Probleme met stelselontwikkeling

- Groot stelsels: *baie* programmeerders nodig om betyds klaar te maak.
- Stelsel: baie programme wat saam werk om gemeenskaplike funksie te verrig.
- Misverstande tussen programmeerders veroorsaak probleme.
- Stelsels is te groot vir een persoon om alles te verstaan.
- Firmas moet "raai" hoe lank dit sal neem om 'n stelsel te voltooi (om die tender te wen) en daar duik gewoonlik later probleme op

Stadiums van ontwikkeling

1. Behoeftebepaling
2. Spesifikasie
3. Stelselontwerp
4. Detailontwerp
5. Kodering
6. Toetsing
7. Onderhoud (foutkorreksies en uitbreidings)

A340 vlugbeheerstelsel

Gesofistikeerde beheerstelsel:

- 7 verwerkers (Intel 386/80186)
- 5 voer beheerstelsel uit
- 2 monitor wat aangaan

Ongeluk

- Verskeie mense sterf weens beheerstelselfout:
  - tydens lae toetsvlug probeer die loods meer brandstof voer om te styg om bome te vermy
  - enjins reageer nie. . .

Waarom is fout nie gevind?

- Fout in spesifikasie!
- Beheerstelsel korrek geïmplementeer
  - spesifikasie vereis: indien vliegtuig laer as sekere hoogte, moenie reageer op "meer brandstof" sein nie, want loods is besig met 'n landing
  - die beheerstelsel laat nie die loods toe om beheer oor te neem nie

Foute sluip in op verskillende plekke

- Is spesifikasie duidelik en ondubbelsinnig?
- Validering: bepaal of die vereistes bevredig word. (Word die regte stelsel ontwikkel?)
- Verifikasie: bepaal of die spesifikasie bevredig word. (Word die stelsel reg ontwikkel?)

Tradisionele spesifikasies

- Dokument met diagramme en beskrywings (gewoonlik in Engels)
- Spesifikasies vir groot stelsels beslaan verskeie boeke
- Dubbelsinnighede kom dikwels voor
- Niemand kan dit alles in detail verstaan nie
- Dis waarskynlik onvolledig op sommige plekke
- Dis dalk teenstrydig (op een plek word vereis dat 'n klep oopgemaak word en op 'n ander plek dat dit toegemaak word onder dieselfde omstandighede)

Mense skryf nie wat hulle bedoel nie

- By ingang na Stellenbosch Tegnopark: "Slegs honde aan leibande toegelaat"
- Wat waarskynlik bedoel word: "geen honde sonder leibande toegelaat"
- Dink oor die betekenis van "no head injury is too trivial to ignore" (dis nie wat bedoel word nie!)

Formele spesifikasies

- Grammatikas (EBNF) is nuttig tydens ontwikkeling van vertalers:
  - notasie is kompak en presies
  - teenstrydighede kan opgespoor word
  - dis moontlik om vas te stel of die spesifikasie volledig is
- Twee ander nuttige formele notasies wat gebruik kan word vir spesifikasie:
  - logiese uitdrukkings
  - outomate

Proposisielogika

- Proposisies word voorgestel as veranderlikes
- 'n proposisie is 'n bewering (stelling) wat waar of vals is
  - *temphi* "die temperatuur van die vloeistof in 'n tenk is te hoog"
  - *eof*(*input*) "end van lêer *input* is bereik"
- Die waarde van 'n proposisie is altyd *waar* of *vals*

Basiese operatore

- $\neg a$ ("nie a")
- $a \wedge b$ (" a en b")
- $a \vee b$ ("a of b")
- $a \Rightarrow b$ ("a impliseer b")
- $a \equiv b$ ("a is ekwivalent aan b")

Spesifikasies as logiese uitdrukkings

- Die uitdrukking "$a \Rightarrow b$" word interpreteer as "if a then b":
- $alarm \Rightarrow (temphi \wedge pressurehi)$
- $(temphi \wedge pressurehi) \Rightarrow alarm$

Verduidelik die verskil tussen bogenoemde twee uitdrukkings.

Voorkeurorde van operatore

- Evalueer eerste $\neg$
- Daarna $\wedge$, $\vee$
- Daarna $\Rightarrow$, $\equiv$
- Gebruik hakies om twyfel uit te skakel

Standaard definisies

- $a \Rightarrow b$ gedefinieer as $\neg a \vee b$
- $a \equiv b$ gedefinieer as $(a \Rightarrow b) \wedge (b \Rightarrow a)$

Toutologieë en teenstrydighede

- Toutologie: uitdrukking wat altyd waar is vir alle waardes van elke veranderlike
- Teenstrydigheid: uitdrukking wat altyd vals is vir alle waardes van elke veranderlike
- $a \vee \neg a$
- $a \wedge \neg a$
- $(p \Rightarrow q) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \Rightarrow r))$
- Hoe kan ons bepaal of 'n gegewe uitdrukking 'n toutologie is of nie?

