

Andreas Stiller

Prozessorgeflüster

Der Bug von Intels Flaggschiff

War es im letzten Monat der wiederaufgeflamte Copyright-Streit von Intel und AMD, so schaffte es diesmal Intel allein, die Aufmerksamkeit der Welt von sonstigen Prozessoren ab – und zu ihrem Pentium hin zu lenken – wenn auch unbeabsichtigt. Die Fließkommaeinheit ihres Flaggschiffs verrechnet sich halt bei einigen Divisionen.

Wohl selten hat im Internet eine Botschaft so die Runde gemacht, wie die von 'dem' Pentium-Bug. Binnen Stunden liefen die Threads in 'comp.sys.Intel' geradezu über. Tatsächlich läßt sich der FDIV-Verrechner (bzw. die Ungenauigkeit) mit drei Zeilen C oder Pascal, aber auch mit Excel oder dem Windows-Taschenrechner für bestimmte Zahlenpaare nachweisen – im Unterschied zu den zahlreichen, subtilen Fehlern, die immer schon Bestandteil aller bisherigen Prozessorgenerationen waren.

Von daher eigentlich nichts Neues: Jeder Prozessor birgt in sich die Gefahr von Fehlfunktionen, die sowohl systematisch beim Zusammentreffen bestimmter Konditionen oder auch zufällig (Timing, Temperatur, Alpha-Teilchen) auftreten können. Verrechner gab es auch schon bei einigen früheren durch ein 'Test Hole' gerutschten 486ern.

Auch die ersten Cyrix-486er hatten einen (vergleichsweise unbedeutenden) Bug in der FPU. Ebenso Sparcs, PA-RISC und andere.

Die 386er hatten erst recht etliche gut versteckte Macken, beispielsweise wenn ein Fließkommabefehl über eine Page-Grenze lief. Eine ganze Charge 386er versagte auch bei 32-Bit-Befehlen. Schon damals bekleckerte sich Intel nicht mit Ruhm: die fehlerhaften 386er wurden zurückbeordert, und mit einem Sigma-Stigma als '16-Bit-Only' markiert tauchten sie wieder im PC-Kreislauf auf.

Prügel!

Beim Pentium sind alle existierenden rund sechs Millionen Exemplare von dem Fehler betroffen, einen einfachen 'work around' gibt es derzeit jedenfalls für existierende Software nicht. Intel bemüht sich, den Fehler massiv herunterzuspielen, scheut auch vor Falschdarstellungen nicht zurück. Zwar hatte wohl das zuerst gemeldete Fehlerpaar $1/(3 \cdot 2^{38} - 18391)$ immerhin noch eine relative Genauigkeit von 10^{-9} , inzwischen sind aber massenhaft Fehler von 10^{-5} und größer bekannt. Wenn Intel tatsächlich Trillionen von Floatingpoint-Tests durchgeführt haben sollte, muß auch das wahre Ausmaß des Verrechners bekannt sein.

Der Fehler ist beileibe nicht, wie Intel glauben macht, auf 'prim number generation or other complex mathematics' beschränkt, sondern kann überall auftauchen, wo mit Double Precision gearbeitet wird. Nur dürfte sich bei typischen zahlentheoretischen Aufgaben der Fehler viel eher manifestieren, da hier häufig besonders fehlerträchtige Divisoren der Form $n \cdot 2^m - k$ auftreten (z. B. $3 \cdot 2^{20} - 1$).

Nach ersten Messungen können wir die von Intel angegebene Fehlerquote für zufällige Zahlen von etwa einem Fall auf neun Milliarden Divisionen bestätigen. Allerdings ist es eine ziemliche Unverfrorenheit zu behaupten, der Fehler käme bei 'normalen Endusern' im Schnitt nur alle 27 000 Jahre zum Tragen. Schon eine kleine Überschlagsrechnung deutet die wahre Dimension an. Bei 90 MHz und 39 Takten pro FDIV-Befehl würde der Prozessor 10^{10} Divisionen in knapp 72 Minuten absolviert haben.

