BERGISCHE UNIVERSITÄT
GESAMTHOCHSCHULE WUPPERTAL
GAUSS-STRASSE 20
42097 WUPPERTAL
(Korrespondenzanschrift)
42119 WUPPERTAL
(Lieferanschrift)
TELEX 8 592 262 bughw
TELEFAX (0202) 439-2901
TELEFON (0202) 439-1

Fachbereich 7

MATHEMATIK

Prof. Dr. Hans-Jürgen Buhl
Praktische Informatik / Numerik

e-mail: Juergen.Buhl@math.uni-wuppertal.de

Algorithmen und Datenstrukturen (Informatik III)

WS1999/2000 – Übungsblatt 2

Abgabetermin: 17. November 1999

Aufgabe 1. *Gütekriterien von Software*

Beschreiben Sie, wo im Falle der Software, die das „THERAC25“ steuert (vgl. Vorlesung), Qualitätsanforderungen nicht erfüllt wurden. Berücksichtigen Sie dabei die besprochenen

a) produktorientierten sowie

b) projektorientierten

Qualitätskriterien.

Aufgabe 2. *ggT-Spezifikation*

Spezifizieren Sie die Funktion

1.0 $ggT : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

.1 $ggT\,(n, m)$

.2 pre — Vorbedingung in n, m

.3 post — Nachbedingung in n, m mit der Funktion $. \mid . : \mathbb{N} \times \mathbb{N} \to \mathbb{B}$ $(teilt)$

mit Hilfe eines Prädikats.

Aufgabe 3. *Flußdiagramme und Hoare-Tripel*

Zeichnen Sie ein Flußdiagramm für die Funktion `power2()`:

```
double power2(double x, int exp)
{
  double erg(1.0);

  if (exp < 0)
        throw "negativer Exponent bei power2 nicht erlaubt!";
  while ( exp > 0 ) {
        if ((exp % 2 ) != 0) {
                erg *= x;
                exp--;
        } else {                  // hier ist exp gerade
                x = x*x;
                exp = exp/2;
        }
  };
  return erg;
};
```

Geben Sie für jede vorkommende ausführbare Anweisung das Hoare-Tripel an. Weisen Sie Terminierung und Korrektheit des Algorithmus nach! Beschreiben Sie kurz die Eigenschaften eines Algorithmus an der Funktion `power2()`. Wie ist es um die *optionale* Qualitätseigenschaft Effektivität bestellt?

Aufgabe 4. *Struktogramme*

Zeichnen Sie ein Struktogramm für die Funktion `power2()` aus Aufgabe 3.

Strahlenpatienten in Kanada und den USA erhielten starke Überdosis

Leichtsinnige Programmierung kann gravierende Folgen haben

Softwareprogramme übernehmen zunehmend auch sicherheitskritische Steuer- und Kontrollfunktionen. Das ist nicht immer ungefährlich: In den USA und Kanada wurden zwischen Juni 1985 und Januar 1987 sechs Unfälle bekannt, bei denen Klinikpatienten aufgrund von Programmfehlern massiven Überdosen radioaktiver Strahlung ausgesetzt waren. Georg Thaller* analysiert einen dieser Fälle und empfiehlt Konsequenzen.

In den Printmedien und im Fernsehen der USA und Kanadas tauchten in den vergangenen Jahren immer wieder Berichte über Todesfälle bei der Behandlung krebskranker Menschen auf, doch gingen diese Meldungen selten ins Detail und trugen daher manchmal eher zur Verwirrung bei.

Unter anderem war das kanadische Unternehmen Atomic Energy of Canada Limited (AECL) wegen seines linearen Teilchenbeschleunigers „Therac-25" in die Kritik geraten. AECL produziert hauptsächlich Geräte, die in Kernreaktoren zum Einsatz kommen, und befindet sich vollständig im Besitz der kanadischen Regierung. Anfang der siebziger Jahre entstand in Zusammenarbeit mit der französischen Firma CGR zunächst die „Therac-6" und Jahre später die „Therac-20". Später trennten sich die beiden Partner, und AECL entwickelte, auf den beiden älteren Modellen aufbauend, das Modell Therac-25 zur Strahlentherapie von krebskranken Patienten.

Therac-25 braucht weniger Platz als die Vorgängergeräte, arbeitet mit einer anderen Energiequelle, ist benutzerfreundlicher und erlaubt vor allem die Anwendung von Röntgenstrahlen (x-rays) und Elektronenstrahlen in einer Maschine. Das ist ein nicht zu unterschätzender finanzieller Vorteil für die Betreiber, denn es muß nur ein Gerät anstatt wie früher zwei angeschafft und gewartet werden. Gesteuert wird die Maschine von einem DEC-PDP-11- Minicomputer, der in Assembler programmiert wurde. Wie kam es nun zu den Unfällen?

Der erste bekanntgewordene Fall ereignete sich im Jahr 1985 in Marietta, Georgia. Er wurde nie systematisch untersucht, obwohl die geschädigte Patientin später behauptete, eine Strahlendosis in der Größenordnung von 15 000 bis 20 000 rad (radiation absorbed dose) erhalten zu haben. Übliche Dosierungen liegen im Bereich von 200 rad. Eine Dosierung von 1000 rad kann tödlich sein. Die Hälfte der Menschen, die am ganzen Körper einer Strahlenbelastung von 500 rad ausgesetzt werden, stirbt daran.

