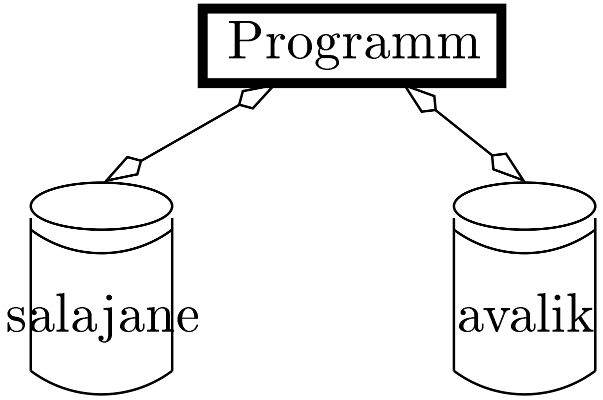
Arvutuslikult turvaline infovoog

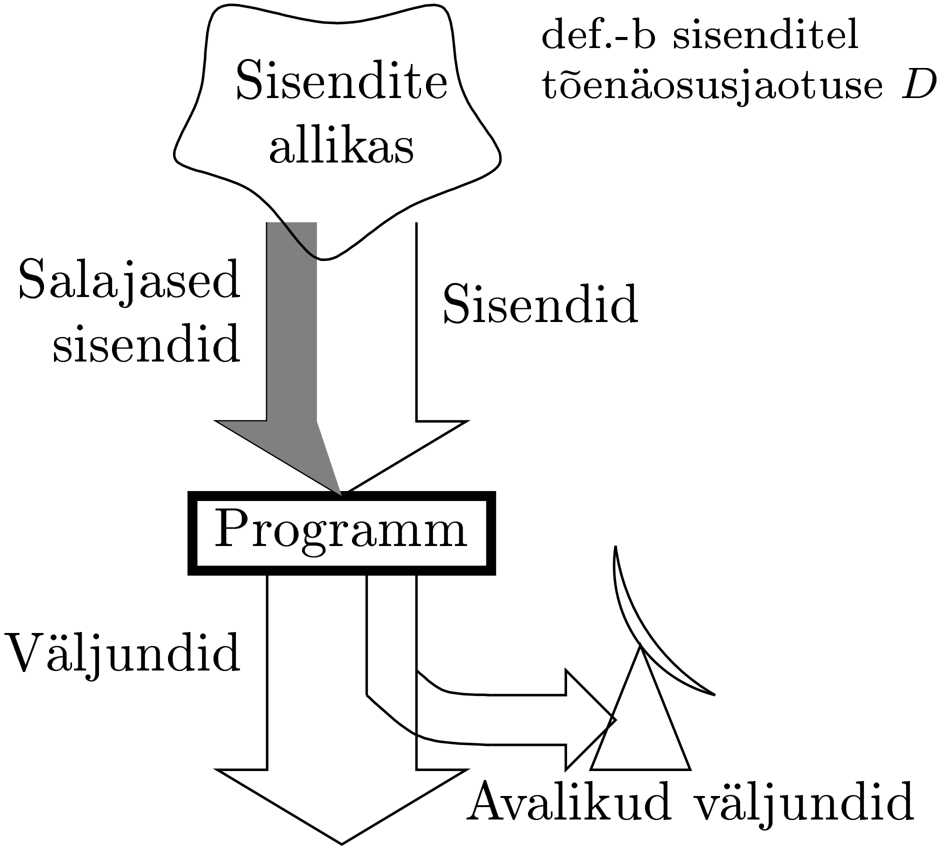
Peeter Laud

$\boxed{\textbf{Ettekande ülesehitus}}$

- Probleemi püstitus ja turvalise infovoo definitsioon.
- Täiendav motivatsioon — kaks erinevat lähenemist krüptole.
- Vaadeldav programmeerimiskeel. Süntaks ja semantika.
  (lihtne imperatiivne keel primitiivse operatsiooniga „krüptimine“)
- Arvutuslikult turvalise infovoo definitsioon.
- Analüüs.
  - Abstraktsiooni olemus.
  - Abstraktne semantika.
  - Vahepeal — turvanõuded krüptimisoperatsiooni semantikale.

