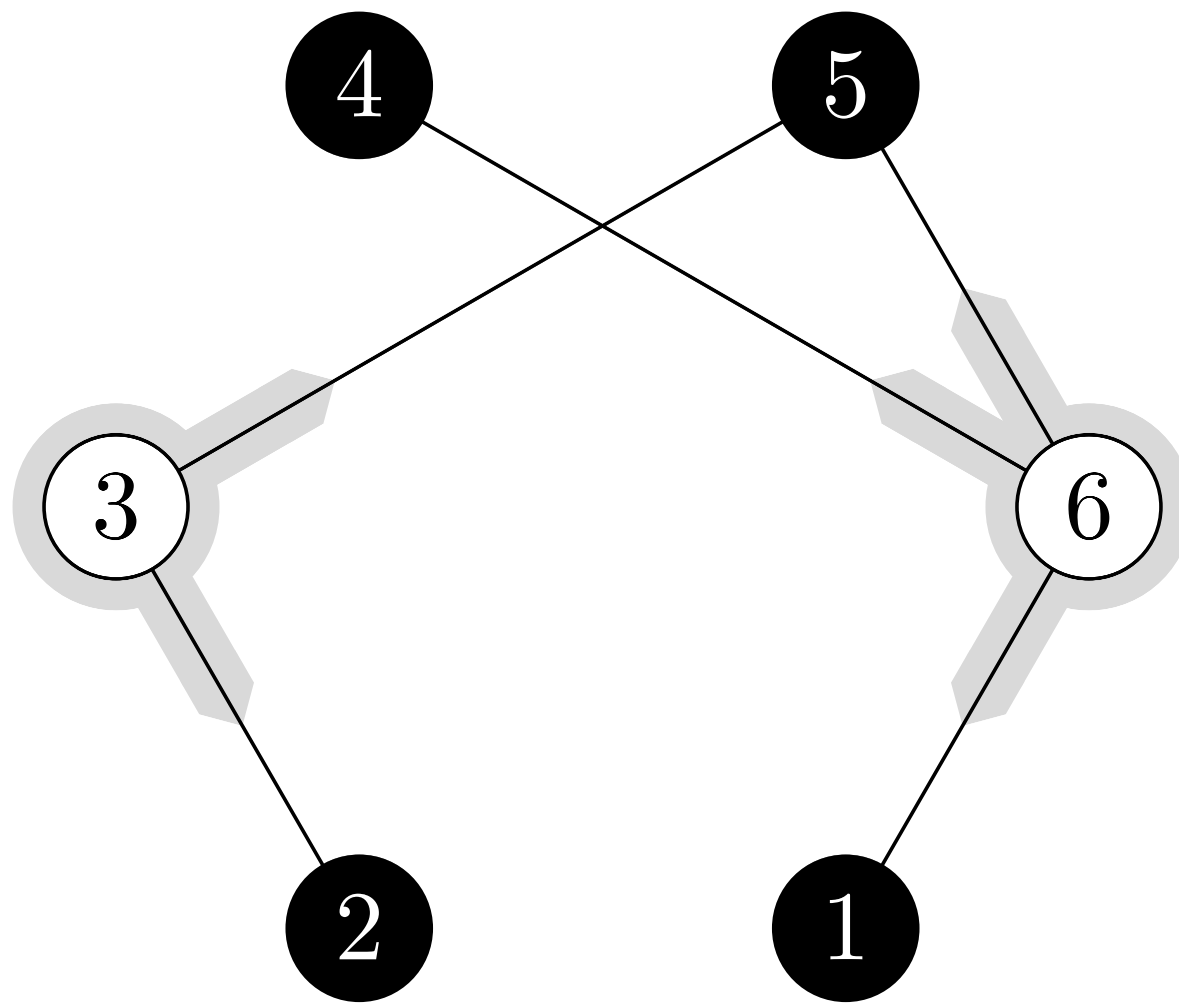
Spørsmål: Finnes en delmengde $\mathrm{S}' \subseteq \mathrm{S}$ så $\sum_{s \in \mathrm{S}'} s = t$?



CLIQUE

Instans: En urettet graf G og et heltall k

Spørsmål: Har G en en komplett delgraf med k noder?

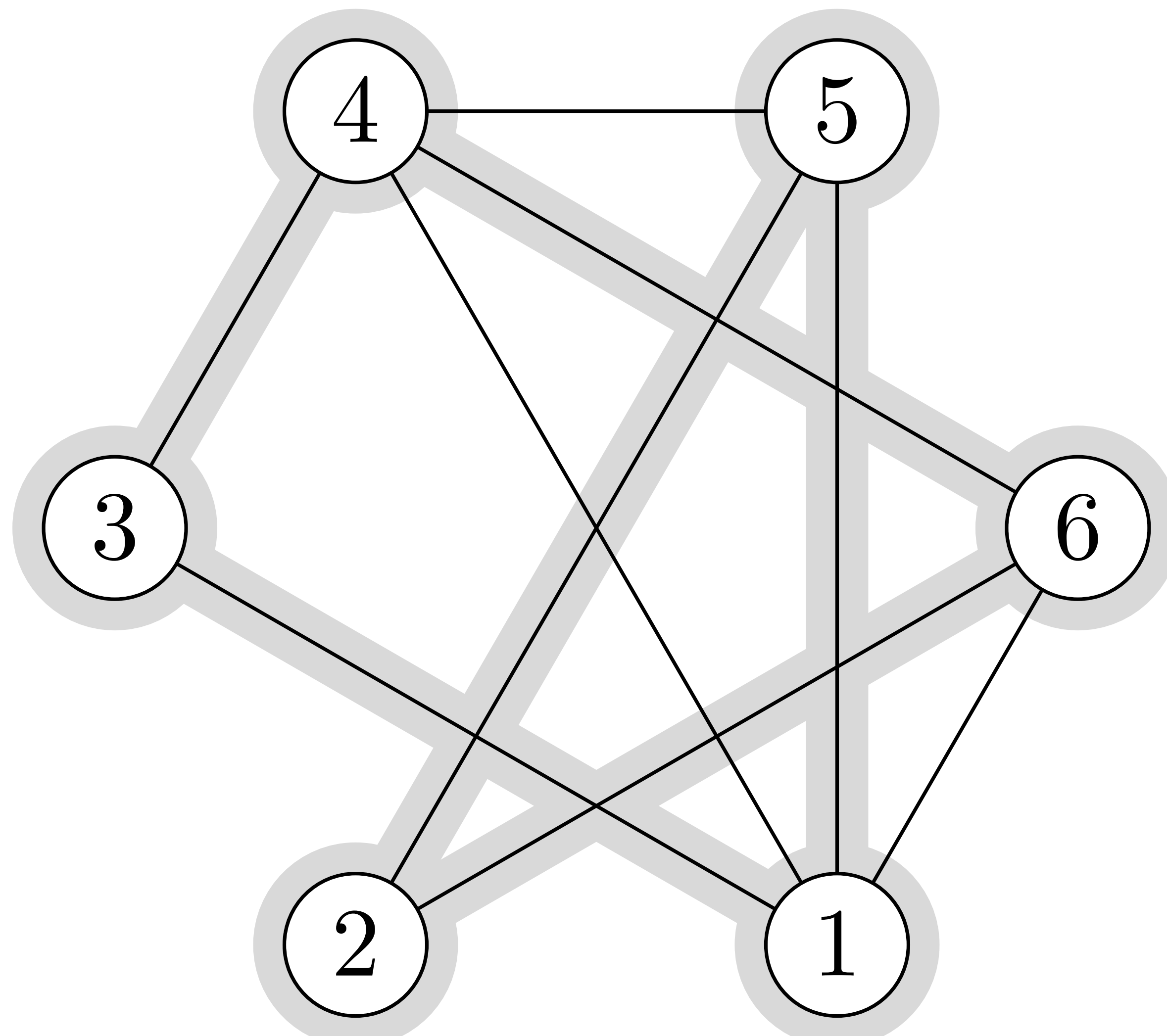


VERTEX-COVER

Instans: En urettet graf G og et heltall k

Spørsmål: Har G en et nodedekke med k noder?

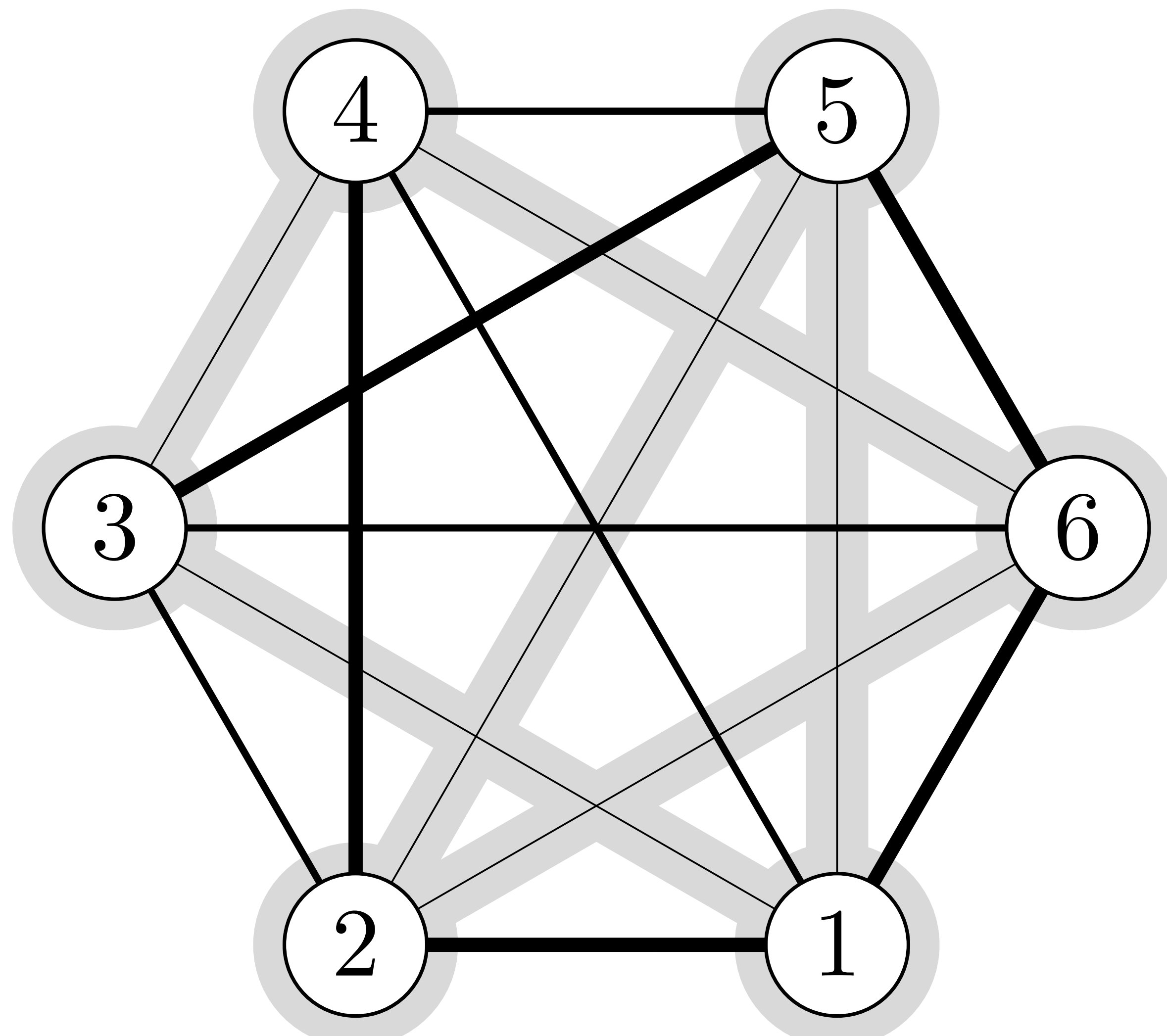
Dvs., k noder som tilsammen ligger inntil alle kantene



HAM-CYCLE

Instans: En urettet graf G

Spørsmål: Finnes det en sykel som inneholder alle nodene?



TSP

Instans: En komplett graf med heltallsvekter og et heltall k

Spørsmål: Finnes det en rundtur med kostnad $\leq k$?

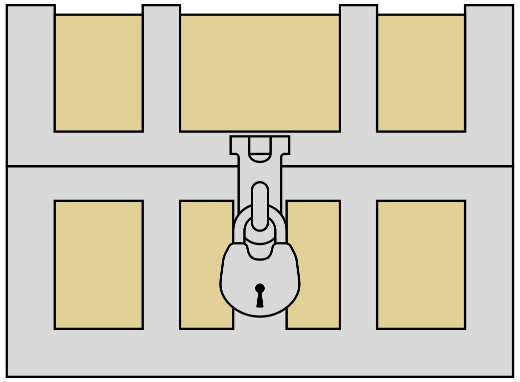
2:4

Reduksjoner

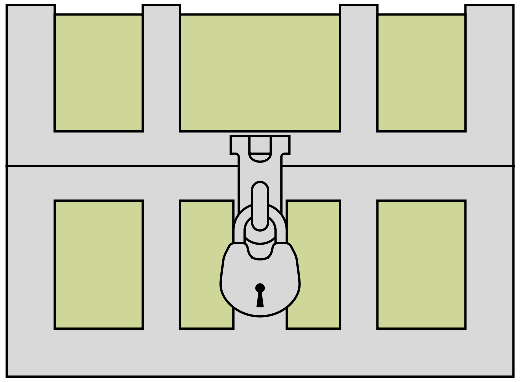
Spesifikt, såkalte Karp-reduksjoner: «Many-one»-reduksjoner som tar polynomisk lang tid.