Nimmt man für fließkommaintensive Software nur einen FDIV-Befehl pro 1000 CPU-Befehle an (ist sicherlich nicht zu hoch angesetzt), so erhält man bei nach oben abgerundeten zwei Takten pro CPU/FPU-

FDIV-Bug

Der FDIV-Bug im Pentium macht sich bei bestimmten Zahlen der Datentypen – Double oder Extended oder Real (bei Borland Pascal) – bemerkbar. Außer FDIV, FIDIV und FPREM sind bislang keine weiteren fehlerhaften FPU-Operationen bekannt. Auch der Zahlentyp COMP scheint betroffen zu sein.

Im Internet wurden vor allem drei Fehlerpaare heiß gehandelt:

$4195835/3145727 = 1,33373907; \quad \delta = 6,101661 \cdot 10^{-5}$
 $5505001/294911 = 1,86666000; \quad \delta = 3,487859 \cdot 10^{-5}$
 $1/1824633702441 = 1,21265962E-0012; \quad \delta = 3,725290 \cdot 10^{-9}$

Solche Paare entlarven sich recht einfach bei der Probe:

$z = x - (x/y) \cdot y$

wo im ersten Fall 256, also alles andere als Null herauskommt.

c't hat sich dem lustigen Spiel: 'Wer findet den größten Fehler?' angeschlossen und präsentiert ein noch geringfügig 'besseres' Spitzenpaar als das erstgenannte 'Internet-Paar'.

$8391667/1572863 = 5,3349560642; \quad \delta = 6,101663 \cdot 10^{-5}$

Die auftretenden Ungenauigkeiten sind natürlich völlig inakzeptabel, weit größer als die von Intel proklamierte neunte Stelle. Beim Aufspüren von Zahlenpaaren in begrenzten Wertebereichen (extending, Mantisse in Hex):

Dividend: xxxx xx00 0000 0000

Divisor : xxFF xx00 0000 0000

(immerhin 2^{38} Berechnungen) haben wir 7209 Ausrutscher gefunden, die zum Teil erheblich über dem erträglichen Rundungsfehler von 10^{-15} liegen. Als potentielle Kandidaten scheinen nur Divisoren mit Mantissen (der Exponent ist unerheblich) in Frage zu kommen, die mit xxFF (extended) beginnen, andere haben wir jedenfalls nicht entdeckt. Die letzten vier Mantissen-Bytes beeinflussen den Fehler nicht. Somit tritt er auch immer in der Umgebung der betroffenen Divisoren auf, also etwa bei 314572,01.

Abhilfe ist derzeit nur Inhabern von Quellcodes möglich. Compiler setzen meist nicht direkt den Coprozessor-Code ein, sondern benutzen die zugeordneten Interrupts 34h bis 3Fh. Die für FDIV zuständigen Interrupts ließen sich abfangen und zu 'Fuß' behandeln. C++-Programmierer könnten auch den '/'-Operator überladen und den Double- oder Extended-Typen spezielle Behandlung zukommen lassen. Pascal-Programmierer müßten für jeden Datentyp eine FDIV-Funktion einbinden.

Wie es scheint, reicht es, nur Divisoren mit dem betroffenen Bitmuster (sieht bei Double etwas anders aus, siehe Listing) speziell zu behandeln, so daß die Performance nicht so arg leiden dürfte. Bewährtheit sich das Muster xxFF, so ist nur in einem Fall von 256 eine länger dauernde Sonderbehandlung nötig. Statt dann gleich zu emulieren, ist es sinnvoller, per Probe zunächst festzustellen, ob das Paar überhaupt zu den Betroffenen gehört. Das vorgestellte FDIV-Beispiel in Pascal verzichtet auf eine Emulation, sondern benutzt eine einfache Rekursion.

Befehl eine MTBF (mittlere Zeit zwischen zwei Fehlern) von circa 60 Stunden! Die 27 000 Jahre können also höchstens für Nur-Word-Benutzer zu treffen. Wer gar laufend irgendwelche Matrizen invertiert oder Eigenwerte bestimmt, dürfte noch viel öfter 'dran' sein.

