



Besser Programmieren

Erfolgreich Klippen umschiffen

Texteditor angeworfen, Programm heruntergeladet, übersetzt, fertig. So einfach funktioniert das nicht, wenn in C++ entwickelt wird. Eines der Hauptprobleme ist dabei C++ selbst. Die Sprache bietet nicht nur eine Unmenge an Sprachfeatures, sondern mindestens ebenso viele Fallstricke.

THOMAS WÖLFER



#define vermeiden

Dies ist einer der häufigsten Ratschläge, die C Programmierer von C++ Programmierern erhalten. Es gibt jede Men-

ge guter Gründe weshalb man #define vermeiden sollte, letztendlich kommen alle auf den gleichen Hauptgrund zurück: #define ist nicht wirklich ein Teil von C++ (oder von C) - zumindest nicht, was den Compiler betrifft, denn der C/C++ Compiler sieht ein per #define definiertes Symbol nie unter seinem symbolischen Namen. Hierzu ein Beispiel: Angenommen man verwendet das Präprozessor-Statement

```
#define PI 4.0
```

in einem Header-File, um später in den C/C++ Dateien das Symbol PI verwenden zu können. Das ist gut und schön - und man kann das auch tun - nur leider sieht der Compiler das Symbol PI nie unter diesem Namen. Statt dessen sieht er nur den Wert "4.0", denn das ist, was im Quelltext nach dem Präprozessorlauf vor dem Kompilieren übrig bleibt. Als Resultat hat man später ein Problem, wenn man sich innerhalb des Debuggers befindet. Auch dieser kennt das Symbol "PI" nicht, denn schließlich wurde dieses zur Übersetzungszeit nie verwendet.

Hier noch ein zweites Beispiel für eine häufige Benutzung des Präprozessors, die man in C++ besser anders macht:

```
#define MAX(a,b) ((a) > (b) ? (a) : (b))
```

Hier handelt es sich um eine typisches "MAX" Makro, mit dem der maximale von zwei Werten ermittelt werden kann. Praktisch an diesem Makro: Man kann es mit jedem beliebigen Datentyp füttern, es funktioniert immer. Zumindest dann, wenn identische Datentypen verwendet werden. Dummerweise handelt es sich hier aber um ein Makro. Das bedeutet: Erneut kommt der Compiler nicht zum Einsatz, sondern der Präprozessor, und das mit unschönen Folgen. Schreibt man unter Verwendung der angegebenen Makros die folgenden Ausdrücke:

```
int a = 1;
int b = 0;
int c;
c = MAX( a++, b);
```

Weil es sich bei MAX() um ein Makro handelt, sieht der Compiler zur Übersetzungszeit das folgende Statement:

```
c = ((a++) > (b) ? (a++) ? (b))
```

Eine dumme Sache, denn "a" wird hier gleich zweimal inkrementiert. Und das ist mit Sicherheit nicht, was der Programmierer eigentlich beabsichtigte. Besser umgeht man solch ein Problem mit einer inline-Funktion, die typbehaftet ist:

```
inline int MAX( int a, int b) { re-
turn a>b ? a : b; }
```

Damit können solche Probleme nicht auftreten. Allerdings leistet diese inline-Variante nicht so viel wie das ursprüngliche MAX-Makro. Dieses konnte man mit beliebigen Datentypen benutzen, während die inline-Funktion nur für Integer nutzbar ist. Abhilfe

QUICK INDEX

- #define vermeiden
- Speicher richtig allozieren
- Copy – Konstruktor und Zuweisung
- Basisklassen brauchen virtuelle Destruktoren
- Operator "=" ist nicht void
- Funktioniert "=" bei Selbstzuweisung
- Parameter "By reference" statt "By value"
- Überladen bei Zeigern und Integern
- Mehrfaches #include vermeiden



schafft ein C++ Template. Das folgende Template kann an allen Stellen benutzt werden, an denen auch das MAX() Makro zum Einsatz kommen könnte. Allerdings typensicher und ohne Nebeneffekte.

```
template <class T>
inline T& MAX( T&a, T&b) { return
a>b ? a : b; }
```

