MA0301 Elementær diskret matematikk, v12 – løsningsforslag

1 Det er 2^{56} forskjellige nøkler, og $2^{56} - 4$ nøkler som ikke er svake.

Det er $(2^{56})^3$ forskjellige 3DES-nøkler. Det er $(2^{56} - 4)^3$ 3DES-nøkler der ingen av DES-nøklene er svake. Det er 4^3 nøkler der alle DES-nøklene er svake, så det er

$$(2^{56})^3 - 4^3$$

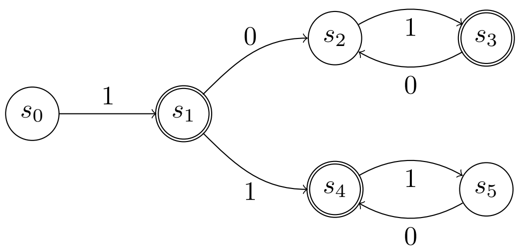
nøkler der minst én av DES-nøklene ikke er svak. Alternativt kan vi se på muligheten for ingen, én eller to svake DES-nøkler, som gir oss

$$\begin{aligned}(2^{56} - 4)^3 + 3 \cdot 4 \cdot (2^{56} - 4)^2 + 3 \cdot 4^2 \cdot (2^{56} - 4)&\\ = (2^{56})^3 - 3 \cdot 4 \cdot (2^{56})^2 + 3 \cdot 4^2 \cdot 2^{56} - 4^3&\\ +3 \cdot 4 \cdot (2^{56})^2 - 3 \cdot 4 \cdot 2 \cdot 4 \cdot 2^{56} + 3 \cdot 4 \cdot 4^2&\\ +3 \cdot 4^2 \cdot 2^{56} - 3 \cdot 4^3&\\ = (2^{56})^3 - 4^3.&\end{aligned}$$

2a $\neg s \leftrightarrow \neg q \Leftrightarrow s \leftrightarrow q$, $\neg t \rightarrow \neg p \Leftrightarrow p \rightarrow t$ og $\neg t \vee s \Leftrightarrow t \rightarrow s$.
$(p \rightarrow t) \wedge (t \rightarrow s) \Rightarrow p \rightarrow s$, $(p \rightarrow s) \wedge (s \leftrightarrow q) \Rightarrow p \rightarrow q$.

2b Moteksempel: p sann, t sann, s sann og q usann.

3 En maskin som gjenkjenner språket $\{1\}\{01\}^* \cup \{11\}\{10\}^*$ er for eksempel:



4a Venstre program bruker $a = O(a)$ multiplikasjoner, høyre program bruker høyst $2(n+1) = O(n) = O(\log a)$ multiplikasjoner.

4b Hvis

$$x^{a_{n-i+1} + 2a_{n-i+2} + 2^2 a_{n-i+3} + \cdots + 2^{i-1} a_n},$$

da er

$$\begin{aligned} u = x^{a_{n-1}} u^2 &= x^{a_{n-1}} x^{2(a_{n-i+1} + 2a_{n-i+2} + 2^2 a_{n-i+3} + \cdots + 2^{i-1} a_n)} \\ &= x^{a_{n-i} + 2a_{n-i+1} + 2^2 a_{n-i+2} + \cdots + 2^i a_n}. \end{aligned}$$

Altså gjelder $P(i) \rightarrow Q(i)$ for alle i.

4c Det er klart at $P(0)$ er sann. Fra **4b** vet vi at $P(0) \to Q(0)$ er sann, og dermed må $Q(0)$ være sann.

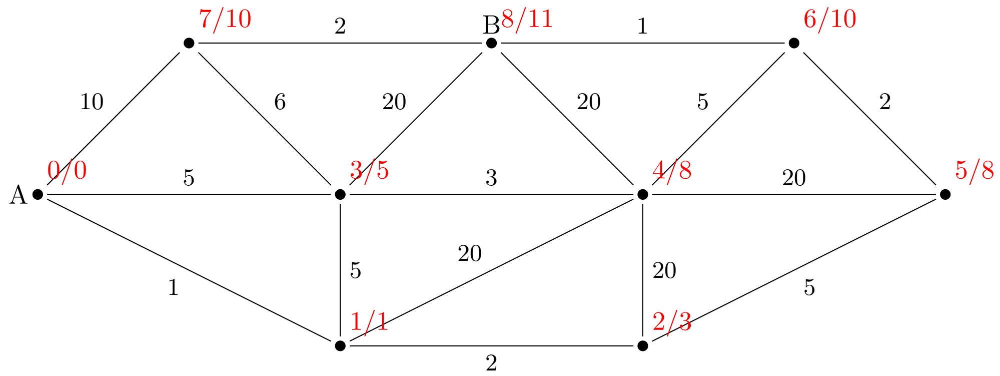
Vi har fått oppgitt at $Q(i) \to P(i+1)$ er sann for alle i. Fra **4b** vet vi at $P(i+1) \to Q(i+1)$ er sann for alle i. Vi får dermed at

$$(Q(i) \to P(i+1)) \wedge (P(i+1) \to Q(i+1)) \Rightarrow Q(i) \to Q(i+1),$$

altså at $Q(i) \to Q(i+1)$ er sann for alle i.

Ved matematisk induksjon følger det at $Q(i)$ er sann for alle i, spesifikt er $Q(n)$ sann.

5 Hjørnene i grafen er merket med n/w, som sier i hvilken iterasjon n hjørnet ble fargelagt og hvilken vekt w det fikk.



6a For $\sim$: Refleksiv er opplagt. Symmetrisk følger fra at bijeksjonene involvert i grafisomorfien er invertible. Transitivitet følger om vi bare setter sammen bijeksjonene. Betingelsene for at sammensetningene utgjør en grafisomorfi er lette å sjekke.

For $\sqsubseteq$: G_1 er en undergraf av G_2 hvis hjørnemengden (kantmengden) til G_1 er en delmengde av hjørnemengden (kantmengden) til G_2, og funksjonen som angir hvilke hjørner kantene i G_1 forbinder er restriksjonen av tilsvarende funksjon for G_2.

Refleksivitet er opplagt. Anti-symmetri følger fra anti-symmetri av $\subseteq$. Transitiv følger fra transitivitet av $\subseteq$.

6b Hvis vi teller kanter ser vi at (i) og (vi) i alene i sine ekvivalensklasser. Hvis vi ser på grader av hjørner ser vi at (iv) og (v) også er alene i sine ekvivalensklasser. Til slutt er det lett å se at (ii) og (iii) er isomorfe. Vi får dermed ekvivalensklassene $\{(\text{i})\}$, $\{(\text{ii}), (\text{iii})\}$, $\{(\text{iv})\}$, $\{(\text{v})\}$ og $\{(\text{vi})\}$.

Hasse-diagrammet er: