INF3170 – Logikk

Forelesning 0: Mengdelære, Induksjon

Martin Giese

Institutt for informatikk, Universitetet i Oslo

23. januar 2008

Dagens plan

Mengder

Definisjon

- *En mengde er en endelig eller uendelig samling objekter der innbyrdes rekkefølge og antall forekomster av hvert objekt ignoreres.*
- *Objektene i en mengde kalles elementer.*
- *Hvis a er element i mengden S, skriver vi $a \in S$. Hvis a ikke er element i S, skriver vi $a \notin S$.*
- *To mengder S og T er like, $S = T$, hvis de inneholder de samme elementene.*

Notasjon

Mengden med elementene a, b, c og d skrives ofte $\{a, b, c, d\}$.

Spørsmål: Hvor mange elementer har $\{a, b, c, d\}$?

Mengder

Antagelse: $a, b, c, d, 1, 2, \gamma, \Phi$ er alle forskellige

Eksempel

- $a \in \{a, b, c\}$
- $d \notin \{a, b, c\}$
- $1 \in \{a, 1, \gamma, \Phi\}$
- $2 \notin \{a, 1, \gamma, \Phi\}$
- $\{a, b\} = \{b, a\}$
- $\{a, a, b\} = \{a, b\}$
- $\{a, b\} \neq \{b, c\}$ *(mengdene er ulike)*

Noen spesielle mengder

Definisjon (Den tomme mengden)

- *Den tomme mengden er mengden som ikke inneholder noen elementer.*
- *Skrives ofte $\{\}$ eller $\emptyset$.*

Definisjon (Singletonmengde)

En singletonmengde er en mengde som har nøyaktig ett element.

Eksempel

Både $\{a\}$, $\{b\}$ og $\{b, b\}$ er singletonmengder.

Union – slå sammen mengder

Definisjon (Union)

- *Unionen av to mengder S og T er den mengden som inneholder alle objekter som er element i S eller T.*
- *Unionen av S og T skrives ofte $S \cup T$.*

Eksempel

- $\{a, b\} \cup \{c, d\} = \{a, b, c, d\}$
- $\{a, b\} \cup \{b, c\} = \{a, b, c\}$
- $\{1, 2, 3\} \cup \emptyset = \{1, 2, 3\}$

Snitt – felles elementer

Definisjon (Snitt)

- *Hvis S og T er mengder, så er snittet mellom S og T, eller S snittet med T, mengden som inneholder alle objekter som er element i både S og T.*
- *S snittet med T skrives ofte $S \cap T$.*

Eksempel

- $\{a, b\} \cap \{c, d\} = \emptyset$
- $\{a, b\} \cap \{b, c\} = \{b\}$
- $\{1, 2, 3\} \cap \emptyset = \emptyset$

Mengdedifferanse – fjerne elementer

Definisjon (Mengdedifferanse)

- *Hvis S og T er mengder, så er mengdedifferansen mellom S og T, eller S minus T, mengden som inneholder alle objekter som er element i S men ikke element i T.*
- *S minus T skrives ofte $S \setminus T$.*

Eksempel

- $\{a, b\} \setminus \{c, d\} = \{a, b\}$
- $\{a, b\} \setminus \{b, c\} = \{a\}$
- $\{1, 2, 3\} \setminus \emptyset = \{1, 2, 3\}$
- $\emptyset \setminus \{a, b, c\} = \emptyset$

Delmengde

Definisjon (Delmengde)

- *En mengde S er en delmengde av en mengde T hvis alle elementer i S også er elementer i T.*
- *Skrives ofte $S \subseteq T$.*

Eksempel

- $\{a, b\} \subseteq \{a, b, c\}$
- $\{a, b\} \subseteq \{a, b\}$ *(enhver mengde er en delmengde av seg selv)*
- $\{a, b, c\} \not\subseteq \{a, b\}$
- $\emptyset \subseteq \{a, b\}$ *(den tomme mengden er en delmengde av alle mengder)*
- $\{a, b\} \not\subseteq \emptyset$

