Systemnahe Software I
WS 2011/2012

Andreas F. Borchert
Universität Ulm

9. Februar 2012

Widmung

Ausschnitt eines Fotos von Denise Panyik-Dale, CC-BY-2.0

Diese Vorlesung ist Dennis M. Ritchie gewidmet, der am 12. Oktober 2011 verstorben ist und ohne dessen Beiträge diese Vorlesung in dieser Form nicht denkbar wäre. Dennis M. Ritchie hat nicht nur die Programmiersprache C entworfen und implementiert, sondern auch zusammen mit Ken Thompson Unix entwickelt. Mit C wurde erstmals eine höhere Programmiersprache statt Assembler für die Systemprogrammierung verwendet. Dennis Ritchie und seinen Kollegen gelang es bei Unix, die Betriebsystemsschnittstellen und die Systemwerkzeuge in einem bis dahin unbekanntem Maß zu vereinfachen. Auf sie geht die Umsetzung des wichtigen Grundsatzes zurück, dass jedes Werkzeug genau eine Aufgabe zu erfüllen habe und das möglichst gut.

Syllabus

Inhalte:

- Einführung in die Programmiersprache C
- Dynamische Speicherverwaltung
- Entwicklungswerkzeuge im Umfeld von C
- Dateisysteme
- Systemnahe Programmierung

Syllabus: Ziele

- Erwerb von Grundkenntnissen der Programmiersprache C, wobei ein besonderer Wert gelegt wird auf den Umgang mit der dynamischen Speicherverwaltung und mit den Zeigern in C. Ziel ist es auch, den versehentlichen Einbau von Sicherheitslücken zu vermeiden.
- Erlernen des Umgangs mit den klassischen Entwicklungswerkzeugen unter UNIX wie beispielsweise make.
- Verständnis der Abstraktion eines Dateisystems, einiger Implementierungen und praktische Erfahrungen mit der zugehörigen System-Schnittstelle.

Syllabus: Prüfung

- Es gibt am Ende des Semesters eine schriftliche Prüfung (Termin steht noch nicht fest).
- Zur Teilnahme an der Prüfung ist eine Vorleistung erforderlich. Diese ist bei einer erfolgreichen Teilnahme an den Übungen gegeben (50% der Übungspunkte).
- Der Umfang beträgt 6 Leistungspunkte.
- Studiengänge:
  - **Bachelor:** Mathematik, Wirtschaftsmathematik, Informatik, Medieninformatik, Software Engineering, Physik, Wirtschaftsphysik und Elektrotechnik.
  - **Master:** Informatik und Medieninformatik (Technische und Systemnahe Informatik).
  - **Diplom:** Mündliche Prüfung. Dazu bitte mit mir Kontakt aufnehmen.

Syllabus: Voraussetzungen

- Grundkenntnisse in Informatik. Insbesondere sollte keine Scheu davor bestehen, etwas zu programmieren.
- Freude daran, etwas auch an einem Rechner auszuprobieren und genügend Ausdauer, dass nicht beim ersten Fehlversuch aufgegeben wird.

Syllabus: Struktur

- Jede Woche gibt es zwei Vorlesungsstunden an jedem Dienstag von 16-18 Uhr im H3.
- Die Übungen finden am Donnerstag von 16-18 Uhr im H12 statt.
- Organisatorische Feinheiten werden in der ersten Übungsstunde erläutert.
- Webseite: http://www.mathematik.uni-ulm.de/sai/ws11/soft1/

Syllabus: Übungen

- Wer an den Übungen teilnehmen möchte (zwingende Voraussetzung für eine Teilnahme an der schriftlichen Prüfung), der muss sich über SLC für die Vorlesung registrieren.
- Ebenso sollten alle über einen Shell-Zugang zu unseren Servern (wie z.B. die Theseus) verfügen.
- Für die Übungen werden Gruppen gebildet und die Gruppe trifft sich dann mit dem Tutor.
- Alle Gruppenmitglieder sollten jeweils an der Lösung mitwirken und mit der gesamten Lösung vertraut sein. Die Tutoren dürfen durchaus die einzelnen Gruppenmitglieder individuell mit Punkten bewerten.
- Einzelheiten werden in der ersten Übungsstunde am Donnerstag, den 20. Oktober, um 16 Uhr im H12 vorgestellt.

Syllabus: Skript

- Es gibt ein Skript (entwickelt von mehreren Mitgliedern unseres Instituts), das auf der Vorlesungswebseite zur Verfügung steht.
- Parallel gibt es gelegentlich Präsentationen (wie diese), die ebenfalls als PDF zur Verfügung gestellt werden.
- Wenn Sie das Skript oder die Präsentationen ausdrucken möchten, nutzen Sie dazu bitte die entsprechenden Einrichtungen des KIZ. Im Prinzip können Sie dort beliebig viel drucken, wenn Sie genügend Punkte dafür erworben haben.
- Das Druck-Kontingent, das Sie bei uns kostenfrei erhalten (das ist ein Privileg und kein natürliches Recht), darf für die Übungen genutzt werden, jedoch nicht für das Ausdrucken von Skripten oder Präsentationen.

Syllabus: Sprechstunden

- Sie sind eingeladen, mich jederzeit per E-Mail zu kontaktieren:
  E-Mail: `andreas.borchert@uni-ulm.de`
- Meine reguläre Sprechzeit ist am Mittwoch 14-16 Uhr. Zu finden bin ich in der Helmholtzstraße 18, Zimmer E02.
- Zu anderen Zeiten können Sie auch gerne vorbeischauen, aber es ist dann nicht immer garantiert, daß ich Zeit habe. Gegebenenfalls lohnt sich vorher ein Telefonanruf: 23572.

Syllabus: Nicht verzweifeln!

- Immer wieder kann es mal vorkommen, dass es zu scheinbar unlösbaren Problemen bei einer Übungsaufgabe kommt.
- Geben Sie dann bitte nicht auf. Nutzen Sie unsere Hilfsangebote.
- Sie können (und sollen) dazu gerne Ihren Tutor oder Tutorin kontaktieren oder den Übungsleiter Markus Schnalke oder bei Bedarf gerne auch mich.
- Schicken Sie bitte in so einem Fall alle Quellen zu und vergessen Sie nicht, eine präzise Beschreibung des Problems mitzuliefern.
- Das kann auch am Wochenende funktionieren.

Syllabus: Feedback

- Feedback ist ausdrücklich erwünscht.
- Es besteht insbesondere auch immer die Möglichkeit, auf Punkte noch einmal einzugehen, die zunächst noch nicht klar geworden sind.
- Vertiefende Fragen und Anregungen sind auch willkommen.
- Wir spulen hier nicht immer das gleiche Programm ab. Jede Vorlesung und jedes Semester verläuft anders und das hängt auch von Ihnen ab!

Syllabus: Wie geht es weiter?

- Im SS 2012 folgt der zweite Teil, der u.a. Interprozesskommunikation und Netzwerke behandelt. (Dies ist auch für an Numerik interessierte Hörer relevant.)
- Voraussichtlich im WS 2012/2013 biete ich wieder eine vertiefende Vorlesung mit C++ an.
- Im SS 2013 werde ich wahrscheinlich wieder Parallele Programmierung mit C++ anbieten.
- Gelegentlich wird auch in Zusammenarbeit mit Prof. Urban und Prof. Funken Scientific Computing gelesen. Dies eröffnet den Weg zur parallen Programmierung mit C++ für numerische Anwendungen. Hierzu empfehlen sich Systemnahe Software I+II und C++ als solide Grundlage.

Was ist Systemnahe Software?

- Der Begriff »System« bezieht sich hier auf den Kern eines Betriebssystems.
- Betriebssysteme (bzw. deren Kerne) erfüllen drei Funktionen:
  - Sie greifen direkt auf die Hardware zu,
  - sie verwalten all die Hardware-Ressourcen wie beispielsweise Speicherplatz, Plattenplatz und CPU-Zeit und
  - sie bieten eine Schnittstelle für Anwendungsprogramme.
- Systemnahe Software ist Software, die direkt mit der Betriebssystems-Schnittstelle zu tun hat.

Wie sehen die Schnittstellen aus?

- Teilweise bieten die Betriebssystems-Schnittstellen (auch Systemaufrufe genannt) ein sehr hohes Abstraktions-Niveau.
- So kann beispielsweise aus der Sicht einer Anwendung eine Netzwerk-Kommunikation abgewickelt werden, ohne darüber nachzudenken, was für Netzwerk-Hardware konkret genutzt wird, wie die Pakete geroutet werden oder wann Pakete erneut zu senden sind, wenn der erste Versuch nicht geklappt hat.
- Zwar gibt es teilweise große Unterschied bei den Schnittstellen, jedoch steht erfreulicherweise ein Standard zur Verfügung, kurz POSIX genannt oder ausführlicher IEEE Standard 1003.1.
- Dieser Standard entspricht weitgehend einer gemeinsamen Schnittmenge von Unix, Linux und den BSD-Varianten. Dank Cygwin gibt es auch weitgehend eine POSIX-Schnittstelle unter Windows.

Warum ist C relevant?

- Durch den Erfolg von Unix erreichte C eine gewisse Monopolstellung für die systemnahe Software.
- Da POSIX (und auch die einzelnen Betriebssysteme) die Schnittstelle nur auf der Ebene von C definieren, führt an C kaum ein Weg vorbei.
- Praktisch alle anderen Sprach-Implementierungen (wie beispielsweise C++, Java, Fortran oder Ada) basieren letztenendes auf C bzw. benötigen die C-Bibliothek, die die Schnittstelle zum Betriebssystem liefert.

Warum überhaupt etwas anderes als C?

- Ursprünglich wurde systemnahe Software in Assembler geschrieben. Das ist sehr umständlich und überhaupt nicht portabel, da jede Prozessor-Architektur anders zu programmieren ist.
- C entstand Mitte der 70er Jahre als Alternative zu Assembler. Manche bezeichnen C deswegen bis heute als »portablen Assembler«.
- C liefert Portabilität, ist aber immer noch sehr maschinennah.
- Wir verlassen mit C die gewohnte »heile Welt« von Java (oder anderer ähnlicher moderner Programmiersprachen).
- C setzt maschinennahes Denken voraus und bietet viele Fallstricke, die wir in der »heilen Welt« nicht kennen.
- Insofern wird heute C bevorzugt nur im systemnahen Bereich eingesetzt.

Wie funktionieren Systemaufrufe?

- Programme laufen auf modernen Betriebssystemen in ihrer eigenen virtuellen Welt ab, d.h. sie sehen in ihrem Adressraum weder das Betriebssystem noch die anderen parallel laufenden Programme.
- Die virtuelle Welt wird nur durch besondere Ereignisse verlassen, wenn z.B. durch 0 geteilt wird, ein `null`-Zeiger dereferenziert wird, die Uhr sagt, dass ein anderer Prozess mal an der Reihe ist, sich die Platte meldet, weil ein gewünschter Datenblock endlich da ist, irgendeine Taste auf der Tastatur gedrückt wurde oder ...
- ... ein Programm mit dem Betriebssytem kommunizieren möchte.
- All diese Ereignisse unterbrechen den regulären Betrieb und führen dazu, dass das Benutzerprogramm zu arbeiten aufhört und der Betriebssystems-Kern die Kontrolle übernimmt, um festzustellen, was zur Unterbrechung geführt hat.
- Im Falle eines Systemaufrufs werden die Parameter aus der Welt des Benutzerprogramms mühsam herausgeholt, der Aufruf bearbeitet und die Resultate in die Benutzer-Welt überführt.
- In Wirklichkeit ist das noch viel komplizierter ...

Wie wird eine Unterbrechung initiiert?

- Für absichtliche Unterbrechungen gibt es spezielle Maschinen-Instruktionen.
- Diese gehören nicht zum Vokabular eines C-Compilers, so dass in jeder C-Bibliothek die Systemaufrufe in Assembler geschrieben sind.
- Die Aufrufsyntax in C ist portabel, die jeweilige Implementierung ist es nicht, da sie in Assembler geschrieben ist.

Wie sehen Systemaufrufe konkret aus?

hello.s

```
/*
   Hello world demo in Assembler
   for the SPARCv8/Solaris platform
*/
        .section ".text"
        .globl  _start
_start:
/* write(1, msg, 13); */
        or      %g0,4,%g1
        or      %g0,1,%o0
        sethi   %hi(msg),%o1
        add     %o1,%lo(msg),%o1
        or      %g0,13,%o2
        ta      8
/* exit(0) */
        or      %g0,1,%g1
        or      %g0,0,%o0
        ta      8
msg:    .ascii  "Hello world!\012"
```

Wie sehen Systemaufrufe konkret aus?

- Das Beispiel wurde für die SPARC-Architektur geschrieben.
- Das Assembler-Programm besteht 9 Instruktionen, die jeweils 4 Bytes benötigen und 13 Bytes Text.
- `%g1`, `%o0`, `%o1` und `%o2` sind alles sogenannte Register, die im 32-Bit-Modus jeweils 32 Bit aufnehmen können.
- `%g0` ist ein spezielles Register, das immer den Wert 0 hat.
- Instruktionen haben bei der SPARC-Architektur normalerweise drei Operanden, wobei der dritte Operand das Ziel ist. Beispiel: `or %g0,4,%g1`
  Das ist eine binäre Oder-Operation mit `%g0` (also dem Wert 0) und der Zahl 4, dessen Resultat in `%g1` abgelegt wird. Kurz gefasst wird damit dem Register `%g1` der Wert 4 zugewiesen.

Wie sehen Systemaufrufe konkret aus?

- Die spezielle Instruktion `ta` (*trap always*) unterbricht die Programmausführung, bis der Prozess vom Betriebssystem wieder zum Leben erweckt wird.
- Die Parameter des Systemaufrufs werden bei der SPARC/Solaris-Plattform in den Registern %o0 bis %o5 abgelegt (bis zu 6 Parameter, die allerdings auf irgendwelche Speicherflächen mit mehr Parametern verweisen können).
- Im Register %g1 wird eine Nummer abgelegt, die den Systemaufruf selektiert. So steht beispielsweise die 1 für `exit()` und 4 für `write()`.
- Die Nummer 8, die bei `ta` angegeben wird, dient als Index in die Trap-Tabelle ...

Was passiert nach einem Systemaufruf?

usr/src/uts/sun4u/ml/trap_table.s

```
trap_table:
    /* hardware traps */
    NOT;                        /* 000  reserved */
    RED;                        /* 001  power on reset */
    RED;                        /* 002  watchdog reset */
    RED;                        /* 003  externally initiated reset */
/* ... */
    /* user traps */
    GOTO(syscall_trap_4x);      /* 100  old system call */
    TRAP(T_BREAKPOINT);         /* 101  user breakpoint */
    TRAP(T_DIV0);               /* 102  user divide by zero */
    FLUSHW();                   /* 103  flush windows */
    GOTO(.clean_windows);       /* 104  clean windows */
    BAD;                        /* 105  range check ?? */
    GOTO(.fix_alignment);       /* 106  do unaligned references */
    BAD;                        /* 107  unused */
    SYSCALL(syscall_trap32)     /* 108  ILP32 system call on LP64 */
/* ... */
```

- (Der Programmtext stammt aus den OpenSolaris-Quellen, siehe `http://www.opensolaris.org/`).

Was passiert nach einem Systemaufruf?

usr/src/uts/sun4u/ml/trap_table.s

```
#define SYSCALL(which)                          \
        TT_TRACE(trace_gen)                     ;\
        set     (which), %g1                    ;\
        ba,pt   %xcc, sys_trap                  ;\
        sub     %g0, 1, %g4                     ;\
        .align  32
```

- Zunächst werden alle Register gesichert und es findet ein Wechsel in den privilegierten Prozessor-Modus statt.
- Zu jeder Unterbrechungsart gibt es eine Nummer, wobei Unterbrechungen durch Benutzerprogramme von Hardware-Unterbrechungen unterschieden werden. Aus `ta 8` wird die Nummer $256 + 8 = 0x108$.
- Zu jedem der 512 verschiedenen Unterbrechungsmöglichkeiten sind in der Trap-Tabelle 32 Bytes Code vorgesehen, die den Trap behandeln, indem sie typischerweise eine entsprechende Routine aufrufen.

Was passiert nach einem Systemaufruf?

usr/src/uts/sparc/v9/ml/syscall_trap.s

```
    ENTRY_NP(syscall_trap32)
    ldx      [THREAD_REG + T_CPU], %g1     ! get cpu pointer
    mov      %o7, %l0                      ! save return addr
/* ... */
    lduw     [%l1 + G1_OFF + 4], %g1       ! get 32-bit code
    set      sysent32, %g3                 ! load address of vector table
    cmp      %g1, NSYSCALL                 ! check range
    sth      %g1, [THREAD_REG + T_SYSNUM] ! save syscall code
    bgeu,pn %ncc, _syscall_ill32
      sll    %g1, SYSENT_SHIFT, %g4        ! delay - get index
    add      %g3, %g4, %g5                 ! g5 = addr of sysentry
    ldx      [%g5 + SY_CALLC], %g3         ! load system call handler
/* ... */
    call     %g3                           ! call system call handler
    nop
/* ... */
    jmp      %l0 + 8
     nop
```

- Danach werden die Parameter so kopiert, dass sie als Parameter einer C-Funktion übergeben werden können (nicht dargestellt) und dann wird passend zur Systemaufrufsnummer die entsprechende Funktion aus einer Tabelle ausgewählt.

Was passiert nach einem Systemaufruf?

usr/src/uts/common/os/sysent.c

```
struct sysent sysent[NSYSCALL] =
{
/* ONC_PLUS EXTRACT END */
    /*  0 */ IF_LP64(
                    SYSENT_NOSYS(),
                    SYSENT_C("indir",       indir,          1)),
    /*  1 */ SYSENT_CI("exit",              rexit,          1),
    /*  2 */ SYSENT_2CI("forkall",          forkall,        0),
    /*  3 */ SYSENT_CL("read",              read,           3),
    /*  4 */ SYSENT_CL("write",             write,          3),
    /*  5 */ SYSENT_CI("open",              open,           3),
```

- In der `sysent`-Tabelle finden sich alle Systemaufrufe zusammen mit einigen Infos zur Anzahl der Parameter und die Art der Rückgabewerte. Unter Solaris hat diese Tabelle inzwischen 256 Einträge.

Was passiert nach einem Systemaufruf?

usr/src/uts/common/syscall/rw.c

```
ssize_t write(int fdes, void *cbuf, size_t count) {
        struct uio auio;
        struct iovec aiov;
/* ... */
        if ((cnt = (ssize_t)count) < 0)
                return (set_errno(EINVAL));
        if ((fp = getf(fdes)) == NULL)
                return (set_errno(EBADF));
        if (((fflag = fp->f_flag) & FWRITE) == 0) {
                error = EBADF;
                goto out;
        }
/* ... */
        aiov.iov_base = cbuf;
        aiov.iov_len = cnt;
/* ... */
        auio.uio_loffset = fileoff;
        auio.uio_iov = &aiov;
/* ... */
        error = VOP_WRITE(vp, &auio, ioflag, fp->f_cred, NULL);
        cnt -= auio.uio_resid;
/* ... */
out:
/* ... */
        if (error)
                return (set_errno(error));
        return (cnt);
}
```

Zusammenfassung

- Die Schnittstelle zwischen Anwendungen und dem Betriebssystems-Kern besteht aus über 200 einzelnen Funktionen, die zu einem großen Teil standardisiert sind.
- Systemaufrufe sind sehr viel teurer als reguläre Funktionsaufrufe. Das liegt an dem Mechanismus der Unterbrechungsbehandlung, dem notwendigen Kontextwechsel, der Parameterschaufelei und auch der asynchronen Natur vieler Funktionen (wie beispielsweise beim I/O).
- Deswegen ist es wichtig, auf der Anwendungsseite Bibliotheken zu entwickeln, die die Zahl der Systemaufrufe bzw. deren Aufwand minimieren.
- Verbunden mit den einzelnen Systemaufrufen sind viele Abstraktionen und Objekte, die wir uns im Laufe der Vorlesung genauer ansehen werden wie etwa das Dateisystem, die Prozesse, die Signalbehandlung (Unterbrechungen auf der Benutzerseite) die Interprozess-Kommunikation und die allgemeine Netzwerk-Kommunikation.

Erste Schritte mit C

- Um einen raschen Start in den praktischen Teil zu ermöglichen, wird C zunächst etwas oberflächlich mit einigen Beispielen vorgestellt.
- Später werden dann die Feinheiten vertieft vorgestellt.
- Im Vergleich zu Java gibt es in C keine Klassen. Stattdessen sind alle Konstrukte recht nah an den gängigen Prozessorarchitekturen, die das ebenfalls nicht kennen.
- Statt Klassen gibt es in C Funktionen, die Parameter erhalten und einen Wert zurückliefern. Da sie sich nicht implizit auf ein Objekt beziehen, sind sie am ehesten vergleichbar mit den statischen Methoden in Java.
- Jedes C-Programm benötigt ähnlich wie in Java eine *main*-Funktion.

Ein erstes C-Programm

hallo.c

```
main() {
   /* puts: Ausgabe einer Zeichenkette nach stdout */
   puts("Hallo zusammen!");
}
```

- Dieses Programm gibt den gezeigten Text aus, gefolgt von einem Zeilentrenner – analog zu *System.out.println*.
- Im Unterschied zu Java muss wirklich eine Zeichenkette angegeben werden. Andere Datentypen werden hier nicht implizit über eine *toString*-Methode in Zeichenketten zum Ausdrucken verwandelt.

Übersetzung des ersten C-Programms

```
doolin$ gcc -Wall hallo.c
hallo.c:1: warning: return type defaults to 'int'
hallo.c: In function 'main':
hallo.c:3: warning: implicit declaration of function 'puts'
hallo.c:4: warning: control reaches end of non-void function
doolin$ a.out
Hallo zusammen!
doolin$
```

- Der *gcc* ist der *GNU-C-Compiler*, mit dem wir unsere Programme übersetzen.
- Ist kein Name für das zu generierende ausführbare Programm angegeben, so wird dieses *a.out* genannt.
- Die Option *-Wall* bedeutet, dass alle Warnungen ausgegeben werden sollen.

Übersetzung des ersten C-Programms

```
doolin$ gcc -Wall -std=c99 hallo.c
hallo.c:1: warning: return type defaults to 'int'
hallo.c: In function 'main':
hallo.c:3: warning: implicit declaration of function 'puts'
doolin$
```

- Voreinstellungsgemäß geht *gcc* von *C89* aus. Es ist auch möglich, den aktuellen Standard *C99* zu verwenden, wenn dies mit der Option „*-std=c99*“ verlangt wird.
- Statt „*-std=c99*“ ist auch „*-std=gnu99*“ möglich – dann stehen auch verschiedene Erweiterungen zur Verfügung, die nicht über C99 vorgegeben sind.
- Für die Übungen empfiehlt sich grundsätzlich die Wahl von *gnu99*.

Verbesserung des ersten C-Programms

hallo1.c

```
#include <stdio.h> /* Standard-I/O-Bibliothek einbinden */

int main() {
   /* puts: Ausgabe eines Strings nach stdout */
   puts("Hallo zusammen!");
   /* Programm explizit mit Exit-Status 0 beenden */
   return 0;
}
```

- Da die Ausgabefunktion *puts()* nicht bekannt war, hat der Übersetzer geraten. Nun ist diese Funktion durch das Einbinden der Deklarationen der Standard-I/O-Bibliothek (siehe **#include** <stdio.h>) bekannt.
- Der *Typ des Rückgabewertes* der *main()*-Funktion ist nun als **int** (Integer) angegeben (der Übersetzer hat vorher auch **int** geraten.)
- Der Rückgabewert der *main()*-Funktion, welcher durch **return** 0 gesetzt wird, ist der *Exit-Status* des Programms. Fehlt dieser, führt dies ab *C99* implizit zu einem ein Exit-Status von 0.

Übersetzung des verbesserten C-Programms

```
doolin$ gcc -Wall -o hallo1 hallo1.c
doolin$ hallo1
Hallo zusammen!
doolin$
```

- Mit der Option „*-o*“ kann der Name des Endprodukts beim Aufruf des *gcc* spezifiziert werden.
- Anders als bei Java ist das Endprodukt selbständig ausführbar, da es in Maschinensprache übersetzt wurde.
- Das bedeutet jedoch auch, dass das Endprodukt nicht portabel ist, d.h. bei anderen Prozessorarchitekturen oder Betriebssystemen muss das Programm erneut übersetzt werden.

Berechnung von Quadratzahlen

quadrate.c

```
#include <stdio.h>

const int MAX = 20;    /* globale Integer-Konstante */

int main() {
   puts("Zahl | Quadratzahl");
   puts("-----+------------");
   for (int n = 1; n <= MAX; n++) {
      printf("%4d | %7d\n", n, n * n); /* formatierte Ausgabe */
   }
}
```

- Dieses Programm gibt die ersten 20 natürlichen Zahlen und ihre zugehörigen Quadratzahlen aus.
- Variablendeklarationen können außerhalb von Funktionen stattfinden. Dann gibt es die Variablen genau einmal und ihre Lebensdauer erstreckt sich über die gesamte Programmlaufzeit.

Ausgabe mit *printf*

quadrate.c

```
printf("%4d | %7d\n", n, n * n); /* formatierte Ausgabe */
```

- Formatierte Ausgaben erfolgen in C mit Hilfe von *printf*.
- Die erste Zeichenkette kann mehrere Platzhalter enthalten, die jeweils mit „%“ beginnen und die Formatierung eines auszugebenden Werts und den Typ spezifizieren.
- „%4d“ bedeutet hier, dass ein Wert des Typs **int** auf eine Breite von vier Zeichen dezimal auszugeben ist.

for-Schleifen

quadrate.c

```
for (int n = 1; n <= MAX; n++) {
   printf("%4d | %7d\n", n, n * n); /* formatierte Ausgabe */
}
```

- Wie in Java kann eine Schleifenvariable im Initialisierungsteil einer **for**-Schleife deklariert und initialisiert werden.
- Dies ist im Normalfall vorzuziehen.
- Gelegentlich finden sich noch Deklarationen von Schleifenvariablen außerhalb der **for**-Schleife, weil dies von frühen C-Versionen nicht unterstützt wurde.

Euklidischer Algorithmus

euklid.c

```
#include <stdio.h>

int main() {
    printf("Geben Sie zwei positive ganze Zahlen ein: ");
    /* das Resultat von scanf ist die
       Anzahl der eingelesenen Zahlen
    */
    int x, y;
    if (scanf("%d %d", &x, &y) != 2) {  /* &-Operator konstruiert Zeiger */
        return 1;       /* Exit-Status ungleich 0 => Fehler */
    }

    int x0 = x;
    int y0 = y;

    while (x != y) {
        if (x > y) {
            x = x - y;
        } else {
            y = y - x;
        }
    }

    printf("ggT(%d, %d) = %d\n", x0, y0, x);

    return 0;
}
```

Einlesen mit *scanf*

euklid.c

```
if (scanf("%d %d", &x, &y) != 2) {
   /* Fehlerbehandlung */
}
```

- Die Programmiersprache C kennt nur die *Werteparameter-Übergabe* (*call by value*).
- Daher stehen auch bei *scanf()* nicht direkt die Variablen x und y als Argumente, weil dann *scanf()* nur die Kopien der beiden Variablen zur Verfügung stehen würden.
- Mit dem Operator & wird hier jeweils ein *Zeiger* auf die folgende Variable erzeugt. Der Wert eines Zeigers ist die *Hauptspeicher-Adresse* der Variablen, auf die er zeigt.
- Daher wird in diesem Zusammenhang der Operator & auch als *Adressoperator* bezeichnet.