Unter den Teppich

Das Problem ist aber nicht so sehr der Fehler, sondern die Tatsache, daß Intel nach eigenem Bekunden seit Juni von dem Fehler weiß und ihn in gewohnter Manier unter den Teppich kehren wollte – bis ihn dann der Mathematiker Dr. Nicely an die große Glocke hängte. Während beispielsweise Mips eine umfangreiche Errata-Liste der R4000 im Mikroprozessor Report veröffentlichte, hat Intel bislang immer ihre Errata hinter Non-Disclosure-Agreements versteckt. Ich meine jedenfalls, daß man die Prozessorhersteller notfalls per Gesetz dazu zwingen muß, bei bekanntgewordenen Fehlern diese unverzüglich zu veröffentlichen!

In aller Schnelle hat Intel eine Maskenrevision durchgeführt, neue von Dr. Nicely verifizierte Chips sollen jetzt auf

den Markt kommen. Für 'Betroffene' mit alten Pentium-Chips hat Intel eine Hotline eingeführt:

USA 0 01-8 00-6 28-86 86
bzw. 0 01-9 16-3 56-35 51

und für Europa:

UK: 00 44-17 93-43 11 55

Wir machten natürlich gleich die Probe aufs Exempel bei der britischen Hotline-Nummer, ein Rückruf wurde versprochen; wir warten noch heute ...

Wie es heißt, ist Intel aber grundsätzlich bereit, 'wirklich Betroffenen' den Prozessor auszutauschen. Richtig ist, daß nur wenige Prozent der Applikationen den Coprozessor nutzen, und auch die brauchen nicht immer doppelt genaue Präzision, so daß die Zahl der wirklich Betroffenen tatsächlich nicht so groß sein dürfte.

Dennoch haben schon erste Hersteller mit Garantieerklärungen (IBM, Gateway 2000, Dell) ihren Kunden generell den Austausch zugesichert.

Das Ganze mag dazu führen, daß demnächst Pentiums mit klitzekleinen Fehlern zu Dumping-Preisen auf dem Markt erscheinen – auch nicht schlecht.

(as)

```

Program TestPentium;           { entlarvt Pentium mit FDIV-Bugs }
($N+,E+)                       { demonstriert Bugfix für Pascal }
var x,y,z,r:double;

Function FDIV(x,y:double):double; { FDIV mit Bug-Test }
var delta,z:double;              { für Datentyp double }
var yp:array[0..3] of word absolute y;

const minerror:double=1e-15;
begin
  IF yp[2] and $1FED <> $1FED { = Bitmuster FF in y[6] extended }
  Then FDIV := x/y           { gültig, falls wirklich nur solche }
  else                       { Divisoren betroffen sind }
  begin
    z:=x/y;
    delta:=abs(1-(z*y)/x); {hier reicht notfalls auch single Precision}
    if delta >= minerror then
    begin
      Writeln(chr(7),'FDIV-Fehler:');
      Writeln(x,'/',y,' delta:',delta);
      z:=FDIV(0.75*x,0.75*y); { nach einem Vorschlag von Tim Coe }
    end;
    FDIV:=z;
  end;
end;

begin
  x:=8391667;
  y:=1572863;
  if (x-(x/y)*y) > 1 then Writeln('Prozessor mit FDIV-Bug=> Intel-Hotline!')
  else Writeln('Prozessor ok, kein FDIV-Bug');
  r:= (x-fdiv(x,y)*y);
  if r > 1 then Writeln('Bugfix hat versagt, ',r:28,'delta:',r/x)
  else Writeln('Bugfix hat geklappt, ',r:28,'delta:',r/x);
end.

```

Zum Entlarven des Fehlers braucht man nur wenige Zeilen. Schwieriger ist es, den Fehler zu umgehen. In Pascal kann man alle Divisionen durch bug-kontrollierende FDIV-Funktionen ersetzen, wie hier gezeigt am Datentyp Double.

Chipset-News: OPTi's Viper & Co.

