Übung zu Betriebssystembau

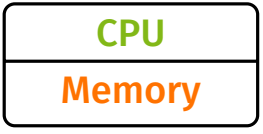
Kontextwechsel

26. November 2024

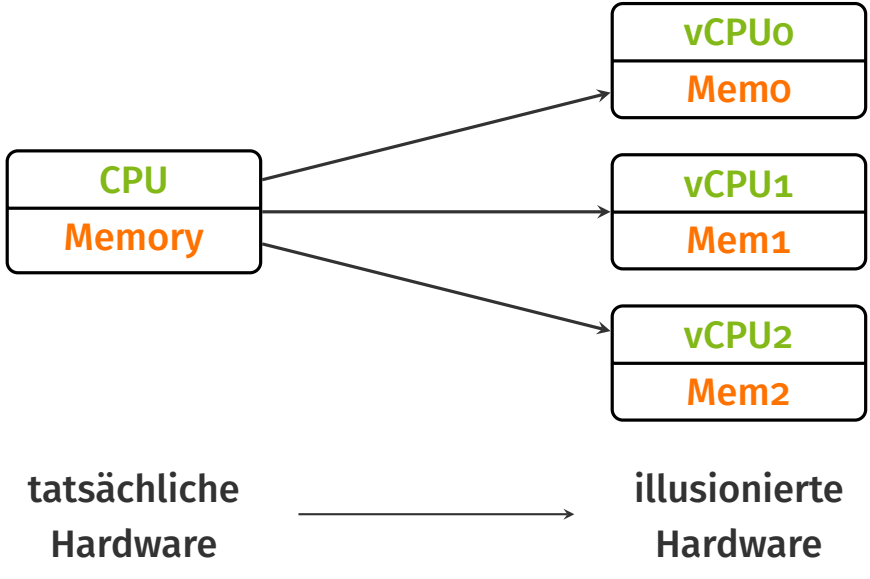
Alexander Krause

Arbeitsgruppe Systemsoftware
Technische Universität Dortmund

(Mit Material vom Lehrstuhl 4 der FAU)



tatsächliche
Hardware


CPU
Memory
vCPU0
Mem0
vCPU1
Mem1
vCPU2
Mem2
tatsächliche Hardware
illusionierte Hardware

- Speicher virtualisieren

- CPU virtualisieren
  - nicht teilbar im Ort
  - aber teilbar in der Zeit

- **Speicher virtualisieren ist einfach:**

```
#define MEMSIZE 100
char Mem0[MEMSIZE];
char Mem1[MEMSIZE];
char Mem2[MEMSIZE];
```

- **CPU virtualisieren**
  - nicht teilbar im Ort
  - aber teilbar in der Zeit

Motivation: mehr Aktivitätsträger als CPUs

```
1  void foo(){
2    int f = 42;
3
4    while (f--){
5      kout << "foo"
6           << f
7           << endl;
8
9    }
10
11 }
```

```
1  void bar(){
2    int b = 23;
3
4    while (b--){
5      kout << "bar"
6           << b
7           << endl;
8
9    }
10
11 }
```

Einseitiger Aufruf

```
1  void foo(){
2    int f = 42;
3
4    while (f--){
5      kout << "foo"
6           << f
7           << endl;
8
9    }
10   bar();
11 }
```

```
1  void bar(){
2    int b = 23;
3
4    while (b--){
5      kout << "bar"
6           << b
7           << endl;
8
9    }
10
11 }
```

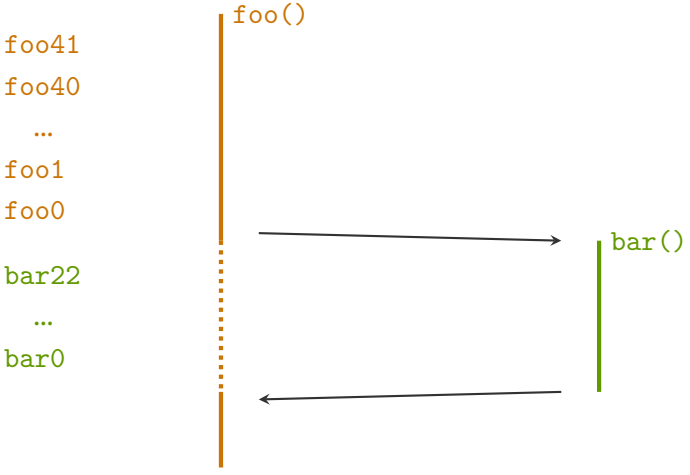
Einseitiger Aufruf

```
foo41
foo40
  ...
foo1
foo0
```

