NP-kompletthet, Polynomtidsreduksjoner

IN2010 – Algoritmer og Datastrukturer

Uke 46, 2020

Institutt for Informatikk

Denne videoen

- en formell definisjon for når et avgjørelsesproblem er “vanskeligere” enn et annet
- “vanskeligste” problemer i NP, hva trengs for å vise at P=NP

Kjap repetisjon

- Et *avgjørelsesproblem* hvor svaret er JA/NEI
  "Sorted: Er en liste sortert?"
  "Reachability: Finnes det en sti mellom to par av noder i en graf?"
- En *instans* av et problem er inputtet
- P var klassen av avgjørelsesproblemer hvor en løsning kan beregnes i polynomisk tid
- NP var klassen av agjørelsesproblemer hvor en løsning kan verifiseres i polynomisk tid

Reduksjoner

"Reduksjon" er et fancy ord for prosessen av å ta et problem og oversette det til et annet

- vi reduserer problemer hele tida!
- i oblig 3 reduserte dere et problem som handler om mobilnettverk og signaltårn til et grafproblem. En løsning for grafproblemet tilsvarte en løsningen for det opprinnelige problemet
- mange forskjellige typer reduksjon; vi er primært interessert i å klassifisere hvor vanskelig et problem er å løse

Polynomtidsreduksjoner

Intuitivt: en måte å si at et avgjørelsesproblem B er minst like vanskelig som et problem A. Vi skriver $A \leq_p B$ for dette.

Mer formelt: En polynomtidsreduksjon fra A til B er en algoritme som oversetter fra instanser i A til instanser i B slik at

- alle JA-instanser i A blir oversatt til JA-instanser i B (tilsvarende for NEI-instanser)
- oversettelsen gjøres i polynomtid

Polynomtidsreduksjoner: eksempler

Even	
Instans:	Et tall n
Spørsmål:	Er n et partall?

Odd	
Instans:	Et tall n
Spørsmål:	Er n et oddetall?

- oversettelse: Even-instans: n blir til Odd-instans: $n + 1$.
- å sjekke om n er et partall er minst like vanskelig som å sjekke om det er et oddetall, Even $\leq_p$ Odd

MST-k	
Instans:	En graf G og et tall k
Spørsmål:	Har G minst k sterkt sammenhengende komponenter?

Sorted	
Instans:	En liste L
Spørsmål:	Er elementene i L sortert?

Oversettelse for MST-k $\leq_p$ Sorted:

- beregn sterkt sammenhengende grafer i MST-k instansen G
- Hvis det er flere enn k sterkt sammenhengende komponenter, oversett til listen $(1, 2, 3)$
- Hvis det er færre enn k sterkt sammenhengende komponenter, oversett til listen $(1, 3, 2)$

Alle polynomtidsløsbare problemer kan reduseres til hverandre!

NP-harde problemer

Et problem L er NP-hardt hvis

- for alle problemer A i NP, $A \leq_p L$.

Intuitivt tilsvarer dette alle problemer som er minst like vanskelig å løse enn alle problemer i NP.

SAT

Boolske uttrykk

- variabler $X_1, X_2, X_3, \dots$ som kan ha verdi 1 eller 0
- flippe bits: Hvis $X = 0$ så er $\overline{X} = 1$, hvis $X = 1$ så er $\overline{X} = 0$.
- addisjon og multiplikasjon

$X_1\overline{X_2}X_2$: NEI-Instans

$(X_1 + \overline{X_3})(\overline{X_2} + X_1)(\overline{X_1} + X_2 + X_3)$: JA-Instans

Satisfiability	
Instans:	Et boolsk uttrykk U
Spørsmål:	Finnes det en tilordning til variablene i U som fører til at resultatet er større enn 0?

SAT

Satisfiability	
Instans:	Et boolsk uttrykk U
Spørsmål:	Finnes det en tilordning til variablene i U som fører til at resultatet er større enn 0?

NP-hardt: Cook-Levins teorem, som viste direkte at alle problemer i NP kan polynomtidreduseres til SAT. Med andre ord, for alle A i NP er $A \leq_p SAT$

Kan et problem som er vanskeligere enn alle problemer i NP være i NP selv?
Kan SAT verifiseres i polynomisk tid?

SAT er i NP

Satisfiability	
Instans:	Et boolsk uttrykk U
Spørsmål:	Finnes det en tilordning til variablene i U som fører til at resultatet er større enn 0?

SAT-Verifier: Sertifikat inneholder 0,1-tilordning for alle variabler. Parse instansen og erstatt hver variabel med sin 0,1-tilordning. Regn ut resultatet og returnér JA hvis større enn 0.

Eksempel:

Instans: $(X_1 + \overline{X_3})(\overline{X_2} + X_1)(\overline{X_1} + X_2 + X_3)$

Sertifikat: $X_1 = 1, X_2 = 0, X_3 = 1$

Verifiserer: $(1 + 0)(1 + 1)(0 + 0 + 1) = 2 > 0$, dermed JA

Verifiseringen er i polynomisk tid (fin øvelse!), dermed er SAT i NP.