Nach ALI, Intel (siehe S. 25) und SiS schicken sich jetzt auch OPTi, PicoPower, UMC und VIA an, PCI-Chipsets für den 90-MHz-Pentium P54C auf den Markt zu bringen. Über die Elaborate von VIA, PicoPower und OPTi ist bisher nur wenig bekannt. Sicher ist, daß diese echte PCI-Chipsets sein werden. Dies war bei VIA und PicoPower durchaus zu erwarten, für OPTi, die bisher stets den VL-Bus priorisierten, grenzt diese Nachricht aber an eine kleine Sensation. Offensichtlich hat man jetzt auch bei OPTi erkannt, daß die Zukunft von VL in der Vergangenheit liegt.

Der unter dem Code-Namen 'Viper' entwickelte OPTi-Chipset besteht aus drei Chips und unterstützt neben normalen DRAMs auch EDO-DRAMs (siehe S. 25). Die Viper bietet die Möglichkeit, zwei P54C-Prozessoren als multiprozessor-System zu betreiben. OPTi hält sich dabei an das in Intels MP-

Spezifikation vorgeschriebene Design mit Local- und I/O-APIC. Neben Pentium-CPU's unterstützt die Viper auch den M1 von Cyrix und AMDs K86.

Mehr Details gibt es von dem aus drei Bausteinen bestehenden UMC-Chipset (UM8890) zu vermehren. Kernstück ist der UM8891, eine Host-Bridge mit integriertem Cache und Memory-Controller. Der wahlweise aus Standard- oder Sync-SRAMs bestehende 2nd-Level-Cache kann bis zu 8 MByte groß sein.

Die weiteren Bestandteile des Chipsets sind der Data Path Controller (UM8892) und die ISA-Bridge (UM8886A). Letztere enthält neben der Power-Management-Unit auch zwei IDE-Hostadapter, die den Anschluß von bis zu vier Laufwerken erlauben.

Die ersten UMC-basierenden Boards dürften noch im ersten Quartal '95 von der Firma Elite-group kommen. (gs)

Ante Portas: Intels P6-Prozessor

Nach Informationen des amerikanischen Fachmagazins Microprozessor Report soll Intel bereits im Oktober die erste Silizium-Version des P6 produziert haben. Dies deutet darauf hin, daß die offizielle Vorstellung des Chips auf der CeBit '95 erfolgen könnte. Erste Details zum P6 will Intel im Februar auf der ISSCC (International Solid State Circuits Conference) bekanntgeben. Bis dato sind nur wenige CPU-Internas bekannt geworden. Dazu gehört, daß der P6 bis zu vier

voneinander unabhängige Befehle parallel verarbeiten kann. Möglich macht dies eine ähnliche interne Struktur wie die von AMDs K86. Auch der P6 wird Register-Renaming und Out of Order Execution unterstützen. Als Einstiegstaktfrequenz gehen wir von 133 MHz aus, Varianten mit 150 und 200 MHz dürften aber schnell folgen. Kommt kein größerer Bug mehr dazwischen, dürften erste Verkaufsversionen des P6 zeitgleich mit denen des K86 und dem M1 auf den Markt kommen. (gs)

Bugfrei: UMCs alte und neue 486er

Erfreuliche Nachrichten gibt es auch in Sachen U5S, einem 486SX-kompatiblen Prozessor aus dem Hause UMC. Der bei unseren Tests in c't 9/94 aufgetretene Fehler bei Windows NT ist dank einer neuen Maskenrevision aus der Welt geschafft. Dies bestätigen auch die Untersuchungen des amerikanischen Testlabors XXCalibration, die dem U5S das begehrte 'Platinum Certified'-Logo verpaßt haben.

Im ersten Quartal '95 soll der U5S dann Gesellschaft bekom-

men: den U5D. Diese CPU besitzt, wie der Name schon vermuten läßt, einen integrierten Coprozessor und ist damit 486DX-kompatibel. UMCs neue CPU soll aber erheblich schneller rechnen als das Intel-Vorbild. Bei Floatingpoint-Operationen verspricht der Hersteller die dreifache Leistung eines i486DX bei gleicher Taktfrequenz. Deutscher Distributor für den U5S und den kommenden U5D ist Rein elektronik in Nettetal. (gs)