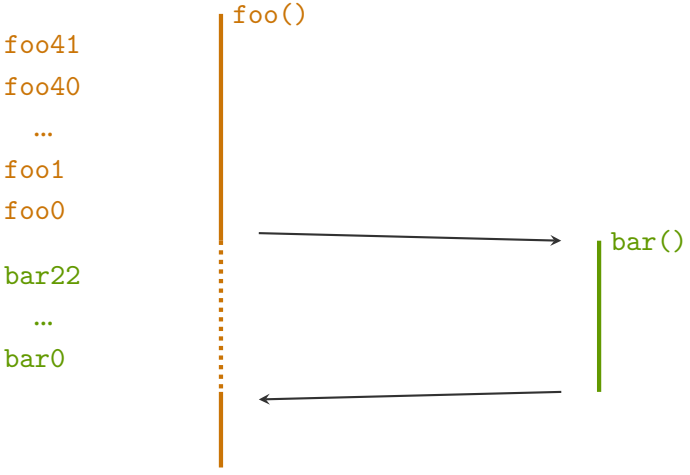
Einseitiger Aufruf

```
foo41
foo40
  ...
foo1
foo0

bar22
  ...
bar0
```

Einseitiger Aufruf



Einseitiger Aufruf



nicht parallel

Gegenseitiger Aufruf

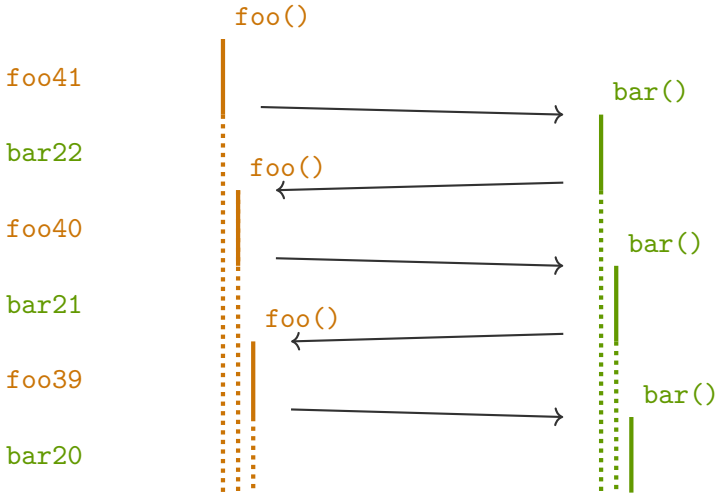
```
1  void foo(){
2    static int f = 42;
3
4    while (f--){
5      kout << "foo"
6           << f
7           << endl;
8      bar();
9    }
10
11 }
```

```
1  void bar(){
2    static int b = 23;
3
4    while (b--){
5      kout << "bar"
6           << b
7           << endl;
8      foo();
9    }
10
11 }
```