Ordnung halten



■ Speicher richtig allozieren und freigeben

C++ kommt mit einem eigenen Konstruktor zum Anfordern und Freigeben von Speicher: new und delete. Diese beiden Operatoren sollte man auf jeden Fall verwenden - und nicht etwa die malloc() / free() Funktionsaufrufe aus der C-Runtime Bibliothek. Diese stehen zwar prinzipiell zur Verfügung, es ist aber keine gute Idee sie zu verwenden. Der Grund dafür ist einfach: Malloc() und free() sind C-Funktionen, und als solche wissen sie nichts über Konstruktoren und Destruktoren. Wird also für ein Objekt per malloc() Speicher angefordert, wird die Instanz des Objektes nicht richtig initialisiert, denn der Konstruktor des Objektes wird nicht aufgerufen: Malloc belegt einfach nur die angeforderte Größe an Speicher auf dem Heap. Das gleiche gilt für free(). Wird ein Speicherblock per free() freigegeben, passiert genau dies und sonst nichts. Der Destruktor des Objektes wird nicht aufgerufen und alle dort durchgeführten Aufräumarbeiten bleiben unerledigt. Das schafft nicht nur unschöne Speicher-Löcher, sondern auch sonst alle möglichen Resource-Leaks und andere unerwartete Seiteneffekte.

AUF WIEDERSEHEN

```
class Base {
    Base() {}
    ~Base( printf("Und Tschuess!"); }
};

class Derived : public Base{
    Derived() {}
    ~Derived( printf("Tschuess aus Derived!"); }
};
```

In diesem Zusammenhang ein Hinweis: Enthält eine Klasse Zeiger als Member, so müssen diese im Destruktor der Klasse mit delete zerstört werden. Anders als vielfach angenommen, werden nicht alle Destrukturen aller Member automatisch aufgerufen, sondern nur die der Member, die keine Zeiger sind. Das ist sinnvoll, woher soll der C++ Compiler schließlich wissen, ob der Member-Pointer auf eine Kopie eines Objektes zeigt oder mehrere Pointer mehrerer Klassen-Instanzen auf das gleiche Objekt zeigen? Für das Zerstören von Objekten, die in einer Klassen-Instanz per Member-Pointer erreichbar sind, ist die Klasse selbst zuständig.

Hier gilt es die normalen Regeln zu beachten. Nicht jeder Zeiger zeigt auf ein Objekt das unbedingt zerstört werden muss!

Klassen vollständig ausstatten



■ Copy-Konstruktor und Zuweisungs-Operator

Wann immer man eine Klasse schreibt in der Speicher dynamisch alloziert wird, muss man die Klasse mit einem Copy-Konstruktor und einem Zuweisungs-Operator ausstatten. Warum klärt das folgende Beispiel, das zu der XString() Klasse aus einigen anderen Beiträgen in diesem Sonderheft passt. Die XString-Klasse soll dabei eine "typische" String-Klasse sein:

Die Klasse hat einen Konstruktor und einen Destruktor, aber keinen Zuweisungsoperator und keinen Copy-Konstruktor. Im folgenden sieht man recht schnell, welche Probleme dies bereitet:

```
XString a("C++ hat");
XString b("Fallstricke");
b = a;
```

IE STRING-KLASSE

```
Class XString {
private:
    char* pData;
public:
    XString( const char* p = 0);
    ~XString();
};
XString::XString( const char* p)
{
    if( p) {
        m_pData = new char[ strlen( p) + 1];
        strcpy( m_pData, p);
    }
    else {
        m_pData = new char[1];
        *m_pData = '\0';
    }
}
XString::~XString() { delete[] m_pData; }
```

Nachdem die beiden Konstruktoren durchgelaufen sind, hat sowohl die Instanz "a" als auch die Instanz "b" der Klasse Speicher alloziert - jeweils für den darin gespeicherten Text. In der dritten Zeile wird eine Zuweisung durchgeführt. Nachdem die Klasse aber keinen Zuweisungs-Operator definiert hat, wird der "normale" Web von C++ verwendet, die Zuweisung kopiert die Member bitweise. Das hat unschöne Auswirkungen, denn nach der Zuweisung ist der ursprünglich von "b" allozierte Speicher ein Speicherleck. Es zeigt kein Zeiger mehr darauf, obwohl der Speicher nie freigegeben wurde. Außerdem zeigt m_pData in "b" auf den gleichen Speicherbereich wie m_pData in "a": Mit Sicherheit nicht das, was der Programmierer beabsichtigte.