A   B

La oss si du har funnet to skattekister

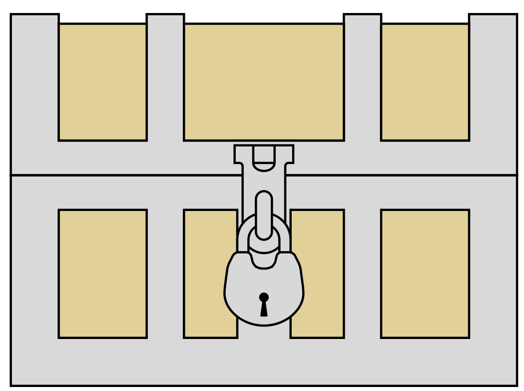


A

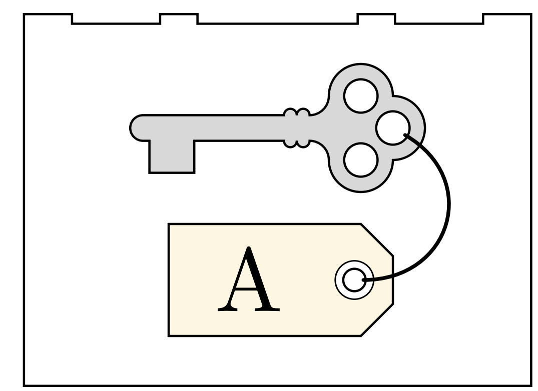


B

Du ønsker å si noe om hvor vanskelige de er å åpne

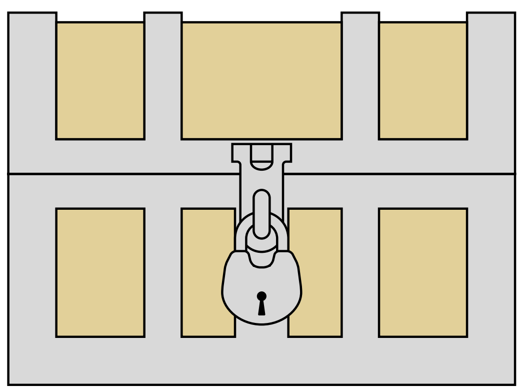


A

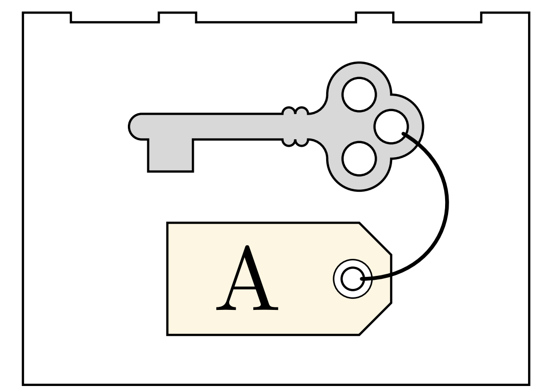


B

Anta at B inneholder nøkkelen til A

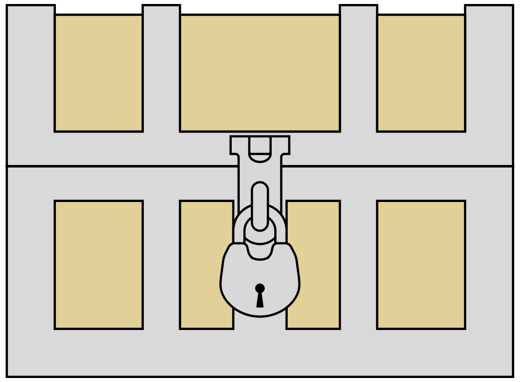


A

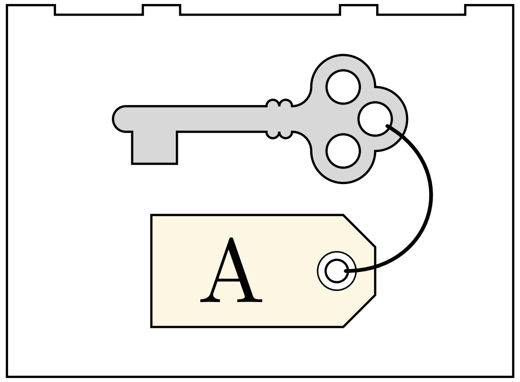


B

Kan det nå være vanskeligere å åpne A enn B?

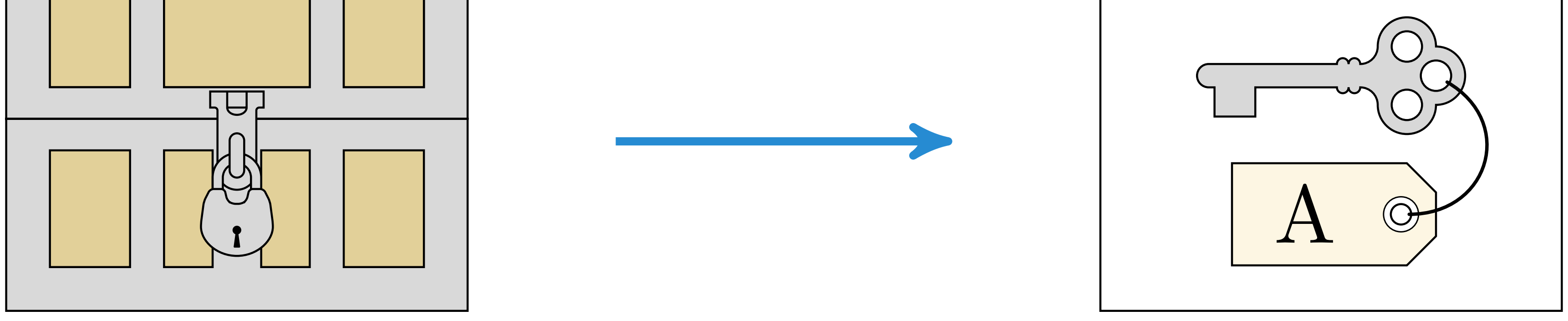


A



B

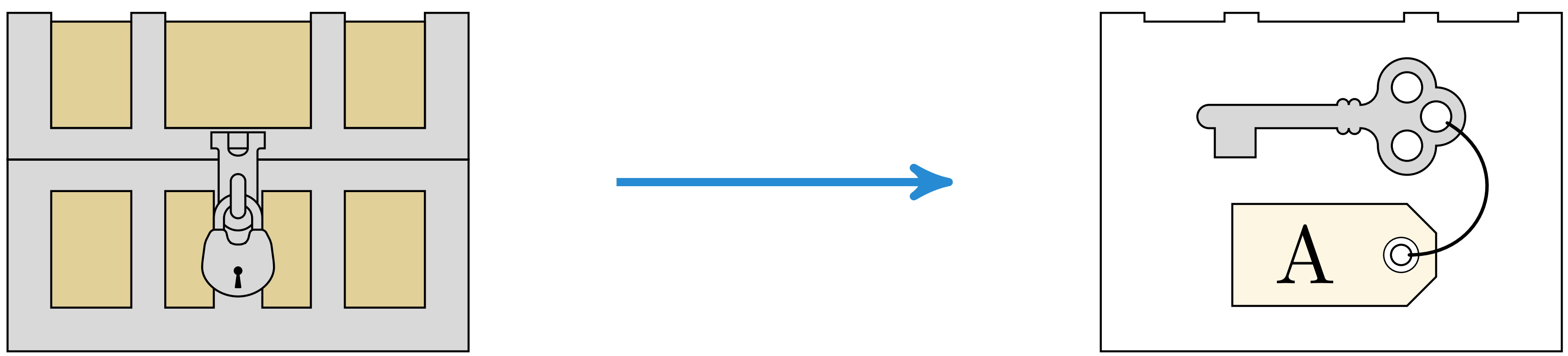
Nei! Om vi kan åpne B, så kan vi naturligvis åpne A



A

B

Vi har <u>redusert</u> problemet «åpne A» til problemet «åpne B»



$$A \leqslant B$$

Da gir det ingen mening å si at A er vanskeligere enn B

Vi vil redusere fra beslutningsproblem Q til beslutningsproblem Q′

Vi formaliserer det som en reduksjon fra språk L_1 til språk L_2

Input: En bitstreng x.

Output: En bitstreng $f(x)$, der

$$x \in \mathrm{L}_1 \iff f(x) \in \mathrm{L}_2 .$$

Om vi kan avgjøre om $f(x) \in \mathrm{L}_2$ kan vi også avgjøre om $x \in \mathrm{L}_1$

Input: En bitstreng x.

Output: En bitstreng $f(x)$, der

$$x \in \mathrm{L}_1 \iff f(x) \in \mathrm{L}_2 \, .$$

Men ikke omvendt!

Ikke omvendt … fordi det er ikke sikker f er invertibel. Om vi kan redusere fra L1 til L2 (med f), betyr ikke det at det finnes noen reduksjon fra L2 til L1.

Merk at det handler om retningen til f og ikke retningen til implikasjonen! Vi må ha "hvis og bare hvis" her, siden det bare betyr at de to svarene (ja eller nei) er de samme, og at reduksjonen er korrekt.

$$\alpha$$

$$\mathrm{A}(\alpha)$$

Et beslutningsproblem

α

β

$A(\alpha)$

$B(\beta)$

Enda et beslutningsproblem

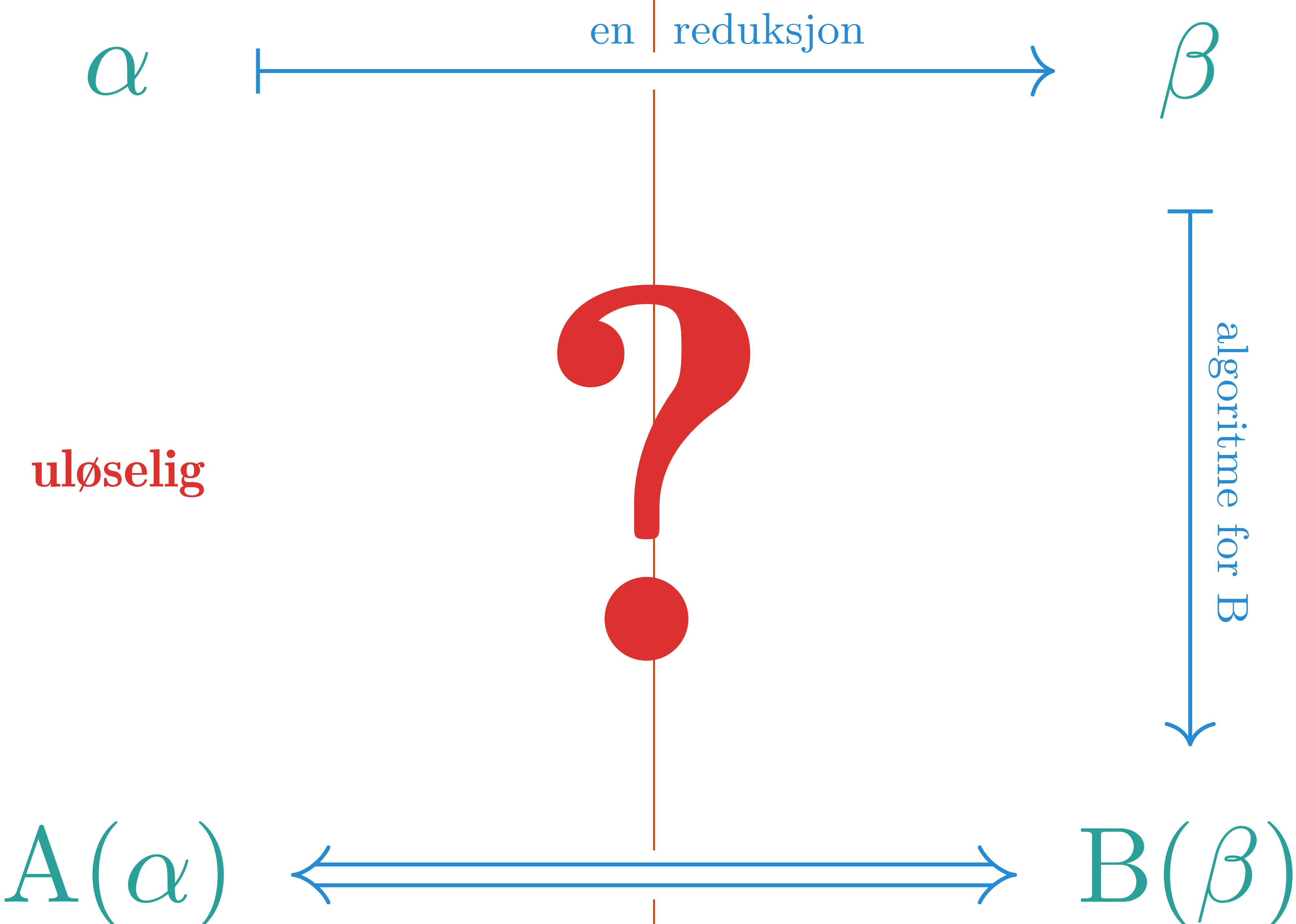
$$\alpha \xmapsto{\text{en reduksjon}} \beta$$