Ülesande püstitus





$\boxed{\textbf{Programmide semantikast}}$

- Vaatame mingis imperatiivses keeles kirjutatud programme.
  - Programmi P *olek* on kujutus tema muutujate hulgast mingisse väärtuste hulka. $\boxed{\textbf{State} = \textbf{Var} \to \textbf{Val}}$
  - Programmi P *semantika* on kujutus, mis teisendab algoleku lõppolekuks. $\boxed{[\![P]\!] = \textbf{State} \to \textbf{State}_\perp}$
  - Stohhastilise programmi semantika teisendab algoleku tõenäosusjaotuseks üle lõppolekute. $\boxed{[\![P]\!] = \textbf{State} \to \mathcal{D}(\textbf{State}_\perp)}$

$\boxed{\textbf{Üldine definitsioon}}$

- Olgu antud *salajaste muutujate* hulk $\mathbf{Var}_{\mathrm{S}} \subseteq \mathbf{Var}$ ja *avalike muutujate* hulk $\mathbf{Var}_{\mathrm{P}} \subseteq \mathbf{Var}$. Need defineerivad salajased sisendid ja avalikud väljundid.

- Programmil P on *turvaline infovoog*, kui jaotused

$$\{\!|(S|_{\mathbf{Var}_{\mathrm{S}}}, T|_{\mathbf{Var}_{\mathrm{P}}}) \,:\, S \leftarrow D, T \leftarrow [\![\mathsf{P}]\!](S)|\!\}$$

ja

$$\{\!|(S|_{\mathbf{Var}_{\mathrm{S}}}, T'|_{\mathbf{Var}_{\mathrm{P}}}) \,:\, S, S' \leftarrow D, T' \leftarrow [\![\mathsf{P}]\!](S')|\!\}$$

on mingis mõttes ekvivalentsed.

$\boxed{\textbf{Def. programmide ekvivalentsi kaudu}}$

- Programm on *triviaalselt turvaline*, kui ta ei kasuta oma sisendeid.
- Programm on *turvaline*, kui ta on ekvivalentne mõne triviaalselt turvalise programmiga.
- Programmid P_1 ja P_2 on ekvivalentsed, kui jaotused
$$\{\!|(S|_{\mathbf{Var}_{\mathrm{S}}}, T|_{\mathbf{Var}_{\mathrm{P}}}) : S \leftarrow D, T \leftarrow [\![\mathsf{P}_1]\!](S)|\!\}$$
ja
$$\{\!|(S|_{\mathbf{Var}_{\mathrm{S}}}, T|_{\mathbf{Var}_{\mathrm{P}}}) : S \leftarrow D, T \leftarrow [\![\mathsf{P}_2]\!](S)|\!\}$$
on mingis mõttes ekvivalentsed.

Olgu P mingi programm. Olgu P' programm, mis genereerib jaotuse D järgi oleku S ja seejärel töötab nagu P sisendil S.

P-l on turvaline infovoog $\Leftrightarrow$ P ja P' on ekvivalentsed.

Kaks vaatepunkti krüptole — sissejuhatus

- Krüptograafilised protokollid
  - koosnevad rollidest („algataja“, „vastaja“, „server“) ja nende vahel saadetavatest teadetest;
  - kasutavad teadete loomisel krüptograafilisi primitiive.
- Krüptimisprimitiiv: $(\mathcal{G}, \mathcal{E}, \mathcal{D})$ — võtme loomise, krüptimise ja dekrüptimise algoritmid.
- Krüptimisprimitiivi turvalisus tuleb kuidagi defineerida või tuleb seda kuidagi modelleerida.
  - Definitsioon / mudel peab olema mugav kasutada.
    - Krüptimist kasutava süsteemi turvalisus peab olema lihtsalt taandatav krüptimisprimitiivi turvalisusele.
- Definitsioonides nõutakse, et krüptimisprimitiiv oleks mingis mõttes ekvivalentne mingi ideaalse krüptijaga.

Reaalsed krüptimisprimitiivid

- Reaalsetel primitiividel (näit. DES, Idea, AES) on fikseeritud võtmepikkus l_k ja avateksti pikkus l_x.
- Ideaalne krüptija: juhuslik permutatsioon üle $\{0,1\}^{l_x}$.
- Turvalisuse definitsioon (valitud lähtetekstiga ründe suhtes): $(\mathcal{G}, \mathcal{E}, \mathcal{D})$ on (s,t,o,ϵ)-*pseudojuhuslik permutatsioon*, kui kehtib:
  - Olgu $b \in_{\mathrm{R}} \{0,1\}$, $\pi \in_{\mathrm{R}} \mathrm{Perm}(\{0,1\}^{l_x})$, $k \leftarrow \mathcal{G}()$.
  - Olgu $\mathcal{O}(\cdot)$ must kast $\pi(\cdot)$ (kui $b=0$) või $\mathcal{E}(k,\cdot)$ (kui $b=1$).