Kryssprodukt

Definisjon (Kryssprodukt)

- *Hvis S og T er mengder, så er kryssproduktet av S og T mengden av alle par $\langle s, t \rangle$ slik at $s \in S$ og $t \in T$.*
- *Kryssproduktet av S og T skrives ofte $S \times T$.*

Eksempel

- $\{a, b\} \times \{c, d\} = \{\langle a, c \rangle, \langle a, d \rangle, \langle b, c \rangle, \langle b, d \rangle\}$
- $\{a, b\} \times \{b, c\} = \{\langle a, b \rangle, \langle a, c \rangle, \langle b, b \rangle, \langle b, c \rangle\}$
- $\{a\} \times \{1, 2\} = \{\langle a, 1 \rangle, \langle a, 2 \rangle\}$

Kryssprodukt

Notasjon

- *En mengde kan krysses med seg selv: $S \times S$*
- $\{a, b\} \times \{a, b\} = \{\langle a, a \rangle, \langle a, b \rangle, \langle b, a \rangle, \langle b, b \rangle\}$
- *$S \times S \times S$ skrives ofte S^3.*
- *Generalisert: $\underbrace{S \times S \times \ldots \times S}_{n}$ skrives S^n.*

Mengdebygger

Notasjon

En definisjon på formen "mengden av alle elementer $x \in S$ slik at ..." kan skrives på formen

$$\{x \mid x \in S \text{ og betingelse på } x\}.$$

En slik konstruksjon kalles en mengdebygger.

Eksempel

- *Definisjonen av kryssprodukt av S og T kunne vært skrevet slik:*

$$S \times T = \{\langle s, t\rangle \mid s \in S \text{ og } t \in T\}$$

- $\{n \mid n \in \mathbb{N}$ *og* n *er partall* $\}$ *definerer mengden av alle partall.*
- $\{n \mid n \in \mathbb{N}$ *og* n *er oddetall* $\}$ *definerer mengden av alle oddetall.*

Mengder av mengder

Det er mulig å konstruere mengder som inneholder andre mengder (med visse restriksjoner)

Eksempel

- $\{\emptyset\} \neq \emptyset$
- $\{\{0\}, \{1\}, \{2\}, \ldots\} = \{\{n\} \mid n \in \mathbb{N}\}$
- $\{\{0\}, \{0,1\}, \{0,1,2\}, \ldots\} = \{\{m \mid 0 \leq m \leq n\} \mid n \in \mathbb{N}\}$
- $\{\{0,2,4,6,\ldots\}, \{1,3,5,7,\ldots\}\}$

Snitt av mengder av mengder

Definisjon

Snittet av en mengde $\mathcal{M}$ av mengder inneholder alle elementer som er element av alle $M \in \mathcal{M}$:

$$\bigcap \mathcal{M} := \{x \mid x \in M \text{ for alle } M \in \mathcal{M}\}$$

Eksempel

- $\bigcap\{\{0\}, \{0,1\}, \{0,1,2\}, \ldots\} = \{0\}$
- $\bigcap\{\{0,2,4,6,\ldots\}, \{1,3,5,7,\ldots\}\} = \emptyset$

Union av mengder av mengder

Definisjon

Unionen av en mengde $\mathcal{M}$ av mengder inneholder alle elementer som er element av minst en $M \in \mathcal{M}$:

$$\bigcup \mathcal{M} := \{x \mid x \in M \text{ for noen } M \in \mathcal{M}\}$$

Eksempel

- $\bigcup\{\{0\}, \{0,1\}, \{0,1,2\}, \ldots\} = \mathbb{N}$
- $\bigcup\{\{0,2,4,6,\ldots\}, \{1,3,5,7,\ldots\}\} = \mathbb{N}$

Relasjoner

Definisjon (Relasjon)

- *En unær relasjon over S er en delmengde av S.*
- *En binær relasjon fra S til T er en delmengde av $S \times T$.*
- *En n-ær relasjon over mengdene $S_1, S_2, \ldots, S_n$ er en delmengde av kryssproduktet $S_1 \times S_2 \times \ldots \times S_n$.*

Eksempel

- *Hvis $S = \{a, b, c\}$, så er $\{a, b\}$ en unær relasjon over S.*
- *Hvis $S = \{a, b\}$ og $T = \{1, 2\}$, så er $\{\langle a, 1\rangle, \langle b, 2\rangle\}$ en binær relasjon fra S til T.*

Relasjoner over én mengde

Definisjon

En n-ær relasjon over mengden S er en delmengde av S^n.

Eksempel

La $S = \{1, 2, 3\}$.

- *$\{\langle 1, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle\}$ er en binær relasjon over S.*
- *$\{\langle 1, 2\rangle, \langle 1, 3\rangle, \langle 2, 3\rangle\}$ er også en binær relasjon over S.*

Refleksive relasjoner

Definisjon (Refleksiv)

En binær relasjon R over mengden S er refleksiv hvis $\langle x, x\rangle \in R$ for alle $x \in S$.

Eksempel

La $S = \{1, 2, 3\}$.

- *Er $R_1 = \{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 1, 3\rangle\}$ refleksiv?*
- *Hva med $R_2 = \{\langle 1, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle\}$?*

Symmetriske relasjoner

Definisjon (Symmetrisk)

En binær relasjon R er symmetrisk hvis for alle x, y med $\langle x, y\rangle \in R$, også $\langle y, x\rangle \in R$.

Eksempel

La $S = \{1, 2, 3\}$.

- *Er $R_1 = \{\langle 1, 2\rangle, \langle 2, 1\rangle, \langle 3, 2\rangle, \langle 2, 3\rangle\}$ symmetrisk?*
- *Hva med $R_2 = \{\langle 1, 2\rangle, \langle 2, 1\rangle, \langle 1, 3\rangle\}$?*

Transitive relasjoner

Definisjon (Transitiv)

En binær relasjon R er transitiv hvis for alle x, y, z med $\langle x, y\rangle \in R$ og $\langle y, z\rangle \in R$, også $\langle x, z\rangle \in R$.

Definisjon (Ekvivalensrelasjon)

En binær relasjon over mengden S er en ekvivalensrelasjon hvis den er refleksiv, symmetrisk og transitiv.

Funksjoner

Definisjon (Funksjon)

La S og T være mengder. En funksjon f fra S til T er en binær relasjon fra S til T med følgende egenskaper:

- *For alle $x \in S$ så finnes en $y \in T$ slik at $\langle x, y\rangle \in f$.*
- *Hvis $\langle x, y\rangle \in f$ og $\langle x, z\rangle \in f$, så er $y = z$.*

Vi kaller S for definisjonsmengden til f og T for verdimengden til f.

Notasjon

Hvis $\langle x, y\rangle \in f$, så skriver vi ofte $f(x) = y$.

Funksjoner

Eksempel

Funksjonen $Par : \mathbb{N} \to \{0, 1\}$ definert ved

$$Par(x) = \begin{cases} 1 \text{ hvis } x \text{ er et partall} \\ 0 \text{ hvis } x \text{ er et oddetall} \end{cases}$$

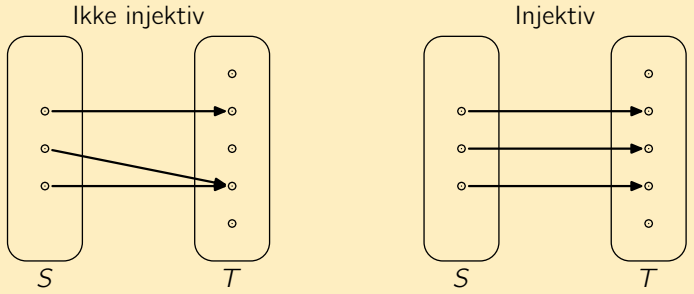
har $\mathbb{N}$ som definisjonsmengde og $\{0, 1\}$ som verdimengde.