Einlesen mit *scanf*

euklid.c

```
if (scanf("%d %d", &x, &y) != 2) {
   /* Fehlerbehandlung */
}
```

- Die Programmiersprache C kennt weder eine Überladung von Operatoren oder Funktionen.
- Entsprechend gibt es nur eine einzige Instanz von *scanf()*, die in geeigneter Weise „erraten“ muss, welche Datentypen sich hinter den Zeigern verbergen.
- Das erfolgt (analog zu *printf*) über Platzhalter. Dabei steht „%d“ für das Einlesen einer ganzen Zahl in Dezimaldarstellung in eine Variable des Typs **int**.
- Variablen des Typs **float** (einfache Genauigkeit) können mit „%f“ eingelesen werden, **double** (doppelte Genauigkeit) mit „%lf“.

Einlesen mit *scanf*

euklid.c

```
if (scanf("%d %d", &x, &y) != 2) {
   /* Fehlerbehandlung */
}
```

- Der Rückgabewert von *scanf* ist die Zahl der erfolgreich eingelesenen Werte.
- Deswegen wird hier das Resultat mit der 2 verglichen.
- Das Vorliegen von Einlesefehlern sollte immer überprüft werden. Normalerweise empfiehlt sich dann eine Fehlermeldung und ein Ausstieg mit *exit*(1) bzw. innerhalb von *main* mit **return** 1.
- Ausnahmenbehandlungen (*exception handling*) gibt es in C nicht. Stattdessen geben alle Ein- und Ausgabefunktionen (in sehr unterschiedlicher Form) den Erfolgsstatus zurück.

Aufbau eines C-Programms

$$
\begin{array}{rcl}
\langle\text{translation-unit}\rangle & \longrightarrow & \langle\text{top-level-declaration}\rangle \\
 & \longrightarrow & \langle\text{translation-unit}\rangle\ \langle\text{top-level-declaration}\rangle \\
\langle\text{top-level-declaration}\rangle & \longrightarrow & \langle\text{declaration}\rangle \\
 & \longrightarrow & \langle\text{function-definition}\rangle \\
\langle\text{declaration}\rangle & \longrightarrow & \langle\text{declaration-specifiers}\rangle \\
 & & \langle\text{initialized-declarator-list}\rangle\ \text{„;“} \\
\langle\text{declaration-specifiers}\rangle & \longrightarrow & \langle\text{declaration-specifier}\rangle \\
 & & [\ \langle\text{declaration-specifiers}\rangle\ ] \\
\langle\text{declaration-specifier}\rangle & \longrightarrow & \langle\text{storage-class-specifier}\rangle \\
 & \longrightarrow & \langle\text{type-specifier}\rangle \\
 & \longrightarrow & \langle\text{type-qualifier}\rangle \\
 & \longrightarrow & \langle\text{function-specifier}\rangle
\end{array}
$$

- Eine Übersetzungseinheit (*translation unit*) in C ist eine Folge von *Vereinbarungen*, zu denen Funktionsdefinitionen, Typ-Vereinbarungen und Variablenvereinbarungen gehören.

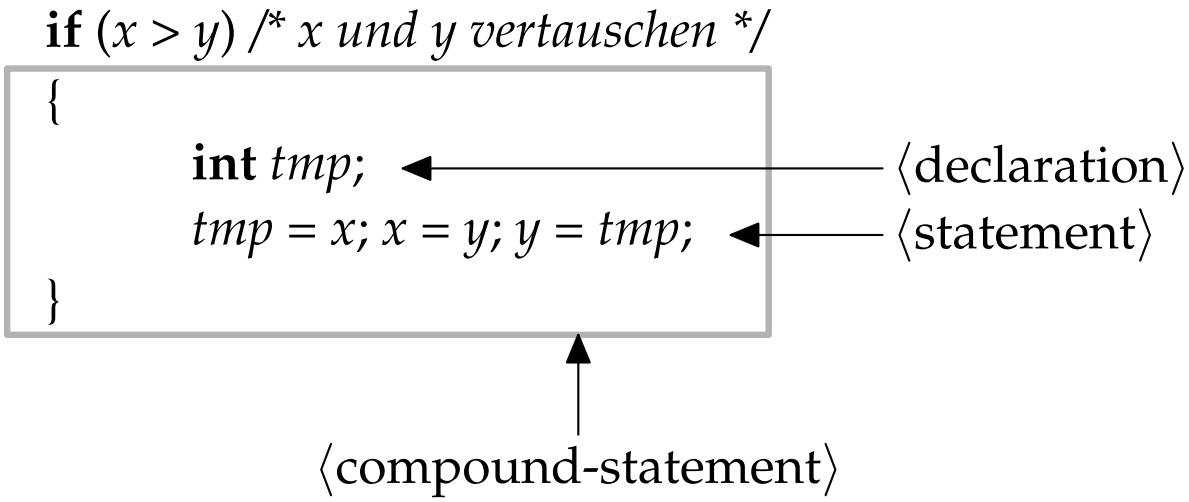
Anweisungen in C

$$
\begin{aligned}
\langle \text{statement} \rangle \quad &\longrightarrow \quad \langle \text{expression-statement} \rangle \\
&\longrightarrow \quad \langle \text{labeled-statement} \rangle \\
&\longrightarrow \quad \langle \text{compound-statement} \rangle \\
&\longrightarrow \quad \langle \text{conditional-statement} \rangle \\
&\longrightarrow \quad \langle \text{iterative-statement} \rangle \\
&\longrightarrow \quad \langle \text{switch-statement} \rangle \\
&\longrightarrow \quad \langle \text{break-statement} \rangle \\
&\longrightarrow \quad \langle \text{continue-statement} \rangle \\
&\longrightarrow \quad \langle \text{return-statement} \rangle \\
&\longrightarrow \quad \langle \text{goto-statement} \rangle \\
&\longrightarrow \quad \langle \text{null-statement} \rangle
\end{aligned}
$$

Blockstruktur in C

$$
\begin{array}{rcl}
\langle\text{compound-statement}\rangle & \longrightarrow & \text{„}\{\text{“} \\
 & & [\ \langle\text{declaration-or-statement-list}\rangle\ ] \\
 & & \text{„}\}\text{“} \\
\langle\text{declaration-or-statement-list}\rangle & \longrightarrow & \langle\text{declaration-or-statement}\rangle \\
 & \longrightarrow & \langle\text{declaration-or-statement-list}\rangle \\
 & & \langle\text{declaration-or-statement}\rangle \\
\langle\text{declaration-or-statement}\rangle & \longrightarrow & \langle\text{declaration}\rangle \\
 & \longrightarrow & \langle\text{statement}\rangle
\end{array}
$$

Blockstruktur in C



- Mit **int** *tmp*; wird eine lokale Variable mit dem Datentyp **int** deklariert.
- Die *Gültigkeit* von *tmp* erstreckt sich auf den umrandeten Anweisungsblock.

Initialisierung lokaler Variablen

varinit.c

```
#include <stdio.h>

int main() {
   int i; /* left uninitialized */
   int j = i; /* effect is undefined, yet compilers accept it */
   printf("%d\n", j);
}
```

- In Java durften lokale Variablen solange nicht verwendet werden, solange sie nicht in jedem Falle initialisiert worden sind. Dies wird bei Java vom Übersetzer zur Übersetzzeit überprüft.
- In C gibt geschieht dies nicht. Der Wert einer uninitialisierten lokalen Variable ist undefiniert.
- Um das Problem zu vermeiden, sollten lokale Variablen entweder bei der Deklaration oder der darauffolgenden Anweisung initialisiert werden.
- Der *gcc* warnt bei eingeschalteter Optimierung und bei neueren Versionen auch ohne Optimierung. Viele Übersetzer tun dies jedoch nicht.

Initialisierung lokaler Variablen

Auf unseren Suns mit einem etwas älteren gcc-Übersetzer:

```
clonard$ gcc --version | sed 1q
gcc (GCC) 4.1.1
clonard$ gcc -std=gnu99 -Wall -o varinit varinit.c && ./varinit
4
clonard$ gcc -O2 -std=gnu99 -Wall -o varinit varinit.c && ./varinit
varinit.c: In function 'main':
varinit.c:5: warning: 'i' is used uninitialized in this function
7168
clonard$
```

Und auf unseren Maschinen mit Debian:

```
hochwanner$ gcc --version | sed 1q
gcc (Debian 4.4.5-8) 4.4.5
hochwanner$ gcc -std=gnu99 -Wall -o varinit varinit.c && ./varinit
varinit.c: In function 'main':
varinit.c:5: warning: 'i' is used uninitialized in this function
0
hochwanner$
```

Kommentare

- Kommentare beginnen mit „/*“, enden mit „*/“, und dürfen nicht geschachtelt werden.
- Alternativ kann seit C99 ein Kommentar auch mit „//“ begonnen werden, der sich bis zum Zeilenende erstreckt.

Schlüsselworte

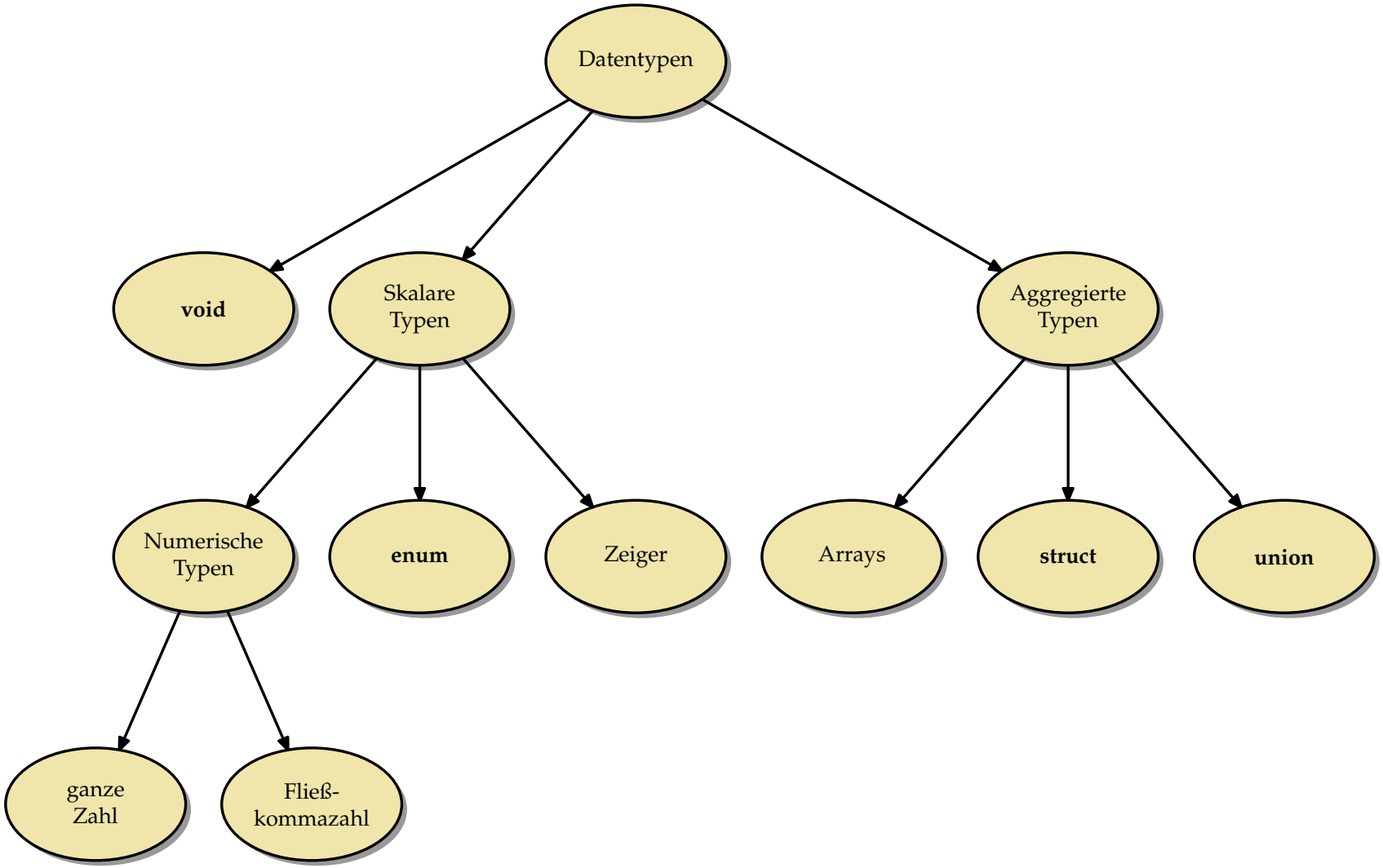
auto	**double**	**inline**	**sizeof**	**volatile**
break	**else**	**int**	**static**	**while**
case	**enum**	**long**	**struct**	**_Bool**
char	**extern**	**register**	**switch**	**_Complex**
const	**float**	**restrict**	**typedef**	**_Imaginary**
continue	**for**	**return**	**union**	
default	**goto**	**short**	**unsigned**	
do	**if**	**signed**	**void**	

Datentypen

Datentypen legen

- den *Speicherbedarf*,
- die *Interpretation* des Speicherplatzes sowie
- die *erlaubten Operationen* fest.

Übersicht


Datentypen
void
Skalare Typen
Aggregierte Typen
Numerische Typen
enum
Zeiger
Arrays
struct
union
ganze Zahl
Fließ-kommazahl

Syntax bei Datentypen

- Im einfachsten Falle lässt sich eine Variablenvereinbarung sehr einfach zerlegen in die Angabe eines Typs und die des Variablennamens:
  int *i*;
  Hier ist *i* der Variablenname und **int** der Typ.
- Diese Zweiteilung entspricht soweit der Grammatik:

$$
\begin{array}{rcl}
\langle\text{declaration}\rangle & \longrightarrow & \langle\text{declaration-specifiers}\rangle \\
 & & [\ \langle\text{init-declarator-list}\rangle\ ] \\
\langle\text{declaration-specifiers}\rangle & \longrightarrow & \langle\text{storage-class-specifier}\rangle \\
 & & [\ \langle\text{declaration-specifiers}\rangle\ ] \\
 & \longrightarrow & \langle\text{type-specifier}\rangle \\
 & & [\ \langle\text{declaration-specifiers}\rangle\ ] \\
 & \longrightarrow & \langle\text{type-qualifier}\rangle \\
 & & [\ \langle\text{declaration-specifiers}\rangle\ ] \\
 & \longrightarrow & \langle\text{function-specifier}\rangle \\
 & & [\ \langle\text{declaration-specifiers}\rangle\ ]
\end{array}
$$

Syntax bei Datentypen

- Leider trennt die Syntax nicht in jedem Falle sauber den Namen von dem Typ.
- Beispiel:
  int∗ *ip*;
- Hier besteht die linke Seite, d.h. der ⟨declaration-specifier⟩ nur aus **int**. Der Dereferenzierungs-Operator wird stattdessen syntaktisch der rechten Seite, dem ⟨init-declarator-list⟩ zugeordnet.
- Dies hat zur Konsequenz, dass bei
  int∗ *ip1*,*ip2*;
  ip1 und *ip2* unterschiedliche Typen erhalten. So ist *ip1* ein Zeiger auf **int**, während *ip2* schlicht nur den Typ **int** hat.

Skalare Datentypen

- Zu den skalaren Datentypen gehören alle Typen, die entweder numerisch sind oder sich zu einem numerischen Typ konvertieren lassen.
- Ein Wert eines skalaren Datentyps kann beispielsweise ohne weitere Konvertierung in einer Bedingung verwendet werden.
- Entsprechend wird die 0 im entsprechenden Kontext auch als Null-Zeiger interpretiert oder umgekehrt ein Null-Zeiger ist äquivalent zu *false* und ein Nicht-Null-Zeiger entspricht innerhalb einer Bedingung *true*.
- Ferner liegt die Nähe zwischen Zeigern und ganzen Zahlen auch in der von C unterstützten Adressarithmetik begründet.

Ganzzahlige Datentypen

⟨integer-type-specifier⟩	$\longrightarrow$	⟨signed-type-specifier⟩
	$\longrightarrow$	⟨unsigned-type-specifier⟩
	$\longrightarrow$	⟨character-type-specifier⟩
	$\longrightarrow$	⟨bool-type-specifier⟩
⟨signed-type-specifier⟩	$\longrightarrow$	[**signed**] **short** [**int**]
	$\longrightarrow$	[**signed**] **int**
	$\longrightarrow$	[**signed**] **long** [**int**]
	$\longrightarrow$	[**signed**] **long long** [**int**]
⟨unsigned-type-specifier⟩	$\longrightarrow$	**unsigned short** [**int**]
	$\longrightarrow$	**unsigned** [**int**]
	$\longrightarrow$	**unsigned long** [**int**]
	$\longrightarrow$	**unsigned long long** [**int**]
⟨character-type-specifier⟩	$\longrightarrow$	**char**
	$\longrightarrow$	**signed char**
	$\longrightarrow$	**unsigned char**
⟨bool-type-specifier⟩	$\longrightarrow$	**_Bool**

Ganzzahlige Datentypen

- Die Spezifikation eines ganzzahligen Datentyps besteht aus einem oder mehreren Schlüsselworten, die die Größe festlegen, und dem optionalen Hinweis, ob der Datentyp vorzeichenbehaftet ist oder nicht.
- Fehlt die Angabe von **signed** oder **unsigned**, so wird grundsätzlich **signed** angenommen.
- Die einzigen Ausnahme hiervon sind **char** und **_Bool**.
- Bei **char** darf der Übersetzer selbst eine Voreinstellung treffen, die sich am effizientesten auf der Zielarchitektur umsetzen lässt.

Ganzzahlige Datentypen

Auch wenn Angaben wie **short** oder **long** auf eine gewisse Größe hindeuten, so legt keiner der C-Standards die damit verbundenen tatsächlichen Größen fest. Stattdessen gelten nur folgende Regeln:

- Der jeweilige „größere“ Datentyp in der Reihe **char**, **short**, **int**, **long**, **long long** umfasst den Wertebereich der kleineren Datentypen, d.h. **char** ist nicht größer als **short**, **short** nicht größer als **int** usw.
- Für jeden der ganzzahligen Datentypen gibt es Mindestintervalle, die abgedeckt sein müssen. (Die zugehörige Übersichtstabelle folgt.)
- Die korrespondierenden Datentypen mit und ohne Vorzeichen (etwa **signed int** und **unsigned int**) belegen exakt den gleichen Speicherplatz und verwenden die gleiche Zahl von Bits. (Entsprechende Konvertierungen erfolgen entsprechend der Semantik des Zweier-Komplements.)

Darstellung ganzer Zahlen

In C werden alle ganzzahligen Datentypen durch Bitfolgen fester Länge repräsentiert: $\{a_i\}_{i=1}^{n}$ mit $a_i \in \{0, 1\}$. Bei ganzzahligen Datentypen ohne Vorzeichen ergibt sich der Wert direkt aus der binären Darstellung:

$$a = \sum_{i=1}^{n} a_i 2^{i-1}$$

Daraus folgt, dass der Wertebereich bei n Bits im Bereich von 0 bis $2^n - 1$ liegt.

Darstellung ganzer Zahlen mit Vorzeichen

Bei ganzzahligen Datentypen mit Vorzeichen übernimmt a_n die Rolle des Vorzeichenbits. Für die Repräsentierung gibt es bei C99 nur drei zugelassene Varianten:

- **Zweier-Komplement**:

$$a = \sum_{i=1}^{n-1} a_i 2^{i-1} - a_n 2^n$$

Wertebereich: $\left[-2^{n-1}, 2^{n-1} - 1\right]$
Diese Darstellung hat sich durchgesetzt und wird von fast allen Prozessor-Architekturen unterstützt.

Darstellung ganzer Zahlen mit Vorzeichen

- **Einer-Komplement**:

$$a = \sum_{i=1}^{n-1} a_i 2^{i-1} - a_n (2^n - 1)$$

Wertebereich: $\left[-2^{n-1} + 1, 2^{n-1} - 1\right]$
Vorsicht: Es gibt zwei Repräsentierungen für die Null. Es gilt:
$-a == \tilde{}a$
Diese Darstellung gibt es auf einigen historischen Architekturen wie etwa der PDP-1, der UNIVAC 1100/2200 oder der 6502-Architektur.

- **Trennung zwischen Vorzeichen und Betrag**:

$$a = (-1)^{a_n} \sum_{i=1}^{n-1} a_i 2^{i-1}$$

Wertebereich: $\left[-2^{n-1} + 1, 2^{n-1} - 1\right]$
Vorsicht: Es gibt zwei Repräsentierungen für die Null.
Diese Darstellung wird ebenfalls nur von historischen Architekturen verwendet wie etwa der IBM 7090.

Was passiert bei Überläufen?

Was passiert bei einer Addition, Subtraktion oder Multiplikation, die den Wertebereich des jeweiligen Datentyps verlässt?

- Bei vorzeichenbehafteten ganzen Zahlen ist das Resultat undefiniert. In der Praxis bedeutet dies, dass wir die repräsentierbaren niederwertigen Bits im Zweierkomplement erhalten.
- Bei ganzen Zahlen ohne Vorzeichen stellt C sicher, dass wir das korrekte Resultat modulo 2^n erhalten.

Alle gängigen Prozessorarchitekturen erkennen einen Überlauf, aber C ignoriert dieses. Das wird in Java genauso gehandhabt.

Was passiert, wenn durch 0 geteilt wird?

div0.c

```
int main() {
   int i = 1; int j = 0;
   int k = i / j;
   return k;
}
```

- Dies ist generell offen.
- Es kann zu einem undefinierten Resultat führen oder zu einem Abbruch der Programmausführung.
- Letzteres ist die Regel.

```
clonard$ gcc -std=gnu99 -Wall -o div0 div0.c && ./div0
Arithmetic Exception (core dumped)
clonard$
```

Mindestbereiche bei ganzen Zahlen

Datentyp	Bits	Intervall	Konstanten
signed char	8	$[-127, 127]$	*SCHAR_MIN*, *SCHAR_MAX*
unsigned char	8	$[0, 255]$	*UCHAR_MAX*
char	8		*CHAR_MIN*, *CHAR_MAX*
short	16	$[-32767, 32767]$	*SHRT_MIN*, *SHRT_MAX*
unsigned short	16	$[0, 65535]$	*USHRT_MAX*
int	16	$[-32767, 32767]$	*INT_MIN*, *INT_MAX*
unsigned int	16	$[0, 65535]$	*UINT_MAX*
long	32	$\left[-2^{31}+1, 2^{31}-1\right]$	*LONG_MIN*, *LONG_MAX*
unsigned long	32	$[0, 4294967295]$	*ULONG_MAX*
long long	64	$\left[-2^{63}+1, 2^{63}-1\right]$	*LLONG_MIN*, *LLONG_MAX*
unsigned long long	64	$\left[0, 2^{64}-1\right]$	*ULLONG_MAX*

Datentypen für Zeichen

- Der Datentyp **char** orientiert sich in seiner Größe typischerweise an dem Byte, der kleinsten adressierbaren Einheit.
- In <*limits.h*> findet sich die Konstante *CHAR_BIT*, die die Anzahl der Bits bei **char** angibt. Dieser Wert muss mindestens 8 betragen und weicht davon auch normalerweise nicht ab.
- Der Datentyp **char** gehört mit zu den ganzzahligen Datentypen und entsprechend können Zeichen wie ganze Zahlen und umgekehrt behandelt werden.
- Der C-Standard überlässt den Implementierungen die Entscheidung, ob **char** vorzeichenbehaftet ist oder nicht. Wer sicher gehen möchte, spezifiziert dies explizit mit **signed char** oder **unsigned char**.
- Für größere Zeichensätze gibt es den Datentyp *wchar_t* aus <*wchar.h*>.

Zeichenkonstanten

Zeichenkonstanten werden in einfache Hochkommata eingeschlossen, etwa 'a' (vom Datentyp **char**) oder *L*'a' (vom Datentyp *wchar_t*).
Für eine Reihe von nicht druckbaren Zeichen gibt es Ersatzdarstellungen:

\b	BS	*backspace*
\f	FF	*formfeed*
\n	LF	*newline*, Zeilentrenner
\r	CR	*carriage return*, „Wagenrücklauf“
\t	HT	Horizontaler Tabulator
\\	\	„Fluchtsymbol“
\'	'	einfaches Hochkomma
\a		*audible bell*, Signalton
\0	NUL	Null-Byte
\ddd		ASCII-Code (oktal)

Zeichen als ganzzahlige Werte

rot13.c

```
#include <stdio.h>

const int letters = 'z' - 'a' + 1;
const int rotate = 13;
int main() {
   int ch;
   while ((ch = getchar()) != EOF) {
      if (ch >= 'a' && ch <= 'z') {
         ch = 'a' + (ch - 'a' + rotate) % letters;
      } else if (ch >= 'A' && ch <= 'Z') {
         ch = 'A' + (ch - 'A' + rotate) % letters;
      }
      putchar(ch);
   }
}
```

Gleitkommazahlen

$$
\begin{aligned}
\langle\text{floating-point-type-specifier}\rangle &\longrightarrow \textbf{float} \\
&\longrightarrow \textbf{double} \\
&\longrightarrow \textbf{long double} \\
&\longrightarrow \langle\text{complex-type-specifier}\rangle \\
\langle\text{complex-type-specifier}\rangle &\longrightarrow \textbf{float \_Complex} \\
&\longrightarrow \textbf{double \_Complex} \\
&\longrightarrow \textbf{long double \_Complex}
\end{aligned}
$$

IEEE-754

- In der Vergangenheit gab es eine Vielzahl stark abweichender Darstellungen für Gleitkommazahlen, bis 1985 mit dem Standard IEEE-754 (auch IEC 60559 genannt) eine Vereinheitlichung gelang, die sich rasch durchsetzte und von allen heute üblichen Prozessor-Architekturen unterstützt wird.
- Der C-Standard bezieht sich ausdrücklich auf IEEE-754, auch wenn die Einhaltung davon nicht für Implementierungen garantiert werden kann, bei denen die Hardware-Voraussetzungen dafür fehlen.

Darstellung von Gleitkommazahlen

Bei IEEE-754 besteht die binäre Darstellung einer Gleitkommazahl aus drei Komponenten,

- dem Vorzeichen s (ein Bit),
- dem aus q Bits bestehenden Exponenten $\{e_i\}_{i=1}^{q}$,
- und der aus p Bits bestehenden Mantisse $\{m_i\}_{i=1}^{p}$.

Darstellung des Exponenten

- Für die Darstellung des Exponenten e hat sich folgende verschobene Darstellung als praktisch erwiesen:

$$e = -2^{q-1} + 1 + \sum_{i=1}^{q} e_i 2^{i-1}$$

- Entsprechend liegt e im Wertebereich $\left[-2^{q-1} + 1, 2^{q-1}\right]$.
- Da die beiden Extremwerte für besondere Kodierungen verwendet werden, beschränkt sich der reguläre Bereich von e auf $[e_{min}, e_{max}]$ mit $e_{min} = -2^{q-1} + 2$ und $e_{max} = 2^{q-1} - 1$.
- Bei dem aus insgesamt 32 Bits bestehenden Format für den Datentyp **float** mit $q = 8$ ergibt das den Bereich $[-126, 127]$.

Normalisierte Darstellung

- Wenn e im Intervall $[e_{min}, e_{max}]$ liegt, dann wird die Mantisse m so interpretiert:

$$m = 1 + \sum_{i=1}^{p} m_i 2^{i-p-1}$$

- Wie sich dieser sogenannten normalisierten Darstellung entnehmen lässt, gibt es ein implizites auf 1 gesetztes Bit, d.h. m entspricht der im Zweier-System notierten Zahl $1, m_p m_{p-1} \ldots m_2 m_1$.
- Der gesamte Wert ergibt sich dann aus $x = (-1)^s \times 2^e \times m$.
- Um die 0 darzustellen, gilt der Sonderfall, dass $m = 0$, wenn alle Bits des Exponenten gleich 0 sind, d.h. $e = -2^{q-1} + 1$, und zusätzlich auch alle Bits der Mantisse gleich 0 sind. Da das Vorzeichenbit unabhängig davon gesetzt sein kann oder nicht, gibt es zwei Darstellungen für die Null: -0 und $+0$.