  Iga algoritmi $\mathcal{A}^{(\cdot)}$ jaoks, kus $|\mathcal{A}| \leq s$:

$$\Pr[\mathcal{A}^{\mathcal{O}(\cdot)} = b, \text{ ning } \mathcal{A} \text{ teeb} \leq t \text{ sammu ja} \leq o \text{ oraaklipäringut}] \leq \frac{1}{2} + \epsilon$$

Arvutuslik mudel / vaatepunkt

- (s, t, o, ϵ) asemel „polünomiaalne“ ja „superpolünomiaalne“.
- Mille suhtes polünomiaalne? Toome sisse *turvaparameetri* $n \in \mathbb{N}$.
  - Võtmepikkus $l_k(n)$, avateksti pikkus $l_x(n)$ — polünomiaalsed n suhtes.
  - n on $\mathcal{G}$, $\mathcal{E}$, $\mathcal{D}$ täiendavaks argumendiks. Need algoritmid töötavad n suhtes polünomiaalses ajas.
- Turvalisuse def.: $(\mathcal{G}, \mathcal{E}, \mathcal{D})$ on *pseudojuhuslik permutatsioon*, kui
  - Olgu $b \in_{\mathrm{R}} \{0, 1\}$, $\pi_n \in_{\mathrm{R}} \mathrm{Perm}(\{0,1\}^{l_x(n)})$, $k \leftarrow \mathcal{G}(n)$.
  - Olgu $\mathcal{O}_n(\cdot)$ must kast $\pi_n(\cdot)$ (kui $b = 0$) või $\mathcal{E}(n, k, \cdot)$ (kui $b = 1$).

  Iga n suhtes polünomiaalses ajas töötava algoritmi $\mathcal{A}^{(\cdot)}$ jaoks:

$$\Pr[\mathcal{A}^{\mathcal{O}_n(\cdot)}(n) = b] \leq \frac{1}{2} + \alpha(n),$$

kus $\alpha(n)$ on *kaduvväike* (asümptootiliselt väiksem $1/q(n)$-st iga polünoomi q jaoks).

Formaalne mudel / vaatepunkt

- Teated / tekstid on teatava *termide algebra* elemendid.
- Tekst E võib olla:
  - hulga **Keys** mingi element K;
  - hulga **Consts** mingi element C;
  - „paar“ (E_1, E_2);
  - „krüptotekst“ $\{E'\}_K$.
- Keegi, teades teksti [tekste]
  - E_1 ja E_2, *võib luua* teksti (E_1, E_2);
  - E ja K, *võib luua* teksti $\{E\}_K$;
  - (E_1, E_2), *võib luua* tekstid E_1 ja E_2;
  - $\{E\}_K$ ja K, *võib luua* teksti E.

  Samuti *võib luua* iga teksti $C \in$ **Consts**.

$\boxed{\textbf{Programmeerimiskeele süntaks}}$

$$
\begin{array}{lcl}
\mathsf{P} & ::= & x := o(x_1, \ldots, x_k) \\
 & & x := \mathcal{E}nc(k, y) \\
 & & x := \mathcal{G}en() \\
 & | & \mathit{skip} \\
 & | & \mathsf{P}_1 ; \mathsf{P}_2 \\
 & | & \mathit{if}\ b\ \mathit{then}\ \mathsf{P}_1\ \mathit{else}\ \mathsf{P}_2 \\
 & | & \mathit{while}\ b\ \mathit{do}\ \mathsf{P}',
\end{array}
$$

Siin $x, x_1, \ldots, x_k, k, y, b$ on muutujad, o on mingi aritmeetiline operatsioon (võimalik, et stohhastilise semantikaga).

$\boxed{\textbf{Semantika}}$

Lisame turvalisusparameetri:

- $\mathbf{State}_n = \mathbf{Var} \to \mathbf{Val}_n$;
- $[\![\mathsf{P}]\!] : \prod_{n\in\mathbb{N}} \mathbf{State}_n \to \mathcal{D}(\mathbf{State}_{n\perp})$.