NP-kompletthet

Et avgjørelsesproblem L er *NP-komplett* hvis

1. L er i NP, og
2. L er NP-hardt, dvs. at hvert problem A i NP kan reduseres i polynomtid til L: $A \leq_p L$.

SAT er så å si det "første" NP-komplette problemet og setter fundamentet for å vise at andre problemer er NP-komplette.

Hvordan vise NP-kompletthet

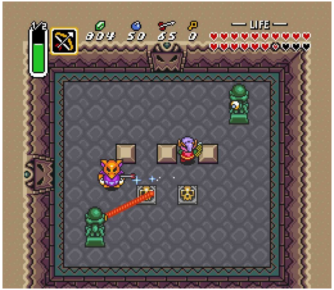
- Vis medlemskap i NP: vis feks. at problemet L kan verifiseres i polynomisk tid
- Vis NP-hardt: velg et "egnet" kjent NP-komplett problem L' og vise at $L' \leq_p L$

Hamiltonsykel	
Instans:	En graf G
Spørsmål:	Finnes det en sykel i G som besøker alle noder nøyaktig en gang?

Knapsack	
Instans:	En mengde objekter med hver sin vekt og verdi, og to tall s og t
Spørsmål:	Finnes det en mengde objekter som som tilsammen er verdt mer enn t og veier mindre enn s?

Sudoku	
Instans:	Et ufullstendig fylt ut $n \times n$ Sudoku brett
Spørsmål:	Har inputbrettet en gyldig løsning?

- kartet består av flere rom som ar forbundet av dører
- inngangshallen inneholder en låst skattekiste og dører til andre rom
- i hvert rom befinner seg enten fiender eller en puzzle
- etter fiendene er drept/puzzlet er løst blir et lys tent
- hvis Link går inn i et rom hvor lyset allerede er tent, blir han drept av en usynlig fiende
- når alle lys er tent åpner seg skattekisten i inngangshallen.



ZeldaDungeon	
Instans:	Et ZeldaDungeon kart K
Spørsmål:	Kan Link åpne skattekisten i dungeon K?

ZeldaDungeon	
Instans:	Et ZeldaDungeon kart K
Spørsmål:	Kan Link åpne skattekisten i dungeon K?

- for å åpne skattekisten, må Link besøke alle rom nøyaktig en gang, slå fiendene/løse puzzlet i hvert rom og komme seg tilbake til inngangshallen
- ligner på Hamiltonsykel...et NP-komplett problem!

Hamiltonsykel	
Instans:	En graf G
Spørsmål:	Finnes det en sykel i G som besøker alle noder nøyaktig en gang?

Hamiltonsykel $\leq_p$ ZeldaDungeon

Vi skal lage en polynomtidsreduksjon. Ta en instans G fra Hamiltonsykel og oversett:

- noder i G blir rom i ZeldaDungeon
- kanter i G blir dør mellom de respektive rommene
- hvert rom inneholder en fiende som dør med en gang Link ser på den

Hvis Link kan åpne skattekisten, så finnes det en vei som går gjennom alle rom nøyaktig en gang og så tilbake til inngangshallen. Denne veien tilsvarer en sykel i grafen G som går gjennom alle noder nøyaktig en gang.

Hvis Link ikke kan åpne skattekisten, så finnes det ingen slik vei, og dermed ingen Hamiltonsykel.

$\rightarrow$ Hamiltonsykel $\leq_p$ ZeldaDungeon

ZeldaDungeon er NP-hardt

Hamiltonsykel $\leq_p$ ZeldaDungeon.

- vi vet at $A \leq_p$ Hamiltonsykel for alle problemer A i NP.
- så $A \leq_p$ Hamiltonsykel $\leq_p$ ZeldaDungeon for alle A i NP.
- dermed $A \leq_p$ ZeldaDungeon for alle A i NP, og ZeldaDungeon er NP-hardt.

Er ZeldaDungeon i NP?

- kan vi ikke si, siden kompleksiteten av puzzles/fiender ikke er kjent
- en variant uten puzzles og fiender er NP-komplett (og er bare en omformulering av Hamiltonsykel)

Flere eksempler av NP-komplette problemer i pensumboka.
Bevis for at klassiske Nintendo spill er NP-harde: `https://arxiv.org/abs/1203.1895`

P=NP?

Så hvorfor vet vi ikke om P=NP?

- det er ukjent om et NP-komplett problem kan løses i polynomtid (alle kjente deterministiske algoritmer for NP-komplette problemer kjører i eksponensiell tid)
- hvis man finner en polynomtidsalgoritme for et NP-komplett problem L, har man funnet en polynomtidsalgoritme for *alle* problemer i NP.
- mange forskjellige måter å prøve å vise P$\neq$NP: ender opp med å vise at det finnes et problem i NP som ikke har en polynomtid algoritme