Ein ähnliches Problem tritt auf, wenn der Zuweisungs-Operator ins Spiel kommt. Angenommen man verwendet bei der gleichen Klasse den folgenden Ausdruck:

```
XString a("Hello World");
XString b = a;
```

Hier tritt das gleiche Problem auf: Da die Klasse keinen Zuweisungs-Operator definiert hat, behandelt der Compiler die Zuweisung genauso wie zuvor den Kopiervorgang. Die Member werden bitweise kopiert und erneut zeigt m_pData von "b" auf die Daten aus "a". Nun mag das vielleicht in einer Implementierung Sinn machen, in diesem Fall ist aber zu beachten, dass der Destruktor der XString() - Klasse den Operator delete verwendet, um m_pData freizugeben. Nach der Zuweisung wird delete zweimal mit den gleichen Daten aufgerufen. Einmal im Destruktor von "a" und einmal in "b".



SELBST?

```
void XString::operator=( const char* p)
{
    m_pData = new char[ strlen( p) + 1];
    // etc. pp -
}
```

SELBST!

```
XString
XString::operator=( const char*
p)
{
    // hier kommt der echte Code
    return *this;
}
```

Spätestens hier tritt also ein unerwarteter Nebeneffekt auf.

Korrekt verabschieden



■ Basisklassen brauchen virtuelle Destruktoren

Angenommen man hat eine Basisklasse und eine abgeleitete Klasse und beide sollen sich in Ihren Destruktoren mit einer kurzen Meldung verabschieden:

Nun sollen diese Klassen verwendet werden - und nachdem C++ praktischerweise Zeiger zu Instanzen von abgeleiteten Klassen in Zeigern auf Basisklassen verwalten kann, ist folgender Code völlig legal - und auch in vielen Fällen sinnvoll:

```
Base* pBase = new Derived;
// hier passiert etwas
// - was ist egal
delete pBase;
```

Was passiert, wenn man die Ausdrücke in ein Beispielprogramm einbettet, übersetzt und ausführt, ist ärgerlich. Am Bildschirm wird nur der Text "Und Tschuess" angezeigt. Das erwartete "Tschuess aus Derived" erscheint einfach nicht.

Der Grund dafür ist einfach. An der Stelle, an der per "delete" das Objekt zerstört werden soll, auf das pBase zeigt, muss der Compiler entscheiden, auf was für ein Objekt der Zeiger tatsächlich zeigt. Im Gegensatz zum Programmierer weiß der Compiler leider nicht, dass

der pBase Zeiger tatsächlich auf ein Derived Objekt zeigt. Resultat: nur der Destruktor von der "Base" Klasse wird aufgerufen - und das ist nicht das gewünschte Verhalten.

Die Lösung ist einfach: Man muss den Destruktor der "Base" Klasse "virtual" machen - dann geht's so, wie man sich das vorstellen würde. Allerdings ein Wort zur Vorsicht: Man ist leicht verleitet nun einfach alle Destrukturen aller Klasse grundsätzlich als "virtual" zu deklarieren, doch das lässt man besser bleiben. Die Gründe dafür sind vielschichtig. Eine Auflistung würde den Rahmen dieses Artikels sprengen. Merken Sie sich daher einfach die Daumenregel, dass die Destrukturen von Basisklassen "virtual" sein müssen und die von anderen Klassen es nicht sein sollten.

Selbstbewußtsein ist wichtig



■ Operator"=" ist nicht void !