Weitere Kodierungen bei Gleitkommazahlen

- IEEE-754 unterstützt auch die sogenannte denormalisierte Darstellung, bei der alle Bits des Exponenten gleich 0 sind, es aber in der Mantisse mindestens ein Bit mit $m_i = 1$ gibt. In diesem Falle ergibt sich folgende Interpretation:

$$
\begin{aligned}
m &= \sum_{i=1}^{p} m_i 2^{i-p-1} \\
x &= (-1)^s \times 2^{e_{min}} \times m
\end{aligned}
$$

- Der Fall $e = e_{max} + 1$ erlaubt es, ∞, $-\infty$ und *NaN* (*not a number*) mit in den Wertebereich der Gleitkommazahlen aufzunehmen. ∞ und $-\infty$ werden bei Überläufen verwendet und NaN bei undefinierten Resultaten (Beispiel: Wurzel aus einer negativen Zahl).

Datentypen für Gleitkommazahlen

- IEEE-754 gibt Konfigurationen für einfache, doppelte und erweiterte Genauigkeiten vor, die auch so von C übernommen wurden.
- Allerdings steht nicht auf jeder Architektur **long double** zur Verfügung, so dass in solchen Fällen ersatzweise nur eine doppelte Genauigkeit verwendet wird.
- Umgekehrt rechnen einige Architekturen grundsätzlich mit einer höheren Genauigkeit und runden dann, wenn eine Zuweisung an eine Variable des Typs **float** oder **double** erfolgt. Dies alles ist entsprechend IEEE-754 zulässig – auch wenn dies zur Konsequenz hat, dass Ergebnisse selbst bei elementaren Operationen auf verschiedenen konformen Architekturen voneinander abweichen können.
- Hier ist die Übersicht:

Datentyp	Bits	q	p
float	32	8	23
double	64	11	52
long double		≥ 15	≥ 63

Problematik von Rundungsfehlern

- Rundungsfehler beim Umgang mit Gleitkomma-Zahlen sind unvermeidlich.
- Sie entstehen in erster Linie, wenn Werte nicht exakt darstellbar sind. So gibt es beispielsweise keine Repräsentierung für 0,1. Stattdessen kann nur eine der „Nachbarn“ verwendet werden.
- Bedauerlicherweise können selbst kleine Rundungsfehler katastrophale Ausmasse nehmen.
- Dies passiert beispielsweise, wenn Werte völlig unterschiedlicher Größenordnungen zueinander addiert oder voneinander subtrahiert werden. Dies kann dann zur Auslöschung wesentlicher Bits der kleineren Größenordnung führen.

Flächenberechnung eines Dreiecks

- Gegeben seien die Längen a, b, c eines Dreiecks. Zu berechnen ist die Fläche A des Dreiecks.
- Dazu bietet sich folgende Berechnungsformel an:

$$
\begin{aligned}
s &= \frac{a+b+c}{2} \\
A &= \sqrt{s(s-a)(s-b)(s-c)}
\end{aligned}
$$

triangle.c

```
double triangle_area1(double a, double b, double c) {
   double s = (a + b + c) / 2;
   return sqrt(s*(s-a)*(s-b)*(s-c));
}
```

Flächenberechnung eines Dreiecks

- Bei der Addition von $a + b + c$ kann bei einem schmalen Dreieck die kleine Seitelänge verschwinden, wenn die Größenordnungen weit genug auseinander liegen.
- Wenn dann später die Differenz zwischen s und der kleinen Seitelänge gebildet wird, kann der Fehler katastrophal werden.
- William Kahan hat folgende alternative Formel vorgeschlagen, die diese Problematik vermeidet:

$$A = \frac{\sqrt{(a+(b+c))(c-(a-b))(c+(a-b))(a+(b-c))}}{4}$$

Wobei hier die Werte a, b und c so zu vertauschen sind, dass gilt: $a > b > c$.

Flächenberechnung eines Dreiecks

triangle.c

```
#define SWAP(a,b) {int tmp; tmp = a; a = b; b = tmp;}
double triangle_area2(double a, double b, double c) {
   /* sort a, b, and c in descending order,
      applying a bubble-sort */
   if (a < b) SWAP(a, b);
   if (b < c) SWAP(b, c);
   if (a < b) SWAP(a, b);
   /* formula by W. Kahan */
   return sqrt((a + (b + c)) * (c - (a - b)) *
               (c + (a - b)) * (a + (b - c)))/4;
}
```

Flächenberechnung eines Dreiecks

triangle.c

```
int main() {
   double a, b, c;
   printf("triangle side lenghts a b c: ");
   if (scanf("%lf %lf %lf", &a, &b, &c) != 3) {
      printf("Unable to read three floats!\n");
      return 1;
   }
   double a1 = triangle_area1(a, b, c);
   double a2 = triangle_area2(a, b, c);
   printf("Formula #1 delivers %.16lf\n", a1);
   printf("Formula #2 delivers %.16lf\n", a2);
   printf("Difference: %lg\n", fabs(a1-a2));
   return 0;
}
```

Flächenberechnung eines Dreiecks

```
dublin$ gcc -Wall -std=c99 triangle.c -lm
dublin$ a.out
triangle side lenghts a b c: 1e10 1e10 1e-10
Formula #1 delivers 0.0000000000000000
Formula #2 delivers 0.5000000000000000
Difference: 0.5
dublin$
```

Vergleich von Gleitkommazahlen

- Wann können zwei Gleitkommazahlen als gleich betrachtet werden?
- Oder wann kann das gleiche Resultat erwartet werden?
- Gilt beispielsweise $(x/y)*y == x$?
- Interessanterweise garantiert hier IEEE-754 die Gleichheit, falls n und m beide ganze Zahlen sind, die sich in doppelter Genauigkeit repräsentieren lassen (also **double**), $|m| < 2^{52}$ und $n = 2^i + 2^j$ für natürliche Zahlen i, j. (siehe Theorem 7 aus dem Aufsatz von Goldberg).
- Aber beliebig verallgemeinern lässt sich dies nicht.

Vergleich von Gleitkommazahlen

equality.c

```
#include <stdio.h>
int main() {
   double x, y;
   printf("x y = ");
   if (scanf("%lf %lf", &x, &y) != 2) {
      printf("Unable to read two floats!\n");
      return 1;
   }
   if ((x/y)*y == x) {
      printf("equal\n");
   } else {
      printf("not equal\n");
   }
   return 0;
}
```

Vergleich von Gleitkommazahlen

```
dublin$ gcc -Wall -std=c99 equality.c
dublin$ a.out
x y = 3 10
equal
dublin$ a.out
x y = 2 0.77777777777777
not equal
dublin$
```

Vergleich von Gleitkommazahlen

- Gelegentlich wird nahegelegt, statt dem ==-Operator auf die Nähe zu testen, d.h. $x \sim y \Leftrightarrow |x - y| < \epsilon$, wobei ϵ für eine angenommene Genauigkeit steht.
- Dies lässt jedoch folgende Fragen offen:
  - Wie sollte ϵ gewählt werden?
  - Ist der Wegfall der (bei == selbstverständlichen) Äquivalenzrelation zu verschmerzen? (Schließlich lässt sich aus $x \sim y$ und $y \sim z$ nicht mehr $x \sim z$ folgern.)
  - Soll auch dann $x \sim y$ gelten, wenn beide genügend nahe an der 0 sind, aber die Vorzeichen sich voneinander unterscheiden.
- Die Frage nach einem Äquivalenztest lässt sich nicht allgemein beantworten, sondern hängt von dem konkreten Fall ab.

Aufzählungstypen

⟨enumeration-type-specifier⟩	⟶	⟨enumeration-type-definition⟩
	⟶	⟨enumeration-type-reference⟩
⟨enumeration-type-definition⟩	⟶	**enum** [⟨enumeration-tag⟩] „{“
		⟨enumeration-definition-list⟩ [„,“] „}“
⟨enumeration-tag⟩	⟶	⟨identifier⟩
⟨enumeration-definition-list⟩	⟶	⟨enumeration-constant-definition⟩
	⟶	⟨enumeration-definition-list⟩ „,“
		⟨enumeration-constant-definition⟩
⟨enumeration-constant-definition⟩	⟶	⟨enumeration-constant⟩
	⟶	⟨enumeration-constant⟩ „=“ ⟨expression⟩
⟨enumeration-constant⟩	⟶	⟨identifier⟩
⟨enumeration-type-reference⟩	⟶	**enum** ⟨enumeration-tag⟩

Aufzählungstypen

- Aufzählungsdatentypen sind grundsätzlich ganzzahlig und entsprechend auch kompatibel mit anderen ganzzahligen Datentypen.
- Welcher vorzeichenbehaftete ganzzahlige Datentyp als Grundtyp für Aufzählungen dient (etwa **int** oder **short**) ist nicht festgelegt.
- Steht zwischen **enum** und der Aufzählung ein Bezeichner (⟨identifier⟩), so kann dieser Name bei späteren Deklarationen (bei einer ⟨enumeration-type-reference⟩) wieder verwendet werden.
- Sofern nichts anderes angegeben ist, erhält das erste Aufzählungselement den Wert 0.
- Bei den übrigen Aufzählungselementen wird jeweils der Wert des Vorgängers genommen und 1 dazuaddiert.
- Diese standardmäßig vergebenen Werte können durch die Angabe einer Konstante verändert werden. Damit wird dann auch implizit der Wert der nächsten Konstante verändert, sofern die nicht ebenfalls explizit gesetzt wird.

Aufzählungstypen

- Gegeben sei folgendes (nicht nachahmenswerte) Beispiel:

```
enum msglevel {
   notice, warning, error = 10,
   alert = error + 10, crit, emerg = crit * 2,
   debug = -1, debug0
};
```

- Dann ergeben sich daraus folgende Werte: *notice* $= 0$, *warning* $= 1$, *error* $= 10$, *alert* $= 20$, *crit* $= 21$, *emerg* $= 42$, *debug* $= -1$ und *debug0* $= 0$. C stört es dabei nicht, dass zwei Konstanten (*notice* und *debug0*) den gleichen Wert haben.

Aufzählungstypen

days.c

```
#include <stdio.h>
#include <stdlib.h>
#include <sys/types.h>
#include <time.h>

enum days { Monday, Tuesday, Wednesday, Thursday,
   Friday, Saturday, Sunday };
char* dayname[] = { "Monday", "Tuesday", "Wednesday",
   "Thursday", "Friday", "Saturday", "Sunday"
};

int main() {
   enum days day;
   for (day = Monday; day <= Sunday; ++day) {
      printf("Day %d = %s\n", day, dayname[day]);
   }
   /* seed the pseudo-random generator */
   unsigned int seed = time(0); srand(seed);
   /* select and print a pseudo-random day */
   enum days favorite_day = rand() % 7;
   printf("My favorite day: %s\n", dayname[favorite_day]);
}
```

Zeigertypen

$$
\begin{array}{rcl}
\langle\text{declaration}\rangle & \longrightarrow & \langle\text{declaration-specifiers}\rangle\ [\ \langle\text{init-declarator-list}\rangle\ ] \\
\langle\text{declaration-specifiers}\rangle & \longrightarrow & \langle\text{storage-class-specifier}\rangle\ [\ \langle\text{declaration-specifiers}\rangle\ ] \\
 & \longrightarrow & \langle\text{type-specifier}\rangle\ [\ \langle\text{declaration-specifiers}\rangle\ ] \\
 & \longrightarrow & \langle\text{type-qualifier}\rangle\ [\ \langle\text{declaration-specifiers}\rangle\ ] \\
 & \longrightarrow & \langle\text{function-specifier}\rangle\ [\ \langle\text{declaration-specifiers}\rangle\ ] \\
\langle\text{init-declarator-list}\rangle & \longrightarrow & \langle\text{init-declarator}\rangle \\
 & \longrightarrow & \langle\text{init-declarator-list}\rangle\ \text{„,“}\ \langle\text{init-declarator}\rangle \\
\langle\text{init-declarator}\rangle & \longrightarrow & \langle\text{declarator}\rangle \\
 & \longrightarrow & \langle\text{declarator}\rangle\ \text{„=“}\ \langle\text{initializer}\rangle \\
\langle\text{declarator}\rangle & \longrightarrow & [\ \langle\text{pointer}\rangle\ ]\ \langle\text{direct-declarator}\rangle \\
\langle\text{pointer}\rangle & \longrightarrow & \text{„*“}\ [\ \langle\text{type-qualifier-list}\rangle\ ] \\
 & \longrightarrow & \text{„*“}\ [\ \langle\text{type-qualifier-list}\rangle\ ]\ \langle\text{pointer}\rangle
\end{array}
$$

Zeigertypen

zeiger.c

```
#include <stdio.h>

int main() {
   int i = 13;
   int* p = &i; /* Zeiger p zeigt auf i; &i = Adresse von i */

   printf("i=%d, p=%p (Adresse), *p=%d (Wert)\n", i, p, *p);

   ++i;
   printf("i=%d, *p=%d\n", i, *p);

   ++*p; /* *p ist ein Links-Wert */
   printf("i=%d, *p=%d\n", i, *p);
}
```

Zeigerarithmetik

- Es ist zulässig, ganze Zahlen zu einem Zeiger zu addieren oder davon zu subtrahieren.
- Dabei wird jedoch der zu addierende oder zu subtrahierende Wert implizit mit der Größe des Typs multipliziert, auf den der Zeiger zeigt.
- Weiter ist es zulässig, Zeiger des gleichen Typs voneinander zu subtrahieren. Das Resultat wird dann implizit durch die Größe des referenzierten Typs geteilt.

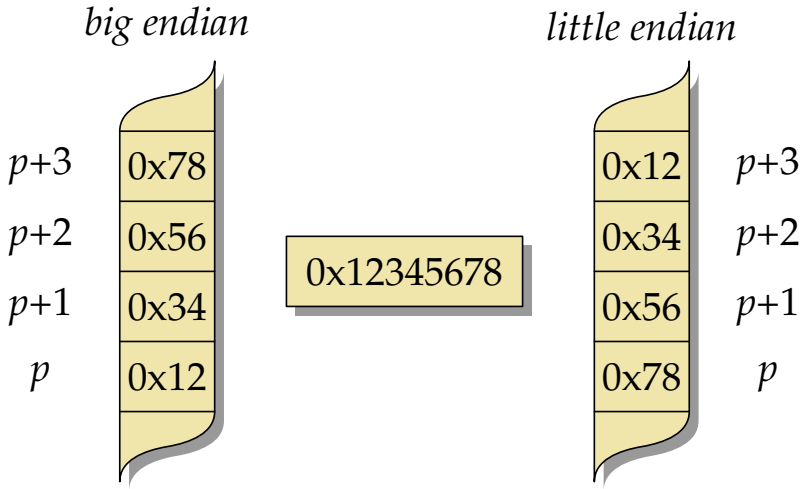
Zeigerarithmetik

zeiger1.c

```
#include <stdio.h>

int main() {
   unsigned int value = 0x12345678;
   unsigned char* p = (unsigned char*) &value;

   for (int i = 0; i < sizeof(unsigned int); ++i) {
      printf("p+%d --> 0x%02hhx\n", i, *(p+i));
   }
}
```

- Hier wird der Speicher byteweise „durchleuchtet“.
- Hierbei fällt auf, dass die interne Speicherung einer ganzen Zahl bei unterschiedlichen Architekturen (SPARC vs. Intel x86) verschieden ist: *big endian* vs. *little endian*.

big vs. little endian



- Bei *little endian* wird das niedrigstwertige Byte an der niedrigsten Adresse abgelegt, während bei
- *big endian* das niedrigstwertige Byte sich bei der höchsten Adresse befindet.

Typkonvertierungen

- Typ-Konvertierungen können in C sowohl implizit als auch explizit erfolgen.
- Implizite Konvertierungen werden angewendet bei Zuweisungs-Operatoren, Parameterübergaben und Operatoren. Letzteres schliesst auch die monadischen Operatoren mit ein.
- Explizite Konvertierungen erfolgen durch den sogenannten Cast-Operator.

Konvertierungen bei numerischen Datentypen

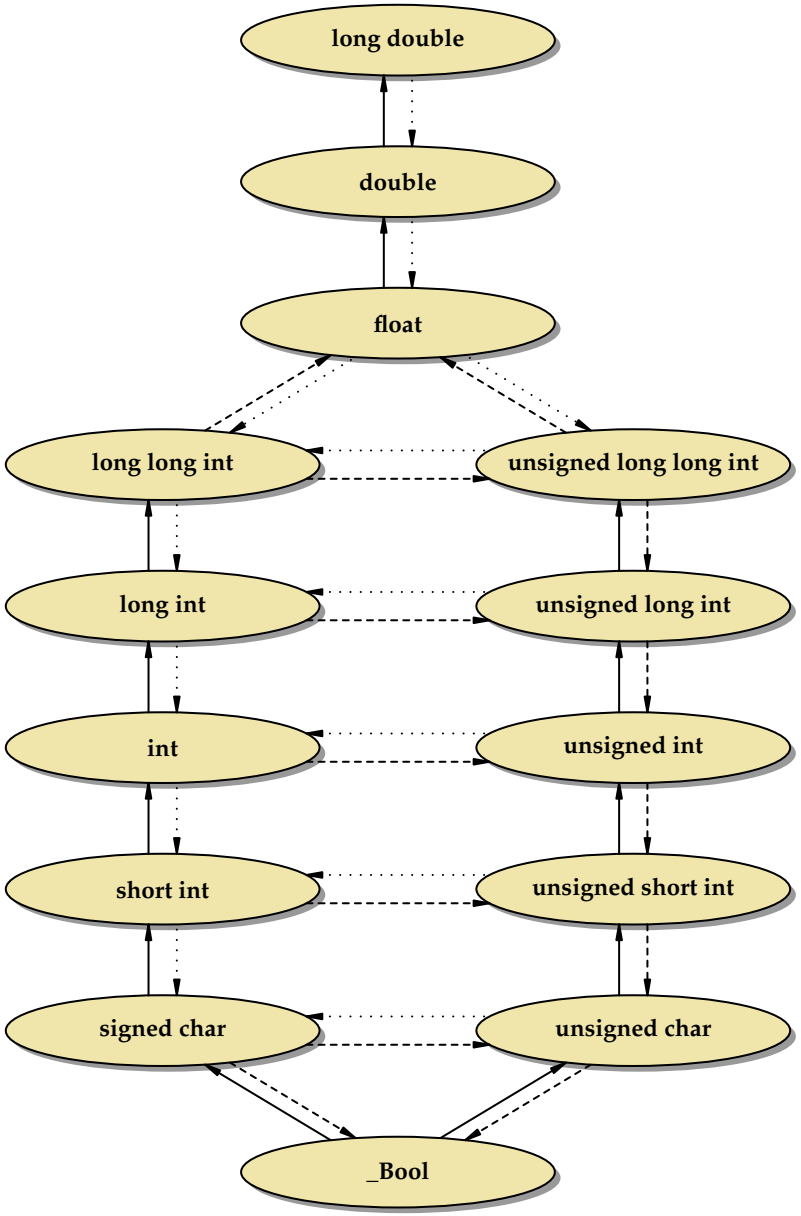
Bei einer Konvertierung zwischen numerischen Typen gilt der Grundsatz, dass – wenn irgendwie möglich – der Wert zu erhalten ist. Falls das jedoch nicht möglich ist, gelten folgende Regeln:

- Bei einer Konvertierung eines vorzeichenbehafteten ganzzahligen Datentyps zum Datentyp ohne Vorzeichen *gleichen Ranges* (also etwa von **int** zu **unsigned int**) wird eine ganze Zahl $a < 0$ zu b konvertiert, wobei gilt, dass $a \bmod 2^n = b \bmod 2^n$ mit n der Anzahl der verwendeten Bits, wobei hier der mod-Operator entsprechend der F-Definition bzw. Euklid gemeint ist. Dies entspricht der Repräsentierung des Zweier-Komplements.
- Der umgekehrte Weg, d.h. vom ganzzahligen Datentyp ohne Vorzeichen zum vorzeichenbehafteten Datentyp gleichen Ranges (also etwa von **unsigned int** zu **int**) hinterlässt ein *undefiniertes* Resultat, falls der Wert nicht darstellbar ist.

Konvertierungen bei numerischen Datentypen

- Bei einer Konvertierung von größeren ganzzahligeren Datentypen zu entsprechenden kleineren Datentypen werden die nicht mehr darstellbaren höherwertigen Bits weggeblendet, d.h. es gilt wiederum $a \bmod 2^n = b \bmod 2^n$, wobei n die Anzahl der Bits im kleineren Datentyp ist. (Das Resultat ist aber nur bei ganzzahligen Datentypen ohne Vorzeichen wohldefiniert.)
- Bei Konvertierungen zu *_Bool* ist das Resultat 0 (*false*), falls der Ausgangswert 0 ist, ansonsten immer 1 (*true*).
- Bei Konvertierungen von Gleitkommazahlen zu ganzzahligen Datentypen wird der ganzzahlige Anteil verwendet. Ist dieser im Zieltyp nicht darstellbar, so ist das Resultat undefiniert.
- Umgekehrt (beispielsweise auf dem Wege von **long long int** zu **float**) ist einer der beiden unmittelbar benachbarten darstellbaren Werte zu nehmen, d.h. es gilt entweder $a = b$ oder $a < b \wedge \nexists x : a < x < b$ oder $a > b \wedge \nexists x : a > x > b$ mit x aus der Menge des Zieltyps.

Konvertierungen bei numerischen Datentypen



Konvertierungen anderer skalarer Datentypen

- Jeder Aufzählungsdatentyp ist einem der ganzzahligen Datentypen implizit und implementierungsabhängig zugeordnet. Eine Konvertierung hängt von dieser (normalerweise nicht bekannten) Zuordnung ab.
- Zeiger lassen sich in C grundsätzlich als ganzzahlige Werte betrachten. Allerdings garantiert C nicht, dass es einen ganzzahligen Datentyp gibt, der den Wert eines Zeigers ohne Verlust aufnehmen kann.
- C99 hat hier die Datentypen *intptr_t* und *uintptr_t* in <*stdint.h*> eingeführt, die für die Repräsentierung von Zeigern als ganze Zahlen den geeignetsten Typ liefern.
- Selbst wenn diese groß genug sind, um Zeiger ohne Verlust aufnehmen zu können, so lässt der Standard dennoch offen, wie sich die beiden Typen *intptr_t* und *uintptr_t* innerhalb der Hierarchie der ganzzahligen Datentypen einordnen. Aber die weiteren Konvertierungsschritte und die damit verbundenen Konsequenzen ergeben sich aus dieser Einordnung.
- Die Zahl 0 wird bei einer Konvertierung in einen Zeigertyp immer in den Null-Zeiger konvertiert.

Implizite Konvertierungen

- Bei Zuweisungen wird der Rechts-Wert in den Datentyp des Links-Wertes konvertiert.
- Dies geschieht analog bei Funktionsaufrufen, wenn eine vollständige Deklaration der Funktion mit allen Parametern vorliegt.
- Wenn diese fehlt oder (wie beispielsweise bei *printf*) nicht vollständig ist, dann wird **float** implizit zu **double** konvertiert.

Implizite Konvertierungen

Die monadischen Operatoren !, $-$, $+$, $\sim$ und $*$ konvertieren implizit ihren Operanden:

- Ein vorzeichenbehafteter ganzzahliger Datentyp mit einem Rang niedriger als **int** wird zu **int** konvertiert,
- Ganzzahlige Datentypen ohne Vorzeichen werden ebenfalls zu **int** konvertiert, falls sie einen Rang niedriger als **int** haben und ihre Werte in jedem Falle von **int** darstellbar sind. Ist nur letzteres nicht der Fall, so erfolgt eine implizite Konvertierung zu **unsigned int**.
- Ranghöhere ganzzahlige Datentypen werden nicht konvertiert.

Die gleichen Regeln werden auch getrennt für die beiden Operanden der Schiebe-Operatoren $<<$ und $>>$ angewendet.

Implizite Konvertierung

Bei dyadischen Operatoren mit numerischen Operanden werden folgende implizite Konvertierungen angewendet:

- Sind die Typen beider Operanden vorzeichenbehaftet oder beide ohne Vorzeichen, so findet eine implizite Konvertierung zu dem Datentyp mit dem höheren Rang statt. So wird beispielsweise bei einer Addition eines Werts des Typs **short int** zu einem Wert des Typs **long int** der erstere in den Datentyp des zweiten Operanden konvertiert, bevor die Addition durchgeführt wird.
- Ist bei einem gemischten Fall (**signed** vs. **unsigned**) in jedem Falle eine Repräsentierung eines Werts des vorzeichenlosen Typs in dem vorzeichenbehafteten Typ möglich (wie etwa typischerweise bei **unsigned short** und **long int**), so wird der Operand des vorzeichenlosen Typs in den vorzeichenbehafteten Typ des anderen Operanden konvertiert.
- Bei den anderen gemischten Fällen werden beide Operanden in die vorzeichenlose Variante des höherrangigen Operandentyps konvertiert. So wird beispielsweise eine Addition bei **unsigned int** und **int** in **unsigned int** durchgeführt.

Datentypen für unveränderliche Werte

C sieht einige spezielle Attribute bei Typ-Deklarationen vor. Darunter ist auch **const**:

$$
\begin{aligned}
\langle\text{declaration-specifiers}\rangle &\longrightarrow \langle\text{storage-class-specifier}\rangle\ [\ \langle\text{declaration-specifiers}\rangle\ ] \\
&\longrightarrow \langle\text{type-specifier}\rangle\ [\ \langle\text{declaration-specifiers}\rangle\ ] \\
&\longrightarrow \langle\text{type-qualifier}\rangle\ [\ \langle\text{declaration-specifiers}\rangle\ ] \\
&\longrightarrow \langle\text{function-specifier}\rangle\ [\ \langle\text{declaration-specifiers}\rangle\ ] \\
\langle\text{type-qualifier}\rangle &\longrightarrow \textbf{const} \\
&\longrightarrow \textbf{volatile} \\
&\longrightarrow \textbf{restrict}
\end{aligned}
$$

Datentypen für unveränderliche Werte

Die Verwendung des **const**-Attributs hat zwei Vorteile:

- Der Programmierer wird davor bewahrt, eine Konstante versehentlich zu verändern. (Dies funktioniert aber nur beschränkt.)
- Besondere Optimierungen sind für den Übersetzer möglich, wenn bekannt ist, dass sich bestimmte Variablen nicht verändern dürfen.

Datentypen für unveränderliche Werte

const.c

```
#include <stdio.h>

int main() {
    const int i = 1;

    i++;        /* das geht doch nicht, oder?! */
    printf("i=%d\n", i);
}
```

- Der gcc beschränkt sich selbst dann nur auf Warnungen, wenn Konstanten offensichtlich verändert werden.

Vektoren

⟨direct-declarator⟩	$\longrightarrow$	⟨simple-declarator⟩
	$\longrightarrow$	„(“ ⟨simple-declarator⟩ „)“
	$\longrightarrow$	⟨function-declarator⟩
	$\longrightarrow$	⟨array-declarator⟩
⟨array-declarator⟩	$\longrightarrow$	⟨direct-declarator⟩ „[“ [⟨array-qualifier-list⟩]
		[⟨array-size-expression⟩] „]“
⟨array-qualifier-list⟩	$\longrightarrow$	⟨array-qualifier⟩
	$\longrightarrow$	⟨array-qualifier-list⟩ ⟨array-qualifier⟩
⟨array-qualifier⟩	$\longrightarrow$	**static**
	$\longrightarrow$	**restrict**
	$\longrightarrow$	**const**
	$\longrightarrow$	**volatile**
⟨array-size-expression⟩	$\longrightarrow$	⟨assignment-expression⟩
	$\longrightarrow$	„*“
⟨simple-declarator⟩	$\longrightarrow$	⟨identifier⟩

Deklaration von Vektoren

- Wie bei den Zeigertypen erfolgen die Typspezifikationen eines Vektors nicht im Rahmen eines ⟨type-specifier⟩.
- Stattdessen gehört eine Vektordeklaration zu dem ⟨init-declarator⟩. Das bedeutet, dass die Präzisierung des Typs zur genannten Variablen unmittelbar gehört.
- Entsprechend deklariert

```
int a[10], i;
```

  eine Vektorvariable *a* und eine ganzzahlige Variable *i*.