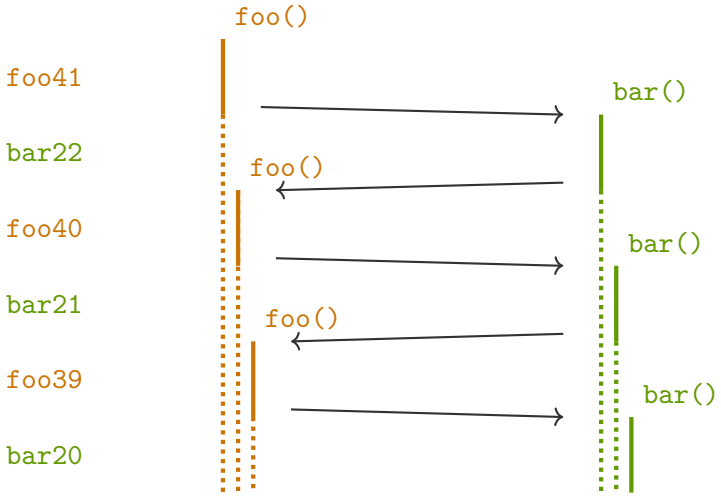
Gegenseitiger Aufruf

```
foo41

bar22

foo40

bar21

foo39

bar20
```

Gegenseitiger Aufruf



Gegenseitiger Aufruf



hoher Speicherverbrauch & (ggf.) Endlosrekursion

Umschaltung

Umschaltung

Kontrollflusszustand sichern & laden

Umschaltung

Kontrollflusszustand sichern & laden

- Stack
- Register

Umschaltung

Kontrollflusszustand sichern & laden

- Stack
- Register

} Kontext

Umschaltung

Kontrollflusszustand sichern & laden

- Stack
- Register

} Kontext

- Umschaltefunktion

Umschaltung

Kontrollflusszustand sichern & laden

- Stack
- Register

} Kontext

- Umschaltefunktion

Umschaltung

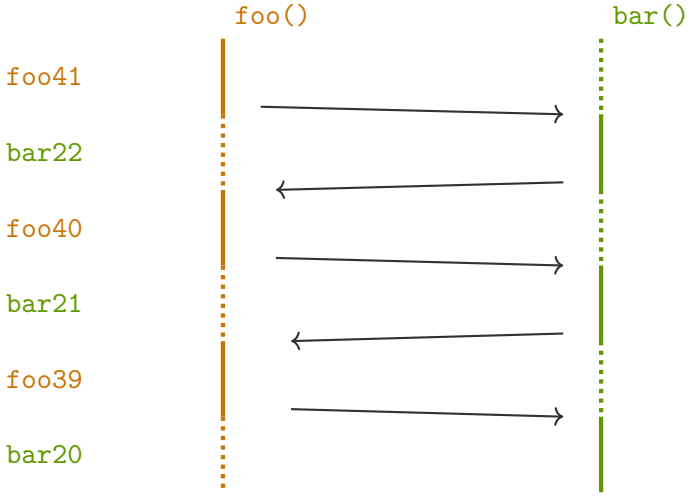
```
1  void foo(){
2    int f = 42;
3
4    while (f--){
5      kout << "foo"
6           << f
7           << endl;
8      context_switch(
9          &stack_foo,
10         &stack_bar
11       );
12   }
13 }
```

```
1  void bar(){
2    int b = 23;
3
4    while (b--){
5      kout << "bar"
6           << b
7           << endl;
8      context_switch(
9          &stack_bar,
10         &stack_foo
11       );
12   }
13 }
```

Umschaltung

```
foo41

bar22

foo40

bar21

foo39

bar20
```

Umschaltung



Genau was wir wollen.