Injektive funksjoner

Definisjon (Injektiv)

En funksjon $f : S \to T$ er injektiv hvis $f(x) \neq f(y)$ for alle $x, y \in S$ med $x \neq y$. Vi sier at f er en-til-en.

Eksempel

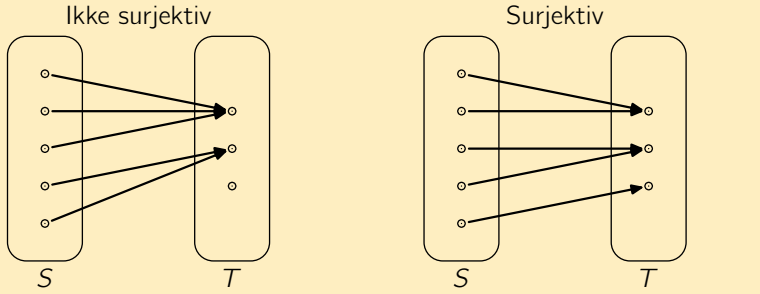


Surjektive funksjoner

Definisjon (Surjektiv)

En funksjon $f : S \to T$ er surjektiv hvis for alle $y \in T$ så finnes $x \in S$ slik at $f(x) = y$. Vi sier at f er på.

Eksempel



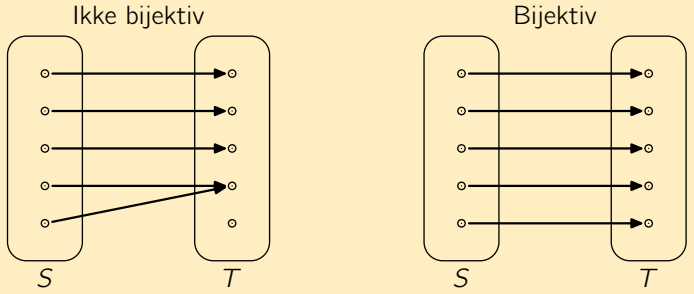
Bijektive funksjoner

Definisjon (Bijektiv)

En funksjon er bijektiv hvis den er injektiv og surjektiv.

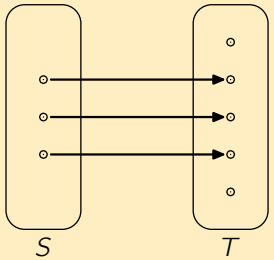
Vi sier at funksjonen er en-til-en og på, eller at vi har en en-til-en korrespondanse.

Eksempel



Injektive og surjektive funksjoner

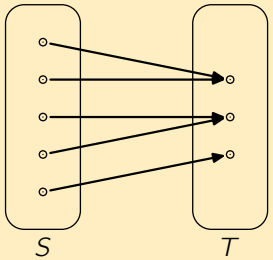
injektiv / en-til-en



for alle $x, y \in S$:
$x \neq y$ impliserer $f(x) \neq f(y)$

"hvert element i definisjonsmengden sendes til et unikt element i verdimengden"

surjektiv / på

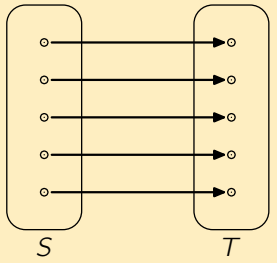


for alle $y \in T$:
det finnes $x \in S$ slik at $f(x) = y$

"alle elementer i verdimengden blir truffet"

Bijektive funksjoner

bijektiv / en-til-en og på / en-til-en korrespondanse



- En bijektiv funksjon er en funksjon som er både *injektiv* og *surjektiv*:
- *"Ethvert element i verdimengden blir truffet av et unikt element i definisjonsmengden"*.