$$\mathrm{A}(\alpha) \iff \mathrm{B}(\beta)$$

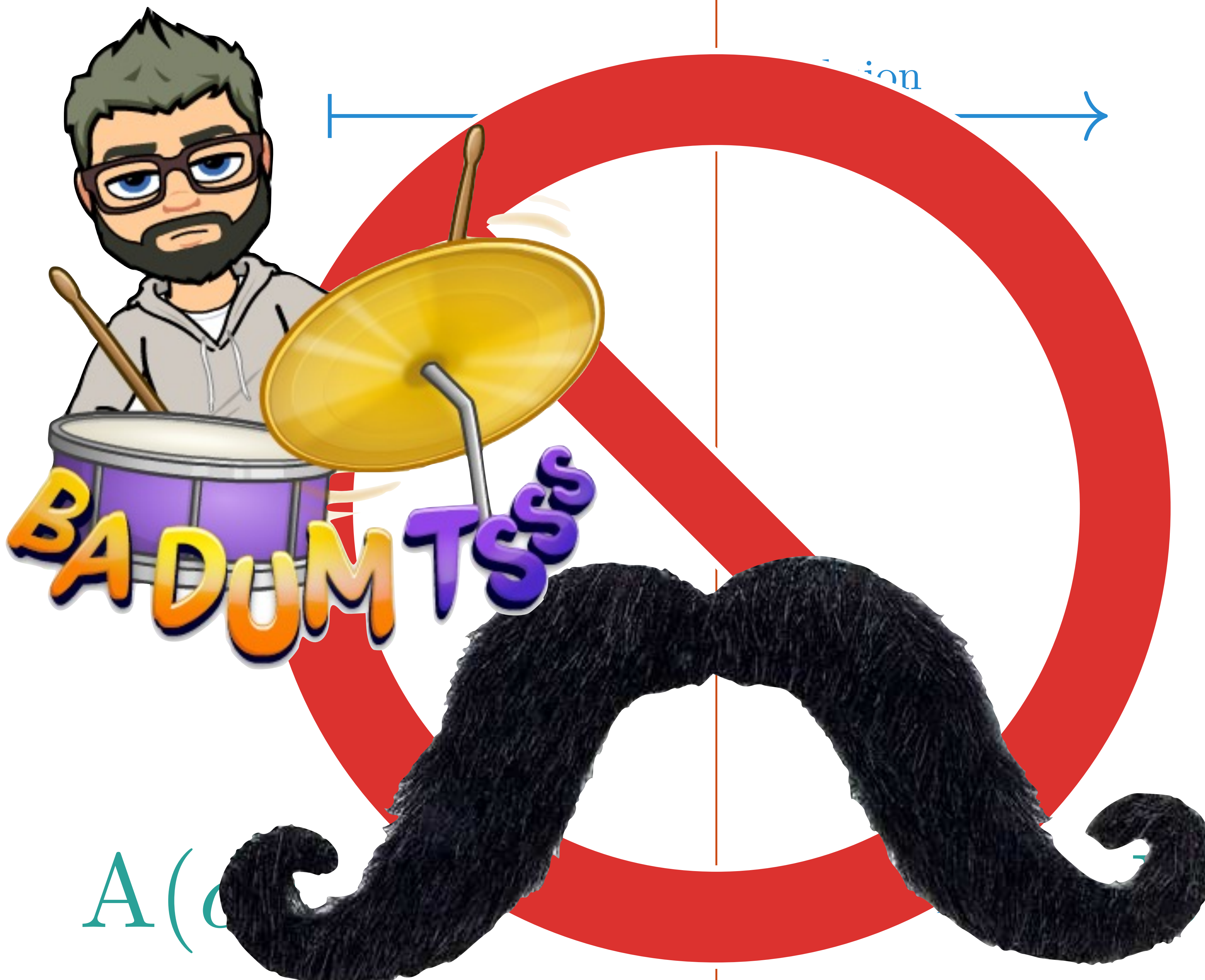
$$
\begin{tikzcd}
\alpha \arrow[r, mapsto, "\text{en reduksjon}"] & \beta \arrow[d, mapsto, "\text{algoritme for B}"] \\
\mathrm{A}(\alpha) \arrow[r, Leftrightarrow] & \mathrm{B}(\beta)
\end{tikzcd}
$$

$$\begin{tikzcd}
\alpha \arrow[r, mapsto, "\text{en reduksjon}"] & \beta \arrow[d, mapsto, "\text{algoritme for B}"] \\
A(\alpha) \arrow[r, Leftrightarrow] & B(\beta)
\end{tikzcd}$$

uløselig



α
en reduksjon
β
algoritme for B
uløselig
?
$A(\alpha)$
$B(\beta)$



ion

β

algoritme for B

$\mathrm{A}(\alpha$ … (β)

Nei! Om A reduserer til et løsbart problem, må A også være løsbart!

$$
\begin{tikzcd}
\alpha \arrow[r, mapsto, "\text{en reduksjon}"] \arrow[d, mapsto, "\text{algoritme for A}"'] & \beta \arrow[d, mapsto, "\text{algoritme for B}"] \\
\mathrm{A}(\alpha) \arrow[r, Leftrightarrow] & \mathrm{B}(\beta)
\end{tikzcd}
$$

$$
\begin{tikzcd}
\alpha \arrow[r, mapsto, "\text{polynomisk reduksjon}"] \arrow[d, mapsto, "\text{beste mulige}"'] & \beta \arrow[d, mapsto, "\text{beste mulige}"] \\
\mathrm{A}(\alpha) \arrow[r, Leftrightarrow] & \mathrm{B}(\beta)
\end{tikzcd}
$$

$$\begin{tikzcd}[column sep=huge, row sep=huge]
\alpha \arrow[r, mapsto, "\text{polynomisk reduksjon}"] \arrow[d, mapsto, "\text{beste mulige}"'] & \beta \arrow[d, mapsto, "\text{beste mulige}"] \\
A(\alpha) \arrow[r, Leftrightarrow] & B(\beta)
\end{tikzcd}$$

Hvis denne er polynomisk . . .

$$\begin{tikzcd}[column sep=huge, row sep=huge]
\alpha \arrow[r, mapsto, "\text{polynomisk reduksjon}"] \arrow[d, mapsto, "\text{beste mulige}"'] & \beta \arrow[d, mapsto, "\text{beste mulige}"] \\
A(\alpha) \arrow[r, Leftrightarrow] & B(\beta)
\end{tikzcd}$$

Hvis denne er polynomisk…

…så må denne også være det

$$
\begin{tikzcd}
\alpha \arrow[r, mapsto, "\text{polynomisk reduksjon}"] \arrow[d, mapsto, "\text{beste mulige}"'] & \beta \arrow[d, mapsto, "\text{beste mulige}"] \\
\mathrm{A}(\alpha) \arrow[r, Leftrightarrow] & \mathrm{B}(\beta)
\end{tikzcd}
$$

Hvis denne er eksponentiell . . .

$$
\begin{tikzcd}[column sep=huge, row sep=huge]
\alpha \arrow[r, mapsto, "\text{polynomisk reduksjon}"] \arrow[d, mapsto, "\text{beste mulige}"'] & \beta \arrow[d, mapsto, "\text{beste mulige}"] \\
A(\alpha) \arrow[r, Leftrightarrow] & B(\beta)
\end{tikzcd}
$$

Hvis denne er eksponentiell…

…så må denne også være det

$$
\begin{tikzcd}
\alpha \arrow[r, mapsto, "\text{«ubetydelig» reduksjon}"] \arrow[d, mapsto, "\text{beste mulige}"'] & \beta \arrow[d, mapsto, "\text{beste mulige}"] \\
\mathrm{A}(\alpha) \arrow[r, Leftrightarrow] & \mathrm{B}(\beta)
\end{tikzcd}
$$

- **Redusibilitet:**
  Hvis A kan reduseres til B i polynomisk tid, skriver vi $A \leq_{\mathbf{P}} B$
- **Ordning:**
  Relasjonen $\leq_{\mathbf{P}}$ utgjør en *preordning*
- **Hardhetsbevis:**
  For å vise at B er vanskelig, redusér fra et vanskelig problem A, dvs., etablér at $A \leq_{\mathbf{P}} B$

Delvis ordning uten antisymmetri, dvs., vi tillater sykler

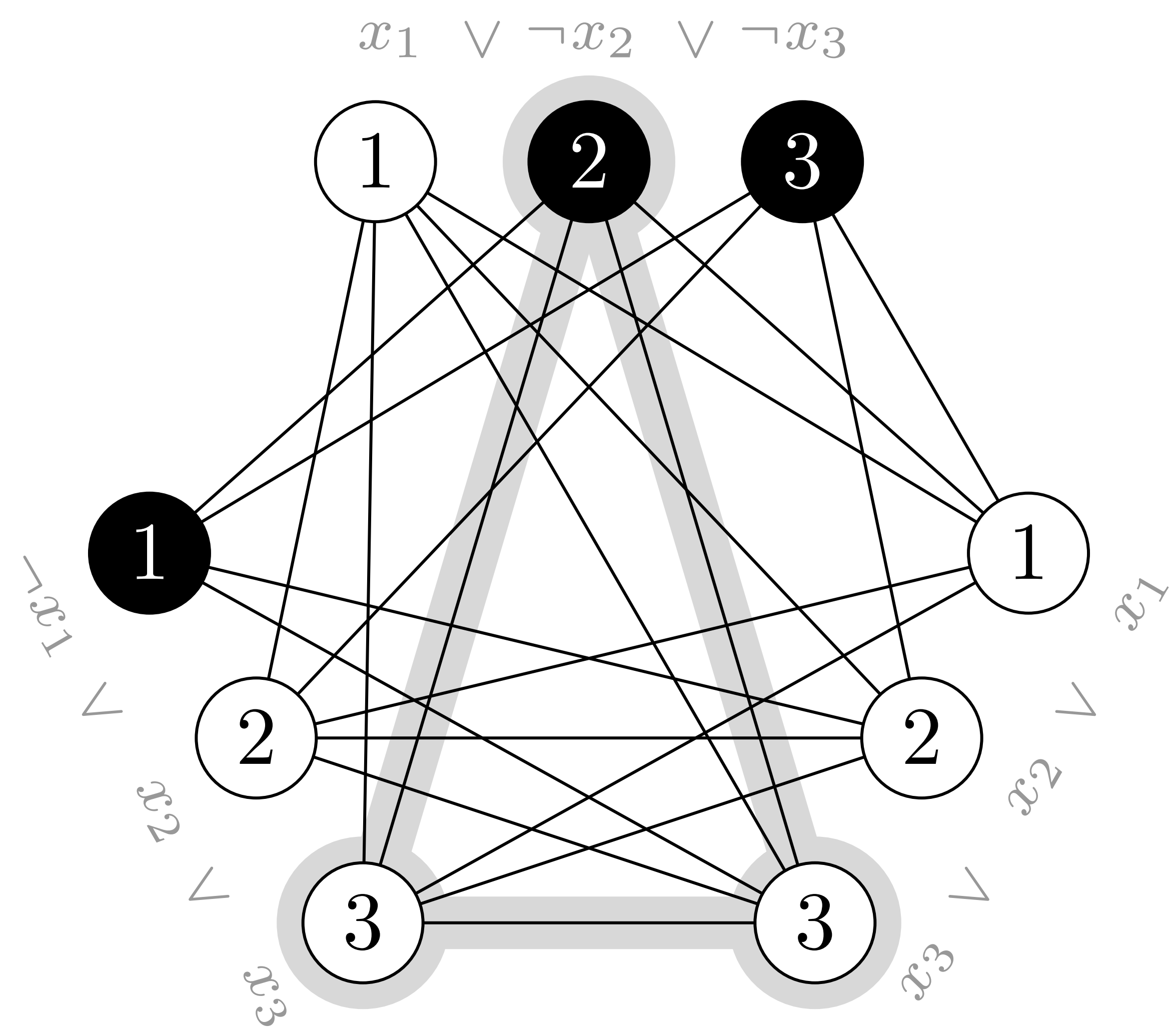
Et eksempel

- **CLIQUE**
  - **Instans:** En urettet graf G og et heltall k
  - **Spørsmål:** Har G en en komplett delgraf med k noder?
- Vi vil redusere fra 3-CNF-SAT
- Lag én node i G for hver literal i formelen
- Ingen kanter mellom noder fra samme term
- Ellers: Kanter mellom literaler som kan være sanne samtidig
- La k være antall termer

$$\begin{aligned}\phi = &(\ \ x_1 \vee \neg x_2 \vee \neg x_3) \wedge \\ &(\neg x_1 \vee \ \ x_2 \vee \ \ x_3) \wedge \\ &(\ \ x_1 \vee \ \ x_2 \vee \ \ x_3)\end{aligned}$$

Kan ϕ være sann? $\Longleftrightarrow$ Finnes en k-klikk?

$$\begin{aligned}\phi = {} & (\ \ x_1 \vee \neg x_2 \vee \neg x_3\,) \ \wedge \\ & (\neg x_1 \vee \ \ x_2 \vee \ \ x_3\,) \ \wedge \\ & (\ \ x_1 \vee \ \ x_2 \vee \ \ x_3\,)\end{aligned}$$