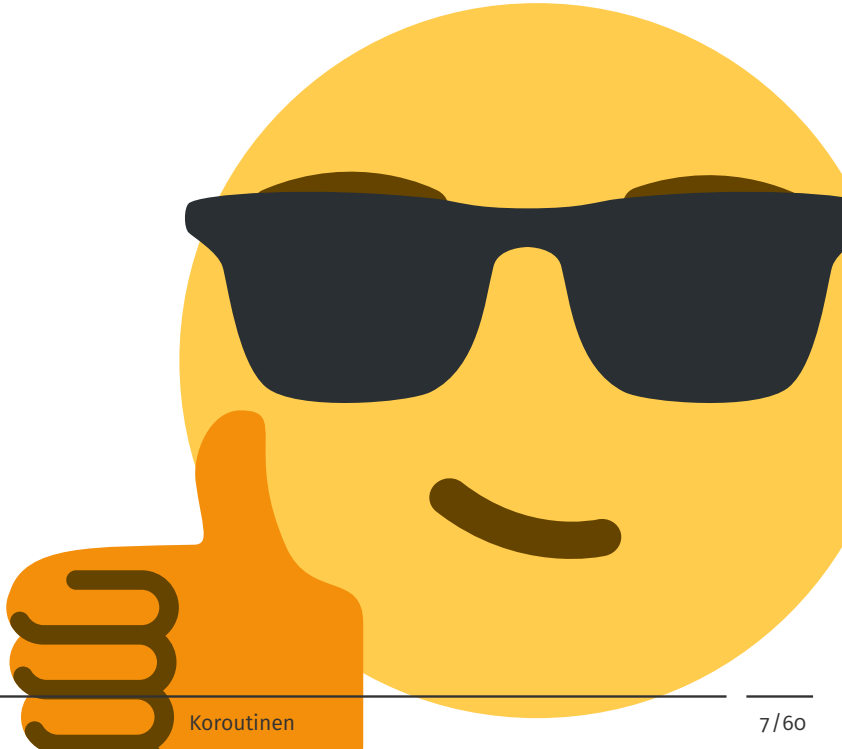


Bild: twemoji (modifiziert)

Ablauf einer Übersetzung

```
1  #include "user/app1/appl.h"
2  #include "device/textstream.h"
3  #include "interrupt/guarded.h"
4  #include "machine/core.h"
5
6  extern TextStream kout;
7
8  void Application::action() {
9      unsigned core = Core::getID();
10     for (unsigned n = 0; ; ++n) {
11         Guarded section;
12         kout.setPos(0, id);
13         kout << n;
14         kout.flush();
15     }
16 }
```

Ablauf einer Übersetzung

```
1  #include "user/app1/appl.h"
2  #include "device/textstream.h"
3  #include "interrupt/guarded.h"
4  #include "machine/core.h"
5
6  extern TextStream kout;
7
8  void Application::action() {
9      unsigned core = Core::getID();
10     for (unsigned n = 0; ; ++n) {
11         Guarded section;
12         kout.setPos(0, id);
13         kout << n;
14         kout.flush();
15     }
16 }
```

höhere Programmiersprache
(3. Generation)

Ablauf einer Übersetzung

```
1  #include "user/app1/appl.h"
2  #include "device/textstream.h"
3  #include "interrupt/guarded.h"
4  #include "machine/core.h"
5
6  extern TextStream kout;
7
8  void Application::action() {
9      unsigned core = Core::getID();
10     for (unsigned n = 0; ; ++n) {
11         Guarded section;
12         kout.setPos(0, id);
13         kout << n;
14         kout.flush();
15     }
16 }
```

höhere Programmiersprache
(3. Generation)

Ablauf einer Übersetzung

```
1  #include "user/app1/appl.h"
2  #include "device/textstream.h"
3  #include "interrupt/guarded.h"
4  #include "machine/core.h"
5
6  extern TextStream kout;
7
8  void Application::action() {
9      unsigned core = Core::getID();
10     for (unsigned n = 0; ; ++n) {
11         Guarded section;
12         kout.setPos(0, id);
13         kout << n;
14         kout.flush();
15     }
16 }
```

```
1
2
3
4
5
6
7     f3 0f 1e fa 55 53 31 db
8     48 83 ec 08 e8 4f d1 ff
9     ff 89 c5 0f 1f 44 00 00
10    e8 e3 c3 ff ff 89 ea 31
11    f6 bf 84 45 02 01 e8 e5
12    d2 ff ff 89 de bf 20 45
13    02 01 83 c3 01 e8 c6 fd
14    ff ff bf 20 45 02 01 e8
15    1c bf ff ff e8 37 c4 ff
16    ff eb cd
```

höhere Programmiersprache
(3. Generation)

Ablauf einer Übersetzung

```
1  #include "user/app1/appl.h"
2  #include "device/textstream.h"
3  #include "interrupt/guarded.h"
4  #include "machine/core.h"
5
6  extern TextStream kout;
7
8  void Application::action() {
9      unsigned core = Core::getID();
10     for (unsigned n = 0; ; ++n) {
11         Guarded section;
12         kout.setPos(0, id);
13         kout << n;
14         kout.flush();
15     }
16 }
```

höhere Programmiersprache
(3. Generation)