Es ist ein weit verbreiteter Irrtum, dass der Zuweisungs-Operator (Operator=) "void" ist. Der Grund für diesen Irrtum ist leicht gefunden, denn was man mit dem Operator= erreichen möchte, ist die Zulässigkeit von folgendem Ausdruck:

```
XString a;
a = "Hallo C++";
```

Auf den ersten Blick sieht es eindeutig so aus, als wäre der Operator= auch völlig ohne Rückgabewert prima zu implementieren:

Hat man seine Klassen - und zwar zusammen mit dem Operator= für die einzelnen davon - implementiert, wird man über lang oder kurz folgenden Ausdruck

hinschreiben wollen - denn für die eingebauten Klassen wie "int" ist es legal:

```
XString a,b,c;
a = b = c = "Hello C++";
```

Das geht jedoch schief. Wie man in diesem Beispiel sehen kann, muss das Resultat einer Zuweisung eine Referenz auf den Wert der Zuweisung sein - ansonsten ist die verkettete Zuweisung nicht möglich. Lösung: Der operator= muß einen Return-Wert haben, und dieser Returnwert ist eine Referenz auf *this.

Begehen Sie keinen Selbstmord



■ Achtung: Funktioniert bei Selbstzuweisungen

Um diesen Fehler zu vermeiden, muss man zunächst einmal wissen, was eine Selbstzuweisung eigentlich ist. Das ist zum Glück einfach darzustellen - eine Selbstzuweisung sieht im einfachsten Fall wie folgt aus;

```
XString a;
a = a;
```

Zugegebenermaßen ist dieses Beispiel nicht sonderlich einleuchtend - allerdings ist es völlig legitimer Code und daher sollte er auch funktionieren. Mit ein wenig Aufwand ist es einfach, ein überzeugenderes Beispiel zu finden:

```
a = b;
```

Zugegeben: Der Aufwand der betrieben werden muss, liegt beim Leser - denn

ELBAUSLÖSCHUNG

```
// .... code ..
delete [] m_pData;
m_pData = new char[ strlen( rCopy.m_pData) + 1] ;
strcpy( m_pData, rCopy.m_pData);
// ... mehr code....
```

SELBSTERHALTUNG

```
// zu Beginn des Operator=
XString& XString::operator=( const XString& rOther)
if( this == &rOther)
    return *this;
```



dieser muss sich nur vorstellen das a eine ganz normale Variable ist, während b ein Alias für "a" darstellt: Zum Beispiel eine Referenz. Schon ist das Ganze durchaus plausibel und wird mit Sicherheit in der Praxis vorkommen – doch wo ist hier der Fallstrick?

Gute Frage – einfache Antwort: Der Zuweisungs-Operator muss sich darum kümmern, dass vor der Zuweisung der neuen Daten die vorhandenen Ressourcen korrekt freigegeben werden. Er muss also etwas in der folgenden Art tun: Handelt es sich um eine Selbstzuweisung, so tritt an dieser Stelle sofort das Problem ans Licht. Die erste ausformulierte Zeile löscht den Daten-Buffer. Nachdem es sich aber um eine Selbstzuweisung handelt, ist dies der gleiche Puffer, aus dem in den nächsten Zeilen die Daten kopiert werden sollen. Dumme Sache: Das Objekt zerstört sich zunächst selbst und kopiert dann die defekten Daten auch noch weiter.

Man kann man verschiedene Dinge tun, um solche Probleme zu vermeiden. So ist es zum Beispiel möglich auf gleiche Inhalte oder gleiche Zeiger zu überprüfen, bevor die Zuweisung wirklich durchgeführt wird: Welchen Weg man beschreitet ist dabei von den Details der Implementierung abhängig. Eine der Möglichkeiten sieht folgendermaßen aus:

Uraltes Problem immer aktuell



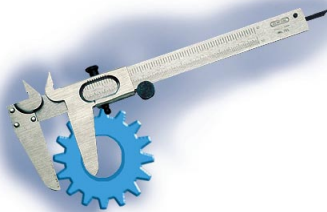
■ Parameter – "By reference" statt "By value"