Semantika defineeritud induktiivselt üle programmi süntaksi.

$$[\![x := o(x_1,\ldots,x_k)]\!]_n(S_n) := \{\!|S_n[x \mapsto v] \;:\; v \leftarrow [\![o]\!]_n(S_n(x_1),\ldots,S_n(x_k))|\!\}$$

$$[\![\mathit{if}\ b\ \mathit{then}\ \mathsf{P}_1\ \mathit{else}\ \mathsf{P}_2]\!]_n(S_n) := \begin{cases} [\![\mathsf{P}_1]\!]_n(S_n), & \text{kui } S_n(b) = \mathsf{true} \\ [\![\mathsf{P}_2]\!]_n(S_n), & \text{kui } S_n(b) = \mathsf{false} \end{cases}$$

$$[\![\mathit{while}\ b\ \mathit{do}\ \mathsf{P}']\!] = [\![\mathit{if}\ b\ \mathit{then}\ \left(\mathsf{P}'; \mathit{while}\ b\ \mathit{do}\ \mathsf{P}'\right)\ \mathit{else}\ \mathit{skip}]\!]$$

$[\![\mathit{skip}]\!]$ on „samasusteisendus“. $[\![\mathsf{P}_1;\mathsf{P}_2]\!]$ on $[\![\mathsf{P}_2]\!]$ ja $[\![\mathsf{P}_1]\!]$ „kompositsioon“.

Arvutuslikult turvaline infovoog

Vaatame ainult programme, mis töötavad polünomiaalses ajas.

Programmil P on *(arvutuslikult) turvaline infovoog*, kui jaotuste pered

$$\{\!|(S_n|_{\mathbf{Var}_{\mathrm{S}}}, T_n|_{\mathbf{Var}_{\mathrm{P}}}) \,:\, S_n \leftarrow D_n, T_n \leftarrow [\![\mathsf{P}]\!]_n(S_n)|\!\}_{n\in\mathbb{N}}$$

ja

$$\{\!|(S_n|_{\mathbf{Var}_{\mathrm{S}}}, T'_n|_{\mathbf{Var}_{\mathrm{P}}}) \,:\, S_n, S'_n \leftarrow D_n, T'_n \leftarrow [\![\mathsf{P}]\!]_n(S'_n)|\!\}_{n\in\mathbb{N}}$$

on *arvutuslikult eristamatud.*

Jaotuste pered $D^{(0)}$ ja $D^{(1)}$ on arvutuslikult eristamatud, kui iga polünomiaalses ajas töötava algoritmi $\mathcal{A}$ jaoks

$$\Pr[\mathcal{A}(n,x) = b \,:\, b \in_{\mathrm{R}} \{0,1\}, x \leftarrow D_n^{(b)}] = \frac{1}{2} + \alpha(n),$$

kus α on kaduvväike. Tähistame $D^{(0)} \approx D^{(1)}$.

Analüüsi eesmärk

- Antud
  - programmi P tekst,
  - muutujate hulgad $\mathbf{Var}_{\mathrm{S}}$ ja $\mathbf{Var}_{\mathrm{P}}$,
  - sisendite jaotuse D kirjeldus,

  leida, kas P-l on arvutuslikult turvaline infovoog.
- See on ilmselt mittearvutatav.
- Lubame programmianalüüsil eksida, aga ainult ühele, „ohutule“ poole:
  - Kui analüüs ütleb: „infovoog on turvaline“, siis on P-l turvaline infovoog.
  - Kui P-l ei ole turvaline infovoog, siis analüüs ütleb :„infovoog ei ole turvaline“.
  - Lubatud on juht, kus P-l on turvaline infovoog ja analüüs ütleb: „infovoog ei ole turvaline“.