Vektoren und Zeiger

- Vektoren und Zeiger sind eng miteinander verwandt.
- Der Variablenname eines Vektors ist ein konstanter Zeiger auf den zugehörigen Element-Typ, der auf das erste Element verweist.
- Allerdings liefert **sizeof** mit dem Vektornamen als Operand die Größe des gesamten Vektors und nicht etwa nur die des Zeigers.

Vektoren und Zeiger

array.c

```
#include <stdio.h>
#include <stddef.h>

int main() {
   int a[] = {1, 2, 3, 4, 5};
   /* Groesse des Arrays bestimmen */
   const size_t SIZE = sizeof(a) / sizeof(a[0]);
   int* p = a;  /* kann statt a verwendet werden */
   /* aber: a weiss noch die Gesamtgroesse, p nicht */
   printf("SIZE=%zd, sizeof(a)=%zd, sizeof(p)=%zd\n",
      SIZE, sizeof(a), sizeof(p));
   for (int i = 0; i < SIZE; ++i) {
      *(a + i) = i+1; /* gleichbedeutend mit a[i] = i+1 */
   }
   /* Elemente von a aufsummieren */
   int sum = 0;
   for (int i = 0; i < SIZE; i++) {
      sum += p[i];   /* gleichbedeutend mit ... = a[i]; */
   }
   printf("Summe: %d\n", sum);
}
```

Indizierung

- Grundsätzlich beginnt die Indizierung bei 0.
- Ein Vektor mit 5 Elementen hat entsprechend zulässige Indizes im Bereich von 0 bis 4.
- Wird mit einem Index außerhalb des zulässigen Bereiches zugegriffen, so ist der Effekt undefiniert.
- Es ist dann damit zu rechnen, dass irgendeine andersweitig belegte Speicherfläche adressiert wird oder es zu einer harten Unterbrechung kommt, weil eine unzulässige Adresse dereferenziert wurde. Was tatsächlich passiert, hängt von der jeweiligen Adressraumbelegung ab.
- Viele bekannte Sicherheitslücken beruhen darauf, dass in C-Programmen die zulässigen Indexbereiche verlassen werden und auf diese Weise eingeschleuster Programmtext zur Ausführung gebracht werden kann.
- Anders als in Modula-2, Oberon oder Java gibt es aber keine automatisierte Überprüfung. Diese wäre auch wegen der Verwandtschaft von Vektoren und Zeigern nicht mit einem vertretbaren Aufwand in C umzusetzen.

Parameterübergabe bei Vektoren

- Da der Name eines Vektors nur ein Zeiger auf das erste Element ist, werden bei der Parameterübergabe entsprechend nur Zeigerwerte übergeben.
- Entsprechend arbeitet die aufgerufene Funktion nicht mit einer Kopie des Vektors, sondern hat dank dem Zeiger den direkten Zugriff auf den Vektor des Aufrufers.
- Die Dimensionierung des Vektors muss explizit mit Hilfe weiterer Parameter übergeben werden, wenn diese variabel sein soll.

Parameterübergabe bei Vektoren

array2.c

```
#include <stdio.h>

const int SIZE = 10;

/* Array wird veraendert, naemlich mit
   0, 1, 2, 3, ... initialisiert! */
void init(int a[], int length) {
   for (int i = 0; i < length; i++) {
      a[i] = i;
   }
}

int summe1(int a[], int length) {
   int sum = 0;
   for (int i = 0; i < length; i++) {
      sum += a[i];
   }
   return sum;
}
```

Parameterübergabe bei Vektoren

array2.c

```
int summe2(int* a, int length) {
   int sum = 0;
   for (int i = 0; i < length; i++) {
      sum += *(a+i); /* aequivalent zu ... += a[i]; */
   }
   return sum;
}

int main() {
   int array[SIZE];

   init(array, SIZE);

   printf("Summe: %d\n", summe1(array, SIZE));
   printf("Summe: %d\n", summe2(array, SIZE));
}
```

Mehrdimensionale Vektoren

- So könnte ein zweidimensionaler Vektor angelegt werden:

```
int matrix[2][3];
```

- Eine Initialisierung ist sofort möglich. Die geschweiften Klammern werden dann entsprechend verschachtelt:

```
int matrix[2][3] = {{0, 1, 2}, {3, 4, 5}};
```

Repräsentierung eines Vektors im Speicher

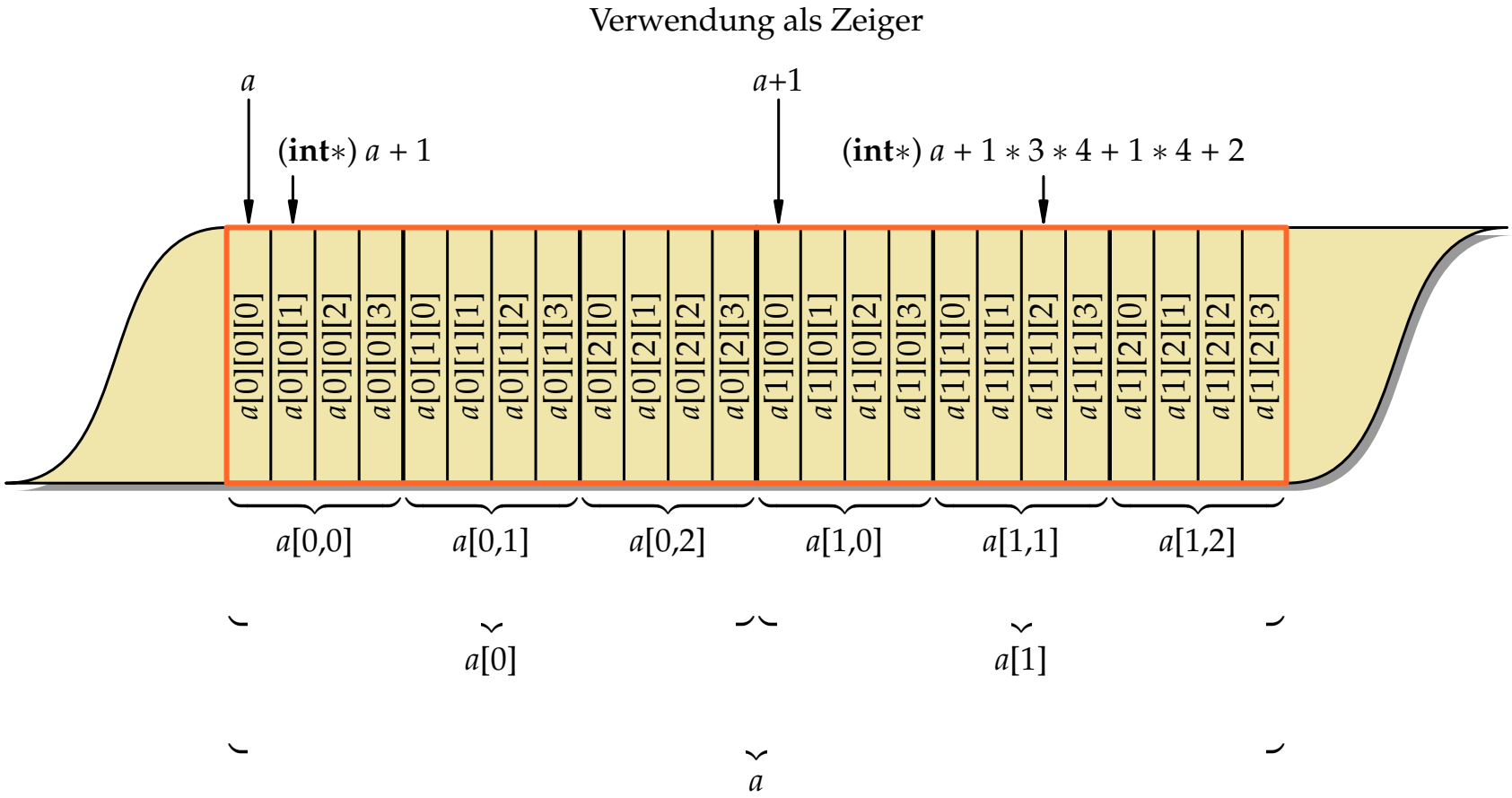
Angenommen die Anfangsadresse des Vektors liege bei 0*x1000* und eine ganze Zahl vom Typ **int** würde vier Bytes belegen, dann würde die Repräsentierung des Vektors *matrix* im Speicher folgendermaßen aussehen:

Element	**Adresse**	**Inhalt**
matrix[0][0]	0x1000	0
matrix[0][1]	0x1004	1
matrix[0][2]	0x1008	2
matrix[1][0]	0x100C	3
matrix[1][1]	0x1010	4
matrix[1][2]	0x1014	5

Repräsentierung eines Vektors im Speicher

- Gegeben sei:

```
int a[2][3][4];
```



Parameterübergabe mehrdimensionaler Vektoren

Folgende Möglichkeiten stehen zur Verfügung:

- Alle Dimensionen mit Ausnahme der ersten werden explizit bei der Parameterdeklaration festgelegt. Nur die erste Dimension ist dann noch variabel.
- Der gesamte Vektor wird zu einem eindimensionalen Vektor verflacht. Eine mehrdimensionale Indizierung erfolgt dann „per Hand“.
- Beginnend mit C99 gibt es auch mehrdimensionale dynamische Parameterübergaben von Vektoren. Dies ist analog zu den offenen mehrdimensionalen Feldparametern in Oberon. Im Unterschied zu Oberon müssen die Dimensionierungsparameter jedoch explizit benannt werden.

Zeichenketten

- Zeichenketten werden in C als Vektoren von Zeichen repräsentiert: **char**[]
- Das Ende der Zeichenkette wird durch ein sogenanntes Null-Byte ('\0') gekennzeichnet.
- Da es sich bei Zeichenketten um Vektoren handelt, werden bei der Parameterübergabe nur die Zeiger als Werteparameter übergeben.
- Die Zeichenkette (also der Inhalt des Vektors) kann entsprechend von der aufgerufenen Funktion verändert werden.

Zeichenketten-Konstanten

- Zeichenketten-Konstanten können durch von Doppelapostrophen eingeschlossene Zeichenfolgen spezifiziert werden. Hier im Rahmen einer Initialisierung:

```
char greeting[] = "Hallo";
```

- Dies ist eine Kurzform für

```
char greeting[] = {'H', 'a', 'l', 'l', 'o', '\0'};
```

- Eine Zeichenketten-Konstante steht für einen Zeiger auf den Anfang der Zeichenkette:

```
char* greeting = "Hallo";
```

- Zeichenketten-Konstanten dürfen nicht verändert werden. Sie werden, falls die zugrundeliegende Architektur dies ermöglicht, in einem Speicherbereich abgelegt, der nur Lesezugriffe zulässt.

Zeichenketten: Was ist zulässig?

strings.c

```
#include <stdio.h>

int main() {
   char array[10];
   char string[] = "Hallo!"; /* Groesse wird vom Compiler bestimmt */
   char* s1 = "Welt";
   char* s2;

   /* array = "not OK"; */   /* nicht zulaessig */
   array[0] = 'A';           /* zulaessig */
   array[1] = '\0';
   printf("array: %s\n", array);
   /* s1[5] = 'B'; */        /* nicht zulaessig */
   s1 = "ok";                /* zulaessig */
   printf("s1: %s\n", s1);
   s2 = s1;                  /* zulaessig */
   printf("s2: %s\n", s2);
   string[0] = 'X';          /* zulaessig */
   printf("string: %s\n", string);
   printf("sizeof(string): %zd\n", sizeof(string));
}
```

Länge einer Zeichenkette

strings1.c

```
/* Laenge einer Zeichenkette bestimmen */
int my_strlen1(char s[]) {
   int i;
   /* bis zum abschliessenden Null-Byte laufen */
   for (i = 0; s[i] != '\0'; i++); /* leere Anweisung! */
   return i;
}
```

- Die Bibliotheksfunktion *strlen()* liefert die Länge einer Zeichenkette zurück.
- Als Länge einer Zeichenkette wird die Zahl der Zeichen *vor* dem Null-Byte betrachtet.
- *my_strlen1()* bildet hier die Funktion nach unter Verwendung der vektoriellen Notation.

Länge einer Zeichenkette

strings1.c

```
/* Laenge einer Zeichenkette bestimmen */
int my_strlen2(char* s) {
   char* t = s;
   while (*t++);
   return t-s-1;
}
```

- Alternativ wäre es auch möglich, mit der Zeigernotation zu arbeiten.
- Zu beachten ist hier, dass der Post-Inkrement-Operator $++$ einen höheren Rang hat als der Dereferenzierungs-Operator $*$.
- Entsprechend bezieht sich das Inkrement auf t. Das Inkrement wird aber erst *nach* der Dereferenzierung als verspäteter Seiteneffekt ausgeführt.

Kopieren einer Zeichenkette

strings1.c

```
/* Kopieren einer Zeichenkette von s nach t
   Vorauss.: genuegend Platz in t */
void my_strcpy1(char t[], char s[]) {
   for (int i = 0; (t[i] = s[i]) != '\0'; i++);
}
```

- Das ist ein Nachbau der Bibliotheksfunktion *strcpy()* die (analog zur Anordnung bei einer Zuweisung) den linken Parameter als Ziel und den rechten Parameter als Quelle der Kopier-Aktion betrachtet.
- Hier zeigt sich auch eines der grossen Probleme von C im Umgang mit Vektoren: Da die tatsächlich zur Verfügung stehende Länge des Vektors *t* unbekannt bleibt, können weder *my_strcpy1()* noch die Laufzeitumgebung dies überprüfen.

Kopieren einer Zeichenkette

strings1.c

```
/* Kopieren einer Zeichenkette von s nach t
   Vorauss.: genuegend Platz in t */
void my_strcpy2(char* t, char* s) {
   for (; (*t = *s) != '\0'; t++, s++);
}
```

- In der Zeigernotation wird es einfacher.

Kopieren einer Zeichenkette

strings1.c

```
/* Kopieren einer Zeichenkette von s nach t
   Vorauss.: genuegend Platz in t */
void my_strcpy3(char* t, char* s) {
   while ((*t++ = *s++) != '\0');
}
```

- Die Inkrementierung lässt sich natürlich (wie schon bei der Längenbestimmung) mit integrieren.

Kopieren einer Zeichenkette

strings1.c

```
/* Kopieren einer Zeichenkette von s nach t
   Vorauss.: genuegend Platz in t */
void my_strcpy4(char* t, char* s) {
   while ((*t++ = *s++));
}
```

- Der Vergleichstest mit dem Nullbyte lässt sich natürlich streichen.
- Allerdings gibt es dann eine Warnung des gcc, dass möglicherweise der Vergleichs-Operator == mit dem Zuweisungs-Operator = verwechselt worden ist.
- Diese Warnung lässt sich (per Konvention) durch die doppelte Klammerung unterdrücken. Damit wird klar lesbar zum Ausdruck gegeben, dass das kein Versehen ist.

Vergleich zweier Zeichenketten

strings1.c

```
/* Vergleich zweier Zeichenketten
   Ergebnis: 0 fuer s = t, > 0 fuer s > t und < 0 fuer s < t */
int my_strcmp1(char s[], char t[]) {
   int i;
   for (i = 0; s[i] == t[i] && s[i] != '\0'; i++);
   return s[i] - t[i];
}
```

- Um alle sechs Vergleichsrelationen mit einer Funktion unterstützen zu können, arbeitet die Bibliotheksfunktion *strcmp()* mit einem ganzzahligen Rückgabewert, der < 0 ist, falls $s < t$, $= 0$ ist, falls s mit t übereinstimmt und > 0, falls $s > t$.

Vergleich zweier Zeichenketten

strings1.c

```
/* Vergleich zweier Zeichenketten
   Ergebnis: 0 fuer s = t, > 0 fuer s > t und < 0 fuer s < t */
int my_strcmp2(char* s, char* t) {
   for (; *s == *t && *s != '\0'; s++, t++);
   return *s - *t;
}
```

- Auch dies lässt sich in die Zeigernotation umsetzen.
- Auf ein integriertes Post-Inkrement wurde hier verzichtet, da dann die beiden Zeiger eins zu weit stehen, wenn es darum geht, die Differenz der unterschiedlichen Zeichen zu berechnen.

Verbundtypen

⟨structure-type-specifier⟩	⟶	**struct** [⟨identifier⟩] „{“
		⟨struct-declaration-list⟩ „}“
	⟶	**struct** ⟨identifier⟩
⟨struct-declaration-list⟩	⟶	⟨struct-declaration⟩
	⟶	⟨struct-declaration-list⟩ ⟨struct-declaration⟩
⟨struct-declaration⟩	⟶	⟨specifier-qualifier-list⟩
		⟨struct-declarator-list⟩ „;“
⟨specifier-qualifier-list⟩	⟶	⟨type-specifier⟩ [⟨specifier-qualifier-list⟩]
	⟶	⟨type-qualifier⟩ [⟨specifier-qualifier-list⟩]
⟨struct-declarator-list⟩	⟶	⟨struct-declarator⟩
	⟶	⟨struct-declarator-list⟩ „,“ ⟨struct-declarator⟩
⟨struct-declarator⟩	⟶	⟨declarator⟩
	⟶	[⟨declarator⟩] „:“ ⟨constant-expression⟩

Einfache Verbundtypen

- Ein *Verbundtyp* (in C auch Struktur genannt) fasst mehrere *Elemente* zu einem Datentyp zusammen. Im Gegensatz zu Vektoren können die Elemente *unterschiedlichen* Typs sein.
- Mit dem Schlüsselwort **struct** kann ein Verbundtyp wie folgt deklariert werden:

```
struct datum {
   short tag, monat, jahr;
};
```

- Hier ist *datum* ist der *Name des Verbundtyps*, der allerdings nur in Verbindung mit dem Schlüsselwort **struct** erkannt wird. Der hier deklarierte Verbundtyp repräsentiert – wie der Name schon andeutet – ein Datum. Jede Variable dieses Verbundtyps besteht aus drei ganzzahligen Komponenten, dem Tag, dem Monat und dem Jahr.

Variablenvereinbarungen bei Verbundtypen

- Eine Variable *geburtsdatum* des Verbundtyps **struct** *datum* kann danach wie folgt angelegt werden:

```
struct datum geburtsdatum;
```

- Analog zu Aufzählungen lassen sich auch Variablen für namenlose Verbundtypen anlegen:

```
struct {
   short tag, monat, jahr;
} my_geburtsdatum;
```

- Ohne den Namen fehlt jedoch die Möglichkeit, weitere Variablen dieses Typs zu deklarieren oder den Typnamen in einer Typkonvertierung oder einem Aggregat zu spezifizieren.

Initialisierungen bei Verbundtypen

- Variablen eines Verbund-Typs können bereits bei ihrer Definition initialisiert werden:

```
struct datum geburtsdatum = {3, 5, 1978};
```

- Alternativ kann auch der Wert eines Verbundtyps innerhalb eines Ausdrucks mit Hilfe eines Aggregats konstruiert werden:

```
struct datum geburtsdatum;
geburtsdatum = (struct datum) {3, 5, 1978};
```

Komponentenzugriff bei Verbundtypen

- Auf die *Komponenten* eines Verbundtyps kann wie folgt zugegriffen werden:

```
struct datum gebdat = ...;

printf("%hd.%hd.%hd", gebdat.tag, gebdat.monat, gebdat.jahr);

struct datum *p = ...;

/* Zeiger zuerst dereferenzieren ... */
printf("%hd.%hd.%hd", (*p).tag, (*p).monat, (*p).jahr);
/* ... oder einfacher (und aequivalent) mit -> ... */
printf("%hd.%hd.%hd", p->tag, p->monat, p->jahr);
```

- Aufgrund der *Vorrang-Regeln* bei Operatoren ist $*p.tag$ äquivalent zu $*(p.tag)$ und nicht zu $(*p).tag$.
- Das Ausgabeformat *%hd* passt genau zu dem verwendeten Datentyp **short**.

Verschachtelte Verbundtypen

- Die Elemente eines Verbundtyps können (beinahe) beliebigen Typs sein. Insbesondere ist es auch möglich, Verbundtypen ineinander zu verschachteln:

```
struct person {
   char* name;
   char* vorname;
   struct datum geburtsdatum;
};
```

- Wenn dann eine Variable *p* als **struct** *person p* vereinbart ist, dann kann wie folgt auf die Elemente zugegriffen werden:

```
p.name = ...;
p.vorname = ...;
p.geburtsdatum.tag = ...;
p.geburtsdatum.monat = ...;
p.geburtsdatum.jahr = ....;
```

Rekursive Verbundtypen

struct.c

```
struct s {
   /* ... */
   struct s* p; /* Zeiger auf die eigene Struktur ist ok */
   /* struct s elem; */ /* nicht erlaubt! */
};

struct s1 {
   /* ... */
   struct s2* p;        /* Zeiger als Vorwaertsverweis ist ok */
   /* struct s2 elem;*/ /* nicht erlaubt! */
};

struct s2 {
   /* ... */
   struct s1* p;        /* Zeiger als Rueckwaertsverweis ok */
   struct s1 elem;      /* ok */
};
```

- Zeiger auf Verbundtypen können bereits verwendet werden, auch wenn die zugehörigen Strukturen noch nicht (bzw. nicht vollständig) deklariert sind.

Zuweisung von Verbundtypen

struct1.c

```
#include <stdio.h>

struct datum {
   short tag, monat, jahr;
};

int main() {
   struct datum vorl_beginn = {18, 10, 2011};
   struct datum ueb_beginn = {20, 10, 2011};

   printf("vorher: %hd.%hd.%hd\n",
      vorl_beginn.tag, vorl_beginn.monat, vorl_beginn.jahr);

   vorl_beginn = ueb_beginn;

   printf("nachher: %hd.%hd.%hd\n",
      vorl_beginn.tag, vorl_beginn.monat, vorl_beginn.jahr);
}
```

- Variablen des gleichen Verbundtyps können einander auch zugewiesen werden.
- Dabei werden die einzelnen *Elemente* der Struktur jeweils *kopiert*.

Verbundtypen als Funktionsargumente

struct2.c

```
/* Werteparameter-Semantik */
void ausgabe1(struct datum d) {
   printf("%hd.%hd.%hd\n", d.tag, d.monat, d.jahr);
}

/* Referenzparameter-Semantik (wirkt sich hier nicht aus) */
void ausgabe2(struct datum* d) {
   printf("%hd.%hd.%hd\n", d->tag, d->monat, d->jahr);
}
```

- Verbunde können als Werteparameter übergeben werden oder – durch die Verwendung von Zeigern – auch als Referenz-Parameter verwendet werden.

Verbundtypen als Funktionsargumente

struct2.c

```
/* Werteparameter-Semantik: Verbund des Aufrufers aendert sich nicht */
void setJahr1(struct datum d, int jahr) {
   d.jahr = jahr;
}

/* Referenzparameter-Semantik erlaubt die Aenderung */
void setJahr2(struct datum* d, int jahr) {
   d->jahr = jahr;
}

int main() {
   struct datum start = {18, 10, 2011};

   ausgabe1(start);
   setJahr1(start, 2012);     /* keine Aenderung! */
   ausgabe2(&start);          /* aequivalent zu ausgabe1(...) */
   setJahr2(&start, 2012);    /* setzt das Jahr auf 2012 */
   ausgabe1(start);
}
```

Verbunde als Ergebnis von Funktionen

- Funktionen können als Ergebnistyp auch einen Verbundtyp verwenden.
- Hingegen ist Vorsicht angebracht, wenn Zeiger auf Verbunde zurückgegeben werden:

struct3.c

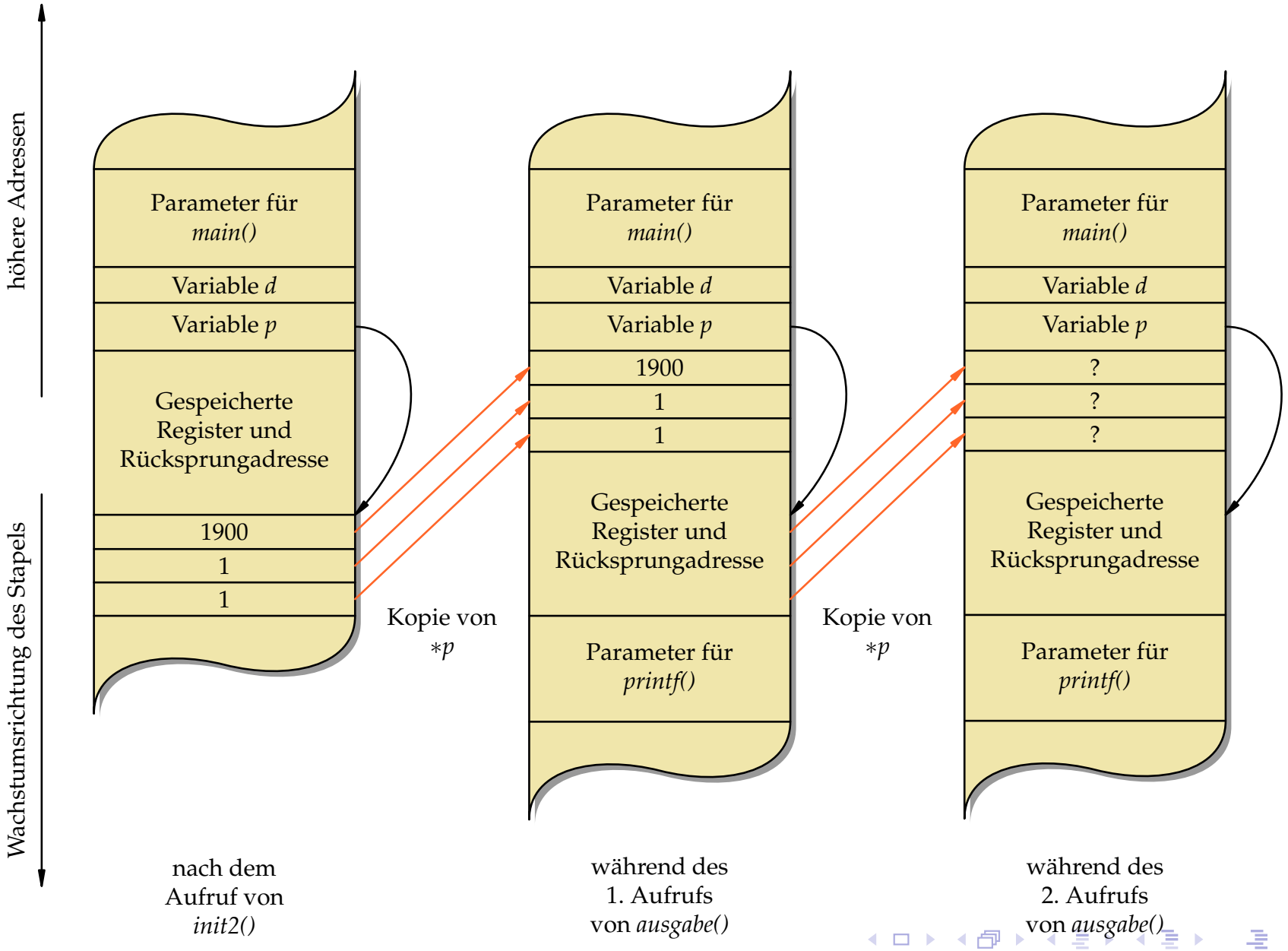
```
struct datum init1() {
   struct datum d = {1, 1, 1900};
   return d;   /* ok, denn es wird eine Kopie erzeugt */
}

struct datum* init2() {
   struct datum d = {1, 1, 1900};
   return &d;  /* nicht zulaessig, da Zeiger auf lokale Variable! */
}
```

Verbunde als Ergebnis von Funktionen

struct3.c

```
#include <stdio.h>

struct datum {
   short tag, monat, jahr;
};

void ausgabe(struct datum d) {
   printf("%hd.%hd.%hd\n", d.tag, d.monat, d.jahr);
}

/* init1() & init2() */

int main() {
   struct datum d;
   struct datum* p;

   d = init1();
   ausgabe(d);

   p = init2(); /* Zeiger auf Variable, die nicht mehr existiert! */
   ausgabe(*p); /* wenn's klappt ... dann ist das Glueck! */
   ausgabe(*p); /* sollte eigentliche dasselbe ausgeben :-( */
}
```

Funktionsaufrufe und lokale Variablen



Funktionsaufrufe und lokale Variablen

- Die Variable *d* in der Funktion *init2()* ist eine lokale Variable, die auf dem Laufzeit-Stapel für Funktionen (im Englischen *runtime stack* genannt) lebt.
- Sie existiert nur solange diese Funktion ausgeführt wird. Danach wird dieser Speicherplatz evtl. anderweitig verwendet.
- Nach dem Aufruf von *init2()* ist zwar die Lebenszeit der Daten hinter *p* zwar vorbei, aber sie liegen typischerweise immer noch intakt auf dem Laufzeit-Stapel.
- Entsprechend werden beim ersten Aufruf von *ausgabe()* die Daten noch korrekt kopiert.
- Allerdings werden die von *p* referenzierten Daten dann während des ersten Aufrufs von *ausgabe()* überschrieben. Deswegen werden beim folgenden zweiten Aufruf von *ausgabe()* vollkommen undefinierte Werte bei der Parameterübergabe kopiert.