Ähnlich wie in C ist die "Default" Methode der Parameter-Übergabe in C++ "by value". Das bedeutet aber, dass bei jedem Funktionsaufruf von allen Parametern Kopien angelegt werden müssen. Das ist zwar bei eingebauten Datentypen wie einem Integer nicht weiter schlimm, bei komplexen Klassen hingegen schon: Angenommen eine Klasse verwendet dynamischen Speicher, dann hat der Copy-Konstruktor mit Sicherheit die Aufgabe neuen Speicher zu al-

lozieren und "alten" freizugeben. So kann der Aufruf einer Funktion im schlimmsten Fall zum Pagen auf die Festplatte führen. Eine einfache Regel für C++ ist daher die: Wenn ein Parameter übergeben wird und wenn es sich bei dem Parameter um eine Instanz einer Klasse handelt, verwendet man entweder eine konstante Referenz – wenn das Objekt nicht verändert werden soll – oder einen Zeiger, wenn es doch verändert werden soll.

```
// Konstante Referenz
void FooBar( const & rObjekt);
```

Weniger ist mehr



■ Überladen – besser nicht mit Zeigern und Integer

Normalerweise meckert der C++ Compiler ja immer mehr Dinge als 'ambiguous' an als man sich wünschen würde – dummerweise gibt es aber außerdem noch einen Spezialfall, bei dem das genaue Gegenteil der Fall ist: Auf den ersten Blick hält der Programmierer die folgenden beiden Funktionen für eine unklare Art und Weise des Überladens, der Compiler hingegen nicht:

```
void foobar( int v);
void foobar( char* pv);
```

Die Frage die sich bei diesen beiden Funktionen stellt ist die: Wenn man im Quellcode den folgenden Aufruf verwendet:

```
foobar( 0);
```

- welche der beiden Funktionen wird dann aufgerufen? Die Antwort lautet: foobar(int). Der Grund dafür ist einfach – auch wenn man auf den ersten Blick glaubt, das foobar(0) nicht ohne weiteres aufgelöst werden kann, so ist bei näherem Hinsehen die Auflösung doch immer eindeutig.

,0' ist eine Integer-Konstante – also ein 'int' – und deshalb wird foobar(int) auch aufgerufen – das ,0' auch als Null-Zeiger verwendet werden kann (und wird) hat darauf keine Einfluß. Eine einfache Lösung für dieses Problem gibt es nicht.

Einfach bleiben



■ Mehrfaches #includieren vermeiden

Ein typisches Problem bei C/C++ wird durch den Präprozessor hervorgerufen: Das doppelte inkludieren von Header-Dateien. Mal angenommen es existieren die beiden Header-Dateien ,a.h' und ,b.h' – sowie die Implementierungs-Datei ,c.cpp'. a.h benötigt nun einige Definitionen aus b.h – und also enthält a.h am Anfang der Datei das Statement

```
#include "b.h"
```

Beim Implementieren von c.cpp hat der Programmierer diesen Umstand natürlich vergessen – und schreibt in c.cpp:

```
#include "a.h"
#include "b.h"
```

Problem: b.h wird nun zweimal inkludiert – einmal indirekt über a.h, das andere mal direkt durch das betreffende #include-Statement.

Daraus können eine ganze Menge Probleme entstehen – nicht zuletzt doppelt definierte Konstante und ähnliches: Diese Art von Problem wird allerdings vom Compiler erkannt und bemängelt, sodaß sich derartige Probleme meist mit ein wenig Nachdenken lösen lassen.

Dieses Problem – und auch das Problem mit den ,doppelten' Konstanten – läßt sich aber einfach und dauerhaft lösen, wenn man sich an ein einfaches Schema hält: Jede Header-Datei definiert ein eindeutiges Symbol, und nur wenn dieses noch nicht definiert ist, wird der Inhalt der Datei tatsächlich an den Präprozessor – und damit später an den Compiler – weitergereicht. Klingt kompliziert – ist aber einfach, und sieht in der Praxis wie folgt aus:

```
#ifndef _INC_NAME_DER_DATE
#define _INC_NAME_DER_DATE1
```

```
// hier steht dann der normale Inhalt
```

```
#endif
```

Auf diese Weise ist man immer auf der sicheren Seite.

UR