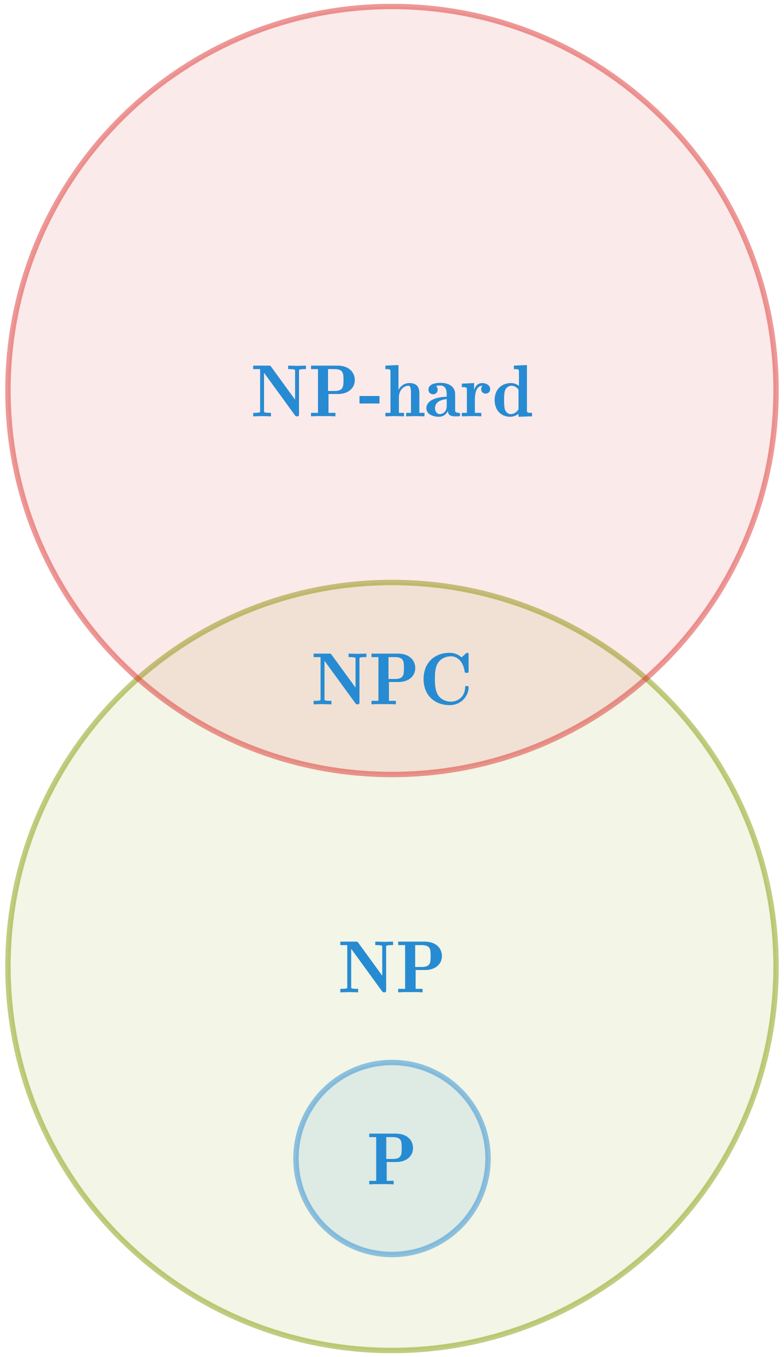


Tilsv. $x_1, x_2, x_3 = -, 0, 1$

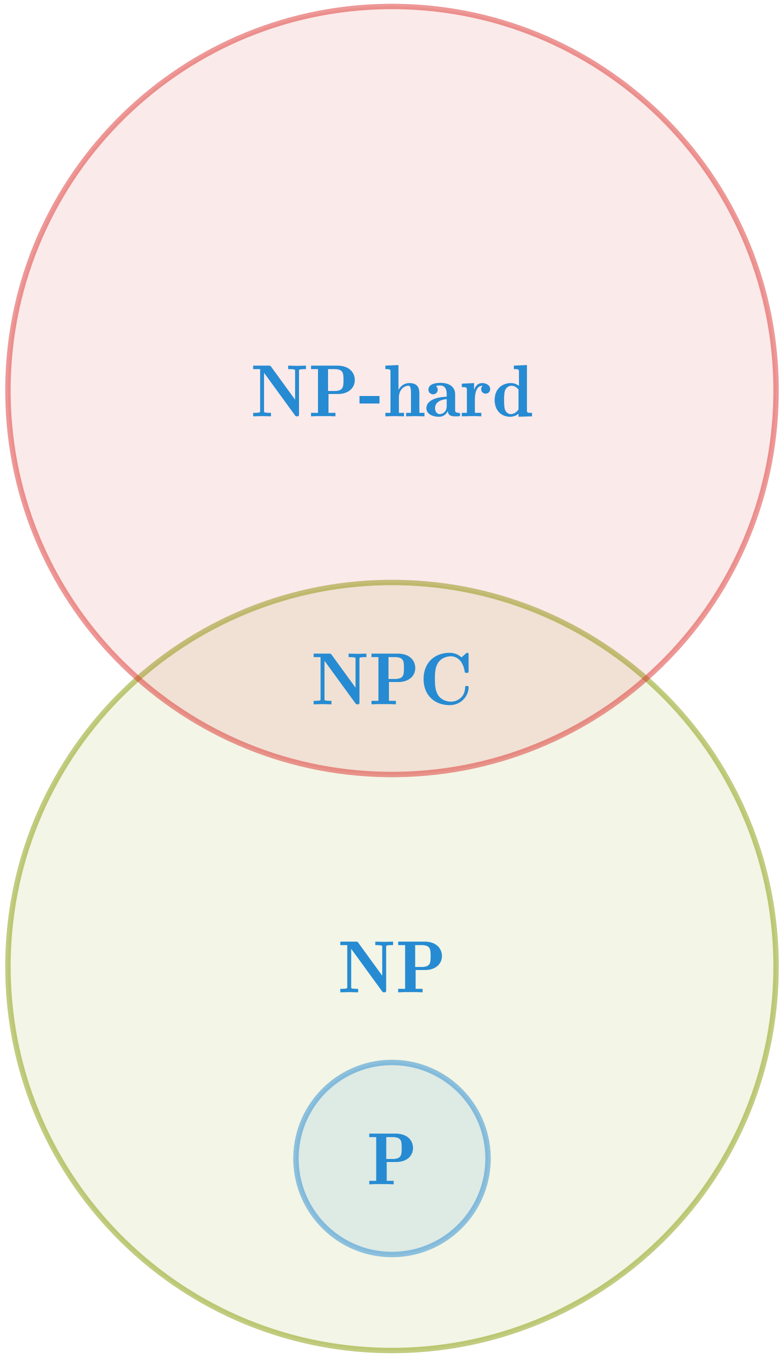
Kan ϕ være sann? $\Longleftrightarrow$ Finnes en k-klikk?

3:4

Komplettheet



Det er altså sånn de fleste *tror* ting er



(Og det finnes *mange* andre klasser . . .)

› **Kompletthet:**
Et problem er *komplett* for en gitt klasse og en gitt type reduksjoner dersom det er *maksimalt* for redusibilitetsrelasjonen.

De komplette problemene er altså de vanskeligste i klassen

- **Kompletthet:**
  Et problem er *komplett* for en gitt klasse og en gitt type reduksjoner dersom det er *maksimalt* for redusibilitetsrelasjonen.
- **Maksimalitet:**
  Et element er *maksimalt* dersom alle andre er mindre eller lik. For reduksjoner: Q er maksimalt dersom alle problemer i klassen kan reduseres til Q.
- **NPC:**
  De komplette språkene i **NP**, under polynomiske reduksjoner.

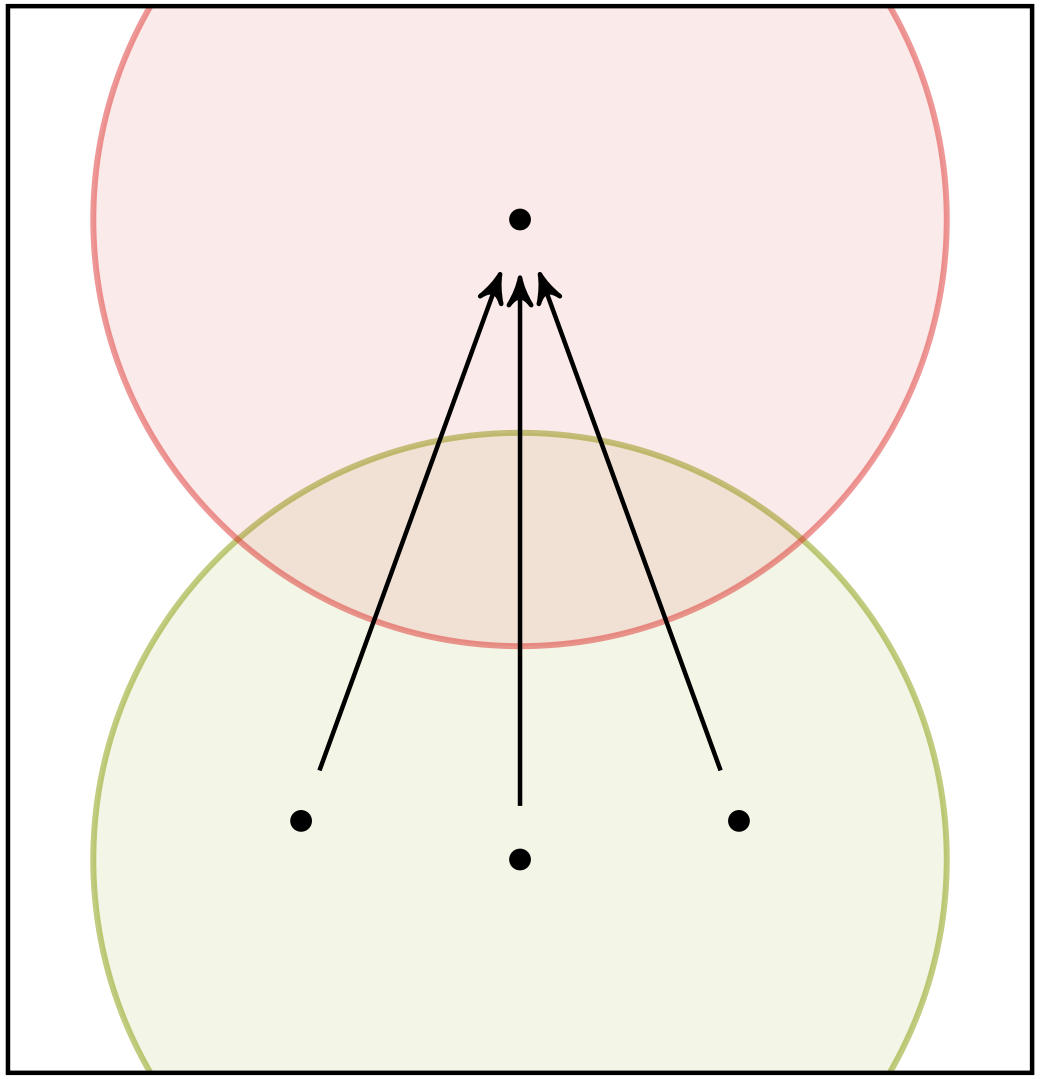
Altså de vanskeligste problemene i **NP**

De vanskelige problemene fra tidligere er altså eksempler på NP-komplette problemer

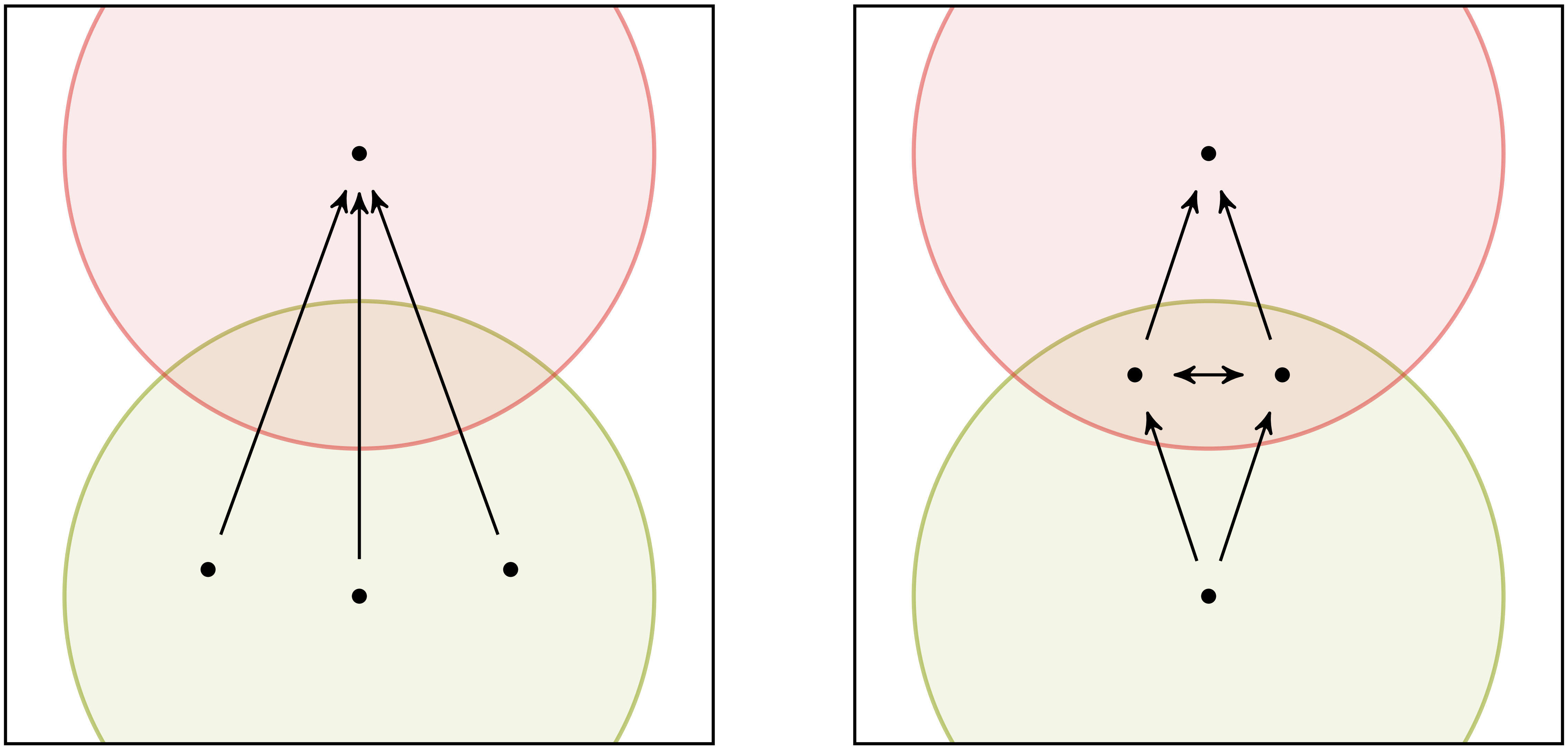
› **NP-hardhet:**
Et problem Q er **NP**-hardt dersom alle problemer i NP kan reduseres til det.