Operatorer

Definisjon (Operator)

La S være en mengde.

- *En unær operator på S er en funksjon fra S til S.*
- *En binær operator på S er en funksjon fra $S \times S$ til S.*

Eksempel

- *Suksessorfunksjonen $(n+1)$ er en unær operator på $\mathbb{N}$.*
- *Addisjonsfunksjonen $(+)$ er en binær operator på $\mathbb{N}$.*
- *Subtraksjonsfunksjonen $(-)$ er en binær operator på $\mathbb{Z}$.*

Multimengder

Mengder der antall forekomster av hvert element teller

Definisjon (Multimengde)

En multimengde er et par $\langle S, m\rangle$ der S er en mengde og $m : S \to \mathbb{N}$. For hver $x \in S$ sier vi at $m(x)$ er multiplisiteten til x, eller antall forekomster av x i S.

Eksempel

Vi skriver multimengder som mengder:

- *I multimengden $\{a, a, a, b, b\}$ er multiplisiteten til a og b henholdsvis 3 og 2.*
- *I multimengden $\{a, b, a, c, a, b\}$ er multiplisiteten til a, b og c henholdsvis 3, 2 og 1.*

$\cup$, $\cap$, $\setminus$ og $\subseteq$ på multimengder

- Vi bruker union ($\cup$), snitt ($\cap$), mengdedifferans ($\setminus$) og delmengderelasjonen ($\subseteq$) også på multimengder.

Eksempel

- $\{a, a, b, c\} \cup \{a, c\} = \{a, a, a, b, c, c\}$
  d.v.s. $m(x) = m_1(x) + m_2(x)$
- $\{a, a, a, b, c\} \cap \{a, a, d\} = \{a, a\}$
  d.v.s. $m(x) = \min(m_1(x), m_2(x))$
- $\{a, a, a, b, c\} \setminus \{a, a, d\} = \{a, b, c\}$
  d.v.s. $m(x) = \max(0, m_1(x) - m_2(x))$
- $\{a, a\} \subseteq \{a, a, b, c\}$, *men* $\{a, a, a\} \not\subseteq \{a, a, b, c\}$
  d.v.s. $m_1(x) \leq m_2(x)$ *for alle* x.

- Vi bruker $\emptyset$ om den tomme multimengden.

Kardinalitet

Definisjon (Kardinalitet)

- *To mengder S og T har lik kardinalitet hvis det finnes en bijeksjon fra S til T.*
- *Mengden S har kardinalitet mindre eller lik T hvis det finnes en injektiv funksjon fra S til T.*
- *Hvis S er en endelig mengde, så er kardinaliteten til S lik antall elementer i S.*
- *Vi bruker notasjonen $|S|$ for kardinaliteten til S.*

Teorem (Bernstein)

Hvis det finnes en injektiv funksjon $f : S \to T$ og en injektiv funksjon $g : T \to S$, så finnes det også en bijeksjon $h : S \to T$.

Eksempel

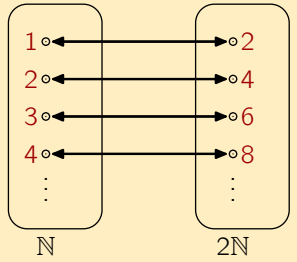
Hva er kardinaliteten til

- $\{a, b, c\}$*?*
- $\{a, b, a\}$*?*
- $\{a\}$*?*
- $\emptyset$*?*

Eksempel

- $\mathbb{N}$ = *mengden av alle naturlige tall* $\{1, 2, 3, 4, 5, \ldots\}$
- $2\mathbb{N}$ = *mengden av alle partall* $\{2, 4, 6, 8, 10, \ldots\}$

$f(x) = 2x$ *er en bijeksjon fra* $\mathbb{N}$ *til* $2\mathbb{N}$*, så* $\mathbb{N}$ *og* $2\mathbb{N}$ *har samme kardinalitet. Vi skriver* $|\mathbb{N}| = |2\mathbb{N}|$*.*



Tellbart vs. overtellbart

Definisjon (Tellbar)

En uendelig mengde S *er tellbar hvis det finnes en en-til-en korrespondanse mellom elementene i* S *og de naturlige tallene. Hvis ikke, er* S *overtellbar.*

- Alle endelige mengder er tellbare.
- Når en uendelig mengde S er tellbar finnes det en bijektiv funksjon fra S til $\mathbb{N}$.