$\boxed{\textbf{Abstraktsioon}}$

- $[\![\mathsf{P}]\!]$ on vaadeldav kui hulga $\prod_{n\in\mathbb{N}}\mathcal{D}(\mathbf{State}_n)$ teisendus. Me tahame abstraheerida selle hulga elemente.
- Olgu $X,Y\subseteq\mathbf{Var}$. X on *sõltumatu* Y-st jaotuses D, kui

  $$\{\!|(S_n|_X,S_n|_Y)\ :\ S_n\leftarrow D_n|\!\}_{n\in\mathbb{N}}\approx\{\!|(S_n|_X,S'_n|_Y)\ :\ S_n,S'_n\leftarrow D_n|\!\}_{n\in\mathbb{N}}.$$

- D-d abstraheerib hulga $\mathcal{P}(\mathbf{Var})\times\mathcal{P}(\mathbf{Var})$ selline alamhulk, mis sisaldab (ülimalt) kõik sellised paarid (X,Y), et X on jaotuses D Y-st sõltumatu.
- Kui P ei muuda hulga $\mathbf{Var}_\mathrm{S}$ elementide väärtusi, siis P-l on turvaline infovoog $\Leftrightarrow$ $\mathbf{Var}_\mathrm{S}$ on sõltumatu $\mathbf{Var}_\mathrm{P}$-st jaotuses $[\![\mathsf{P}]\!](D)$.
- Programmi P analüüs (tähist. $\langle\!\langle\mathsf{P}\rangle\!\rangle$) on hulga $\mathcal{P}(\mathcal{P}(\mathbf{Var})\times\mathcal{P}(\mathbf{Var}))$ teisendus. Ta kujutab D abstraktsiooni (mingiks) $[\![\mathsf{P}]\!](D)$ abstraktsiooniks.

Abstraktne semantika — omistamine

Olgu $\mathsf{P} \equiv x := o(x_1, \ldots, x_k)$.

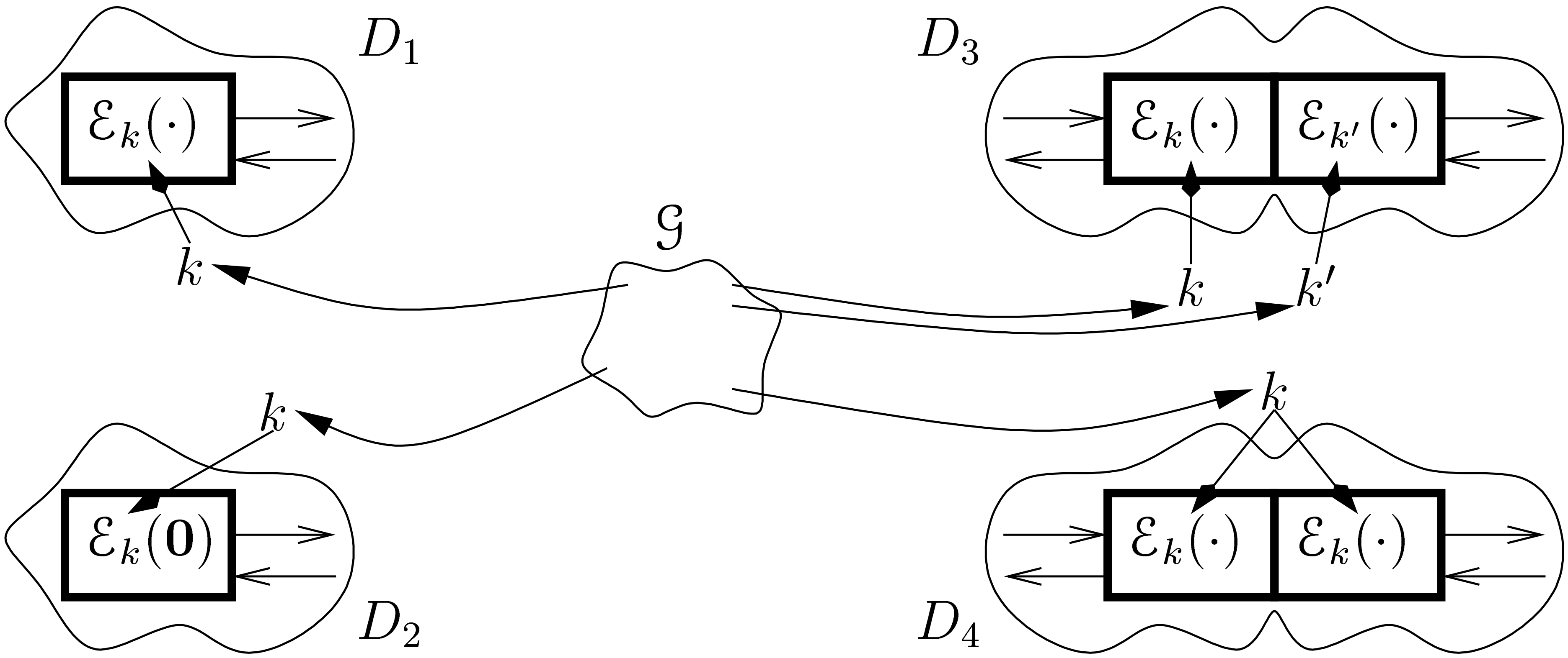
- Olgu $\mathcal{X} \subseteq \mathcal{P}(\mathbf{Var}) \times \mathcal{P}(\mathbf{Var})$. Me võime eeldada, et $\mathcal{X}$ on sümmeetriline ja *monotoonne*:
  - kui $(X, Y) \in \mathcal{X}$, $X' \subseteq X$ ja $Y' \subseteq Y$, siis $(X', Y') \in \mathcal{X}$