Variante Verbünde

$$
\begin{array}{lcl}
\langle\text{union-type-specifier}\rangle & \longrightarrow & \textbf{union}\ [\ \langle\text{identifier}\rangle\ ]\ \text{„}\{\text{“} \\
 & & \langle\text{struct-declaration-list}\rangle\ \text{„}\}\text{“} \\
 & \longrightarrow & \textbf{union}\ \langle\text{identifier}\rangle
\end{array}
$$

- Syntaktisch gleichen variante Verbünde den regulären Verbünden – es wird nur das Schlüsselwort **union** an Stelle von **struct** verwendet.
- Im Vergleich zu den regulären Verbünden liegen alle Komponenten eines varianten Verbunds an der gleichen Position im Speicher.

Wozu variante Verbünde?

Es gibt zwei Gründe, die für die Verwendung eines varianten Verbunds sprechen können:

- Variante Verbünde sparen Speicherplatz ein, wenn immer nur eine Variante benötigt wird. In diesem Falle muss (außerhalb des varianten Verbunds) ein Status verwaltet werden, der mitteilt, welche Variante gerade in Benutzung ist.
- Durch variante Verbünde sind zwei (oder mehr) Sichten durch verschiedene Datentypen auf ein gemeinsames Stück Speicher möglich, ohne dass hierfür jeweils umständliche Konvertierungen notwendig wären. Allerdings ist hier Vorsicht geboten, da dies sehr von der jeweiligen Plattform abhängen kann.

Beispiel eines varianten Verbunds

union.c

```
union IPAddr {
   unsigned int ip;
   unsigned char b[4];
};
```

- Alle Komponenten eines Verbunds liegen an der gleichen Speicheradresse.
- Der Speicherbedarf der größten Komponente bestimmt den Speicherbedarf für den gesamten varianten Verbund.
- In diesem Beispiel sind *ip* und *b* zwei Sichten auf das gleiche Stück Speicher: Einerseits kann eine IP-Adresse als ganze Zahl betrachtet werden, andererseits aber auch als Sequenz von vier Bytes.
- Der Unterschied zwischen *big* und *little endian* ist hier wieder relevant.

Beispiel eines varianten Verbunds

union.c

```
int main() {
   union IPAddr a;

   a.ip = 0x863c4205;  /* bel. IP-Adresse in int-Darst. zuweisen */
   /* Zugriff auf a ueber die Komponente ip */
   printf("%u [%x]\n", a.ip, a.ip);
   /* Zugriff auf a ueber die Komponente b */
   printf("%hhu.%hhu.%hhu.%hhu ", a.b[0], a.b[1], a.b[2], a.b[3]);
   printf("[%02hhx.%02hhx.%02hhx.%02hhx]\n",
      a.b[0], a.b[1], a.b[2], a.b[3]);
   puts("");
   printf("Speicherplatzbedarf: %zd\n", sizeof(a));

   puts("");   /* Anordung im Speicher analysieren */
   puts("Position im Speicher:");
   printf("a:    %p\n", &a);
   printf("ip:   %p\n", &a.ip);
   printf("b[0]: %p\n", &a.b[0]);
   printf("b[1]: %p\n", &a.b[1]);
   printf("b[2]: %p\n", &a.b[2]);
   printf("b[3]: %p\n", &a.b[3]);
}
```

Beispiel eines varianten Verbunds

```
doolin$ uname -m
sun4u
doolin$ gcc -Wall -std=c99 union.c
doolin$ a.out
2252096005 [863c4205]
134.60.66.5 [86.3c.42.05]

Speicherplatzbedarf: 4

Position im Speicher:
a:    ffbff464
ip:   ffbff464
b[0]: ffbff464
b[1]: ffbff465
b[2]: ffbff466
b[3]: ffbff467
doolin$
```

- Ausführung auf einer *big endian*-Maschine.

Beispiel eines varianten Verbunds

```
zeus$ uname -m
x86_64
zeus$ gcc -Wall -std=c99 union.c
zeus$ a.out
2252096005 [863c4205]
5.66.60.134 [05.42.3c.86]

Speicherplatzbedarf: 4

Position im Speicher:
a:    0x7fff0034a430
ip:   0x7fff0034a430
b[0]: 0x7fff0034a430
b[1]: 0x7fff0034a431
b[2]: 0x7fff0034a432
b[3]: 0x7fff0034a433
zeus$
```

- Ausführung auf einer *little endian*-Maschine.

Typdefinitionen

$$
\begin{aligned}
\langle\text{typedef-name}\rangle &\longrightarrow \langle\text{identifier}\rangle \\
\langle\text{storage-class-specifier}\rangle &\longrightarrow \textbf{typedef} \\
&\longrightarrow \textbf{extern} \\
&\longrightarrow \textbf{static} \\
&\longrightarrow \textbf{auto} \\
&\longrightarrow \textbf{register}
\end{aligned}
$$

- Einer Deklaration kann das Schlüsselwort **typedef** vorausgehen. Dann wird der Name, der sonst ein Variablenname geworden wäre, stattdessen zu einem neu definierten Typnamen. Dieser Typname kann anschließend überall dort verwendet werden, wo die Angabe eines ⟨type-specifier⟩ zulässig ist.

Ein einfaches Beispiel einer Typdefinition

```
typedef int Laenge; /* Vereinbarung des eigenen Typnames "Laenge" */

/* ... */

Laenge i, j; /* Vereinbarung der Variablen i und j vom Typ Laenge */
```

- Hier ist *Laenge* zu einem Synonym für **int** geworden.
- Damit sind **int** *i*, *j*; und *Laenge i*, *j*; äquivalente Vereinbarungen.
- Hier bieten Typdefinitionen die Flexibilität, einen Typ an einer zentralen Stelle zu vereinbaren, um ihn dann bequem für das gesamte Programm verändern zu können.
- Das ist insbesondere sinnvoll bei der Verwendung numerischer Datentypen. Synonyme können auch zur Lesbarkeit beitragen, wenn besonders „sprechende“ Namen verwendet werden.

Typdefinitionen dienen der Vereinfachung

```
typedef char* CharPointer;
typedef int TenIntegers[10];
CharPointer cp1, cp2; // beide sind vom Typ char*
char* cp3, cp4; // cp4 hat nur den Typ char!
TenIntegers a, b; // beides sind Vektoren
int c[10], d; // d hat nur den Typ int!
```

- Typdefinitionen ermöglichen es, komplexere Typen in einen ⟨type-specifier⟩ zu integrieren, die sich sonst nur im Rahmen einer ⟨declaration⟩ formulieren liessen.
- Das betrifft insbesondere Zeiger und Vektoren.

Typdefinition für Verbünde

```
typedef struct datum {
   short tag, monat, jahr;
} datum;
datum geburtsdatum; // aequivalent zu struct datum geburtsdatum
datum heute, morgen;
```

- Bei Verbünden werden ebenfalls Typdefinitionen verwendet, um anschließend nur den Namen ohne das Schlüsselwort **struct** verwenden zu können.
- Die Verwendung von Typnamen aus Typdefinitionen bleibt – abgesehen von den syntaktischen Unterschieden – äquivalent zur Verwendung des ursprünglichen Datentyps. Entsprechend entsteht durch eine Typdefinition kein neuer Typ, der nicht mehr mit dem alten Typ kompatibel wäre.

Komplexe Deklarationen

- Durch die unglückliche Aufteilung von Typ-Spezifikationen in ⟨type-specifier⟩ (links stehend) und ⟨declarator⟩ (rechts stehend, sich um den Namen anordnend), werden komplexere Deklarationen rasch unübersichtlich.
- Die Motivation für diese Syntax kam wohl aus dem Wunsch, dass die Deklaration einer Variablen ihrer Verwendung gleichen solle.
- Entsprechend hilft es, sich bei komplexeren Deklarationen die Vorränge und Assoziativitäten der zugehörigen Operatoren in Erinnerung zu rufen.

Beispiel für die Analyse einer Deklaration

```
char* x[10];
```

- Der Vorrangtabelle lässt sich entnehmen, dass der []-Operator einen höheren Vorrang (16) im Vergleich zum $*$-Operator (15) hat.
- Entsprechend handelt es sich bei x um einen Vektor mit 10 Elementen des Typs Zeiger auf **char**.
- Im Einzelnen:

$x[10]$	Vektor mit 10 Elementen
$*\ x[10]$	Vektor mit 10 Zeigern
char$*\ x[10]$	Vektor mit 10 Zeigern auf Zeichen

Zweites Beispiel für die Analyse einer Deklaration

```
int* (*(*x)())[5];
```

- Die Analyse beginnt hier wieder beim Variablennamen x in der Mitte der Deklaration:

$*x$	ein Zeiger
$(*x)()$	ein Zeiger auf eine Funktion
$*(*x)()$	ein Zeiger auf eine Funktion, die einen Zeiger liefert
$(*(*x)())[5]$	ein Zeiger auf eine Funktion, die einen Zeiger auf einen 5-elementigen Vektor liefert
$*\ (*(*x)())[5]$	ein Zeiger auf eine Funktion, die einen Zeiger auf einen 5-elementigen Vektor aus Zeigern liefert
int$*\ (*(*x)())[5]$	ein Zeiger auf eine Funktion, die einen Zeiger auf einen 5-elementigen Vektor aus Zeigern auf **int** liefert

Zweites Beispiel für die Analyse einer Deklaration

```
int* (*(*x)())[5];
```

- An zwei Stellen waren hier Vorränge relevant: Im zweiten Schritt war wesentlich, dass Funktionsaufrufe (Vorrangstufe 16) Vorrang haben vor der Dereferenzierung (Vorrangstufe 15) und im vierten Schritt hatte die Indizierung (Vorrangstufe 16) ebenfalls Vorrang vor der Dereferenzierung.
- Zusammenfassend:
  - [] und () haben einen höheren Rang als $*$.
  - [] und () assoziieren von *links nach rechts*, während $*$ von *rechts nach links* gruppiert.

Abhilfe mit Typdefinitionen

```
int* (*(*x)())[5];
```

- Lesbarer wird dies durch einen stufenweisen Aufbau mit Typdefinitionen:

```
typedef int* intp; // intp = Zeiger auf int
typedef intp intpa[5]; // intpa = Vektor mit 5 Zeigern auf int
typedef intpa f(); // f = Funktion, die intpa liefert
typedef f* fp; // Zeiger auf eine Funktion
fp x;
```

Verwendung von Klammern by Typdeklarationen

```
int (*x[10])();
```

- Klammern können verwendet werden, um die Operatoren anders zu gruppieren und damit den Typ entsprechend zu verändern.
- Hier ist x ein 10-elementiger Vektor von Zeigern auf Funktionen mit Rückgabewerten des Typs **int**. Im Einzelnen:

$x[10]$	x als 10-elementiger Vektor
$(*x[10])$	x als 10-elementiger Vektor von Zeigern
$(*x[10])()$	x als 10-elementiger Vektor von Zeigern auf Funktionen
int $(*x[10])()$	x als 10-elementiger Vektor von Zeigern auf Funktionen, mit Rückgabewerten des Typs **int**.

Beispiele für unzulässige Typdeklarationen

int *af*[]()	Vektor von Funktionen, die Rückgabewerte des Typs **int** liefern
int *fa*()[]	Funktion, die einen Vektor von ganzen Zahlen liefert; hier wäre **int**∗ *fa*() akzeptabel gewesen
int *ff*()()	Funktion, die eine Funktion liefert, welche wiederum **int** liefert

Betriebssysteme

Die *DIN-Norm 44300* definiert ein Betriebssystem wie folgt:

> *Zum Betriebssystem zählen die Programme eines digitalen Rechensystems, die zusammen mit den Eigenschaften der Rechenanlage die Basis der möglichen Betriebsarten des digitalen Rechensystems bilden und die insbesondere die Abwicklung von Programmen steuern und überwachen.*

Start des Betriebssystems

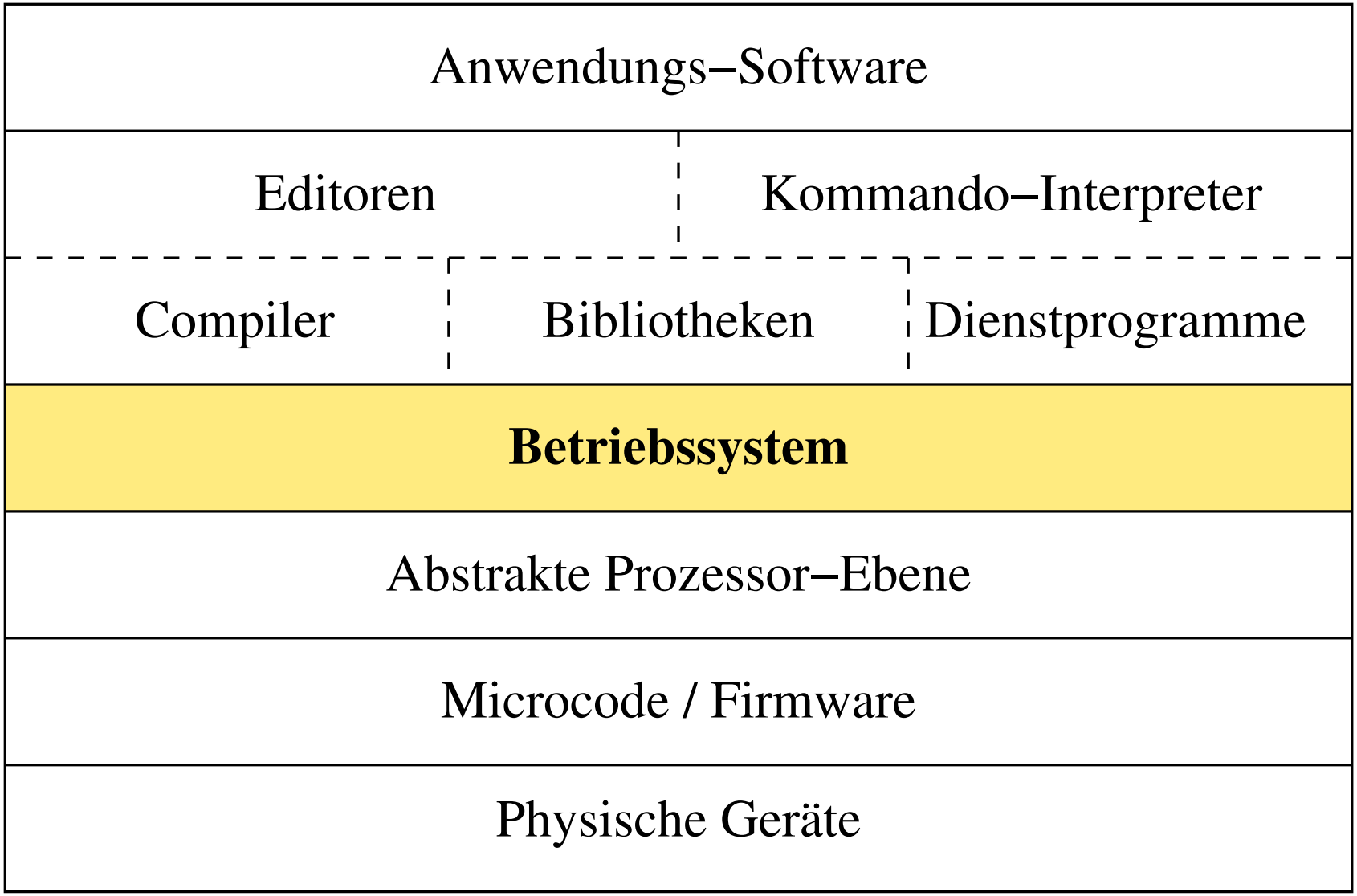
- Das Betriebssystem ist (abgesehen von der Firmware und einigen Zwischenstufen) das erste Programm, das von einem Rechner beim Hochfahren geladen wird.
- Das Betriebsystem läuft die gesamte Zeit, bis der Rechner wieder heruntergefahren wird.

Aufgaben des Betriebssystems

Das Betriebssystem hat zwei zentrale *Aufgaben*:

- **Ressourcen-Management:** Das Betriebssystem verwaltet und kontrolliert alle Hardware- und Software-Komponenten eines Rechners und teilt sie möglichst fair und effizient den einzelnen Nachfragern zu.
- **Erweiterte oder virtuelle Maschine:** Das Betriebssystem besteht aus einer (oder mehreren) Software-Schichten, die über der „nackten“ Hardware liegen. Diese erweiterte Maschine ist einfacher zu verstehen und zu programmieren, da sich komplizierte Zugriffe und Abhängigkeiten hinter einer einfacheren und einheitlichen Schnittstelle verbergen – den Systemaufrufen.

Schichtenmodell



Schichtenmodell

- **Physische Geräte:**
  Prozessor, Festplatten, Grafikkarte, Stromversorgung, etc.
- **Microcode / Firmware:**
  Software, die die physikalischen Geräte direkt kontrolliert und sich teilweise direkt auf den Geräten befindet. Diese bietet der nächsten Schicht eine einheitlichere Schnittstelle zu den physikalischen Geräten. Dabei werden einige Details der direkten Gerätesteuerung verborgen.

  Beispiel: Abbildung logischer Adressen auf physische Adressen bei Festplatten.
- **Abstrakte Prozessor-Ebene:**
  Schnittstelle zwischen Hard- und Software. Hierzu gehören nicht nur alle Instruktionen des Prozessors, sondern auch die Kommunikationsmöglichkeiten mit den Geräten und die Behandlung von Unterbrechungen.

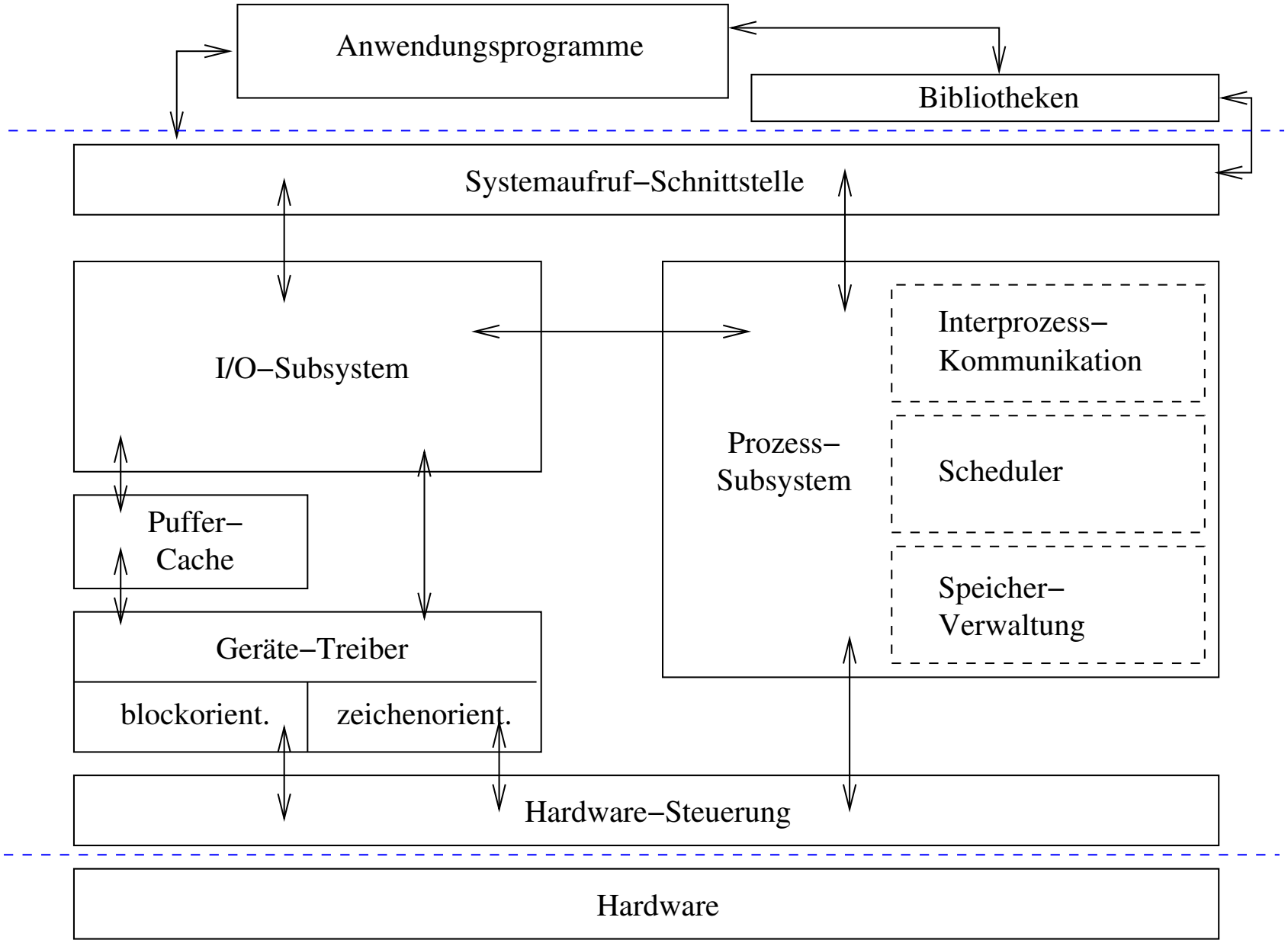
Schichtenmodell

- **System-Software:**
  Software, die von der Schnittstelle des Betriebssystems abhängt und typischerweise vom Hersteller des Betriebssystems mit ausgeliefert wird.

  Beispiele: Bibliotheken (libc.a), Kommandozeilen-Interpreter (Shells), graphische Benutzeroberflächen (X-Windows), systemnahe Werkzeuge, Netzwerkdienste (Web-Server)

- **Anwendungen:**
  Von Benutzern bzw. für Benutzer zur Lösung ihrer Probleme entwickelte Programme *Beispiel:* Textverarbeitungsprogramm

Interner Aufbau von Unix

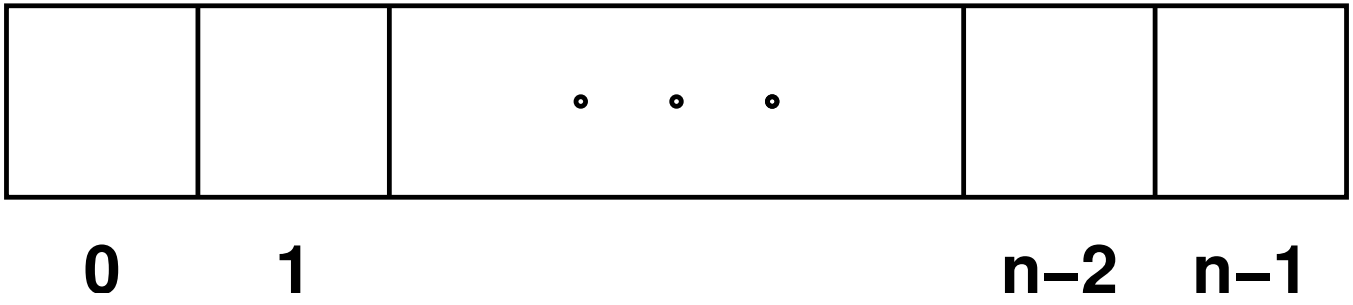


Definition einer Datei

Aus IEEE Std 1003.1 (POSIX):

> *An object that can be written to, or read from, or both. A file has certain attributes, including access permissions and type. File types include regular file, character special file, block special file, FIFO special file, symbolic link, socket, and directory. Other types of files may be supported by the implementation.*

Modell einer gewöhnlichen Datei



- Eine gewöhnliche Datei entspricht einem Array aus Bytes.
- Wenn eine Datei eine Länge von n Bytes hat, sind diese über die Positionen 0 bis $n - 1$ abrufbar.
- Eine Dateiverbindung hat eine aktuelle Position p.
- Wenn ein Byte über eine Verbindung gelesen oder geschrieben wird, dann erfolgt der Zugriff auf der aktuellen Position p, die anschließend, falls die Operation erfolgreich war, um eins erhöht wird.
- Lese-Operationen bei einer Position von n sind nicht erfolgreich.

Struktur einer Datei

- Unix verlangt und unterstellt bei regulären Dateien *keinerlei Struktur* und unterstützt auch keine.
- Die Konzepte variabel oder konstant langer Datensätze (Records) sind im Kernel von UNIX nicht implementiert.
- Entsprechend sind gewöhnliche Dateien ganz schlichte Byte-Arrays.
- Die einzige Besonderheit ist, dass Dateien unter Unix „Löcher“ haben dürfen, d.h. einzelne Indexbereiche des Arrays können unbelegt sein. Diese werden dann als Nullbytes ausgelesen.

Verwaltungsinformationen einer Datei

Zu einer Datei gehören

- ein oder auch mehrere *Namen*,
- der *Inhalt* und *Aufbewahrungsort* (Menge von Blöcken auf der Platte, etc.) und
- *Verwaltungsinformationen* (Besitzer, erlaubter Zugriff, Zeitstempel, Länge, Dateityp, etc.).

Spezielle Dateien

- Neben den gewöhnlichen Dateien gibt es unter Unix weitere Dateiformen.
- Neben den Verzeichnissen gibt es insbesondere Dateivarianten, die der Interprozess-Kommunikation oder direkten Schnittstelle zu Treibern des Betriebssystems dienen.
- Diese weichen in der Semantik von dem Byte-Array ab und bieten beispielsweise uni- oder bidirektionale Kommunikationskanäle.

Gerätedateien

- Gerätedateien erlauben die direkte Kommunikation mit einem (das jeweilige Gerät repräsentierenden) Treiber.
- Sie erlauben beispielsweise den direkten Zugriff auf eine Festplatte vorbei an dem Dateisystem.
- Für Gerätedateien gibt es zwei verschiedene Schnittstellen:
  - **Zeichenweise arbeitende Geräte** (*character devices / raw devices*):
    Diese Dateien erlauben einen ungepufferten zeichenweisen Lese- und/oder Schreibzugriff.
  - **Blockweise arbeitende Geräte** (*block devices*):
    Diese Dateien erlauben Lese- und Schreibzugriffe nur für vollständige Blöcke. Diese Zugriffe laufen implizit über den Puffer-Cache von Unix.

Zugriffe auf eine Platte

Auf eine Festplatte kann typischerweise auf drei verschiedene Weisen zugegriffen werden:

- Über ein Dateisystem.
- Über die zugehörige blockweise arbeitende Gerätedatei indirekt über den Puffer-Cache.
- Über die zugehörige zeichenweise arbeitende Gerätedatei.

Intern im Betriebsystem liegt die gleiche Schichtenstruktur der Schnittstellen vor: Zugriffe auf ein Dateisystem werden abgebildet auf Zugriffe auf einzelne Blöcke innerhalb des Puffer-Cache. Wenn der gewünschte Block zum Lesen nicht vorliegt oder ein verändeter Block im Cache zu schreiben ist, dann wird der zugehörige Treiber direkt kontaktiert.