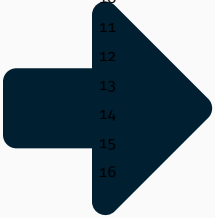
```
1
2
3
4
5
6
7   f3 0f 1e fa 55 53 31 db
8   48 83 ec 08 e8 4f d1 ff
9   ff 89 c5 0f 1f 44 00 00
10  e8 e3 c3 ff ff 89 ea 31
11  f6 bf 84 45 02 01 e8 e5
12  d2 ff ff 89 de bf 20 45
13  02 01 83 c3 01 e8 c6 fd
14  ff ff bf 20 45 02 01 e8
15  1c bf ff ff e8 37 c4 ff
16  ff eb cd
```

Maschinensprache
(1. Generation)

Ablauf einer Übersetzung

```
1  #include "user/app1/appl.h"
2  #include "device/textstream.h"
3  #include "interrupt/guarded.h"
4  #include "machine/core.h"
5
6  extern TextStream kout;
7
8  void Application::action() {
9      unsigned core = Core::getID();
10     for (unsigned n = 0; ; ++n) {
11         Guarded section;
12         kout.setPos(0, id);
13         kout << n;
14         kout.flush();
15     }
16 }
```

höhere Programmiersprache
(3. Generation)



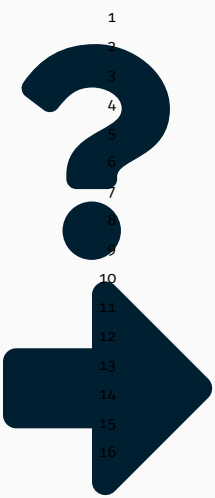
```
1
2
3
4
5
6
7   f3 0f 1e fa 55 53 31 db
8   48 83 ec 08 e8 4f d1 ff
9   ff 89 c5 0f 1f 44 00 00
10  e8 e3 c3 ff ff 89 ea 31
11  f6 bf 84 45 02 01 e8 e5
12  d2 ff ff 89 de bf 20 45
13  02 01 83 c3 01 e8 c6 fd
14  ff ff bf 20 45 02 01 e8
15  1c bf ff ff e8 37 c4 ff
16  ff eb cd
```

Maschinensprache
(1. Generation)

Ablauf einer Übersetzung

```
1  #include "user/app1/appl.h"
2  #include "device/textstream.h"
3  #include "interrupt/guarded.h"
4  #include "machine/core.h"
5
6  extern TextStream kout;
7
8  void Application::action() {
9      unsigned core = Core::getID();
10     for (unsigned n = 0; ; ++n) {
11         Guarded section;
12         kout.setPos(0, id);
13         kout << n;
14         kout.flush();
15     }
16 }
```

höhere Programmiersprache
(3. Generation)



```
f3 0f 1e fa 55 53 31 db
48 83 ec 08 e8 4f d1 ff
ff 89 c5 0f 1f 44 00 00
e8 e3 c3 ff ff 89 ea 31
f6 bf 84 45 02 01 e8 e5
d2 ff ff 89 de bf 20 45
02 01 83 c3 01 e8 c6 fd
ff ff bf 20 45 02 01 e8
1c bf ff ff e8 37 c4 ff
ff eb cd
```

Maschinensprache
(1. Generation)

Ablauf einer Übersetzung

```
1  #include "user/app1/appl.h"
2  #include "device/textstream.h"
3  #include "interrupt/guarded.h"
4  #include "machine/core.h"
5
6  extern TextStream kout;
7
8  void Application::action() {
9      unsigned core = Core::getID();
10     for (unsigned n = 0; ; ++n) {
11         Guarded section;
12         kout.setPos(0, id);
13         kout << n;
14         kout.flush();
15     }
16 }
```