Eksempel

- *Mengden* $2\mathbb{N}$ *av alle partall er tellbar.*
- *Mengden* $\mathbb{B}$ *av binære tall er tellbar.*
- *Mengden* $\mathbb{Q}$ *av brøktall er tellbar.*
- *Mengden av nålevende mennesker er tellbar.*
- *Mengden* $\mathbb{R}$ *av reelle tall er ikke tellbar.*

Induktive definisjoner

Definisjon (Induktiv definisjon)

Å definere en mengde induktivt betyr å konstruere den minste mengden som inneholder en gitt mengde B—kalt en basismengde—og som er lukket under gitte operasjoner.

Eksempel

Mengden $\mathbb{N}$ av naturlige tall kan defineres induktivt som minste mengde $\mathbb{N}$ med

- $0 \in \mathbb{N}$, *og*
- *hvis* $x \in \mathbb{N}$, *så* $x + 1 \in \mathbb{N}$.

Her er basismengden $\{0\}$ *og* $\mathbb{N}$ *er lukket under suksessorfunksjonen (x+1).*

Eksempel

Mengden $\mathbb{B}$ av binære tall kan defineres som minste mengde så at

- 0 *og* 1 *er binære tall, og*
- *hvis b er et binært tall, så er b*0 *og b*1 *binære tall.*

steg 0: 0 1
steg 1: 00 10 01 11
steg 2: 000 100 010 110 001 101 011 111
⋮

Eksempel

Mengden S av symmetriske strenger over alfabetet $\{a, b\}$ *kan defineres induktivt som minste mengde S slik at*

- $\epsilon \in S$ *(den tomme strengen),*
- *hvis* $x \in S$, *så* $axa \in S$ *og* $bxb \in S$.

steg 0: ϵ
steg 1: *aa* *bb*
steg 2: *aaaa* *abba* *baab* *bbbb*
⋮

Hvorfor den minste mengden?

Det er mange mengder som inkluderer *B* og som er lukket under gitte operasjoner.

Eksempel

Hvilke mengder N oppfyller:

- $0 \in N$, *og*
- *hvis* $x \in N$, *så* $x + 1 \in N$*?*

For eksempel:

- $\mathbb{N}$
- $\mathbb{Z}$
- $\{0, \frac{1}{2}, 1, \frac{3}{2}, \ldots\}$

Hva betyr egentlig 'minst'?

- La

$$\mathcal{M} := \{M \mid B \subseteq M \text{ og } M \text{ er lukket under operasjonene}\}$$

- $\mathcal{M}$ inneholder alle M som oppfyller kravene
- Ta snittet av alle sånne mengder:

$$M^* := \bigcap \mathcal{M}$$

- Da er $M^* \in \mathcal{M}$.
- Også er $M^* \subseteq M$ for alle $M \in \mathcal{M}$.
- Hvis $N \subseteq M$ for alle $M \in \mathcal{M}$ for noen mengde $N \in \mathcal{M}$, så er $N = M^*$.
- M^* er altså den entydige minste mengden i $\mathcal{M}$ med hensyn til $\subseteq$.

Induktiv definisjon av en funksjon

Hvis en mengde M er definert induktivt, så er det naturlig å definere funksjoner $M \to X$ induktivt.