Arten von Dateisystemen

Prinzipiell lassen sich Dateisysteme in vier Gruppen unterteilen:

- *Plattenbasierte Dateisysteme:*
  Die Daten des Dateisystems liegen auf einer lokalen Platte.
- *Netzwerk-Dateisystem:*
  Das Dateisystem wird von einem anderen Rechner über das Netzwerk angeboten. Beispiele: NFS, AFS und Samba.
- *Meta-Dateisysteme:*
  Das Dateisystem ist eine Abbildungsvorschrift eines oder mehrerer anderer Dateisysteme. Beispiele: *tfs* und *unionfs*.
- *Pseudo-Dateisystem:*
  Das Dateisystem ist nicht mit persistenten Daten verbunden. Beispiel: Das *procfs* unter */proc*, das die einzelnen aktuell laufenden Prozesse repräsentiert.

Plattenbasierte Dateisysteme

- Gegeben ist die abstrakte Schnittstelle eines Arrays von Blöcken. (Dies kann eine vollständige Platte sein, eine Partition davon oder eine virtuelle Platte, wie sie etwa bei diversen RAID-Verfahren entsteht.)
- Zu den Aufgaben eines plattenbasierten Dateisystems gehört es, ein Array von Blöcken so zu verwalten, dass
  - über ein hierarchisches Namenssystem
  - Dateien (bis zu irgendeinem Maxium) frei wählbarer Länge
  - gespeichert und gelesen werden können.

Integrität eines Dateisystems

Aus dem Werk von Marc J. Rochkind, Seite 29, zum Umgang mit einer Schreib-Operation:

> *I've taken note of your request, and rest assured that your file descriptor is OK,*
>
> *I've copied your data successfully, and there's enough disk space. Later, when it's convenient for me, and if I'm still alive, I'll put your data on the disk where it belongs.*
>
> *If I discover an error then I'll try to print something on the console, but I won't tell you about it (indeed, you may have terminated by then).*
>
> *If you, or any other process, tries to read this data before I've written it out, I'll give it to you from the buffer cache, so, if all goes well, you'll never be able to find out when and if I've completed your request.*
>
> *You may ask no further questions. Trust me. And thank me for the speedy reply.*

Integrität eines Dateisystems

Was passiert, wenn dann mittendrin der Strom ausfällt?

- Blöcke einer Datei oder gar ein Verwaltungsblock sind nur teilweise beschrieben.
- Verwaltungsinformationen stimmen nicht mit den Dateiinhalten überein.

(Wieder-)herstellung der Integrität

Im Laufe der Zeit gab es mehrere Entwicklungsstufen bei Dateisystemen in Bezug auf die Integrität:

- Im Falle eines Falles muss die Integrität mit speziellen Werkzeugen überprüft bzw. hergestellt werden. Beispiele: Alte Unix-Dateisysteme wie UFS (alt), ext2 oder aus der Windows-Welt die Familie der FAT-Dateisysteme.
- Ein Journalling erlaubt normalerweise die Rückkehr zu einem konsistenten Zustand. Beispiele: Neuere Versionen von UFS, ext3 und reiser3.
- Das Dateisystem ist immer im konsistenten Zustand und arbeitet entsprechend mit Transaktionen analog wie Datenbanken. Hinzu kommen Überprüfungssummen und Selbstheilungsmechanismen (bei redundanten RAID-Verfahren). Beispiele: ZFS, btrfs, ext4, reiser4 und NTFS.

Organisation moderner Dateisysteme

Moderne Dateisysteme wie ZFS und btrfs werden als B-Bäume organisiert:

- B-Bäume sind sortierte und balancierte Mehrwege-Bäume, bei denen Knoten so dimensioniert werden, dass sie in einen physischen Block auf der Platte passen. (Wobei es Verfahren gibt, die mit dynamischen Blockgrößen arbeiten.)
- Entsprechend besteht jeder Block aus einer Folge aus Schlüsseln, Zeigern auf zugehörige Inhalte und Zeiger auf untergeordnete Teilbäume.
- Es werden nie bestehende Blöcke verändert. Stattdessen werden sie zunächst kopiert, angepasst, geschrieben und danach der neue statt dem alten Block verwendet (*copy on write*).
- Alte Versionen können so auch bei Bedarf problemlos erhalten bleiben (*snapshots*).

Hierarchie der Dateisysteme

- Jedes Dateisystem enthält eine Hierarchie der Verzeichnisse.
- Darüber hinaus gibt es auch eine Hierarchie der Dateisysteme.
- Es beginnt mit der Wurzel / und dem die Wurzel repräsentierenden Wurzel-Dateisystem. (Dies ist das erste Dateisystem, das verwendet wird und das auch das Betriebssystem oder zumindest wesentliche Teile davon enthält.)
- Weitere Dateisysteme können bei einem bereits existierenden Verzeichnis eingehängt werden.
- So entsteht eine globale Hierarchie, die sich über mehrere Dateisysteme erstreckt.

Hierarchie der Dateisysteme

```
doolin$ cd /
doolin$ df .
Filesystem            kbytes    used   avail capacity  Mounted on
/dev/dsk/c0t0d0s0    8263277 3705376 4475269    46%    /
doolin$ cd /var
doolin$ df .
Filesystem            kbytes    used   avail capacity  Mounted on
/dev/dsk/c0t0d0s7    8263277 2002000 6178645    25%    /var
doolin$
doolin$ cd /
doolin$ df -h .
Filesystem             size   used  avail capacity  Mounted on
/dev/dsk/c0t0d0s0      7.9G   3.5G   4.3G    46%    /
doolin$ cd var
doolin$ df -h .
Filesystem             size   used  avail capacity  Mounted on
/dev/dsk/c0t0d0s7      7.9G   1.9G   5.9G    25%    /var
doolin$ cd run
doolin$ df -h .
Filesystem             size   used  avail capacity  Mounted on
swap                   1.6G    48K   1.6G     1%    /var/run
doolin$
```

Historischer Aufbau eines Unix-Dateisystems

Boot–block	Super–block	Inode–Liste	Datenblöcke

- In den 70er Jahren (bis einschließlich UNIX Edition VII) hatte ein Unix-Dateisystem einen sehr einfachen Aufbau, bestehend aus
  - dem Boot-Block (reserviert für den Boot-Vorgang oder ohne Verwendung),
  - dem Super-Block (mit Verwaltungsinformationen für die gesamte Platte),
  - einem festdimensionierten Array von Inodes (Verwaltungsinformationen für einzelne Dateien) und
  - einem Array von Blöcken, die entweder für Dateiinhalte oder (im Falle sehr großer Dateien) für Verweise auf weitere Blöcke einer Datei verwendet werden.

Das UFS-Dateisystem

- Das heutige UFS (*UNIX file system*) geht zurück auf das von Marshall Kirk McKusick, William N. Joy, Samuel J. Leffler und Robert S. Fabry Anfang der 80er Jahre entwickelte Berkeley Fast File System.
- Gegenüber dem historischen Aufbau enthält es einige wesentliche Veränderungen:
  - Die Verwaltungsinformationen einer Datei und der Dateiinhalt werden so auf der Platte abgelegt, dass sie möglichst schnell hintereinander gelesen werden können.
  - Dazu wird die Platte entsprechend ihrer Geometrie in Zylindergruppen aufgeteilt. Zusammenhängende Inodes und Datenblöcke liegen dann möglichst in der gleichen oder der benachbarten Zylindergruppe.
  - Die Blockgröße wurde vergrößert (von 1k auf 8k) und gleichzeitig wurden für kleine Dateien fragmentierte Blöcke eingeführt.
  - Damit der Verlust des Super-Blocks nicht katastrophal ist, gibt es zahlreiche Sicherungskopien des Super-Blocks an Orten, die sich durch die Geometrie ableiten lassen.
- Das unter Linux lange Zeit populäre ext2-Dateisystem hatte UFS als Vorbild.

Inode

- Eine Inode enthält sämtliche Verwaltungsinformationen, die zu einer Datei gehören.
- Jede Inode ist (innerhalb eines Dateisystems) eindeutig über die Inode-Nummer identifizierbar.
- Die Namen einer Datei sind *nicht* Bestandteil der Inode. Stattdessen bilden Verzeichnisse Namen in Inode-Nummern ab.
- U.a. finden sich folgende Informationen in einer Inode:
  - Eigentümer und Gruppe
  - Dateityp (etwa gewöhnliche Datei oder Verzeichnis oder einer der speziellen Dateien)
  - Zeitstempel: Letzter Lesezugriff, letzter Schreibzugriff und letzte Änderung der Inode.
  - Anzahl der Verweise aus Verzeichnissen
  - Länge der Datei in Bytes (bei gewöhnlichen Dateien und Verzeichnissen)
  - Blockadressen (bei gewöhnlichen Dateien und Verzeichnissen)

Auslesen eines Verzeichnisses

- In der Unix-Welt gibt es keine standardisierten Systemaufrufe, die ein Auslesen eines Verzeichnisses ermöglichen.
- Der Standard IEEE Std 1003.1 bietet jedoch die Funktionen *opendir*, *readdir* und *closedir* als portable Schnittstelle oberhalb der (nicht portablen) Systemaufrufe an.
- Alle anderen Funktionalitäten (Auslesen des öffentlichen Teils einer Inode, Wechseln des Verzeichnisses und sonstige Zugriffe auf Dateien) sind auch auf der Ebene der Systemaufrufe standardisiert.

Auslesen eines Verzeichnisses

dir.c

```
#include <dirent.h>
#include <stdio.h>
#include <stdlib.h>
#include <sys/stat.h>
#include <unistd.h>

int main(int argc, char* argv[]) {
   char* cmdname = *argv++; --argc;
   char usage[] = "Usage: %s [directory]\n";
   if (argc > 1) {
      fprintf(stderr, usage, cmdname);
      exit(1);
   }
   char* dirname;
   if (argc > 0) {
      dirname = *argv;
   } else {
      dirname = ".";
   }
   /**** Auslesen von dirname ****/
}
```

Auslesen eines Verzeichnisses

dir.c

```
if (chdir(dirname) < 0) {
   perror(dirname);
   exit(1);
}
DIR* dir = opendir(".");
if (!dir) {
   perror(dirname);
   exit(1);
}
```

- Mit *chdir()* ist es möglich, das aktuelle Verzeichnis zu wechseln. Dies betrifft den aufrufenden Prozess (und wird später an neu erzeugte Prozesse weiter vererbt).
- *chdir()* wird hier verwendet, um im weiteren Verlauf den Zusammenbau zusammengesetzter Pfade aus dem Verzeichnisnamen und dem darin enthaltenen Dateinamen zu vermeiden.
- Nach dem Aufruf von *chdir()* ist das gewünschte (dann aktuelle) Verzeichnis unter dem Namen . erreichbar.

Auslesen eines Verzeichnisses

dir.c

```
struct dirent* entry;
while ((entry = readdir(dir))) {
   printf("%s: ", entry->d_name);
   struct stat statbuf;
   if (lstat(entry->d_name, &statbuf) < 0) {
      perror(entry->d_name); exit(1);
   }
   if (S_ISREG(statbuf.st_mode)) {
      printf("regular file with %jd bytes\n",
         (intmax_t) statbuf.st_size);
   } else if (S_ISDIR(statbuf.st_mode)) {
      puts("directory");
   } else if (S_ISLNK(statbuf.st_mode)) {
      char buf[1024];
      ssize_t len = readlink(entry->d_name, buf, sizeof buf);
      if (len < 0) {
         perror(entry->d_name); exit(1);
      }
      printf("symbolic link pointing to %.*s\n", len, buf);
   } else {
      puts("special");
   }
}
closedir(dir);
```

Auslesen eines Verzeichnisses

dir.c

```
struct dirent* entry;
while ((entry = readdir(dir))) {
   printf("%s: ", entry->d_name);
```

- *readdir* liefert einen Zeiger auf eine (statische) Struktur mit Informationen über die nächste Datei aus dem Verzeichnis.
- Die Struktur mag mehrere systemabhängige Komponenten haben. Relevant und portabel ist jedoch nur der Dateiname in dem Feld *d_name*

Auslesen einer Inode

dir.c

```
struct stat statbuf;
if (lstat(entry->d_name, &statbuf) < 0) {
   perror(entry->d_name); exit(1);
}
```

- Es gibt mehrere Systemaufrufe, die den öffentlichen Teil einer Inode auslesen können.
- Dazu gehört *lstat*, das einen Dateinamen erhält und dann in dem per Zeiger referenzierten Struktur die gewünschten Informationen aus der Inode ablegt.
- Im Unterschied zu *stat*, das genauso aufgerufen wird, folgt *lstat* nicht implizit symbolischen Links, so dass wir hier die Chance haben, diese als solche zu erkennen.

Das Feld *st_mode*

dir.c

```
      if (S_ISREG(statbuf.st_mode)) {
         printf("regular file with %jd bytes\n",
            (intmax_t) statbuf.st_size);
```

- Das Feld *st_mode* aus der von *lstat()* gefüllten Datenstruktur enthält in kombinierter Form mehrere Informationen über eine Datei:
  - den Dateityp,
  - die Zugriffsrechte (rwx) für Besitzer, Gruppe und den Rest der Welt und
  - eventuelle weitere besondere Attribute wie etwa das Setuid-Bit oder das Sticky-Bit.
- Damit der Zugriff weniger kompliziert ist, gibt es standardisierte Makros im Umgang mit *st_mode*. So liefert etwa *S_ISREG* den Wert **true**, falls es sich um eine gewöhnliche Datei handelt.

Auslesen eines symbolischen Links

dir.c

```
      } else if (S_ISLNK(statbuf.st_mode)) {
         char buf[1024];
         ssize_t len = readlink(entry->d_name, buf, sizeof buf);
         if (len < 0) {
            perror(entry->d_name); exit(1);
         }
         printf("symbolic link pointing to %.*s\n", len, buf);
```

- Wäre *stat()* an Stelle von *lstat()* verwendet worden, würde dieser Fall nie erreicht werden, da normalerweise symbolische Links implizit gefolgt wird.
- Mit *readlink()* kann der Link selbst ausgelesen werden.
- Das Ziel eines symbolischen Links muss nicht notwendigerweise existieren. Falls das Ziel nicht existiert, liefert *stat()* einen Fehler, während *lstat()* uns unabhängig von der Existenz das Ziel nennt.

Identitäten

- Bei Systemaufrufen sind, soweit sie von Privilegien und/oder einem Zugriffsschutz abhängig sind, folgende u.a. folgende vier Identitäten von Belang:

effektive Benutzernummer	*geteuid()*
effektive Gruppennummer	*getegid()*
reale Benutzernummer	*getuid()*
reale Gruppennummer	*getgid()*

- Normalerweise gleichen sich die effektiven und realen Nummern. Im Falle von Programmen mit dem s-bit werden die effektiven Identitätsnummern von dem Besitzer des Programmes übernommen, während die realen Nummern gleichbleiben.
- In Bezug auf Zugriffe im Dateisystem sind die effektiven Nummern von Belang.

Zugriffsschutz bei Dateien

- Zu jeder Inode gehören die elementaren Zugriffsrechte die Lese-, Schreib- und Ausführungsrechte angeben für den Besitzer, die Gruppe und den Rest der Welt.
- Wenn die effektive Benutzernummer die 0 ist, dann ist alles erlaubt (Super-User-Privilegien).
- Falls die effektive Benutzernummer mit der der Datei übereinstimmt, dann sind die Zugriffsrechte für den Besitzer relevant.
- Falls nur die effektive Gruppennummer mit der Gruppenzugehörigkeit der Datei übereinstimmt, dann sind die Zugriffsrechte für die Gruppe relevant.
- Andernfalls gelten die Zugriffsrechte für den Rest der Welt.

Zugriffsschutz bei Verzeichnissen

- Lese-, Schreib- und Ausführungsrechte haben bei Verzeichnissen besondere Bedeutungen.
- Das Leserecht gibt die Möglichkeit, das Verzeichnis mit *opendir* und *readdir* anzusehen, aber noch *nicht* das Recht, *stat* für eine darin enthaltene Datei aufzurufen.
- Das Ausführungsrecht lässt die Verwendung des Verzeichnisses in einem Pfad zu, der an einem Systemaufruf weitergereicht wird.
- Das Schreibrecht gewährt die Möglichkeit, Dateien in dem Verzeichnis zu entfernen (*unlink*), umzutaufen (*rename*) oder neu anzulegen. Das Ausführungsrecht ist aber eine Voraussetzung dafür.

Weitere Bits in *st_mode*

- Zusätzlich gibt es noch drei weitere Bits:

  Set-UID-Bit Bei einer Ausführung wird die effektive Benutzernummer (UID) gesetzt auf die Benutzernummer des Besitzers.

  Set-GID-Bit Entsprechend wird auch die effektive Gruppennummer (GID) gesetzt. Bei Verzeichnissen bedeutet dies, dass neu angelegte Dateien die Gruppe des Verzeichnisses erben.

  Sticky-Bit Programme mit dem Sticky-Bit bleiben im Speicher. Verzeichnisse mit diesem Bit schränken die Schreibrechte für fremde Dateien ein – nützlich für gemeinsam genutzte Verzeichnisse wie etwa */tmp*.

Sichere Programmierung in C

- Systemnahe Software ist in vielen Fällen in Besitz von Privilegien und gleichzeitig im Kontakt mit potentiell gefährlichen Nutzern, denen diese Privilegien nicht zustehen.
- Daher muß bei der Entwicklung systemnaher Software nicht nur auf die korrekte Implementierung der gewünschten Funktionalitäten geachtet werden, sondern auch auf die umfassende Verhinderung nicht gewünschter Zugriffe.
- Dazu ist die Kenntnis der typischen Angriffstechniken notwendig und die konsequente Verwendung von Programmiertechniken, die diese zuverlässig abwehren.

Beispiel: Das Werkzeug *pubfile*

- Das Werkzeug *p*ubfile soll dazu dienen, Dateien im Verzeichnis `pub` unterhalb meines nicht-öffentlichen Heimatkataloges zur Verfügung zu stellen.
- So könnte *pubfile* übersetzt und in */tmp* öffentlich zur Verfügung gestellt werden:

```
cordelia$ id
uid=120(borchert) gid=200(sai)
cordelia$ gcc -Wall -o pubfile pubfile.c
cordelia$ cp pubfile /tmp
cordelia$ cat ~/pub/READ_ME
This is the READ_ME file within my pub directory.
cordelia$ /tmp/pubfile READ_ME
This is the READ_ME file within my pub directory.
cordelia$
```

Beispiel: Das Werkzeug *pubfile*

```
cordelia$ id
uid=6201(waborche) gid=230(student)
cordelia$ /tmp/pubfile READ_ME
/home/thales/borchert/pub/READ_ME: Permission denied
cordelia$ cat ~borchert/pub/READ_ME
cat: /home/thales/borchert/pub/READ_ME: Permission denied
cordelia$
```

- Im Normalfall bringt das Programm, selbst wenn es öffentlich installiert ist, noch keine besonderen Privilegien für andere Benutzer; d.h. obwohl das Programm dem Benutzer *borchert* gehört, operiert es nicht notwendigerweise mit den Privilegien von *borchert*.

Setzen des s-Bits für ein Programm

```
cordelia$ ls -l /tmp/pubfile
-rwxr-xr-x    1 borchert sai          7523 Feb 25 18:32 /tmp/pubfile
cordelia$ chmod u+s /tmp/pubfile
cordelia$ ls -l /tmp/pubfile
-rwsr-xr-x    1 borchert sai          7523 Feb 25 18:32 /tmp/pubfile
cordelia$
```

- Das läßt sich aber ändern, wenn der Eigentümer des Programmes dem Programm das s-bit spendiert. Dabei steht "s" für **setuid**. Konkret bedeutet dies, daß das Programm mit den Privilegien des Programmeigentümers operiert und nicht mit denen des Aufrufers.

Setzen des s-Bits für ein Programm

```
cordelia$ id
uid=6201(waborche) gid=230(student)
cordelia$ /tmp/pubfile READ_ME
This is the READ_ME file within my pub directory.
cordelia$
```

- Nun klappt es für andere Benutzer.

Sicherheitsproblematik

- Wir haben nun den Fall, daß das Programm Privilegien besitzt, die der Aufrufer normalerweise nicht hat.
- Natürlich sollte so ein Programm nicht all seine Privilegien (im Beispiel die Rechte von *borchert*) dem Aufrufer preisgeben.
- Stattdessen hatte der Autor von *pubfile* die Absicht, daß nur die Dateien aus dem Unterverzeichnis *pub* der Öffentlichkeit zur Verfügung stehen sollen. Wenn es möglich ist, auf andere Dateien zuzugreifen oder gar beliebige Privilegien des Programmeigentümers ausnutzen zu können, dann würden Sicherheitslücken vorliegen.

Die erste Lösung für *pubfile*

pubfile.c

```
/*
 * Display files within my pub directory.
 * Usage: pubfile {file}
 * WARNING: This program has several security flaws.
 * afb 2/2003
 */

#include <errno.h>
#include <fcntl.h>
#include <stdio.h>
#include <stdlib.h>
#include <strings.h>
#include <unistd.h>

const int BUFFER_SIZE = 8192;
const char* pubdir = "/home/thales/borchert/pub";

int main(int argc, char** argv) {
   *argv++; --argc; /* skip command name */
   while (argc-- > 0) {
      /* ... process *argv++ ... */
   }
}
```

Die erste Lösung für *pubfile*

pubfile.c

```
/* process *argv++ */
char pathname[BUFFER_SIZE];
char buffer[BUFFER_SIZE];
int fd;
int count;

strcpy(pathname, pubdir);
strcat(pathname, "/");
strcat(pathname, *argv++);

if ((fd = open(pathname, O_RDONLY)) < 0) {
   perror(pathname); exit(1);
}
while ((count = read(fd, buffer, sizeof buffer)) > 0) {
   if (write(1, buffer, count) != count) {
      perror("write to stdout"); exit(1);
   }
}
if (count < 0) {
   perror(pathname); exit(1);
}
close(fd);
```

Die erste Sicherheitslücke

```
cordelia$ id
uid=6201(waborche) gid=230(student)
cordelia$ /tmp/pubfile ../.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
[...]
-----END RSA PRIVATE KEY-----
cordelia$
```

- Unter Angabe eines relativen Pfadnamens können beliebige Dateien mit den Rechten des Benutzers *borchert* betrachtet werden.
- In diesem Beispiel wird der private RSA-Schlüssel ausgelesen, mit dessen Hilfe möglicherweise ein passwortloser Zugang auf andere Systeme mit den dortigen Privilegien von *borchert* eröffnet werden kann. Gelegentlich funktioniert das sogar auf dem gleichen System. Und hierfür genügte nur ein zu weitreichender Lesezugriff!

Die zweite Sicherheitslücke

pubfile.c

```
/* process *argv++ */
char pathname[BUFFER_SIZE];
/* ... */
strcpy(pathname, pubdir);
strcat(pathname, "/");
strcat(pathname, *argv++);
```

- Hier wird der lokale Puffer *pathname* gefüllt, ohne auf die Größe des Puffers zu achten.
- Zwar mag *BUFFER_SIZE* großzügig gewählt sein, aber ein Argument auf der Kommandozeile kann deutlich länger sein.
- Die Frage ist ganz einfach: Was kann passieren, wenn der Indexbereich verlassen wird? Die Sprachdefinition von C selbst gibt keine Antwort darauf, abgesehen davon, daß das Verhalten dann als "undefiniert" deklariert wird. Bei den gängigen Implementierungen mit einem rückwärts wachsenden Stack besteht die Möglichkeit, die Rücksprungadresse zu modifizieren und damit statt zum Aufrufer zu einem eingeschleusten Code springen zu lassen. Typischerweise kann der Code innerhalb des überlaufenden Puffers untergebracht werden.

Typische Schwachstellen bei C

In der Programmiersprache C hat es bereits erfolgreiche Einbrüche aufgrund folgender Programmierfehler gegeben:

- Unzureichende Überprüfung von Argumenten beim Eröffnen von Dateien, Ausführen von Kommandos oder anderen Systemaufrufen.
- Fehlende Einhaltung der Index-Grenzen eines Arrays. Gefahr besteht hier sowohl bei Arrays auf dem Stack als auch auf dem Heap (also per *malloc()* beschafft). Gefahr droht hier auch bei beliebten Funktionen der Bibliothek wie *strcpy*, *strcat*, *sprintf* und *gets*.
- Doppelte Freigabe eines Zeigers mit *free()*.
- Benutzung eines Zeigers, nachdem er bereits freigegeben worden ist.
- Weglassen des Formats bei *printf*. Statt *printf*(*s*) sollte besser *printf*("%s", *s*) verwendet werden.

Fehlervermeidung in C

- Leider ist die Vermeidung dieser Fehler nicht einfach.
- Selbst bei sicherheitsrelevanter Software wie der ssh (*secure shell*) oder der SSL-Bibliothek (*secure socket layer*) wurden immer wieder neue Fehler bei aufwendigen Untersuchungen des Programmtexts gefunden.
- Deswegen ist es bei C sinnvoll, bei systemnaher Software auf die Standard-Bibliotheken von C teilweise zu verzichten und stattdessen auf Alternativen auszuweichen, die die Verwendung sicherer Techniken unterstützen.

Dynamische Zeichenketten in C

- Die Unterstützung dynamischer Zeichenketten in C ist nicht sehr ausgeprägt.
- Zwar ist es leicht möglich, mit *malloc()* ein Array der gewünschten Länge zu erhalten, aber danach gibt es keine zuverlässige Längeninformation mehr.
- *strlen* ist nur sinnvoll im Falle wohldefinierter Zeichenketten, da es nach dem Nullbyte sucht.
- Entsprechend haben Standardfunktionen wie *strcpy* oder *sprintf* keine Möglichkeit zu überprüfen, ob genügend Platz für das Ergebnis vorhanden ist.
- Folglich muß die Abschätzung dem Programmierer im Vorfeld überlassen werden, die dann häufig unterlassen wird oder fehlerhaft ist.

Beispiel: Einlesen einer Zeile in eine Zeichenkette

readline.c

```
/*
 * Read a string of arbitrary length from a
 * given file pointer. LF is accepted as terminator.
 * 0 is returned in case of errors.
 * afb 3/2003
 */

#include <stdio.h>
#include <stdlib.h>

static const int INITIAL_LEN = 8;

char* readline(FILE* fp) {
   /* ... */
}
```

- Der Umgang mit Zeichenketten ist in C sehr umständlich, wenn die benötigte Länge nicht zu Beginn bekannt ist, wie dieses Beispiel demonstriert.

Beispiel: Einlesen einer Zeile in eine Zeichenkette

readline.c

```
size_t len = 0; /* current length of string */
size_t alloc_len = INITIAL_LEN; /* allocated length */
char* buf = malloc(alloc_len);
int ch;

if (buf == 0) return 0;
while ((ch = getc(fp)) != EOF && ch != '\n') {
   if (len + 1 >= alloc_len) {
      alloc_len *= 2;
      char* newbuf = realloc(buf, alloc_len);
      if (newbuf == 0) {
         free(buf);
         return 0;
      }
      buf = newbuf;
   }
   buf[len++] = ch;
}
buf[len++] = '\0';
return realloc(buf, len);
```

Anforderungen an eine Alternative

Ein Ausweg besteht in der Schaffung einer alternativen Bibliothek für dynamische Zeichenketten in C, die folgende Anforderungen erfüllen sollte:

- Neben der eigentlichen Zeichenkette muß auch eine Längenangabe vorliegen.
- Bibliotheksfunktionen analog zu *strcpy()* und *strcat()* müssen unterstützt werden. Diese Funktionen müssen entweder die Längenangabe einhalten oder automatisch die Zeichenketten in ihrer Größe anpassen.
- Hinzu kommen Funktionen für die Initialisierung und die Freigabe von Zeichenketten.

