

Regner regnemaskiner rigtigt?

Med to patenter under opsejling samt en verdensrekord er Danmark med helt fremme når det gælder test af computere. En gruppe forskere ved Danmarks Tekniske Universitet udvikler metoder til at finde fejl i de computere, der er bygget ind i maskiner som lommeregnerne, elevatorer og videoer.

Af Jakob Lichtenberg, Jørn Lind-Nielsen og Poul Frederick Williams

Med et ryk stopper elevatoren midt mellem fjerde og femte sal. Du trykker på knapperne. Intet sker fordi computeren i elevatoren er gået i baglås. Elevatoren rør sig ikke ud af stedet, og du er spærret inde.

Med computere er sådanne situationer desværre ikke utænkelige. Men hvorfor opstår de, og hvordan kan det undgås?

På Institut for Informationsteknologi på Danmarks Tekniske Universitet arbejder vi med kontrol af computere, som sidder inde i maskiner, som vi alle bruger i hverdagen; for eksempel regnemaskiner, elevatorer og videoer.

Et alvorligt eksempel på hvor galt det kan gå, hvis der sker

en fejl, er den europæiske Ariane 5 raket, som blev opsendt den 4. juni 1996. 37 sekunder efter start opstod der en fejl i den ene navigations-computer, og en brøkdelen af et sekund senere opstod der også en fejl i den anden. Resultatet blev at raketten kom ud af kurs og måtte destrueres. Heldigvis kostede denne ulykke ingen menneskeliv.

Computerne findes ikke kun i Ariane raketterne. De er overalt i vores dagligdag. Og de vinder større og større indpas. På mange måder gør de livet lettere for os, men computerne har en alvorlig begrænsning: De gør kun det, de har fået besked på. Og kun det!

I dag går udviklingen så stærkt at computerne fordobler deres hastighed omtrent hver 18. måned. Samtidig bliver der også dobbelt så mange af dem. Computerne er blevet så komplicerede, at det er vanskeligt eller helt umuligt for mennesker at overskue, hvad der sker i dem. Det gælder ikke bare almindelige mennesker, men også de folk, som udvikler computere.

Men hvis computerne kun gør, som de får besked på, og udviklerne ikke kan overskue den besked de giver compu-

terne, så er det der opstår fejl. For eksempel kan elevatoren stoppe midt mellem to etager, bilens centrallås kan nægte at åbne for døren og videoen kan gå i baglås.

Videoen kender vi alle fra hverdagen. Du fortæller den, hvordan den skal opføre sig ved at trykke på fjernbetjeningen eller på knapperne på dens frontpanel. Inde i videoen er der en lille computer, som omsætter dine ønsker til virkelighed. Denne computer husker, hvad du har bedt den om; for eksempel optag Lykkehjullet, spol tilbage eller skift til ny kanal.

Med et fagord siger vi, at computeren er i en "tilstand", og at hvert tryk på videoens knapper får computeren til at skifte fra en tilstand til en anden. Computeren i en video har millioner af forskellige tilstande, og hvis bare én af dem er forkert, kan det være, at videoen ikke virker.

Nu lyder en million tilstande måske som mange. Men sammenlignet med andre computere er det ganske få. En computer skal ikke styre særlig komplicerede ting, før antallet af tilstande bliver meget større. Tænk på de computere, som styrer fly, rumraketter eller atomkraftværker. De

har milliarder og atter milliarder af tilstande.

Nogle computere har endda flere tilstande, end der er atomer i universet. At antallet af tilstande hurtigt kan blive meget stort er velkendt i forskningsverdenen. Det kaldes for *den kombinatoriske eksplosion*.

På trods af disse enorme mængder tilstande bliver der alligevel lavet både elevatorer, videoer og rumraketter, der fungerer. Men hvordan?

For at sikre sig at computeren i videoen virker korrekt, bliver den afprøvet og testet. Fabrikanten har ganske enkelt en række test-eksempler, som han afprøver videoen med, før den forlader fabrikken.

Problemet med test-eksemplerne er, at de ikke dækker alle de muligheder, der findes for at lave fejl. For at være 100% sikker på at videoen fungerer korrekt, bliver han nødt til at have så mange eksempler, at han aldrig vil kunne nå at afprøve dem alle sammen.

En regnemaskine er et godt eksempel. Forestil dig en simpel regnemaskine, som kun kan lægge to tal sammen. Tallene kan være op til otte cifre lange hver. Fabrikanten kan afprøve regnemaskinen ved at lægge forskellige tal sammen. Men han har måske kun tid til at lægge tusinde tal sammen per regnemaskine. Er det nok til at sikre, at regnemaskiner regner rigtigt?