Vererbung auflösen

```
1  class TextStream : public OutputStream, public TextWindow {
2    // ...
3
4  } kout;
5
6  void Application::action() {
7      unsigned n = 0;
8      unsigned core;
9      core = Core::getID();
10     while(true) {
11         Guard::enter();
12         kout.setPos(0, id);
13         unsigned i = n
14         n += 1;
15         kout.operator<<(i);
16         kout.flush();
17         Guard::leave();
18     }
19 }
```

Methoden zu Funktionen „umwandeln“

```
1  class TextStream : public OutputStream, public TextWindow {
2    // ...
3
4  } kout;
5
6  void Application::action(Application * this) {
7      unsigned n = 0;
8      unsigned core;
9      core = Core::getID();
10     while(true) {
11         Guard::enter();
12         TextWindow::setPos(&kout, 0, id);
13         unsigned i = n
14         n += 1;
15         OutputStream::operator<<(&kout, i);
16         TextStream::flush(&kout);
17         Guard::leave();
18     }
19 }
```

Objekte zu Basisklassen

```
1  class TextStream  {
2    class OutputStream { ... };
3    class TextWindow { ... };
4  } kout;
5
6  void Application::action(Application * this) {
7      unsigned n = 0;
8      unsigned core;
9      core = Core::getID();
10     while(true) {
11         Guard::enter();
12         TextWindow::setPos(&(kout.TextWindow), 0, id);
13         unsigned i = n
14         n += 1;
15         OutputStream::operator<<(&(kout.OutputStream), i);
16         TextStream::flush(&(kout.OutputStream));
17         Guard::leave();
18     }
19 }
```

Offsets brechnen und einsetzen

```
1  class TextStream  {
2    class OutputStream { ... };  // offset 0
3    class TextWindow { ... };    // offset 64
4  } kout;
5
6  void Application::action(Application * this) {
7      unsigned n = 0;
8      unsigned core;
9      core = Core::getID();
10     while(true) {
11         Guard::enter();
12         TextWindow::setPos(&kout+64, 0, id);
13         unsigned i = n
14         n += 1;
15         OutputStream::operator<<(&kout+0, i);
16         TextStream::flush(&kout+0);
17         Guard::leave();
18     }
19 }
```

name mangling in C++

```
1  class TextStream  {
2    class OutputStream { ... };  // offset 0
3    class TextWindow { ... };    // offset 64
4  } kout;
5
6  void _ZN11Application6actionEv(Application * this) {
7      unsigned n = 0;
8      unsigned core;
9      core = _ZN4Core5getIDEv();
10     while(true) {
11         _ZN5Guard5enterEv();
12         _ZN10TextWindow6setPosEjj(&kout+64, 0, id);
13         unsigned i = n
14         n += 1;
15         _ZN12OutputStreamlsEj(&kout, i);
16         _ZN10TextStream5flushEv(&kout);
17         _ZN5Guard5leaveEv();
18     }
19 }
```

Maschinencode

```
1   void _ZN11Application6actionEv(Application * this) {
2
3
4
5           unsigned n = 0
6           unsigned core;
7           core = _ZN4Core5getIDEv();
8
9           while(true) {
10                  _ZN5Guard5enterEv();
11
12
13
14                  _ZN10TextWindow6setPosEjj(&kout+64, 0, core)
15                  unsigned i = n
16
17                  n += 1;
18                  _ZN12OutputStreamlsEj(&kout, i);
19
20                  _ZN10TextStream5flushEv(&kout);
21                  _ZN5Guard5leaveEv();
22          }
23  }
```