Denkbare Ansätze einer Bibliothek für Zeichenketten

Bei der Semantik gibt es zwei grundsätzliche Ansätze:

- Jede Zeichenkette ist in ihrer Repräsentierung unabhängig von allen anderen Zeichenketten und kann daher auch jederzeit frei verändert werden. Dies entspricht der traditionellen Vorgehensweise in C und der *string*-Template-Klasse in C++.
- Jede Zeichenkette ist konstant. Daher kann bei einer Operation analog zu *strcpy()* auf das Kopieren verzichtet werden. Änderungen erfordern hingegen das vorherige Anfertigen von Kopien. Dies entspricht der Vorgehensweise von Java.

stralloc-Bibliothek von Dan Bernstein

- Eine C-Bibliothek, die dem ersten Ansatz folgt, wurde von Dan J. Bernstein entwickelt (u.a. für das Qmail-Paket).
- Später wurde sie von Felix von Leitner nachprogrammiert, um die Bibliothek unter der GPL (GNU General Public License) zur Verfügung stellen zu können.
- Zu finden ist sie unter *http://www.fefe.de/libowfat/*.

Datenstruktur für Zeichenketten

/usr/local/diet/include/stralloc.h

```
typedef struct stralloc {
  char* s;
  unsigned int len;
  unsigned int a;
} stralloc;
```

- Diese öffentlich einsehbare Datenstruktur wird von Bernsteins Bibliothek verwendet.
- s verweist auf einen Puffer der Länge a, in dem eine Zeichenkette der Länge *len* untergebracht ist. Es gilt: $len \leq a$.
- Der Zeiger s darf gleich 0 sein, um eine leere Zeichenkette zu repräsentieren.
- Im Gegensatz zu den normalen Zeichenketten unter C dürfen diese auch Nullbytes enthalten. Entsprechend gibt es keine Nullbyte-Terminierung.

Initialisierung einer Zeichenkette

```
stralloc sa = {0};
```

- Wichtig ist die korrekte Initialisierung einer Variablen vom Typ *stralloc*. C sieht bei lokalen Variablen keine automatische Initialisierung vor, so daß hier die Initialisierung nicht vergessen werden darf.
- Damit wird übrigens nicht nur *sa.s* auf 0 initialisiert, sondern auch gleichzeitig *sa.len* und *sa.a* auf 0 gesetzt.

Einlesen einer Zeile mit der stralloc-Bibliothek

sareadline.c

```
/*
 * Read a string of arbitrary length from a
 * given file pointer. LF is accepted as terminator.
 * 1 is returned in case of success, 0 in case of errors.
 * afb 4/2003
 */

#include <stralloc.h>
#include <stdio.h>

int readline(FILE* fp, stralloc* sa) {
   if (!stralloc_copys(sa, "")) return 0;
   for(;;) {
      if (!stralloc_readyplus(sa, 1)) return 0;
      if (fread(sa->s + sa->len, sizeof(char), 1, fp) <= 0) return 0;
      if (sa->s[sa->len] == '\n') break;
      ++sa->len;
   }
   return 1;
}
```

Einlesen einer Zeile mit der stralloc-Bibliothek

sareadline.c

```
int readline(FILE* fp, stralloc* sa) {
   if (!stralloc_copys(sa, "")) return 0;
   /* ... */
}
```

- Hier wird zunächst *sa* mit Hilfe von *stralloc_copys* zu einer leeren Zeichenkette initialisiert.
- Generell dient *stralloc_copys* dazu, traditionelle nullbyte-terminierte Zeichenketten in C zu einem *stralloc*-Objekt zu kopieren.
- Nicht vergessen werden sollte die Überprüfung des Rückgabewerts. Bei 1 war die Operation erfolgreich, bei 0 konnte nicht genügend Speicher belegt werden.

Einlesen einer Zeile mit der stralloc-Bibliothek

sareadline.c

```
for(;;) {
   if (!stralloc_readyplus(sa, 1)) return 0;
   if (fread(sa->s + sa->len, sizeof(char), 1, fp) <= 0) return 0;
   if (sa->s[sa->len] == '\n') break;
   ++sa->len;
}
```

- Die **for**-Schleife behandelt das zeichenweise Einlesen, bis entweder das Zeilenende erkannt wird oder ein Fehler auftritt.
- Die Funktion *stralloc_readyplus* sorgt dafür, dass in *sa->s* mindestens ein Byte mehr Platz vorhanden ist, als die augenblickliche Länge *sa->len* beträgt.
- Wenn dies sichergestellt ist, kann mit *fread* das nächste Zeichen an der Position *sa->len* abgelegt werden.
- Wenn dies ein Zeilentrenner war, wird die **for**-Schleife beendet. Ansonsten wird das Zeichen akzeptiert, indem die Länge der Zeichenkette um 1 erhöht wird.

Sichere Fassung von *pubfile*

spubfile.c

```
while (argc-- > 0) {
   stralloc pathname = {0};
   char buffer[BUFFER_SIZE];
   int fd;
   int count;

   if (**argv == '.' || strchr(*argv, '/')) {
      fprintf(stderr, "invalid filename: %s\n", *argv);
      exit(1);
   }

   stralloc_copys(&pathname, pubdir);
   stralloc_cats(&pathname, "/");
   stralloc_cats(&pathname, *argv++);
   stralloc_0(&pathname);

   if ((fd = open(pathname.s, O_RDONLY)) < 0) {
      perror(pathname.s); exit(1);
   }
   /* ... copy contents of fd to stdout ... */
   close(fd);
}
```

Sichere Fassung von *pubfile*

spubfile.c

```
    stralloc_copys(&pathname, pubdir);
    stralloc_cats(&pathname, "/");
    stralloc_cats(&pathname, *argv++);
    stralloc_0(&pathname);
```

- Hinzugekommen ist hier die Funktion *stralloc_cats*, die eine traditionelle Zeichenkette an ein *stralloc*-Objekt anhängt.
- Die Funktion *stralloc_0* hängt genau ein Nullbyte an das *stralloc*-Objekt. Dies erlaubt es, *pathname.s* als traditionelle Zeichenkette in C zu verwenden — beispielsweise bei der Übergabe an die Funktion *open()*.
- Darüber hinaus wird in der korrigierten Version jeder Dateiname dahingehend überprüft, ob er mit einem Punkt beginnt (um sich insbesondere gegen die Verwendung von "." und ".." zu schützen) und ob er einen Schrägstrich enthält, um sich gegen die Angabe relativer Pfadnamen zu schützen.

Überblick der stralloc-Bibliothek

stralloc sa = 0;	Initialisierung einer Zeichenkette.
stralloc_ready(*sa*, *len*)	Bereitstellung von *len* Bytes.
stralloc_readyplus(*sa*, *len*)	Bereitstellung von *len* weiteren Bytes.
stralloc_free(*sa*)	Freigabe von *sa*.
sa.s	Direkter Zugriff auf den Zeiger.
sa.len	Länge der Zeichenkette.
stralloc_copys(*sa*, *s*)	Kopieren von *s* nach *sa*.
stralloc_copy(*sa1*, *sa2*)	Kopieren von *sa2* nach *sa1*.
stralloc_cats(*sa*, *s*)	Anhängen von *s* an *sa*.
stralloc_cat(*sa1*, *sa2*)	Anhängen von *sa2* an *sa1*.
stralloc_0(*sa*)	Anhängen eines Nullbytes an *sa*.
stralloc_starts(*sa*, *s*)	Findet sich *s* zu Beginn von *sa*?

Richtlinien

- Sicherheit sollte von Anfang an ein Kriterium sein. Es ist meistens ein hoffnungsloses Unterfangen, erst später Sicherheitsüberprüfungen einbauen zu wollen.
- Sicherheit sollte bei jedem Programm relevant sein, da sich sonst die Verwendung in einem sicherheitskritischen Kontext ausschließt. Nur bei temporären Wegwerf-Programmen können Sicherheitsbedenken wegfallen.
- Programme sollten nur ein Minimum an Privilegien erhalten. Häufig ist es ratsam, nicht nur auf `root`-Privilegien zu verzichten, sondern auch noch zusätzliche Restriktionen aufzunehmen wie die Limitierung des Ressourcen-Verbrauches und die Verwendung von `chroot`-Gefängnissen.
- Falls das Arbeiten mit Privilegien unverzichtbar ist, sollte das Aufteilen in mehrere Programme mit unterschiedlichen Privilegien in Betracht gezogen werden.

Richtlinien

- Grundsätzlich sollte nichts und niemanden getraut werden, was von außen kommt.
- Bei der Überprüfung von Benutzereingaben sind Positivlisten (was ist erlaubt) besser als Negativlisten (was ist gefährlich).
- Sicherheit beruht auf Verantwortlichkeiten. Damit klar ist, welcher Programmteil für welche Überprüfungen verantwortlich ist, sollten entsprechende Vorgaben und Annahmen klar dokumentiert sein. So sollte beispielsweise innerhalb eines Programmes immer klar hervorgehen, wo mit ungeprüften Eingaben zu rechnen ist.
- Der wohldefinierte Bereich einer Programmiersprache sollte auf keinen Fall verlassen werden, unabhängig davon wie schwierig es sein mag, für Verletzungen passende Einbruchstechniken zu finden.

Richtlinien

- Alle angebotenen automatischen Überprüfungen zur Übersetz- und Laufzeit sind zu verwenden.
- Wenn die Programmiersprache oder die Bibliothek nicht genügend automatische Überprüfungen mit sich bringen, ist es ratsam, Bibliotheken zu verwenden, die die Überprüfungen entweder durchführen oder überflüssig machen (Beispiel: **stralloc**-Bibliothek).
- Besser als das stille Abschneiden (Beispiel: *snprintf*()) ist die prinzipielle Unterstützung beliebig langer Eingaben. Der Speicherbedarf wird besser zentral limitiert als bei jeder einzelnen Eingabe.

Richtlinien

- Die Grenzen aller Sicherheitsbemühungen sollten nicht vergessen werden.
- Das sicherste Programm nützt nichts, wenn die Bibliothek, der Compiler, das Betriebssystem oder die Hardware Sicherheitslücken aufweisen, die das Programm betreffen.
- Ebenso ist der korrekte Umgang mit einer sicherheitskritischen Anwendung relevant. Das schwächste Glied in der Kette ist allzu häufig der Mensch.

Das Ein- und Ausgabe-System

- Die Systemschnittstelle für Ein- und Ausgabe dient primär zwei Zielen:
  - Sie sollte möglichst gut abstrahieren und somit Anwendungen befreien von Hardware-Abhängigkeiten und bis zu einem gewissen Umfange auch von den Besonderheiten eines Dateisystems.
  - Sie sollte eine höchstmögliche Effizienz erlauben bis hin zum Verzicht auf jegliche zusätzliche Kopieraktionen zwischen dem Betriebssystem und dem Adressraum des Prozesses (*zero copy*).

Dateideskriptoren

- Dateideskriptoren sind ganzzahlige Werte aus dem Bereich $[0, N-1]$, wobei N typischerweise eine Zweierpotenz ist (etwa 512 oder 1024).
- Dateideskriptoren werden innerhalb des Betriebssystems als Indizes für Verwaltungstabellen verwendet.
- Dateideskriptoren referenzieren somit vom Betriebssystem verwaltete Objekte.
- Für jeden Prozess verwaltet das System eine eigene Tabelle. Entsprechend kann beispielsweise der Dateideskriptor 2 bei zwei Prozessen mit völlig unterschiedlichen Objekten verbunden sein.
- Die so referenzierten Objekte sind typischerweise Dateien, können aber auch Netzwerkverbindungen, Verbindungen zu anderen Prozessen, Geräte und Speicherbereiche sein.
- In C wird für Dateideskriptoren der Datentyp **int** verwendet.

Wieviel Dateideskriptoren gibt es?

openmax.c

```
#include <stdio.h>
#include <unistd.h>

int main() {
   long maxfds = sysconf(_SC_OPEN_MAX);
   printf("maximal number of open file descriptors: %ld\n", maxfds);
}
```

- Der Systemaufruf *sysconf* erlaubt die Abfrage zahlreicher Größen, von denen auch einige erst zur Laufzeit festliegen.
- Der Parameter *_SC_OPEN_MAX* liefert die maximale Zahl offener Dateien und die damit die Größe der systeminternen Tabelle der Objekte für diesen Prozess.

```
doolin$ gcc -Wall -std=c99 openmax.c
doolin$ a.out
maximal number of open file descriptors: 512
doolin$
```

Vererbung von Dateideskriptoren

- Wenn ein neuer Prozess erzeugt wird, dann wird die Tabelle mit den Dateideskriptoren kopiert.
- Entsprechend kann die Shell einige Dateideskriptoren für ein Programm, das sie startet, vorbereiten.
- Wenn nichts anderes spezifiziert wird, sind dies folgende Dateideskriptoren:

  0 Standard-Eingabe
  1 Standard-Ausgabe
  2 Standard-Fehlerausgabe

- Die Bourne-Shell und die von ihr abgeleiteten Shells erlauben das Öffnen und Schließen beliebiger Dateideskriptoren. Folgendes Beispiel ruft a.out auf, wobei 0 geschlossen wird, 7 zum Schreiben geöffnet wird auf die Datei *out* und 10 zum Lesen für die Datei *in* eröffnet wird:

```
a.out 0<&- 7>out 10<in
```

Kopieren mit der stdio

scopy.c

```
#include <stdio.h>
#include <stdlib.h>

int main(int argc, char* argv[]) {
   char* cmdname = argv[0];
   if (argc != 3) {
      fprintf(stderr, "Usage: %s infile outfile\n", cmdname);
      exit(1);
   }
   char* infile = argv[1]; char* outfile = argv[2];
   FILE* in = fopen(infile, "r"); if (!in) perror(infile), exit(1);
   FILE* out = fopen(outfile, "w"); if (!out) perror(outfile), exit(1);
   int ch;
   while ((ch = getc(in)) != EOF) {
      if (putc(ch, out) == EOF) perror(outfile), exit(1);
   }
   fclose(in);
   if (fclose(out) == EOF) perror(outfile), exit(1);
}
```

Kopieren mit Systemaufrufen

copy.c

```
#include <errno.h>
#include <fcntl.h>
#include <stdlib.h>
#include <stralloc.h>
#include <string.h>
#include <unistd.h>

char* cmdname;
/* ... */

int main(int argc, char* argv[]) {
   cmdname = argv[0];
   if (argc != 3) {
      stralloc usage = {0};
      if (stralloc_copys(&usage, "Usage: ") &&
            stralloc_cats(&usage, cmdname) &&
            stralloc_cats(&usage, " infile outfile\n")) {
         write(2, usage.s, usage.len);
      }
      exit(1);
   }
   /* ... */
}
```

Kopieren mit Systemaufrufen

copy.c

```
char* infile = argv[1]; char* outfile = argv[2];

int infd = open(infile, O_RDONLY);
if (infd < 0) die(infile);
int outfd = open(outfile, O_WRONLY|O_CREAT|O_TRUNC, 0666);
if (outfd < 0) die(outfile);
char buf[8192]; ssize_t nbytes;
while ((nbytes = read(infd, buf, sizeof buf)) > 0) {
   ssize_t count;
   for (ssize_t written = 0; written < nbytes; written += count) {
      count = write(outfd, buf + written, nbytes - written);
      if (count <= 0) die(outfile);
   }
}
if (nbytes < 0) die(infile);
close(infd);
if (close(outfd) < 0) die(outfile);
```

Das Eröffnen einer Datei

copy.c

```
int infd = open(infile, O_RDONLY);
if (infd < 0) die(infile);
int outfd = open(outfile, O_WRONLY|O_CREAT|O_TRUNC, 0666);
if (outfd < 0) die(outfile);
```

- Mit dem Systemaufruf *open* kann eine Datei eröffnet werden. Im Erfolgsfalle wird ein (zuvor unbenutzter) Dateideskriptor zurückgeliefert.
- Der zweite Parameter gibt an, wie die Datei zu eröffnen ist. Hier können zahlreiche Werte mit einem bitweisen Oder verknüpft werden, wobei nicht jede Kombination sinnvoll ist. Eine Auswahl:

O_RDONLY	Nur zum Lesen eröffnen
O_WRONLY	Nur zum Schreiben eröffnen
O_RDWR	Zum Lesen und Schreiben eröffnen
O_CREAT	Datei neu anlegen, falls noch nicht existent
O_TRUNC	Datei auf Länge 0 kürzen, falls existent

- Der optionale dritte Parameter wird nur hinzugefügt, falls bei dem zweiten Parameter *O_CREAT* mit angegeben wurde. Er legt die Zugriffsrechte fest. 0666 steht für rw-rw-rw.

Die Systemaufrufe read und write

copy.c

```
while ((nbytes = read(infd, buf, sizeof buf)) > 0) {
   ssize_t count;
   for (ssize_t written = 0; written < nbytes; written += count) {
      count = write(outfd, buf + written, nbytes - written);
      if (count <= 0) die(outfile);
   }
}
if (nbytes < 0) die(infile);
```

- Die Systemaufrufe *read* und *write* erhalten jeweils als Parameter, einen Dateideskriptor, einen Zeiger auf einen Puffer und eine Angabe, wieviel Bytes maximal zu transferieren sind.
- Grundsätzlich haben *read* und *write* die Freiheit, weniger Bytes zu übertragen als angegeben.
- Der Rückgabewert gibt die Zahl der übertragenen Bytes im Erfolgsfalle (immer positiv) oder ist gleich 0 (bei *read* steht dies für das Eingabeende) oder -1 bei Fehlern.

Das Schließen eines Dateideskriptors

copy.c

```
  close(infd);
  if (close(outfd) < 0) die(outfile);
```

- Mit *close* können Dateideskriptoren geschlossen werden.
- Bei einem zuvor zum Schreiben geöffneten Dateideskriptor ist es sinnvoll, den Erfolg zu überprüfen, weil so noch am Ende aufgetretene Fehler erkannt werden können – auch wenn dies eher selten der Fall sein dürfte.

Kopieren mit Systemaufrufen

copy.c

```
void die(char* filename) {
   stralloc msg = {0};
   if (stralloc_copys(&msg, cmdname) &&
         stralloc_cats(&msg, ": ") &&
         stralloc_cats(&msg, strerror(errno)) &&
         stralloc_cats(&msg, ": ") &&
         stralloc_cats(&msg, filename) &&
         stralloc_cats(&msg, "\n")) {
      write(2, msg.s, msg.len);
   }
   exit(1);
}
```

- *strerror* liefert die Fehlermeldung passend zu *errno*. Die bislang bekannte Funktion *perror* basiert auf *strerror*.

Kopieren mit mmap

mcopy.c

```
struct stat statbuf; if (fstat(infd, &statbuf) < 0) die(infile);
off_t nbytes = statbuf.st_size;
char* buf = (char*) mmap(0, nbytes, PROT_READ, MAP_SHARED, infd, 0);
if (buf == MAP_FAILED) die(infile);
ssize_t count;
for (ssize_t written = 0; written < nbytes; written += count) {
   count = write(outfd, buf + written, nbytes - written);
   if (count <= 0) die(outfile);
}
```

- Der Systemaufruf *mmap* (*memory map*) erlaubt es, den Inhalt des Puffer-Cache, der zu einer Datei gehört, direkt in den eigenen Adressraum zu legen.
- Auf diese Weise entfällt das Kopieren des Inhalts der zu kopierenden Datei in den Adressraum des Kopierprogramms.

Vergleich der Kopierprogramme

```
turing$ mkfile 10m 10m
turing$ time scopy 10m out && rm out

real    0m0.64s
user    0m0.59s
sys     0m0.05s
turing$ time copy 10m out && rm out

real    0m0.09s
user    0m0.01s
sys     0m0.08s
turing$ time mcopy 10m out && rm out

real    0m0.07s
user    0m0.00s
sys     0m0.07s
turing$
```

Konkurrierende Zugriffe

- Prinzipiell erlaubt Unix den konkurrierenden Zugriff mehrerer Prozesse auf die gleiche Datei.
- Das u.U. notwendige gegenseitige Ausschließen und die Atomizität von Änderungen ergeben sich dabei nicht von selbst, sondern sind Aufgabe der parallel zugreifenden Anwendungen.
- Es gibt aber einige Systemaufrufe, die hier eine Hilfestellung leisten können.

Beispiel für eine Problemstellung

Es ist ein kleines Werkzeug *unique* zu entwickeln, das einen Dateinamen als Parameter erhält und folgende Anforderungen erfüllt:

- Die Zahl in der gegebenen Datei ist auszulesen, um eins zu erhöhen, wieder in die Datei zu schreiben und auf der Standardausgabe auszugeben.
- Gegenseitiger Ausschluss: Jeder Wert darf höchstens einmal ausgegeben werden, egal wieviele Instanzen des Programms gleichzeitig auf die Datei zugreifen.
- Atomizität: Die Datei muss immer einen gültigen Inhalt haben, selbst wenn inmitten einer Operation der Strom ausfällt.

Gegenseitiger Ausschluss

Wenn mehrere gleichzeitig zugreifende Prozesse sich gegenseitig ausschließen möchten, kommen folgende auf dem Dateisystem basierende Techniken in Frage, die alle ohne Interprozess-Kommunikation auskommen:

- Option *O_EXCL* zusammen mit *O_CREAT* bei *open* setzen. Dann ist *open* nur erfolgreich, wenn die Datei vorher noch nicht existiert.
- Mit *link* zu einer existierende Datei einen weiteren Namen hinzufügen. Dies ist nur erfolgreich, wenn der neue Name noch nicht existiert.
- Mit *lockf* können bei einem gegebenen Deskriptor einzelne Bereiche reserviert werden. Jedoch wird *lockf* nicht überall unterstützt oder ist (wie bei NFS) nicht ausreichend zuverlässig.

Atomizität

- Wenn das Ergebnis einer Schreib-Operation abgesichert werden soll, dann empfiehlt sich *fsync*, das einen Dateideskriptor erhält und im Erfolgsfalle wartet, bis der aktuelle Stand auf die Platte gesichert ist.
- Datenbanken und andere Anwendungen arbeiten bei Transaktionen mit mehreren Versionen (der alten und der neuen). Erst wenn die neue Version mit *fsync* abgesichert worden ist, wird ein Versionszeiger in der Datei so aktualisiert, dass er auf die neue Fassung verweist.

Atomizität

- Im einfachen Falle empfiehlt sich die Verwendung des Systemaufrufs *rename*.
- Hier wird zunächst eine vollständig neue Version der Daten in einer temporären Datei erstellt.
- Dann wird *rename* aufgerufen mit der temporären Datei und der eigentlichen Datei als Ziel.
- Das ist auch zulässig, wenn das Ziel existiert. In diesem Falle wird implizit zuvor der alte Verweis gekappt.
- Diese Operation ist atomar und alle anderen Prozesse sehen entweder den alten oder den neuen Inhalt, vermissen aber nie die Datei und sehen unter keinen Umständen eine nur teilweise beschriebene Datei.

Beispiel: *unique*

unique.c

```
#include <ctype.h>
#include <errno.h>
#include <fcntl.h>
#include <stdbool.h>
#include <stdlib.h>
#include <stralloc.h>
#include <string.h>
#include <unistd.h>

char* cmdname;
stralloc tmpfile = {0}; bool tmpfile_created = false;

/* print an out of memory message to standard error and exit */
void memerr() { /* ... */ }

/* print a error message to standard error and exit;
   include "message" in the output message, if not 0,
   otherwise strerror(errno) is being used
*/
void die(char* filename, char* message) { /* ... */ }

int main(int argc, char* argv[]) { /* ... */ }
```

Beispiel: *unique*

unique.c

```
/* print an out of memory message to standard error and exit */
void memerr() {
   static char memerrmsg[] = "out of memory error\n";
   write(2, memerrmsg, sizeof(memerrmsg) - 1);
   if (tmpfile_created) unlink(tmpfile.s);
   exit(1);
}
```

- Sollte tatsächlich der Speicher ausgehen, dann sollte die Ausgabe der zugehörigen Fehlermeldung ohne dynamische Speicheranforderungen auskommen.
- Von **sizeof**(*memerrmsg*) wird 1 abgezogen, weil das Nullbyte nicht auszugeben ist.
- Wenn die Ausführung abgebrochen wird, sollten ggf. temporäre Dateien aufgeräumt werden. Mit *unlink* kann eine Verweis aus einem Verzeichnis auf eine Datei entfernt werden.

Beispiel: *unique*

unique.c

```
/* print a error message to standard error and exit;
   include "message" in the output message, if not 0,
   otherwise strerror(errno) is being used
*/
void die(char* filename, char* message) {
   stralloc msg = {0};
   if (stralloc_copys(&msg, cmdname) &&
         stralloc_cats(&msg, ": ") && (
            message?
               stralloc_cats(&msg, message)
            :
               stralloc_cats(&msg, strerror(errno))
         ) && stralloc_cats(&msg, ": ") &&
         stralloc_cats(&msg, filename) &&
         stralloc_cats(&msg, "\n")) {
      write(2, msg.s, msg.len);
   } else {
      memerr();
   }
   if (tmpfile_created) unlink(tmpfile.s);
   exit(1);
}
```

Beispiel: *unique*

unique.c

```
int main(int argc, char* argv[]) {
   /* process command line arguments */

   /* try to open the temporary file which also serves as a lock */

   /* determine current value of the counter */

   /* increment the counter and write it to the tmpfile */

   /* update counter file atomically by a rename */

   /* write counter value to stdout */
}
```

- Vorgehensweise: Wir erhalten einen Dateinamen als Argument, leiten daraus den Namen einer temporären Datei ab, eröffnen diese exklusiv zum Schreiben, lesen den alten Zählerwert aus, erhöhen diesen um eins, schreiben den neuen Zählerwert in die temporäre Datei, taufen diese in den gegebenen Dateinamen um und geben am Ende den neuen Zählerwert aus.

Beispiel: *unique*

unique.c

```
/* process command line arguments */
cmdname = argv[0];
if (argc != 2) {
   stralloc usage = {0};
   if (stralloc_copys(&usage, "Usage: ") &&
         stralloc_cats(&usage, cmdname) &&
         stralloc_cats(&usage, " counter\n")) {
      write(2, usage.s, usage.len);
   } else {
      memerr();
   }
   exit(1);
}
char* counter_file = argv[1];
```

- Genau ein Dateiname wird als Argument erwartet. In dieser Datei wird der Zähler verwaltet.

Beispiel: *unique*

unique.c

```
/* try to open the temporary file which also serves as a lock */
if (!stralloc_copys(&tmpfile, counter_file) ||
      !stralloc_cats(&tmpfile, ".tmp") ||
      !stralloc_0(&tmpfile)) {
   memerr();
}
int outfd;
for (int tries = 0; tries < 10; ++tries) {
   outfd = open(tmpfile.s, O_WRONLY|O_CREAT|O_TRUNC|O_EXCL, 0666);
   if (outfd >= 0) break;
   if (errno != EEXIST) break;
   sleep(1);
}
if (outfd < 0) die(tmpfile.s, 0);
tmpfile_created = true;
```

- Den Namen der temporären Datei gewinnen wir durch ein Anhängen der Endung ».tmp« an den übergebenen Dateinamen.
- Damit liegt die temporäre Datei im gleichen Verzeichnis wie die angegebene Datei und damit auch auf dem gleichen Dateisystem.
- Das Nullbyte am Ende der Zeichenkette *tmpfile* wird für *open* benötigt.

Beispiel: *unique*

unique.c

```
int outfd;
for (int tries = 0; tries < 10; ++tries) {
   outfd = open(tmpfile.s, O_WRONLY|O_CREAT|O_TRUNC|O_EXCL, 0666);
   if (outfd >= 0) break;
   if (errno != EEXIST) break;
   sleep(1);
}
```

- Die Option *O_EXCL* lässt den Aufruf von *open* scheitern, wenn die Datei bereits existiert. In diesem Falle hat *errno* den Wert *EEXIST*.
- Wenn *open* aus diesem Grunde schiefgeht, wird die Operation mit Zeitverzögerung wiederholt. *sleep* erlaubt ein sekundengenaues Suspendieren des eigenen Prozesses.
- Sobald der Aufruf von *open* erfolgreich ist, schließen wir alle Konkurrenten aus.