Vi kaller gjerne klassen **NP-hard**

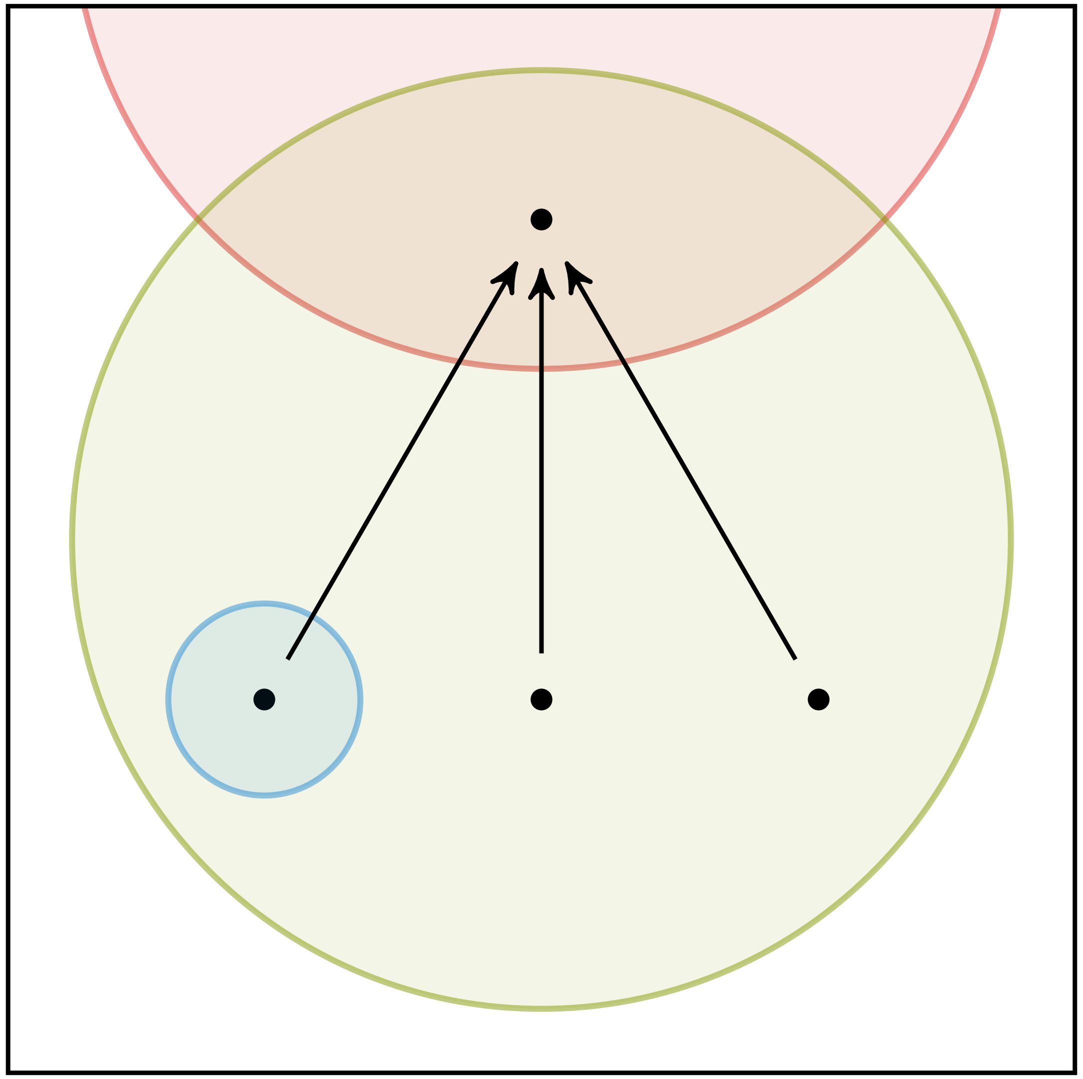
- **NP-hardhet:**
  Et problem Q er **NP**-hardt dersom alle problemer i NP kan reduseres til det.
- Et problem er altså **NP**-komplett dersom det
  - er **NP**-hardt, og
  - er i **NP**.



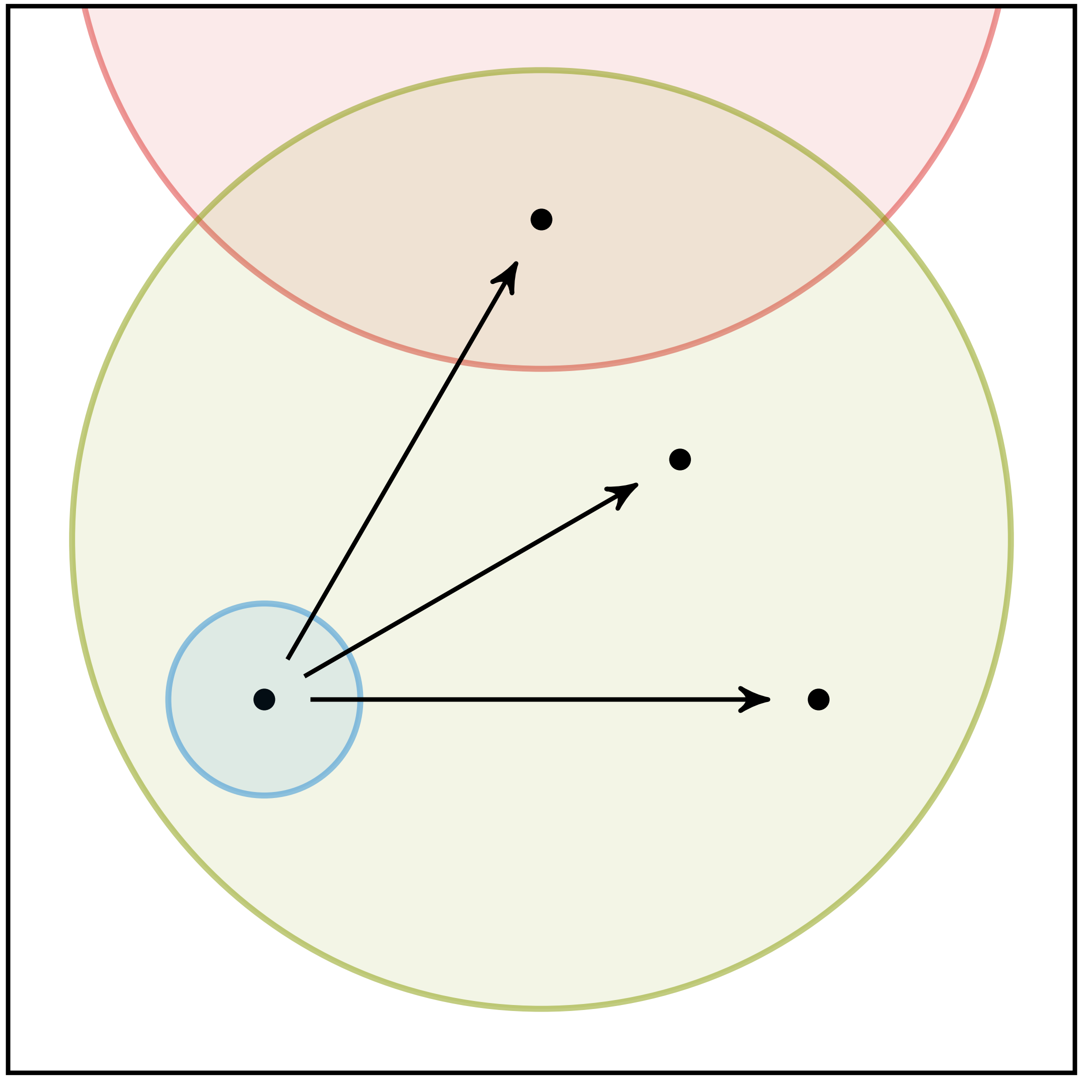
Alt i **NP** kan reduseres til alt i **NPH**



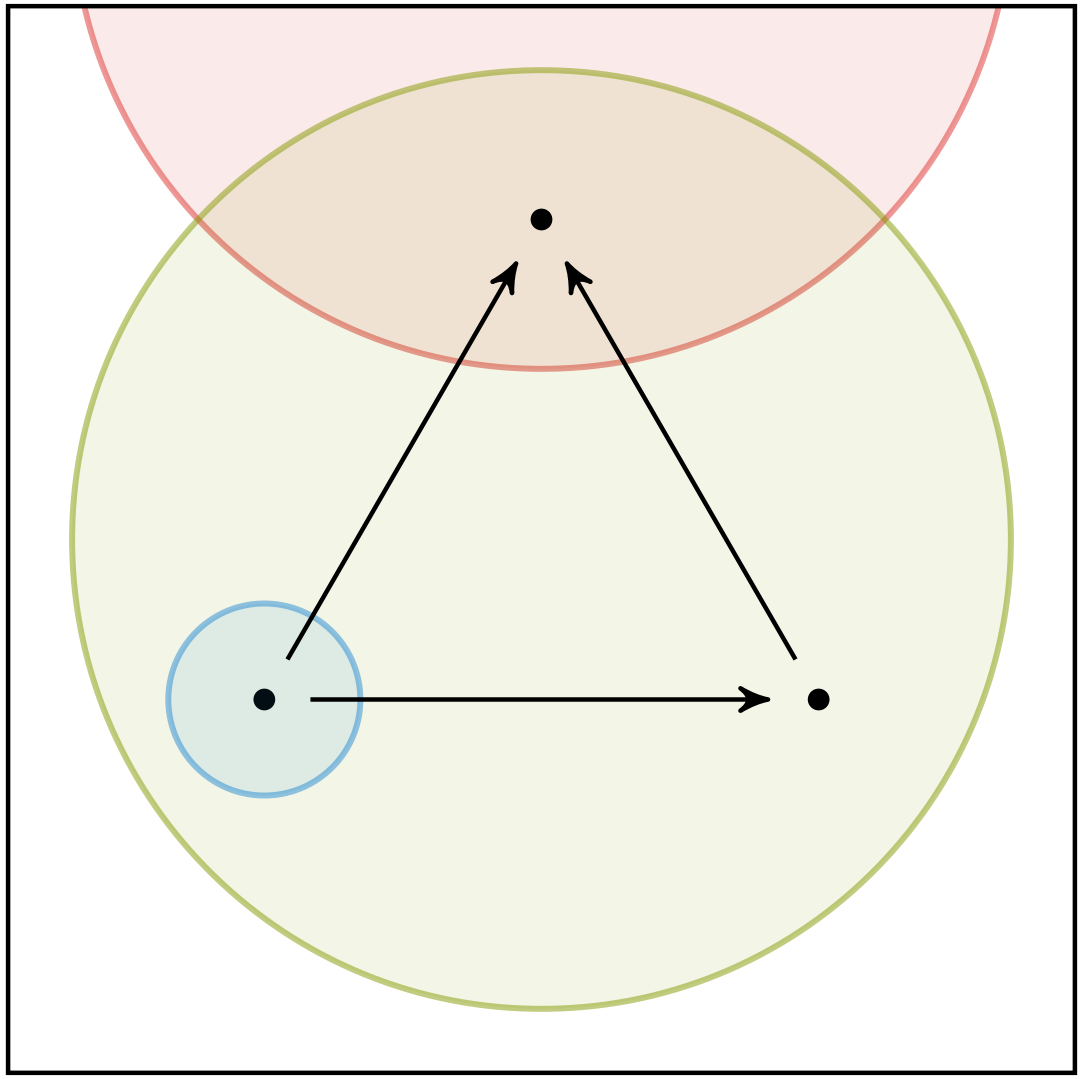
Dermed kan problemer i **NPC** reduseres til hverandre