Toetse vir toutologieë

1. Stel 'n waarheidstabel op (ken elke moonlike kombinasie van waardes toe aan elke verandelike)
2. Vereenvoudig die uitdrukking en toon dat dit ekwivalent is aan *true* (herskryf die uitdrukking sonder om die betekenis te verander)
3. Aanvaar die uitdrukking is vals en bepaal of dit 'n teenstrydigheid veroorsaak

Oefening

Bepaal watter van die volgende uitdrukkings toutologieë is:

1. $p \vee \neg p$
2. $p \wedge q$
3. $p \Rightarrow (q \Rightarrow (p \wedge q))$
4. $(p \Rightarrow q) \Rightarrow (\neg q \Rightarrow \neg p)$
5. $(p \Rightarrow q) \Rightarrow (\neg p \Rightarrow \neg q)$

Vereenvoudiging van logiese uitdrukkings

- Gebruik afleidingsreëls (sommige reëls het algemeen aanvaarde name)
- $\frac{p \wedge q}{p}$ (as p en q albei waar is, lei ons af dat p waar is)
- $\frac{p \wedge true}{p}$
- $\frac{p \wedge false}{false}$

Belangrike reels

- $\frac{\neg\neg p}{p}$ [*dubbel negering*]
- $\frac{p \vee \neg p}{true}$
- $\frac{\neg(p \vee q)}{\neg p \wedge \neg q}$ [*De Morgan*]
- $\frac{p \wedge \neg p}{false}$ [*teenstrydigheid*]
- $\frac{p \Rightarrow q,\ \neg q}{\neg p}$
- $\frac{p,\ p \Rightarrow q}{q}$
- $\frac{p \vee (q \wedge r)}{(p \vee q) \wedge (p \vee r)}$ [*distributiewe reël*]

Vereenvoudiging: formele notasie

[1] $(open \vee \neg open) \wedge open$

[2] $true \wedge open$ [1, $\frac{p \vee \neg p}{true}$]

[3] $open$ [2, $\frac{true \wedge p}{p}$]

Ontleding van spesifikasies: metode 1

- Aannames: S_1, S_2, S_3 (spesifikasie)
- Gevolgtrekking: C
- Toon aan dat $S_1, S_2, S_3 \vdash C$ (betekenis: C is afleibaar van S_1, S_2, S_3)
- Herskryf as: $S_1 \wedge S_2 \wedge S_3 \Rightarrow C$ (betekenis: as S_1 en S_2 en S_3 waar is, dan is C waar)
- Vereenvoudig om vas te stel of uitdrukking waar is.
- Nadeel van tegniek: uitdrukkings raak lomp en groot.

Ontleding van spesifikasies: metode 2

- Bekend as "teenstrydigheidsbewys" of "indirekte bewys"
- Opdrag: toon aan dat $S_1, S_2, S_3 \vdash C$ (S_1, S_2 en S_3 verteenwoordig die spesifikasie en C die gevolgtrekking—dit wat bewys moet word)
- Aanvaar $\neg C$ (negeer die gevolgtrekking)
- Probeer 'n teenstrydigheid aflei vanaf S_1, S_2, S_3 en $\neg C$
- Gevolgtrekking is geldig indien teenstrydigheid gevind word; anders nie

Voorbeeld: teenstrydigheidsbewys

$S1$ $p \Rightarrow q$

$S2$ $q \Rightarrow r$

C $p \Rightarrow r$ (gevolgtrekking)

$S3$ $\neg(p \Rightarrow r)$ (negeer die gevolgtrekking)

[1] $\neg(\neg p \vee r)$ $[S_3, def\ impl]$

[2] $p \wedge \neg r$ $[1, DeM]$

[3] p $[2, and]$

[4] $\neg r$ $[2, and]$

[5] q $[3, S_1, def\ impl]$

[6] r $[5, S_2, def\ impl]$

[7] $false$ $[4, 6, teenstr]$

Oefening

Bewys dat die deure van 'n motor ontsluit sal wees as die enjin loop. Die sentrale sluitstelsel is soos volg gespesifiseer:

- If the alarm is enabled, the immobiliser is also enabled:

  $S1 : AlarmEnabled \Rightarrow ImmobiliserEnabled$

- The engine cannot be running while the immobiliser is enabled:

  $S2 : \neg(Running \wedge ImmobiliserEnabled)$

- If the doors are locked, the immobiliser will be enabled:

  $S3 : DoorsLocked \Rightarrow AlarmEnabled$

Teenstrydige spesifikasies

- 'n Lys van uitdrukkings is teenstrydig as en slegs as elke toekenning van waardes aan die veranderlikes minstens een van die uitdrukkings vals maak.

- Is die volgende uitdrukkings teenstrydig? (Stel waardes in.)

  1. $(a \vee b) \wedge \neg(a \wedge b)$

  2. $a \equiv b$

- Hoe kan teenstrydige spesifikasies opgespoor word?

'n Toets vir teenstrydighede

- Gebruik teenstrydigheidsbewys om aan te toon dat $(S_1 \wedge S_2 \wedge S_3 \ldots \wedge S_n) \Rightarrow \mathit{false}$

- Dit beteken dat $S_1 \wedge S_2 \wedge S_3 \ldots \wedge S_n$ vals is. (Dis al manier wat die implikasie waar kan wees.)

- Gevolglik moet minstens een van die uitdrukkings $S_1, S_2, \ldots \wedge S_n$ vals wees—dieselfde as definisie van 'n teenstrydige spesifikasie.

Oefening

Bepaal of die volgende spesifikasie teenstrydig is:

$Pr1 : \mathit{HighPressure} \Rightarrow \mathit{ValveOpen}$

$Pr2 : \mathit{ValveOpen} \Rightarrow \mathit{Bell}$

$Pr3 : \neg \mathit{Bell} \vee \mathit{Reset}$

$Pr4 : \neg \mathit{HighPressure} \Rightarrow \mathit{Reset}$

$Pr5 : \neg \mathit{Reset}$