Maschinencode

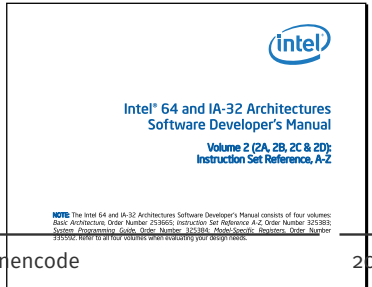
```
1           _ZN11Application6actionEv:
2             endbr64
3             push   rbp
4             push   rbx
5             xor    ebx, ebx
6             sub    rsp, 0x8
7             call   _ZN4Core5getIDEv
8             mov    ebp, eax
9           LOOP:
10            call   _ZN5Guard5enterEv
11            mov    edx, ebp
12            xor    esi, esi
13            mov    edi, kout+64
14            call   _ZN10TextWindow6setPosEjj
15            mov    esi, ebx
16            mov    edi, kout
17            add    ebx, 0x1
18            call   _ZN12OutputStreamlsEj
19            mov    edi, kout
20            call   _ZN10TextStream5flushEv
21            call   _ZN5Guard5leaveEv
22            jmp    LOOP
23
```

Maschinencode

```
1           _ZN11Application6actionEv:
2             endbr64
3             push    rbp
4             push    rbx
5             xor     ebx, ebx
6             sub     rsp, 0x8
7             call    _ZN4Core5getIDEv
8             mov     ebp, eax
9           LOOP:
10            call    _ZN5Guard5enterEv
11            mov     edx, ebp
12            xor     esi, esi
13            mov     edi, kout+64
14            call    _ZN10TextWindow6setPosEjj
15            mov     esi, ebx
16            mov     edi, kout
17            add     ebx, 0x1
18            call    _ZN12OutputStreamlsEj
19            mov     edi, kout
20            call    _ZN10TextStream5flushEv
21            call    _ZN5Guard5leaveEv
22            jmp     LOOP
23
```

Assembler

- Sprache der 2. Gen. (maschinenorientiert)
- **Mnemonics** statt Bytes
- 1:1-Übersetzung
- für x64-Architektur Dokumentation im *Intel-Manual, Vol. 2*



Maschinencode

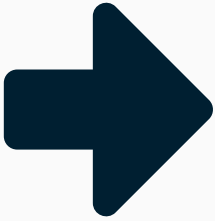
```
0100ba80 <_ZN11Application6actionEv>:
 100ba80:   endbr64
 100ba84:   push   rbp
 100ba85:   push   rbx
 100ba86:   xor    ebx, ebx
 100ba88:   sub    rsp, 0x8
 100ba8c:   call   1008be0 <_ZN4Core5getIDEv>
 100ba91:   mov    ebp, eax
 100ba93:   nop    DWORD PTR [rax+rax*1+0x0]
 100ba98:   call   1007e80 <_ZN5Guard5enterEv>
 100ba9d:   mov    edx, ebp
 100ba9f:   xor    esi, esi
 100baa1:   mov    edi, 0x1024584 <kout+64>
 100baa6:   call   1008d90 <_ZN10TextWindow6setPosEjj>
 100baab:   mov    esi, ebx
 100baad:   mov    edi, 0x1024520 <kout>
 100bab2:   add    ebx, 0x1
 100bab5:   call   100b880 <_ZN12OutputStreamlsEj>
 100baba:   mov    edi, 0x1024520 <kout>
 100babf:   call   10079e0 <_ZN10TextStream5flushEv>
 100bac4:   call   1007f00 <_ZN5Guard5leaveEv>
 100bac9:   jmp    100ba98 <_ZN11Application6actionEv+0x18>
```

Maschinencode

```
0100ba80 <_ZN11Application6actionEv>:
 100ba80:   endbr64
 100ba84:   push   rbp
 100ba85:   push   rbx
 100ba86:   xor    ebx, ebx
 100ba88:   sub    rsp, 0x8
 100ba8c:   call   1008be0
 100ba91:   mov    ebp, eax
 100ba93:   nop    DWORD PTR [rax+rax*1+0x0]
 100ba98:   call   1007e80
 100ba9d:   mov    edx, ebp
 100ba9f:   xor    esi, esi
 100baa1:   mov    edi, 0x1024584
 100baa6:   call   1008d90
 100baab:   mov    esi, ebx
 100baad:   mov    edi, 0x1024520
 100bab2:   add    ebx, 0x1
 100bab5:   call   100b880
 100baba:   mov    edi, 0x1024520
 100babf:   call   10079e0
 100bac4:   call   1007f00
 100bac9:   jmp    100ba98
```