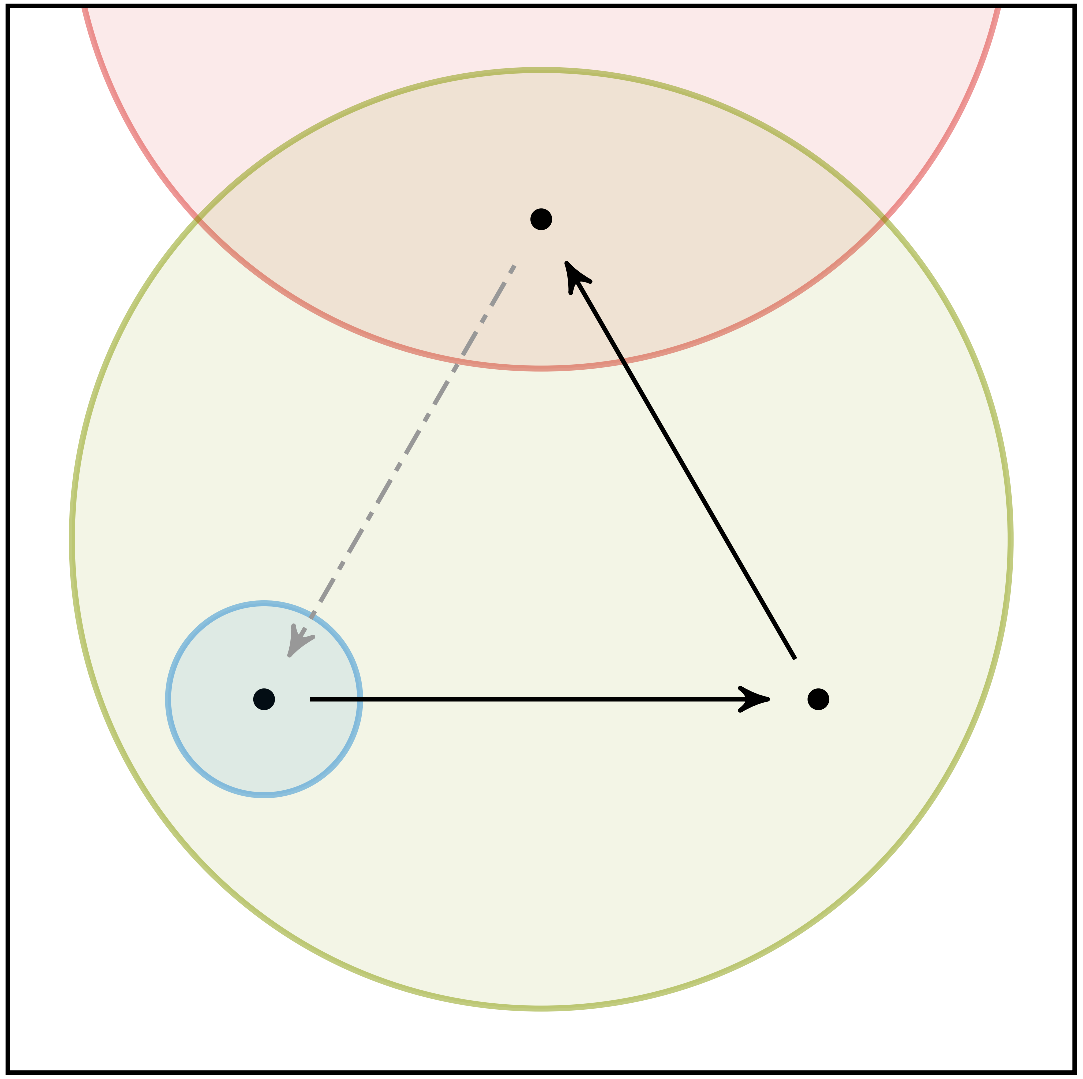
Alt i **NP** kan (per def.) reduseres til alt i **NPH**, og dermed **NPC**



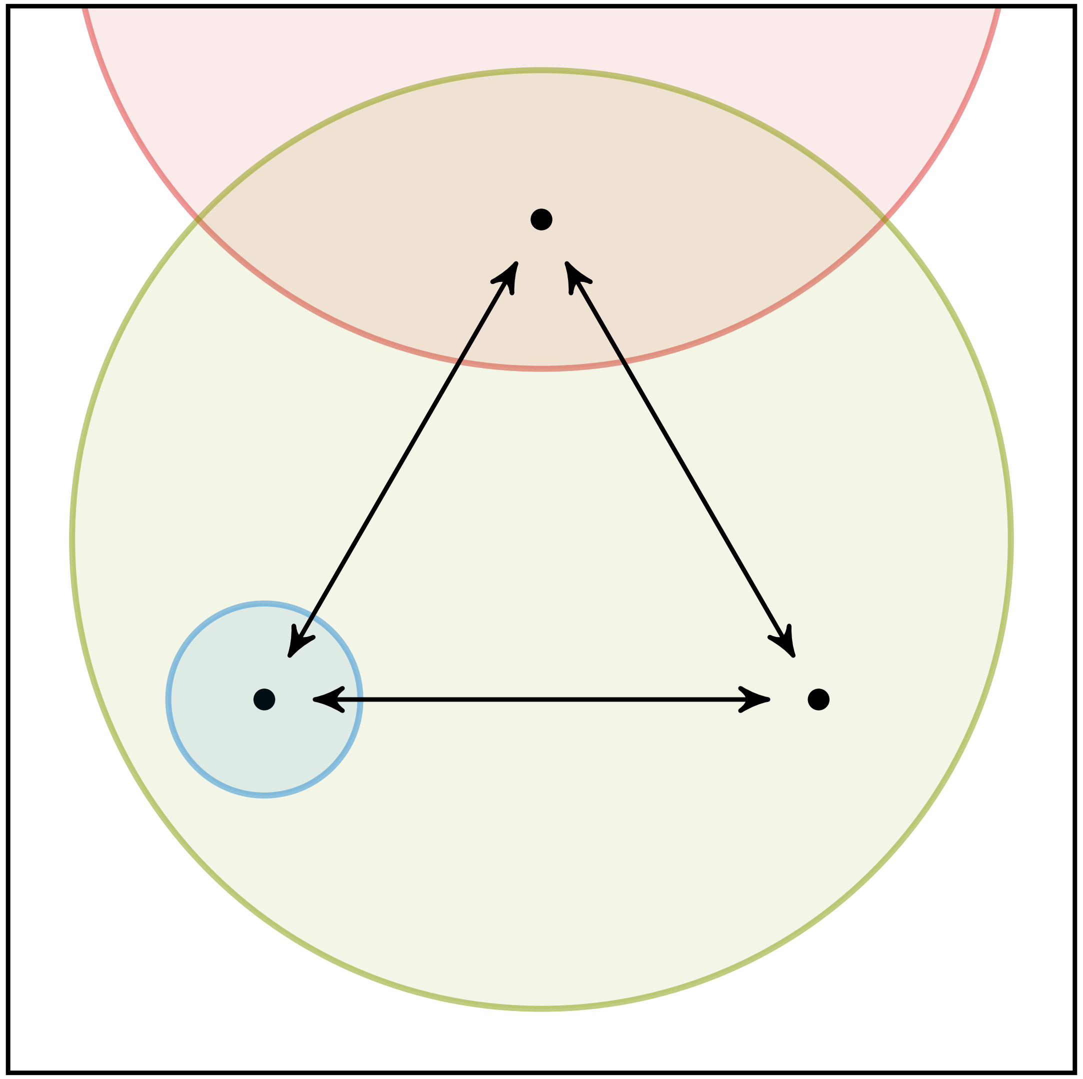
Problemer i **P** kan (trivielt, ved å løses) reduseres til alt i **NP**



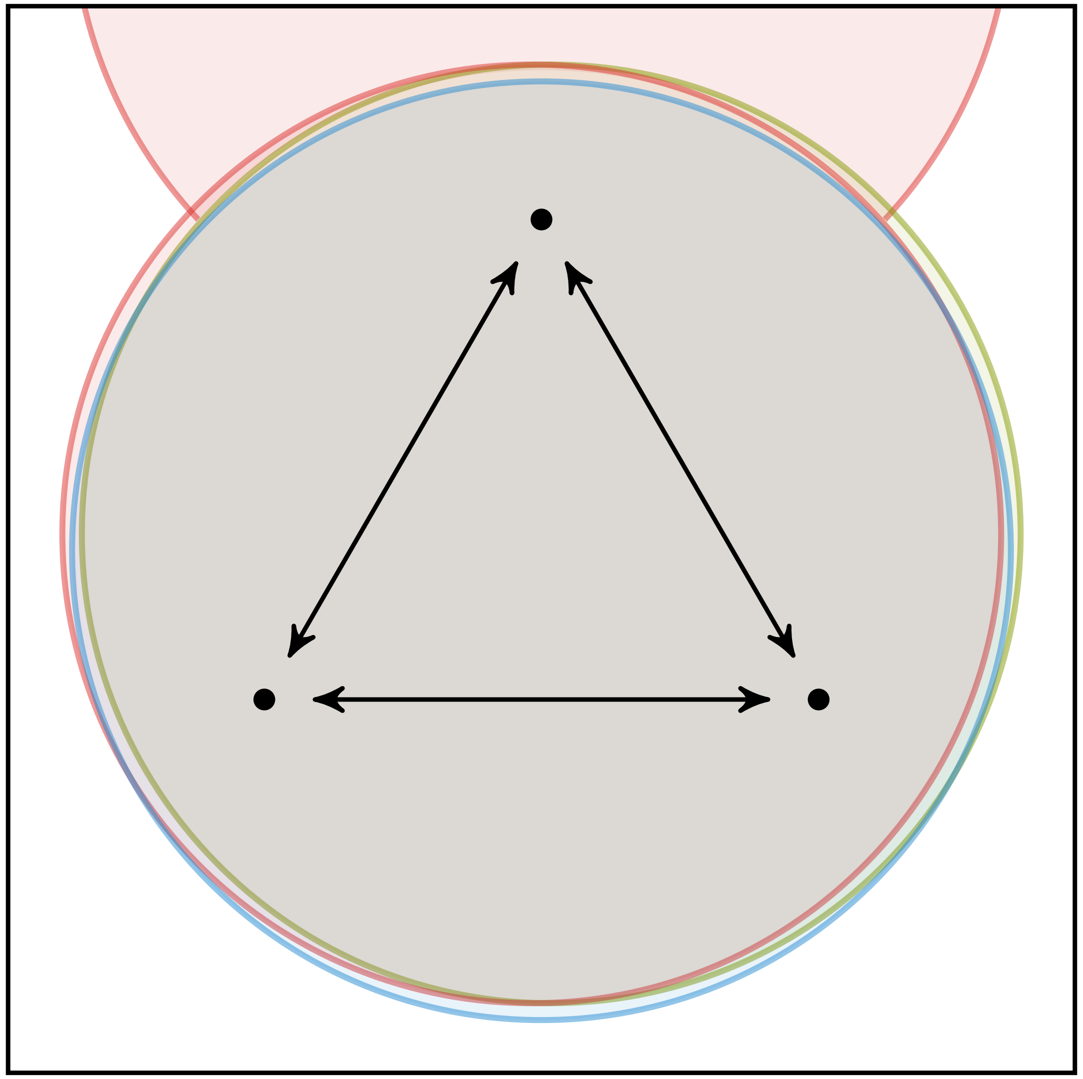
Dette er slik vi tror verden ser ut



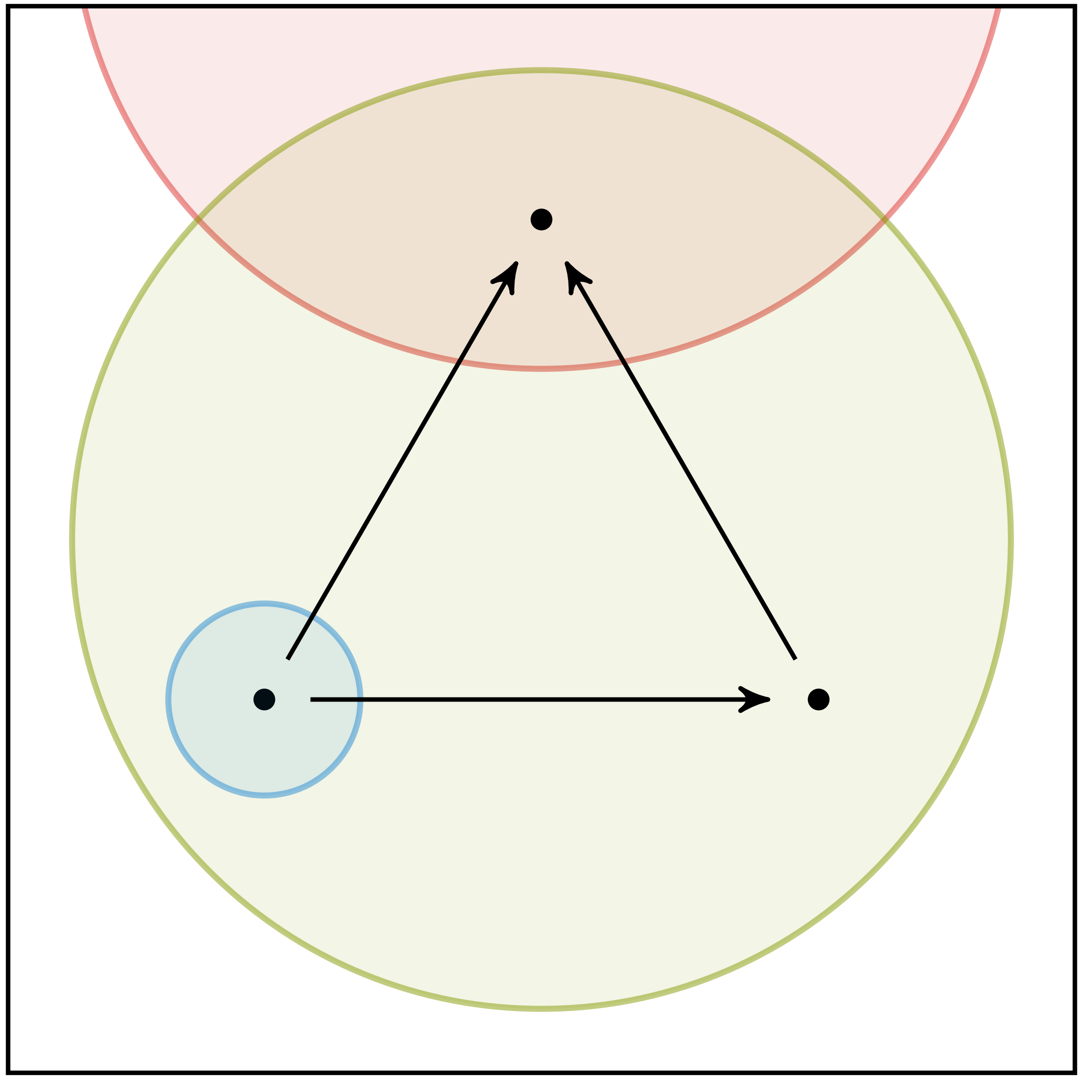
Hva om vi finner en reduksjon fra **NPC** til **P**?