  kuna sõltumatus on sümmeetriline ja monotoonne.
- Olgu $(X, Y) \in \mathcal{X}$.
  - Kui $x \notin X \cup Y$, siis $(X, Y) \in \langle\!\langle \mathsf{P} \rangle\!\rangle(\mathcal{X})$.
  - Kui $x \notin X$ ja $x_1, \ldots, x_k \in Y$, siis $(X, Y \cup \{x\}) \in \langle\!\langle \mathsf{P} \rangle\!\rangle(\mathcal{X})$.
- $\langle\!\langle \mathsf{P} \rangle\!\rangle(\mathcal{X})$ on sümmeetriline ja monotoonne.

$\boxed{\textbf{Turvanõuded krüptimisprimitiivile}}$

Krüptimisprimitiiv $(\mathcal{G}, \mathcal{E}, \mathcal{D})$ on

- *kordust varjav*, kui D_1 ja D_2 on eristamatud;
- *võtmete samasust varjav*, kui D_3 ja D_4 on eristamatud.



$\boxed{\textbf{Virtuaalsed elemendid hulgas Var}}$

- Peale operatsiooni $x := \mathcal{E}nc(k, y)$ on hulgad $\{x\}$ ja $\{k\}$ sõltuvad.
- Peale operatsiooni $l := k + 1$ on hulgad $\{l\}$ ja $\{k\}$ sõltuvad.
- Need sõltuvused on „erinevat laadi“.
- Kui $k \in \mathbf{Var}$, siis olgu $[k]_{\mathcal{E}}$ selline objekt, et kui $S_n \in \mathbf{State}_n$, siis $S_n([k]_{\mathcal{E}})$ tähistab musta kasti, mis krüptib võtmega $S_n(k)$.
- Ka objektide $[k]_{\mathcal{E}}$ jaoks on defineeritud sõltumatus.
- $\{x\}$ ja $\{[k]_{\mathcal{E}}\}$ on sõltumatud. $\{l\}$ ja $\{[k]_{\mathcal{E}}\}$ on sõltuvad.
- Me „lisame“ objektid $[k]_{\mathcal{E}}$ hulka $\mathbf{Var}$.

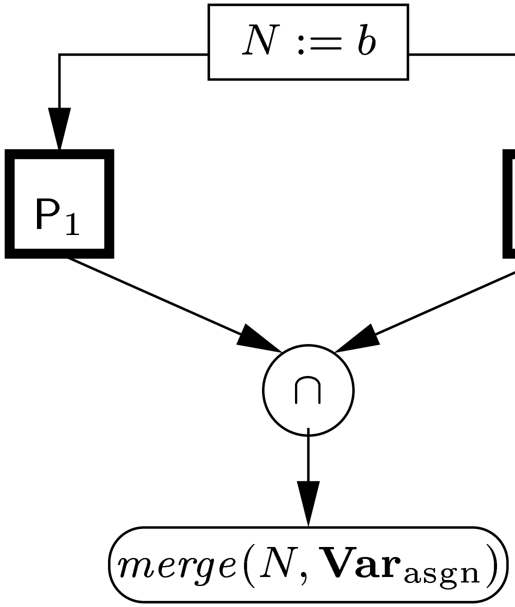
$\boxed{\textbf{Abstraktne semantika — krüptimine}}$