Eksempel

Definer funksjonen $d : \mathbb{N} \to \mathbb{N}$ *induktivt ved*

- $d(0) := 0$
- $d(n+1) := d(n) + 1 + 1$ *for alle* $n \in \mathbb{N}$

Dette definerer d som minste relasjon $\subseteq \mathbb{N} \times \mathbb{N}$ som oppfyller

- $\langle 0, 0 \rangle \in d$ og
- $\langle n+1, m+1+1 \rangle \in d$ for alle $\langle n, m \rangle \in d$.

Eksempel (Naturlig tall representert av binær tall)

- $v(0) = 0$
- $v(1) = 1$
- $v(b0) = 2v(b)$ *for alle* $b \in \mathbb{B}$
- $v(b1) = 2v(b) + 1$ *for alle* $b \in \mathbb{B}$

Eksempel (Lengden av symmetrisk streng)

- $l(\epsilon) = 0$
- $l(axa) = l(x) + 2$ *for alle* $x \in S$
- $l(bxb) = l(x) + 2$ *for alle* $x \in S$

Strukturell induksjon

For å vise at alle naturlige tall $n \in \mathbb{N}$ har et egenskap $P(n)$

- Vis at egenskapet holder for 0, d.v.s. $P(0)$
- For alle $n \in \mathbb{N}$ med $P(n)$, vis at $P(n+1)$

Eksempel

For å vise at $d(n) = 2n$ *for alle* $n \in \mathbb{N}$, *definer:*

$$P(n) \quad \Leftrightarrow \quad d(n) = 2n$$

- $P(0)$*:* $d(0) = 2 \cdot 0$, *gjelder enligt def. av* d
- *Under antakelsen* $P(n)$, *d.v.s.* $d(n) = 2n$, *vis* $P(n+1)$, *d.v.s.* $d(n+1) = 2(n+1)$.

For å vise at alle binære tall $b \in \mathbb{B}$ har et egenskap $P(b)$

- Vis at egenskapet holder for 0, d.v.s. $P(0)$
- Vis at egenskapet holder for 1, d.v.s. $P(1)$
- For alle $b \in \mathbb{B}$ med $P(b)$, vis at $P(b0)$
- For alle $n \in \mathbb{B}$ med $P(b)$, vis at $P(b1)$

For å vise at alle symmetriske strenger $x \in S$ har et egenskap $P(x)$

- Vis at egenskapet holder for ϵ, d.v.s. $P(\epsilon)$
- For alle $x \in S$ med $P(x)$, vis at $P(axa)$
- For alle $x \in s$ med $P(x)$, vis at $P(bxb)$

Vis at $v(b) = v(0b)$ for alle $b \in \mathbb{B}$.

- $P(b) \quad :\Leftrightarrow \quad v(b) = v(0b)$
- $P(0)$: $v(0) = 0 = 2 \cdot 0 = 2v(0) = v(00)$
- $P(1)$: $v(1) = 1 = 2 \cdot 0 + 1 = 2v(0) + 1 = v(01)$
- Anta $P(b)$, d.v.s. $v(b) = v(0b)$.
  - $P(b0)$: $v(b0) = 2v(b) = 2v(0b) = v(0b0)$
  - $P(b1)$: $v(b1) = 2v(b) + 1 = 2v(0b) + 1 = v(0b1)$

Hvorfor er strukturell induksjon korrekt?

- La M være en induktivt definert mengde og P et egenskap
- Undersøk mengden N av alle $x \in M$ med $P(x)$.
- Se på induktivt bevis:
  - Basis: $P(b)$ for alle $b \in B$
    $\Rightarrow B \subseteq N$
  - Operasjoner: $P(x)$ og $P(y)$ impliserer $P(f(x, y))$ for alle $x, y \in M$
    $\Rightarrow f(x, y) \in N$ for alle $x, y \in N$.
- Derfor, $N \in \mathcal{M}$, som vi definert tidligere!
- $M \subseteq N$ fordi M er minst i $\mathcal{M}$.
- Med andre ord, $P(x)$ for alle $x \in M$.