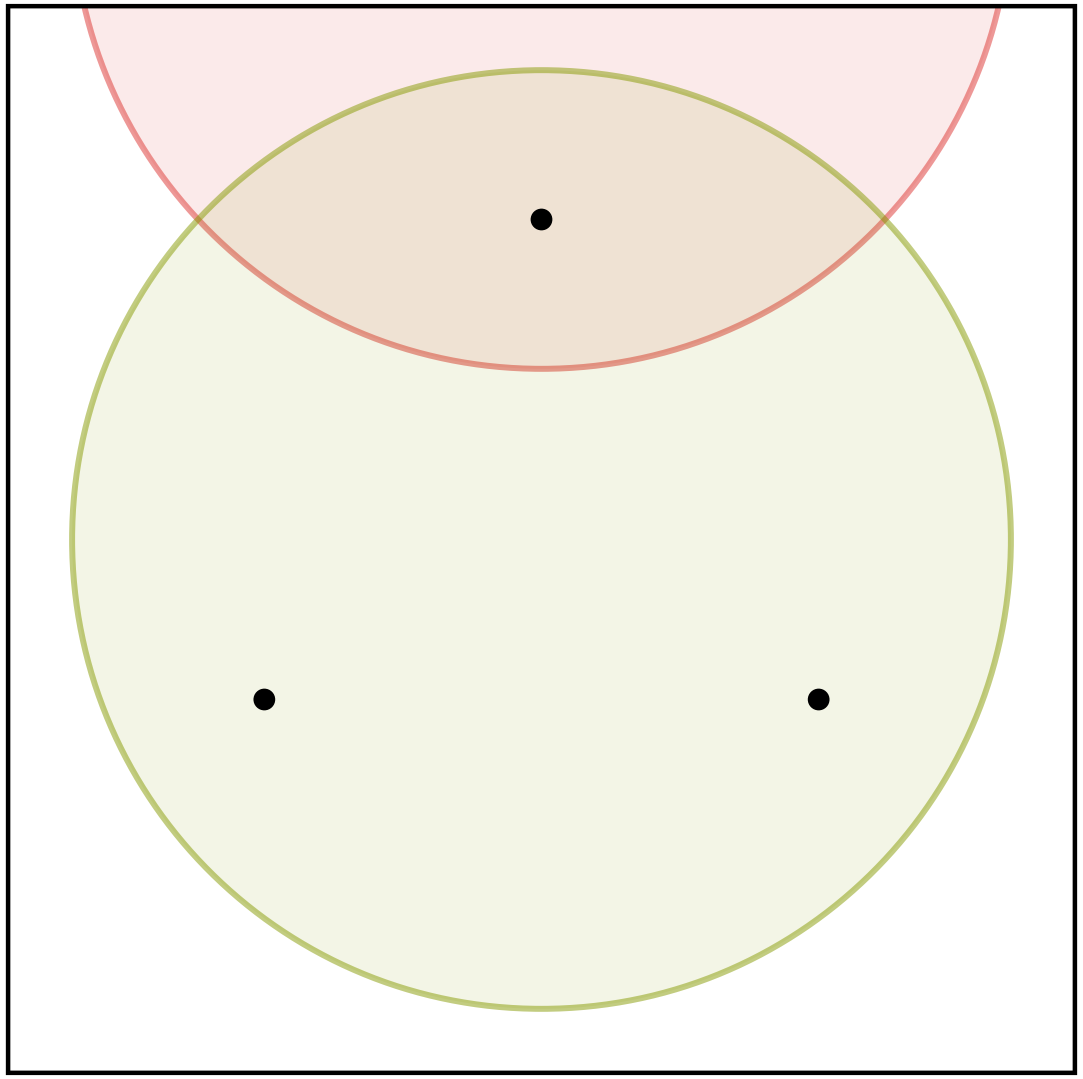
Da kan vi redusere alt i **NP** til alt annet i **NP** . . .



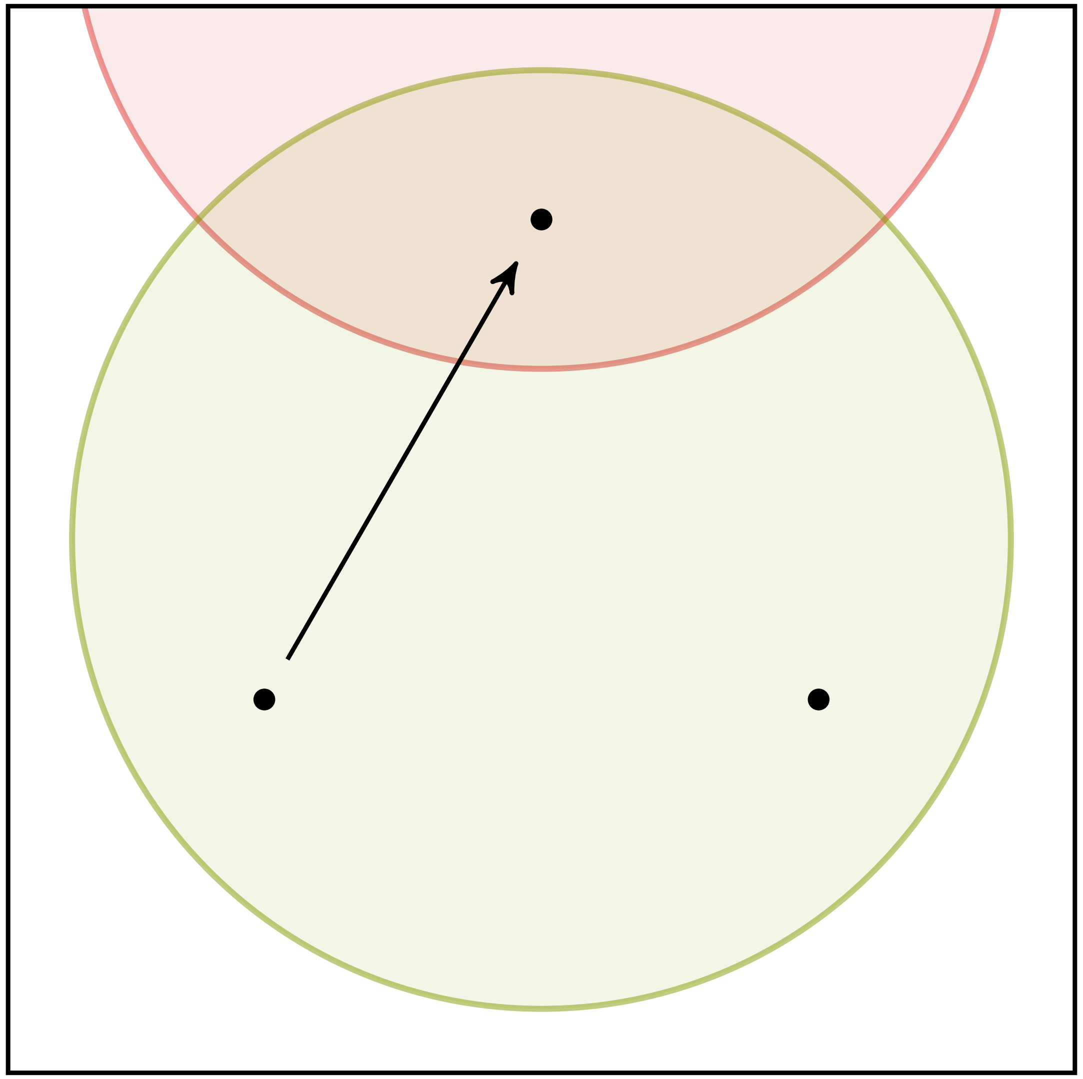
. . . som betyr at **P**, **NP** og **NPC** er samme klasse!



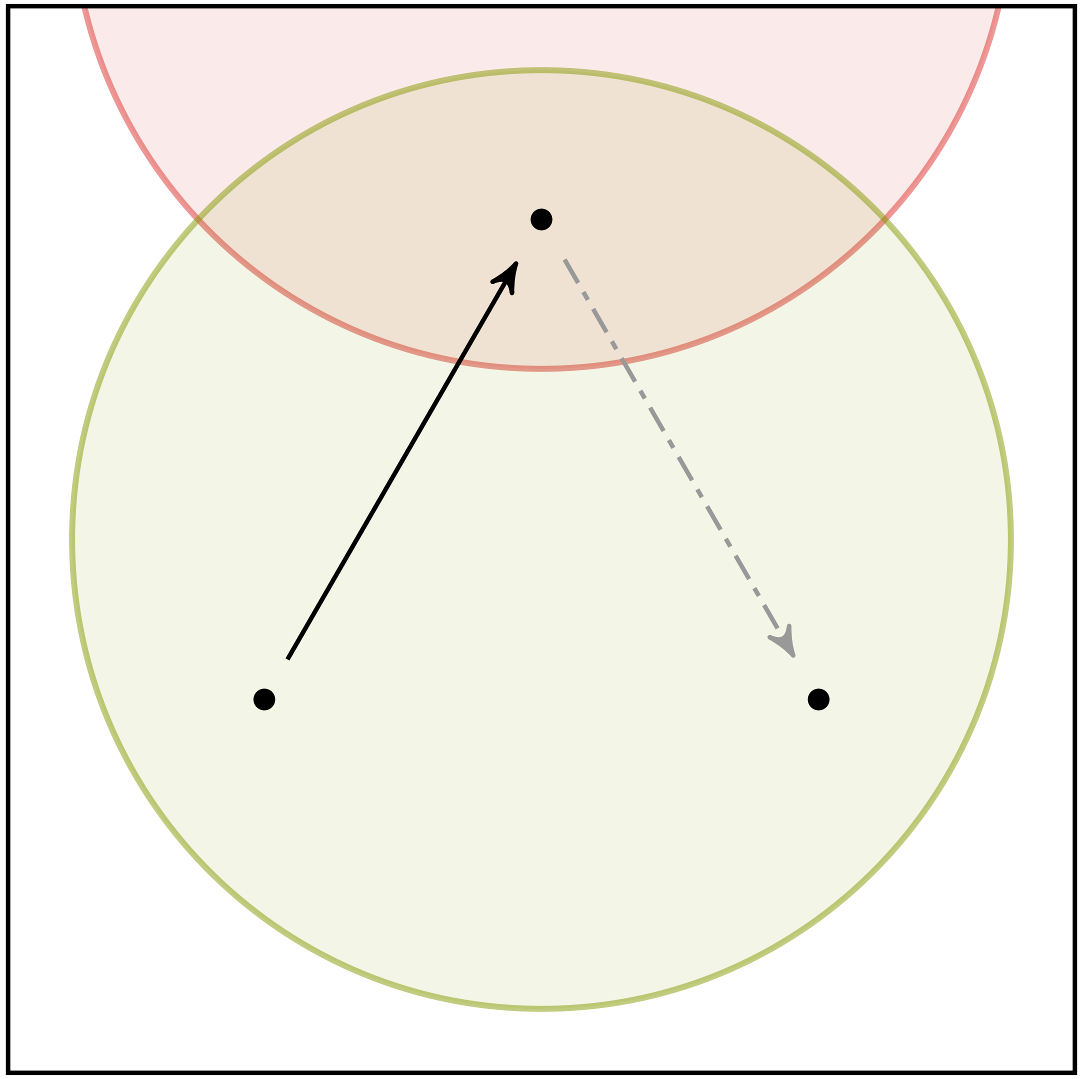
De fleste av oss tror ikke at $\mathbf{P} = \mathbf{NP}$