Antallet af mulige regnestykker på denne simple regnemaskine er 10^{16} ; et et-tal efterfulgt af 16 nuller. Selvom alle

jordens fem milliarder mennesker hver prøved et tusinde regnestykker, ville de til sammen kun afprøve under én procent af alle de mulige regnestykker. Langt under.

At forvente at fabrikantens tusinde test-eksempler finder en fejl, kan sammenlignes med at sætte en flok aber foran hver deres skrivemaskine og forvente, at de får skrevet Shakespeares Hamlet på et par timer. Sandsynligheden for at det sker er så mikroskopisk, at metoden nærmest er ubrugelig.

Hvad gør fabrikanten så? Han udvælger sine test-eksempler med omhu. Ved at foretage én bestemt test kan han måske indirekte få afprøvet andre test-eksempler. På den måde kan han nedsætte antallet af tests, selvom det sjældent er nok til at han kan være 100% sikker på, at videoen eller regnemaskinen virker korrekt.

Der er to typer fejl, som kan være årsagen til, at regnemaskinen regner forkert: Den kan være fabrikeret forkert, eller den kan være designet forkert.

En fabriktionsfejl kan være en kortslutning, manglende forbindelse mellem to komponenter eller en defekt komponent. Det er fejl, som ikke nødvendigvis vil forekomme i hvert eneste eksemplar af maskinen.

Designfejl opstår allerede under udviklingen af regnemaskinen og vil medføre fejl i hvert eneste eksemplar af den færdige maskine.

Fabriktionsfejl kan først findes *efter* produktet er frem-

stillet. Det kræver at alle de færdige eksemplarer bliver afprøvet hver for sig. Omvendt kan designfejl findes *før* det endelige produkt bliver produceret, og det er kun nødvendigt at afprøve designet en gang for alle for at finde designfejlene.

Det kan sammenlignes med at bygge huse. Arkitekten bygger først en lille model af et hus. Modellen bruges til at undersøge husene for designfejl; for eksempel, er der døre ind til alle rum? Når modellen er godkendt, bliver husene bygget. De enkelte huse er bygget efter samme model, men enkelte af husene kan have fabriktionsfejl.

På samme måde som en model bruges til at finde designfejl i huse, kan en model også bruges til at finde fejl i computere. Her er modellen ikke lavet af pap og træ, men af matematik.

En matematisk model for videoen er en beskrivelse af den ved hjælp af ligninger og regler. På baggrund af en sådan model er det muligt at udtale sig om opførslen af videoen. Det er så at sige muligt at "regne" på videoen og se om den opfører sig korrekt. I stedet for at afprøve den færdige video kan fabrikanten afprøve modellen.

På Danmarks Tekniske Universitet forsker vi i metoder til at finde designfejl. Vi koncentrerer os om de computere, som er del af andre maskiner. Gennem de sidste par år er det lykkedes for os at finde fejl i nogle computere, som er meget komplicerede, og at erklære an-

dre for fejlfri.

Nogle af vores metoder er allerede i dag i brug i industrien, og to af dem er ved at blive patenteret. For et par år siden satte vi på universitetet en verdensrekord i kontrol af multiplikationsdelen af en regnemaskine.

Vi arbejder med matematiske modeller af computerne. Størrelsen af modellerne hænger nøje sammen med antallet

af tilstande, der, som sagt, kan være astronomisk stort.

Vi kan derfor ikke direkte håndtere hver enkelt af disse tilstande, men må gøre noget andet. Ved hjælp af andre computere og metoder som vi har udviklet, gør vi det muligt at arbejde med store mængder af tilstande på én gang. Således kan vi alligevel checke om modellen er fejlfri.

Nu kan fabrikanten vise,

at regnemaskinen fra før regner rigtigt. Selv med en lille hjemme computer kan det i mange tilfælde gøres på få sekunder, og han kan på sin egen computer en gang for alle vise, at regnemaskinen regner rigtigt.

Men hvordan ved fabrikanten, at hans computer regner rigtigt?

Den kombinatoriske eksplosion

Det kan være svært at forstå at computeren i en simpel video kan indeholde millioner af forskellige tilstande. Det er en følge af et matematisk fænomen, der kaldes *den kombinatoriske eksplosion*.

En video består af en række komponenter: et display, et par

motorer, nogle knapper, osv. Disse komponenter er hver for sig enkle at styre. Men når computeren skal til at styre flere komponenter samtidigt, begynder der at være problemer.

Forestil dig at video består af seks komponenter. Hver

komponent har ti tilstande. Kombinationen af komponenternes tilstande skal håndteres af computeren. For hver komponent man tilføjer tildobles antallet af tilstande. Med alle seks komponenter tildobles altså seks gange, og der bliver en million tilstande.