- Kui $\mathsf{P} \equiv x := \mathcal{G}en()$, $\mathcal{X} \subseteq \mathcal{P}(\mathbf{Var}) \times \mathcal{P}(\mathbf{Var})$ ja $(X, Y) \in \mathcal{X}$, siis $(X \cup \{[x]_\mathcal{E}\}, Y \cup \{[x]_\mathcal{E}\}) \in \langle\!\langle \mathsf{P} \rangle\!\rangle(\mathcal{X})$.
- Loeme, et iga programmipunkti kohta on eelnevalt teada, millised muutujad seal krüptimisvõtmetena kasutatavad on.
- Olgu $\mathsf{P} \equiv x := \mathcal{E}nc(k, y)$, $\mathcal{X} \subseteq \mathcal{P}(\mathbf{Var}) \times \mathcal{P}(\mathbf{Var})$ ja $(X, Y) \in \mathcal{X}$.
  - Kui
    - k on kasutatav krüptimisvõtmena;
    - $(\{[k]_\mathcal{E}\}, X \cup Y \cup \{y\}) \in \mathcal{X}$,

    siis $(X, Y \cup \{x\}) \in \langle\!\langle \mathsf{P} \rangle\!\rangle(\mathcal{X})$.
  - Kui $(X, Y \cup \{[k]_\mathcal{E}, y\}) \in \mathcal{X}$, siis $(X, Y \cup \{x\}) \in \langle\!\langle \mathsf{P} \rangle\!\rangle(\mathcal{X})$.

$\boxed{\textbf{Abstraktne semantika — hargnemised (1/2)}}$

Olgu $\mathsf{P} \equiv \mathit{if}\ b\ \mathit{then}\ \mathsf{P}_1\ \mathit{else}\ \mathsf{P}_2$



- N — uus muutuja
- $\mathbf{Var}_{\mathrm{asgn}} \subseteq \mathbf{Var}$ — muutujad, millele omistatakse P_1-s või P_2-s.

Abstraktne semantika — hargnemised (2/2)

Olgu $\mathcal{X} \subseteq \mathcal{P}(\mathbf{Var}) \times \mathcal{P}(\mathbf{Var})$. Tähistame $\mathcal{Y} = \langle\langle merge(N, \mathbf{Var}_{\mathrm{asgn}})\rangle\rangle(\mathcal{X})$.

- Kui $(X, Y \cup \{N\}) \in \mathcal{X}$ ja $X \perp \mathbf{Var}_{\mathrm{asgn}}$, siis $(X, Y) \in \mathcal{Y}$.
- Olgu $X \perp \mathbf{Var}_{\mathrm{asgn}}$, $Y \perp \mathbf{Var}_{\mathrm{asgn}}$. Olgu K_X, K_Y K_{XY} krüptivate mustade kastide hulgad, nii et kõik nende elemendid krüptivad võtmena kasutatava muutujaga ning $K_X \perp K_Y \perp K_{XY}$. Kui
  - $(X, Y) \in \mathcal{X}$,
  - $(K_X \cup K_Y \cup K_{XY}, X \cup Y \cup \{N\}) \in \mathcal{X}$,
  - $K_X \cup K_Y \cup K_{XY}$ elemendid on kõik üksteisest sõltumatud,
  - iga K_{XY} element on iseendast sõltumatu,

  siis $(X \cup K_X \cup K_{XY}, Y \cup K_Y \cup K_{XY}) \in \mathcal{Y}$.

$\boxed{\textbf{Abstraktne semantika — muud}}$

- $\langle\!\langle \mathit{skip} \rangle\!\rangle$ on samasusteisendus.
- $\langle\!\langle \mathsf{P}_1 ; \mathsf{P}_2 \rangle\!\rangle := \langle\!\langle \mathsf{P}_2 \rangle\!\rangle \circ \langle\!\langle \mathsf{P}_1 \rangle\!\rangle$.
- $\langle\!\langle \mathit{while}\ b\ \mathit{do}\ \mathsf{P} \rangle\!\rangle = \langle\!\langle \mathit{if}\ b\ \mathit{then}\ \mathsf{P}\ \mathit{else}\ \mathit{skip} \rangle\!\rangle^*$, kus

$$f^* := \bigcap_{n \in \mathbb{N}} \underbrace{f \circ f \circ \cdots \circ f}_{n} .$$