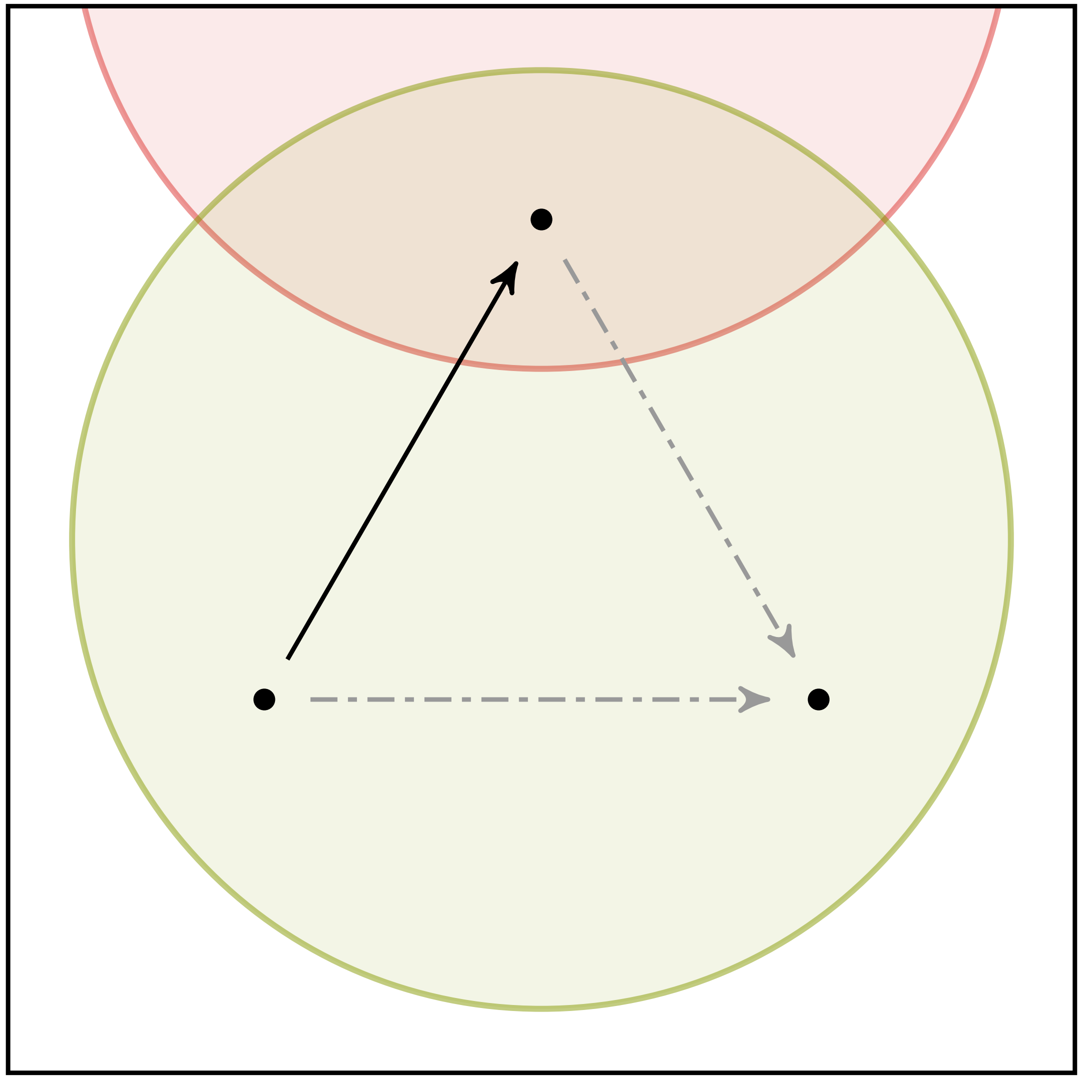
Vi kan bruke reduksjoner til å karakterisere problemer



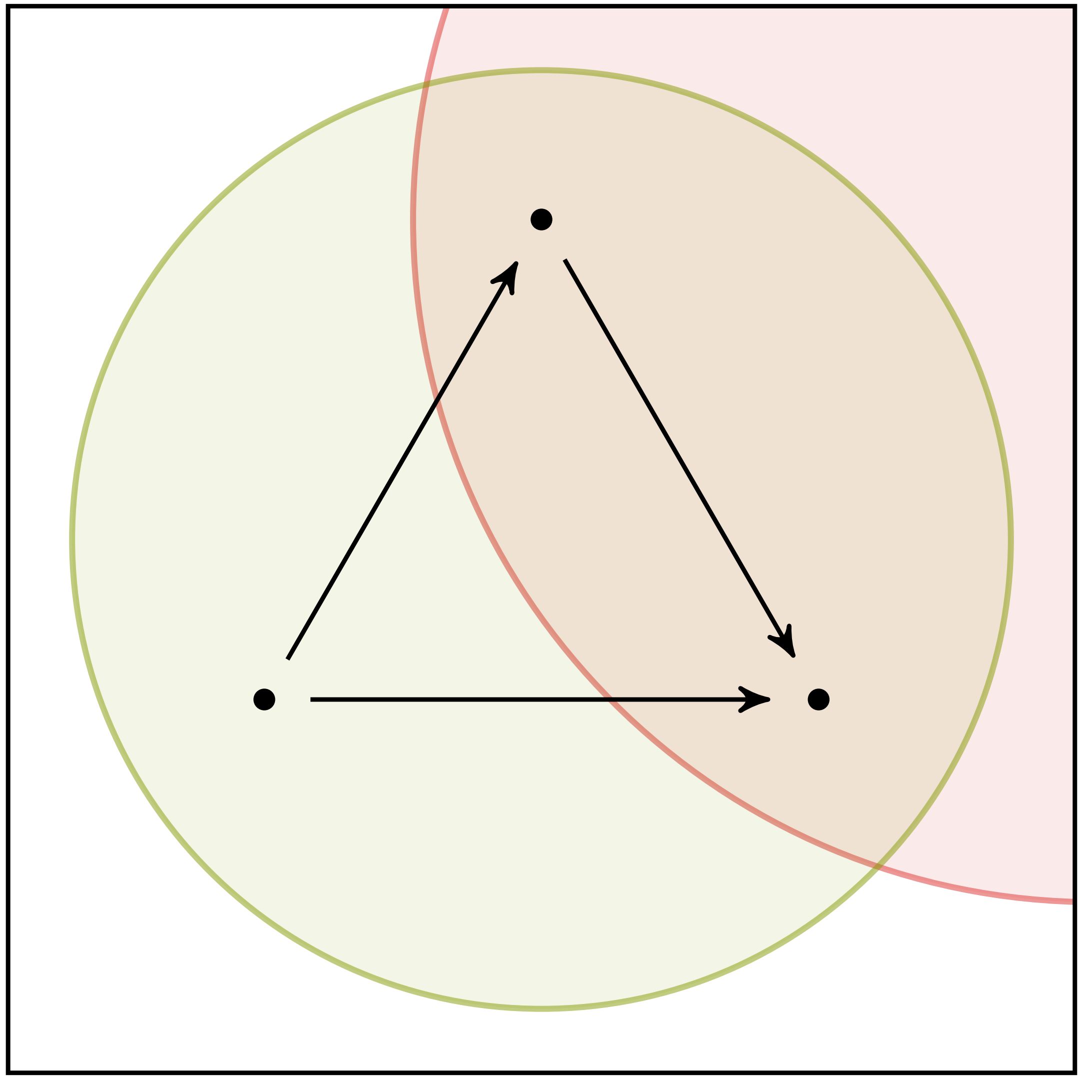
Om vi reduserer til **NPC** forteller det ingenting



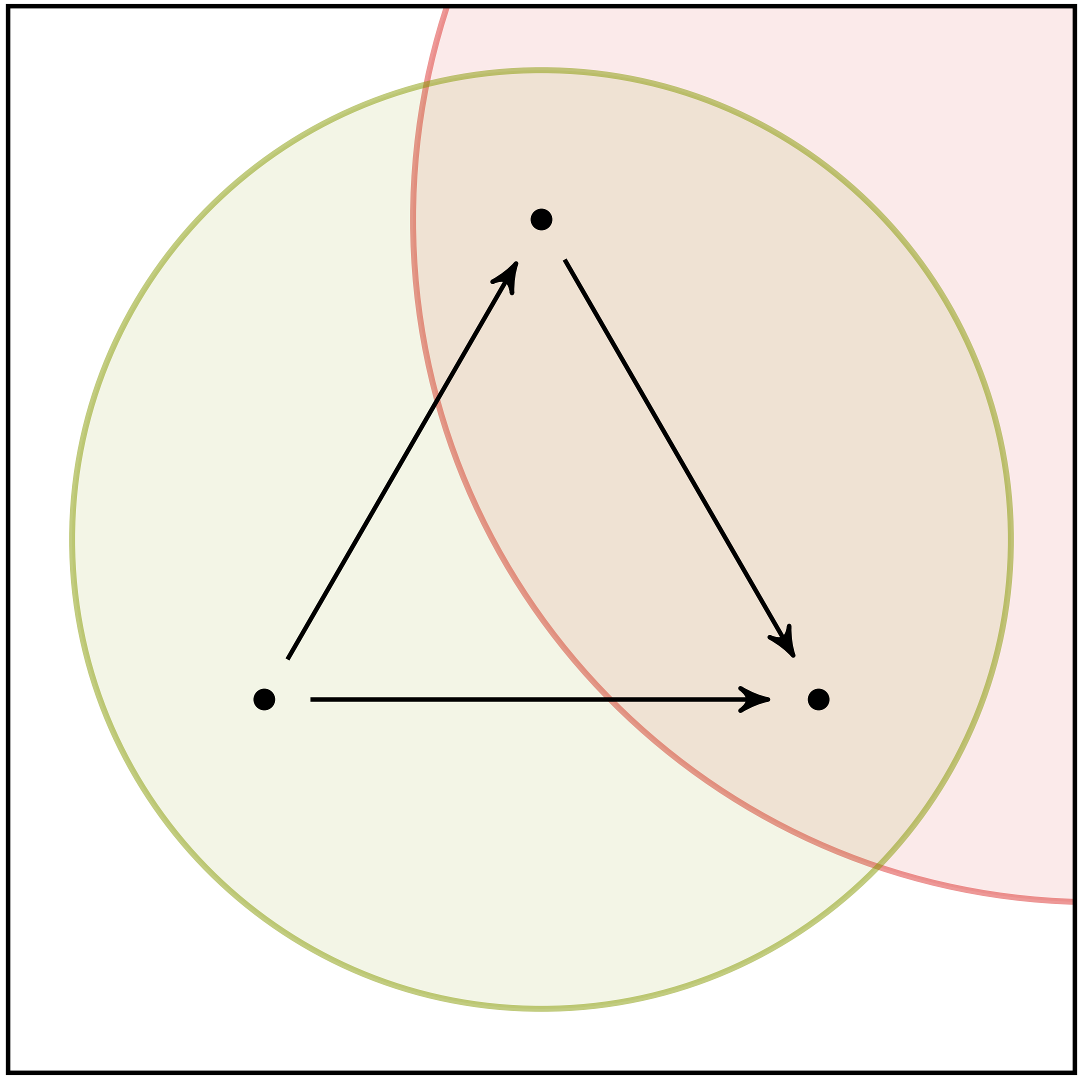
Hva med en reduksjon fra **NPC** til **NP**?



Alt i **NP** kan da reduseres til problemet vårt



Det er jo definisjonen på et **NP**-komplett problem!



Altså: For å vise at et problem er i **NPC** må vi redusere fra **NPC**

$$L \in \mathbf{NPC}$$

Hvordan viser vi at L er **NP**-komplett?

› Vis at L $\in$ **NP**

At sertifikat for ja-svar kan verifiseres i pol. tid

- Vis at $\mathrm{L} \in \mathbf{NP}$
- Velg et kjent **NP**-komplett språk L'

- Vis at L $\in$ **NP**
- Velg et kjent **NP**-komplett språk L$'$
- Beskriv en algoritme som beregner en funksjon

$$f : \{0,1\}^* \rightarrow \{0,1\}^*$$

som mapper instanser av L$'$ til instanser av L

Dette er altså reduksjonen fra L$'$ til L, som viser L$' \leq_{\mathbf{P}}$ L

- Vis at L $\in$ **NP**
- Velg et kjent **NP**-komplett språk L$'$
- Beskriv en algoritme som beregner en funksjon

$$f : \{0,1\}^* \to \{0,1\}^*$$

som mapper instanser av L$'$ til instanser av L
- Vis at

$$x \in \mathrm{L}' \iff f(x) \in \mathrm{L}\,,$$

for alle $x \in \{0,1\}^*$

Vi må sørge for at vi får samme svar for $f(x)$

- Vis at $\mathrm{L} \in \mathbf{NP}$
- Velg et kjent **NP**-komplett språk L'
- Beskriv en algoritme som beregner en funksjon

$$f : \{0,1\}^* \to \{0,1\}^*$$

  som mapper instanser av L' til instanser av L
- Vis at

$$x \in \mathrm{L}' \iff f(x) \in \mathrm{L}\,,$$

  for alle $x \in \{0,1\}^*$
- Vis at algoritimen som beregner f har polynomisk kjøretid

1. Problemer

2. Reduksjoner

3. Kompletthet