Der zweite Fall ereignete sich in einer Klinik in Toronto, der dritte im amerikanischen Bundesstaat Washington. Licht in die Angelegenheit brachten eigentlich erst die Unfälle in Tyler, Texas, im Frühjahr 1986. Hier gelang es zum ersten Mal, das Fehlverhalten des Systems im Feld zu rekonstruieren.

Ein Patient sollte am Rücken mit einer Dosis von 180 rad bestrahlt werden. Die medizinisch-technische Assistentin (MTA) bereitete alles vor und verließ dann den abgeschirmten Raum, in dem die Bestrahlung verabreicht wird. Sie tippte am Bildschirm ihres VT-220-Terminals schnell die notwendigen Daten ein. Dann bemerkte sie, daß sie versehentlich x (für x-ray) anstatt e (für electron) eingegeben hatte. Das ist ein verständlicher Flüchtigkeitsfehler, da die Behandlung mit Röntgenstrahlen (x-rays) häufiger ist. Die MTA fuhr deshalb unter Benutzung der Pfeiltasten schnell in die entsprechende Zeile hoch und ersetzte das x durch ein e. Sie bestätigte die Eingaben mit der Return-Taste und drückte b für „beam". Damit begann im Nebenraum die Bestrahlung.

Einen Augenblick später unterbrach Therac-25 die Behandlung und brachte die Fehlermeldung „malfunction 54" auf den Bildschirm des Terminals. Außerdem wurde „treatment pause" angezeigt, ein minder schwerer Fehler. In der Dokumentation zu der Therac-25 wurde die Fehlermeldung 54 kurz als „dose input 2" erklärt. Da derartige Meldungen des Geräts häufig waren und von den Operatoren als nicht weiter schlimm betrachtet wurden, drückte die MTA die P-Taste für „proceed". Sie setzte damit die Behandlung fort.

Der Patient auf dem Behandlungstisch hatte keinerlei Kontakt zur MTA am Bildschirm. Er fühlte sich, als hätte jemand brühend heißen Kaffee auf seinen Rücken geschüttet. Dann hörte er ein summendes Geräusch von der Maschine. Da dies bereits seine neunte Sitzung war, wußte er, daß das nicht normal war. Als er sich gerade vom Tisch wälzen wollte, bekam er einen Schlag, den er wie einen elektrischen Schock empfand. Das geschah in genau dem Moment, als die MTA draußen die P-Taste gedrückt hatte.

Der Patient klopfte heftig an die Tür des Behandlungsraums. Die MTA war geschockt und rief nach einem Arzt. Es wurden schwere Schäden festgestellt. Der Patient in Tyler überlebte den Vorfall nur um fünf Monate.

Einen Monat später ereignete sich in derselben Klinik und mit derselben MTA ein ähnlicher Unfall. Der Patient starb als Folge der Überdosis am 1. Mai 1986, drei Wochen nach dem Unfall. Nun glaubte das verantwortliche Personal der Klinik den Beteuerungen des Herstellers AECL nicht mehr. Es ging daran, den Fehler zu rekonstruieren.

Beim Vorgängermodell hatten sich die Benutzer oft über eine zu umständliche und zeitraubende Benutzerführung beklagt. Bei der Therac-25 konnten daher gewisse Daten aus dem Behandlungsplan einfach kopiert werden. Das macht auf den ersten Blick Sinn, da bei Langzeitpatienten gewisse Angaben über Wochen und Monate hinweg immer wieder benötigt werden.

Die Umstellung der Therac-25 von Röntgenstrahlen (x-rays) auf Photonen (electrons) erfolgte, wie die obige Beschreibung des Unfalls gezeigt hat, durch den Austausch eines einzigen Buchstabens. Die MTA war mit der Benutzung der Maschine bereits so vertraut, daß sie die verhängnisvolle Handlung rasch ausführte. Das Programm auf der PDP-11 befand sich zu der Zeit in einer Routine, die der Einstellung von Magneten im Behandlungsraum dient. Dieses Unterprogramm benötigt dafür acht Sekunden, und während dieser Zeitspanne wird das Terminal nicht abgefragt.

Infolge dieser allzu benutzerfreundlichen Programmierung wurden zwar die Daten auf dem Bildschirm geändert, vom Programm aber nie übernommen. Innerhalb der PDP-11 waren weiterhin die Daten für Röntgenstrahlen gespeichert, und deshalb wurde der Patient bestrahlt. Man könnte auch sagen, das Programm belog seinen Benutzer.

Mensch-Maschine-Interface war zu bedienerfreundlich

Gefährlich war auch die Fortsetzung der Behandlung bei vermeintlich minder schweren Störungen des Programmablaufs. Den MTAs hatte man bei der Schulung erklärt, die Therac-25 sei so sicher, daß gar kein Unfall passieren könne. Bei minder schweren Fehlern, und so wurde malfunction 54 zunächst eingestuft, bediente die MTA daher einfach die P-Taste zur Fortsetzung der Behandlung. Die nichtssagende Meldung malfunction 54 und die Nachricht dose input 2 bedeuteten jedoch, daß der Patient bestrahlt worden und die verabreichte Dosis entweder zu hoch oder zu niedrig gewesen war. Durch das Drücken der P-Taste wurde der Röntgenstrahl ein zweites Mal aktiviert.

Das summende Geräusch, das der Patient nach der Verbrennung seines Rückens gehört hatte, war das Überlaufen der Ionenkammer unter dem Behandlungstisch gewesen. Nach der ersten Überdosis wurde er durch die leichtfertig fortgesetzte Behandlung noch einmal bestrahlt. Schätzungsweise war er in weni-

*Georg Thaller ist bei den Diehl-Werken in Nürnberg zuständig für Softwarequalität.