Beispiel: *unique*

unique.c

```
/* determine current value of the counter */
int current_value;
int infd = open(counter_file, O_RDONLY);
if (infd >= 0) {
   char buf[512];
   ssize_t nbytes = read(infd, buf, sizeof buf);
   if (nbytes <= 0) die(counter_file, 0);
   current_value = 0;
   for (char* cp = buf; cp < buf + nbytes; ++cp) {
     if (!isdigit(*cp)) die(counter_file, "decimal digits expected");
       current_value = current_value * 10 + *cp - '0';
   }
} else if (errno != ENOENT) {
   die(counter_file, 0);
} else {
   /* start a new counter */
   current_value = 0;
}
```

- Sobald wir einen exklusiven Zugriff haben, lohnt es sich, den bisherigen Zählerstand auszulesen.
- Falls die Datei noch nicht existiert, gehen wir von einem bisherigen Zählerwert von 0 aus.

Beispiel: *unique*

unique.c

```
/* increment the counter and write it to the tmpfile */
++current_value;
stralloc outbuf = {0};
if (!stralloc_copys(&outbuf, "") ||
      !stralloc_catint(&outbuf, current_value)) {
   memerr();
}
int nbytes = write(outfd, outbuf.s, outbuf.len);
if (nbytes < outbuf.len) die(tmpfile.s, 0);
if (fsync(outfd) < 0) die(tmpfile.s, 0);
if (close(outfd) < 0) die(tmpfile.s, 0);
```

- Der um eins erhöhte Zählerwert wird in die temporäre Datei geschrieben.
- Mit *fsync* wird der Inhalt der temporären Datei mit der Festplatte synchronisiert.

Beispiel: *unique*

unique.c

```
/* update counter file atomically by a rename */
if (rename(tmpfile.s, counter_file) < 0) die(counter_file, 0);
tmpfile_created = false;
```

- Mit *rename* wird der Verweis auf die Zieldatei, falls dieser zuvor existierte, implizit mit *unlink* entfernt und danach die temporäre Datei in die Zieldatei umgetauft.
- IEEE Std 1003.1 verlangt ausdrücklich, dass *rename* atomar ist. Dies in Erweiterung zu ISO 9989-1999 (C99-Standard), das den Fall, dass die Zieldatei existiert, ausdrücklich offen lässt.

Beispiel: *unique*

unique.c

```
/* write counter value to stdout */
if (!stralloc_cats(&outbuf, "\n")) memerr();
nbytes = write(1, outbuf.s, outbuf.len);
if (nbytes < outbuf.len) die("stdout", 0);
```

- Am Ende wird hier, falls alles soweit erfolgreich war, der neue Zählerwert auf der Standard-Ausgabe ausgegeben.

Probleme des Beispiels

Folgende Nachteile sind mit dem vorgestellten Beispiel verbunden:

- Sollte das Programm gewaltsam terminiert werden, während die temporäre Datei noch existiert, kommt keine weitere Instanz mehr zum Zuge, da alle darauf warten, dass diese irgendwann verschwindet. Das Problem kann dahingehend angegangen werden, dass die anderen Instanzen überprüfen, ob derjenige, der dem die Datei gehört, noch lebt. Dies ist möglich, wenn die Prozess-ID bekannt ist und der Prozess auf dem gleichen Rechner läuft. Andernfalls läuft es nur über Netzwerkprotokolle oder über Heuristiken, die eine zeitliche Beschränkung einführen.
- Eine Wartezeit von einer Sekunde ist recht grob. Kleinere Wartezeiten sind mit Hilfe des Systemaufrufs *poll* möglich.

Zufällige Wartezeiten

unique2.c

```
void randsleep() {
   static int invocations = 0;
   if (invocations == 0) {
      srand(getpid());
   }
   ++invocations;
   /* determine timeout value (in milliseconds) */
   int timeout = rand() % (10 * invocations + 100);
   if (poll(0, 0, timeout) < 0) die("poll", 0);
}
```

- *poll* blockiert den aufrufenden Prozess bis zum Eintreffen eines Ereignisses (aus einer Menge gegebener Ereignisse im Kontext von Dateideskriptoren) oder wenn ein Zeitlimit abgelaufen ist.
- Das Zeitlimit wird in Millisekunden als ganze Zahl spezifiziert.
- Im einfachsten Falle kann *poll* wie hier auch als reines Suspendierungs-Werkzeug verwendet werden, das im Gegensatz zu *sleep* Zeitangaben in Millisekunden akzeptiert.
- Wie genau das jedoch aufgelöst wird, hängt vom Betriebssystem ab.

Konkurrierende Zugriffe auf eine Datei

- Grundsätzlich können beliebig viele Prozesse gleichzeitig auf die gleiche Datei zugreifen.
- Eine Synchronisierung oder Koordinierung bleibt grundsätzlich den Anwendungen überlassen.
- Es gibt aber einen entscheidenden Punkt: Arbeiten die konkurrierende Prozesse mit unabhängig voneinander geöffneten Dateideskriptoren oder sind die Dateideskriptoren gemeinsamen Ursprungs?
- Dateideskriptoren können vererbt werden. Bei der Shell wird dies intensiv ausgenutzt, um beispielsweise die Standard-Kanäle im gewünschten Sinne vorzubereiten.
- Zu jedem Dateideskriptor gibt es eine aktuelle Position. Wenn Dateideskriptoren vererbt werden, arbeiten alle Erben mit der gleichen Position.

Eine Testanwendung

write10.c

```
int main(int argc, char* argv[]) {
   cmdname = argv[0];
   for (int i = 1; i <= 10; ++i) {
      stralloc text = {0};
      if (!stralloc_copys(&text, "")) memerr();
      if (!stralloc_catint(&text, getpid())) memerr();
      if (!stralloc_cats(&text, ": ")) memerr();
      if (!stralloc_catint(&text, i)) memerr();
      if (!stralloc_cats(&text, "\n")) memerr();
      ssize_t nbytes = write(1, text.s, text.len);
      if (nbytes < text.len) die("stdout", 0);
   }
}
```

- Dieses Programm ruft 10 mal *write* auf, um die eigene Prozess-ID zusammen mit einer laufenden Nummer auf der Standardausgabe auszugeben.
- Dies dient im folgenden als Testkandidat.

Testfall 1

test1

```
#!/bin/sh

rm -f out

./write10 >out & ./write10 >out & ./write10 >out &
./write10 >out & ./write10 >out & ./write10 >out &
./write10 >out & ./write10 >out & ./write10 >out &
./write10 >out & ./write10 >out & ./write10 >out &
./write10 >out & ./write10 >out & ./write10 >out &
./write10 >out & ./write10 >out & ./write10 >out &
./write10 >out & ./write10 >out & ./write10 >out &
./write10 >out & ./write10 >out & ./write10 >out &
./write10 >out & ./write10 >out & ./write10 >out &
./write10 >out & ./write10 >out & ./write10 >out &
```

- Hier wird das Testprogramm 30 mal aufgerufen und dabei jeweils individuell die Ausgabedatei zum Schreiben eröffnet.
- Das Eröffnen erfolgt durch die Shell mit den Optionen *O_WRONLY*, *O_CREAT* und *O_TRUNC*.
- Jedes Programm arbeitet mit einem eigenen unabhängigen Dateideskriptor, der jeweils ab Position 0 beginnt.

Testfall 2

test2

```
#!/bin/sh

rm -f out

./write10 >>out & ./write10 >>out & ./write10 >>out &
./write10 >>out & ./write10 >>out & ./write10 >>out &
./write10 >>out & ./write10 >>out & ./write10 >>out &
./write10 >>out & ./write10 >>out & ./write10 >>out &
./write10 >>out & ./write10 >>out & ./write10 >>out &
./write10 >>out & ./write10 >>out & ./write10 >>out &
./write10 >>out & ./write10 >>out & ./write10 >>out &
./write10 >>out & ./write10 >>out & ./write10 >>out &
./write10 >>out & ./write10 >>out & ./write10 >>out &
./write10 >>out & ./write10 >>out & ./write10 >>out &
```

- Hier wird von der Shell die Ausgabedaei wiederum jeweils individuell zum Schreiben eröffnet.
- Aber diesmal fällt die Option *O_TRUNC* weg.
- Stattdessen positioniert die Shell den Dateideskriptor an das aktuelle Ende.
- Nach wie vor arbeitet jeder der aufgerufenen Prozesse mit einer eigenen Dateiposition.

Testfall 3

test3

```
#!/bin/sh

rm -f out

exec >out

./write10 & ./write10 & ./write10 &
./write10 & ./write10 & ./write10 &
./write10 & ./write10 & ./write10 &
./write10 & ./write10 & ./write10 &
./write10 & ./write10 & ./write10 &
./write10 & ./write10 & ./write10 &
./write10 & ./write10 & ./write10 &
./write10 & ./write10 & ./write10 &
./write10 & ./write10 & ./write10 &
```

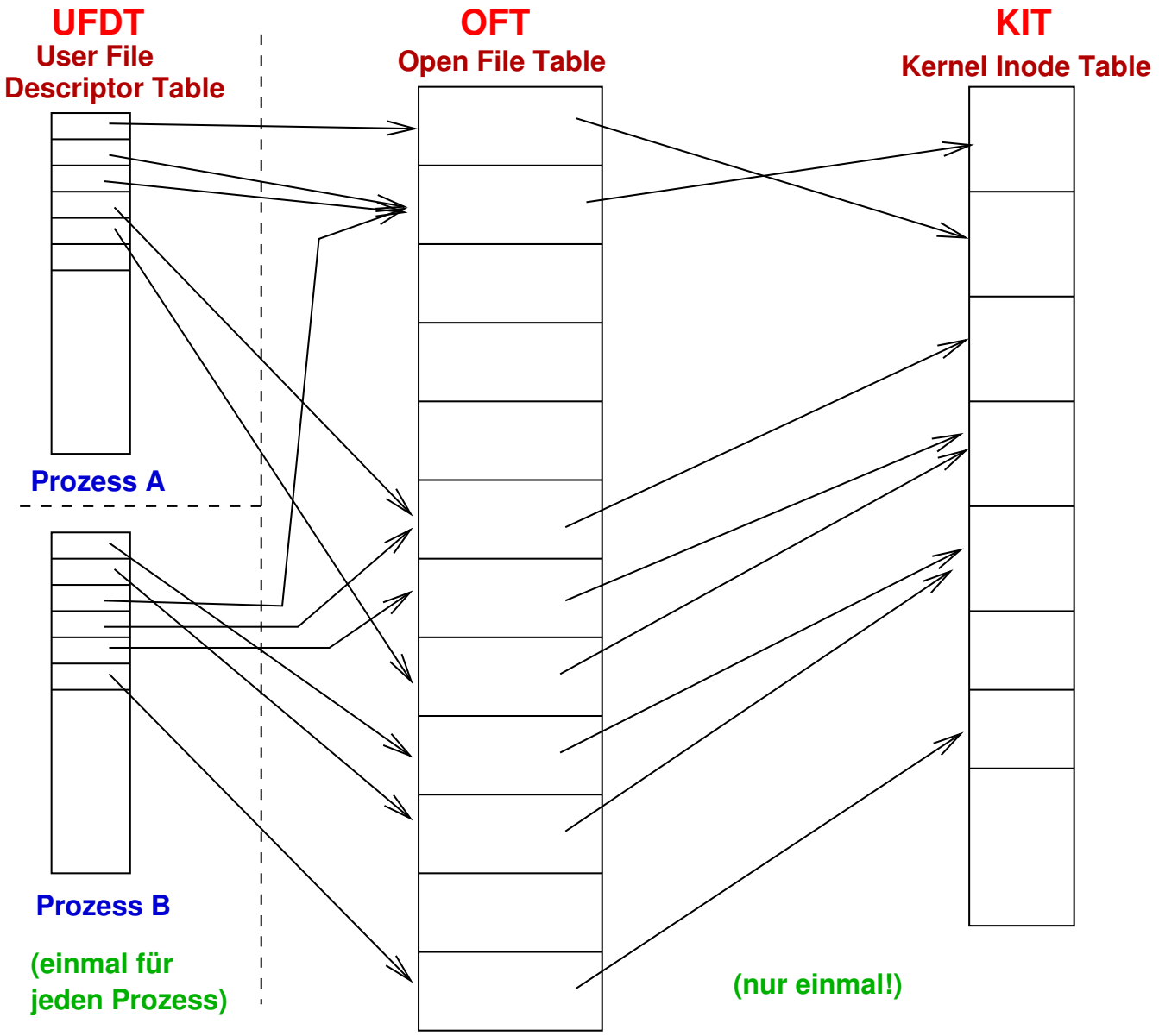
- Hier eröffnet die Shell die Ausgabedatei genau einmal zu Beginn im Rahmen der *exec*-Anweisung.
- Dieser Dateideskriptor wird danach an alle aufgerufenen Prozesse vererbt.
- Entsprechend arbeiten alle Prozesse mit einer gemeinsamen Dateiposition.

Ausführung der Testfälle

```
turing$ ./testit1
turing$ wc -l out
     10 out
turing$ ./testit2
turing$ wc -l out
     50 out
turing$ ./testit2
turing$ wc -l out
     29 out
turing$ ./testit3
turing$ wc -l out
    300 out
turing$
```

- Nur im dritten Falle geht hier keine Ausgabe verloren. Allerdings könnte diese bunt gemischt sein.
- IEEE Std 1003.1 garantiert allerdings hier nicht die Verlustfreiheit, weil das Betriebssystem nicht notwendigerweise entsprechend intern synchronisiert. In der Praxis kann dies allerdings bei *write* dennoch klappen. Bei *read* wird aus Performance-Gründen jedoch weitgehend darauf verzichtet.

Die internen Datenstrukturen für Dateien



User File Descriptor Table (UFDT)

- Diese Tabelle gibt es für jeden Prozess.
- Dateideskriptoren dienen als Index zu dieser Tabelle.
- Als Werte hat die Tabelle
  - einen Zeiger in die systemweite *Open File Table* und
  - Optionen, die nur dem Dateideskriptor zugeordnet sind – das ist momentan nur *FD_CLOEXEC*, mit dem Dateideskriptoren automatisiert beim Aufruf des Systemaufrufs *exec* geschlossen werden können. (Diese Option kann mit dem Systemaufruf *fcntl* und dem Parameter *F_GETFD* bzw. *F_SETFD* angesehen bzw. verändert werden).

Open File Table (OFT)

- Diese Tabelle gibt es nur einmal global im Betriebssystem.
- Zu einem Eintrag gehören folgende Komponenten:
  - Ein Zeiger in die *Kernel Inode Table*.
  - Die Optionen, die bei *open* angegeben wurden und später durch *fcntl* und dem Parameter *F_GETFL* bzw. *F_SETFL* angesehen bzw. verändert werden können.
  - Die aktuelle Dateiposition.
  - Eine ganze Zahl, die die Zahl der Verweise aus der UFDT auf den jeweiligen Eintrag spezifiziert. Geht diese auf 0 zurück, kann der entsprechende Eintrag freigegeben werden.

Kernel Inode Table (KIT)

- Diese Tabelle gibt es nur einmal global im Betriebssystem.
- Jede geöffnete Datei ist in dieser Tabelle genau einmal vertreten.
- Zu einem Eintrag gehören folgende Komponenten:
  - Eine vollständige Kopie der Inode von der Platte.
  - Eine ganze Zahl, die die Zahl der Verweise aus der OFT auf den jeweiligen Eintrag spezifiziert. Solange diese positiv ist, bleibt die Inode auch auf der Platte enthalten, selbst wenn der Referenzzähler innerhalb der Inode auf 0 ist, weil die Datei aus sämtlichen Verzeichnissen entfernt wurde.

Eine kleine Anwendung: shuffle

Aufgabenstellung:

- Die Zeilen aus der Standard-Eingabe sind in einer zufälligen Reihenfolge auszugeben.
- Dies sollte möglichst effizient und mit geringem Speicherplatzbedarf geschehen.
- Die Standard-Eingabe muss nicht notwendigerweise eine Datei sein – sie könnte auch beispielsweise aus einer Pipeline kommen.
- Die Zeilen sollen beliebig lange sein können.
- Alle Permutationen sollen mit gleicher Wahrscheinlichkeit ausgewählt werden. Dies ist nicht-trivial, da die Zahl der Permutationen ($n!$ für n Zeilen) rasch die Zahl der möglichen Seed-Werte eines Pseudo-Zufallszahlengenerators übersteigt.

Eine kleine Anwendung: shuffle

Vorgehensweise:

- Zunächst wird die gesamte Eingabe gelesen und dabei Buch geführt über alle gefundenen Zeilen, jeweils mit Anfangsposition und Zeilenlänge.
- Dies ist die einzige dynamische Datenstruktur, die im Speicher verbleibt.
- Danach werden Zeilen zufällig ausgewählt und ausgegeben.
- Da letzteres nur für Dateien funktioniert, wird bei Bedarf die gesamte Eingabe im ersten Durchgang in eine temporäre Datei kopiert, aus der dann später gelesen wird.

Die Datenstruktur für die Zeilen

lposlist.h

```
#ifndef LPOSLIST_H
#define LPOSLIST_H

#include <sys/types.h>
#include <unistd.h>

typedef struct lpos {
   off_t pos;
   ssize_t len; /* length without line terminator */
} lpos;

typedef struct lposlist {
   int allocated;
   int length;
   lpos* line;
} lposlist;

int add_lpos(lposlist* list, off_t pos, ssize_t len);
#endif
```

Die Datenstruktur für die Zeilen

lposlist.c

```
#include <stdlib.h>
#include <unistd.h>
#include "lposlist.h"

int add_lpos(lposlist* list, off_t pos, ssize_t len) {
   if (list->length == list->allocated) {
      int allocated = (list->allocated << 1) + 16;
      lpos* new = realloc(list->line, allocated * sizeof(lpos));
      if (!new) return 0;
      list->line = new; list->allocated = allocated;
   }
   list->line[list->length++] = (lpos) {pos, len};
   return 1;
}
```

- Wenn das erste Argument von *realloc* ein Nullzeiger ist, dann ist der Aufruf äquivalent zu *malloc*.
- Beginnend mit C99 können Strukturen auch innerhalb eines Ausdrucks konstruiert werden. Die Syntax gleicht der Initialisierung. Hinzukommen muss jedoch der Datentyp in Klammern vor den geschweiften Klammern.

Zufallszahlen aus dem Betriebssystem

rval.h

```
#ifndef RGEN_H
#define RGEN_H

int get_rval(int* rval);
#endif
```

- Die Aufgabe dieser Funktion ist die Generierung von Pseudo-Zufallszahlen, die nicht von einem begrenzten Seed-Wert abhängen.
- Die Funktion liefert 0 zurück, falls es nicht geklappt hat. Ansonsten wird der Zufallswert hinter dem Zeiger abgelegt und 1 zurückgeliefert.

Zufallszahlen aus dem Betriebssystem

rval.c

```
#include <fcntl.h>
#include <unistd.h>
#include "rgen.h"

int get_rval(int* rval) {
   static int fd = 0;
   if (fd == 0) {
      fd = open("/dev/urandom", O_RDONLY);
      if (fd < 0) return 0;
   }
   ssize_t nbytes = read(fd, rval, sizeof(int));
   return nbytes == sizeof(int);
}
```

- Es bietet sich die spezielle Gerätedatei */dev/urandom* an, die sich aus dem Entropie-Pool des Betriebssystems bedient.
- Alternativ gibt es auch */dev/random*, das aber solange blockiert, bis genügend Zufallswerte höchster Qualität (in Bezug auf Unvorhersehbarkeit) zur Verfügung stehen. Im Vergleich dazu blockiert */dev/urandom* nicht und überbrückt stattdessen mit einem gewöhnlichen Pseudo-Zufallszahlengenerator.

Das Anlegen temporärer Dateien

tmpfile.h

```
#ifndef TMPFILE_H
#define TMPFILE_H

int get_tmpfile();
#endif
```

- Es ist möglich, eine Datei zu kreieren, sie mit *unlink* sofort wieder aus dem Verzeichnis zu entfernen und den Dateideskriptor zu behalten.
- Auch wenn dann die Datei nirgends im Dateisystem zu sehen ist, so bleibt sie dennoch erhalten, bis der letzte auf sie verweisende Dateideskriptor geschlossen wird.
- Die Funktion *get_tmpfile* legt eine entsprechende temporäre Datei an, entfernt sie gleich wieder und liefert den Dateideskriptor zurück. Die Datei ist sinnvollerweise zum Lesen und Schreiben geöffnet.

Das Anlegen temporärer Dateien

tmpfile.c

```
#include <fcntl.h>
#include <stralloc.h>
#include <unistd.h>
#include "tmpfile.h"
#include "rgen.h"

int get_tmpfile() {
   stralloc tmpfile = {0};
   for (int attempt = 0; attempt < 10; ++attempt) {
      if (!stralloc_copys(&tmpfile, "/tmp/tmp.")) return -1;
      int rval;
      if (!get_rval(&rval)) return -1;
      if (!stralloc_catint(&tmpfile, rval)) return -1;
      if (!stralloc_0(&tmpfile)) return -1;
      int outfd = open(tmpfile.s, O_RDWR|O_CREAT|O_EXCL, 0);
      if (outfd >= 0) {
         if (unlink(tmpfile.s) < 0) { close(outfd); return -1; }
         return outfd;
      }
   }
   return -1;
}
```

Das Anlegen temporärer Dateien

tmpfile.c

```
for (int attempt = 0; attempt < 10; ++attempt) {
   if (!stralloc_copys(&tmpfile, "/tmp/tmp.")) return -1;
   int rval;
   if (!get_rval(&rval)) return -1;
   if (!stralloc_catint(&tmpfile, rval)) return -1;
   if (!stralloc_0(&tmpfile)) return -1;
   int outfd = open(tmpfile.s, O_RDWR|O_CREAT|O_EXCL, 0);
   if (outfd >= 0) {
      if (unlink(tmpfile.s) < 0) { close(outfd); return -1; }
      return outfd;
   }
}
```

- Da */tmp* von vielen gleichzeitig genutzt wird, ist es sinnvoll, möglichst noch nicht gewählte Dateinamen auszuwählen. Dafür bietet sich etwa die Prozess-ID oder eine Zufallszahl an. Mehrere Versuche müssen aber in jedem Falle einkalkuliert werden.

Der erste Durchgang

lscan.h

```
#ifndef LSCAN_H
#define LSCAN_H

#include "lposlist.h"

int scan_lines(int fd, int out, lposlist* list);
#endif
```

- Die Funktion *scan_lines*
  - liest die gesamte Eingabe aus *fd*,
  - kopiert sie nach *out*, falls *out* nicht-negativ ist, und
  - legt die gefundenen Zeilen unter *list* ab.

Der erste Durchgang

lscan.c

```
#include <sys/stat.h>
#include "lposlist.h"
#include "lscan.h"

static off_t get_blocksize(int fd) {
   struct stat statbuf;
   if (fstat(fd, &statbuf) < 0) return 0;
   return statbuf.st_blksize;
}

int scan_lines(int fd, int out, lposlist* list) {
   off_t blocksize;
   if (out >= 0) {
      blocksize = get_blocksize(out);
   } else {
      blocksize = get_blocksize(fd);
   }
   if (!blocksize) return 0;

   char buf[blocksize];
   // ...
}
```

Der erste Durchgang

lscan.c

```
static off_t get_blocksize(int fd) {
   struct stat statbuf;
   if (fstat(fd, &statbuf) < 0) return 0;
   return statbuf.st_blksize;
}
```

- Bei regulären Dateien lässt sich über das Feld *st_blksize* die vom zugehörigen Dateisystem bevorzugte Blockgrösse ermitteln.
- Diese liegt typischerweise bei 4096 oder 8192 Bytes.

Der erste Durchgang

lscan.c

```
off_t pos = 0;
ssize_t llen = 0; /* length of current line */
off_t blockpos = pos; /* keep track of current position */
ssize_t nbytes;
while ((nbytes = read(fd, buf, blocksize)) > 0) {
   if (out >= 0) {
      ssize_t written = write(out, buf, nbytes);
      if (written < nbytes) return 0;
   }
   for (char* cp = buf; cp < buf + nbytes; ++cp) {
      if (*cp == '\n') {
         add_lpos(list, pos, llen);
         pos = blockpos + cp - buf + 1;
         llen = 0;
      } else {
         ++llen;
      }
   }
   blockpos += nbytes;
}
if (nbytes < 0) return 0;
if (llen) add_lpos(list, pos, llen);
return 1;
```

Das Hauptprogramm

shuffle.c

```
#include <errno.h>
#include <stdbool.h>
#include <stdlib.h>
#include <stralloc.h>
#include <string.h>
#include "lscan.h"
#include "lposlist.h"
#include "rgen.h"
#include "tmpfile.h"

char* cmdname;
static void memerr() { /* ... */ }
static void die(char* filename, char* message) { /* ... */ }
static int select_line(int noflines) { /* ... */ }
static void print_line(int fd, off_t pos, ssize_t len) { /* ... */ }
static bool seekable(int fd) { /* ... */ }

int main(int argc, char* argv[]) { /* ... */ }
```

Das Hauptprogramm

shuffle.c

```
static bool seekable(int fd) {
   return lseek(fd, 0, SEEK_CUR) >= 0;
}

int main(int argc, char* argv[]) {
   cmdname = argv[0];
   int fd = 0;
   int out = -1;
   if (!seekable(fd)) {
      out = get_tmpfile();
      if (out < 0) die("tmpfile", 0);
   }
   lposlist list = {0};
   if (!scan_lines(fd, out, &list)) die("scan_lines", 0);
   if (out >= 0) fd = out;
   while (list.length > 0) {
      int i = select_line(list.length);
      print_line(fd, list.line[i].pos, list.line[i].len);
      int j = list.length - 1;
      if (i != j) list.line[i] = list.line[j];
      --list.length;
   }
}
```

Das Hauptprogramm

shuffle.c

```
static int select_line(int noflines) {
   int selected;
   if (!get_rval(&selected)) die("get_rval", 0);
   if (selected < 0) {
      selected = -(selected+1);
   }
   selected %= noflines;
   return selected;
}
```

- Zu beachten ist hier, dass die Werte von *get_rval* negativ sein können und der Modulo-Operator in C nicht genügt, um den Wert in den Bereich $[0, \text{noflines} - 1)$ zu bringen.

Das Hauptprogramm

shuffle.c

```
static void print_line(int fd, off_t pos, ssize_t len) {
   char buf[len+1];
   ssize_t copied = 0;
   ssize_t nbytes;
   if (len > 0) {
      if (lseek(fd, pos, SEEK_SET) < 0) die("lseek", 0);
      while (copied < len &&
            (nbytes = read(fd, buf + copied, len - copied)) > 0) {
         copied += nbytes;
      }
      if (nbytes < 0) die("read", 0);
      if (nbytes == 0) die("read", "unexpected end of file");
   }
   buf[len++] = '\n';
   copied = 0;
   while (copied < len &&
         (nbytes = write(1, buf + copied, len - copied)) > 0) {
      copied += nbytes;
   }
   if (nbytes < 0) die("write", 0);
}
```

Das Positionieren in einer Datei

shuffle.c

```
if (lseek(fd, pos, SEEK_SET) < 0) die("lseek", 0);
```

- Der Systemaufruf *lseek* hat drei Parameter: Den Dateideskriptor, eine relative Position und die Angabe wozu die Position relativ ist.
- Für den dritten Parameter gibt es folgende Varianten:

  SEEK_SET: Die Positionsangabe wird relativ zur Position 0, also absolut interpretiert.

  SEEK_CUR: Die Positionsangabe wird relativ zur aktuellen Dateiposition interpretiert.

  SEEK_END: Die Positionsangabe wird relativ zum Ende der Datei interpretiert.
- Die Funktion *lseek* liefert entweder einen Fehler zurück (-1) oder die aktuelle Position nach der durchgeführten Operation.