Maschinencode

```
0100ba80 <_ZN11Application6actionEv>:
 100ba80:   endbr64
 100ba84:   push   rbp
 100ba85:   push   rbx
 100ba86:   xor    ebx, ebx
 100ba88:   sub    rsp, 0x8
 100ba8c:   call   1008be0
 100ba91:   mov    ebp, eax
 100ba93:   nop    DWORD PTR [rax+rax*1+0x0]
 100ba98:   call   1007e80
 100ba9d:   mov    edx, ebp
 100ba9f:   xor    esi, esi
 100baa1:   mov    edi, 0x1024584
 100baa6:   call   1008d90
 100baab:   mov    esi, ebx
 100baad:   mov    edi, 0x1024520
 100bab2:   add    ebx, 0x1
 100bab5:   call   100b880
 100baba:   mov    edi, 0x1024520
 100babf:   call   10079e0
 100bac4:   call   1007f00
 100bac9:   jmp    100ba98
```



```

f3 0f 1e fa
55
53
31 db
48 83 ec 08
e8 4f d1 ff ff
89 c5
0f 1f 44 00 00
e8 e3 c3 ff ff
89 ea
31 f6
bf 84 45 02 01
e8 e5 d2 ff ff
89 de
bf 20 45 02 01
83 c3 01
e8 c6 fd ff ff
bf 20 45 02 01
e8 1c bf ff ff
e8 37 c4 ff ff
eb cd
```

Syntaxunterschiede bei x86-Assembler

Intel:

`mov edi, 0x17`

(Ziel, Quelle)

`objdump -M intel`

Standard bei `nasm` (Netwide Assembler)

AT&T:

`mov $0x17, %edi`

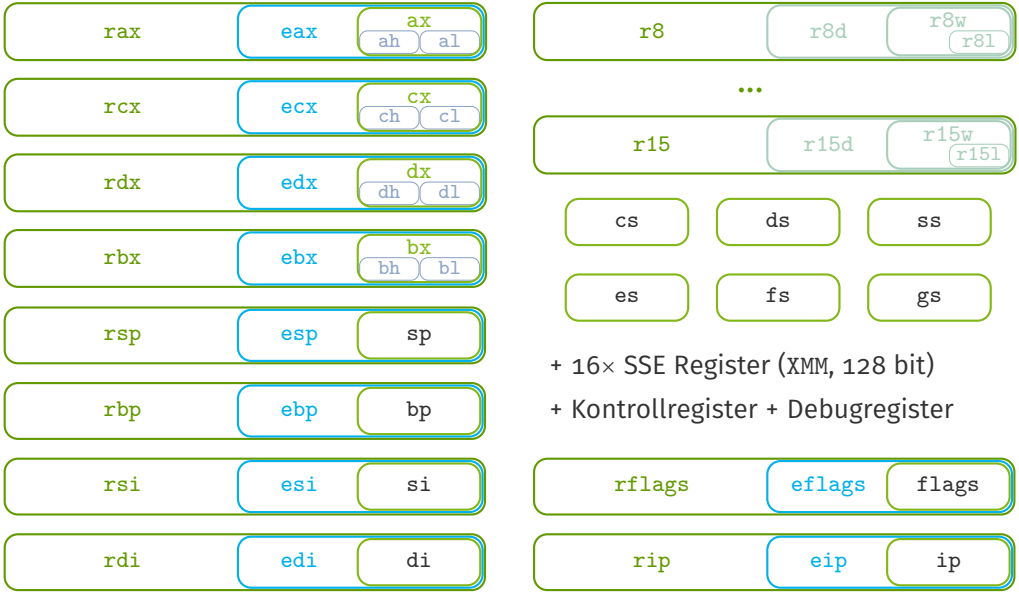
(Quelle, Ziel)

Standard bei `objdump`

und GCC `inline asm`

Berechnungen auf Registern,

Long Mode Register



Assembler

Berechnungen auf Registern, Zugriff mittels `mov`-**Instruktion**

Assembler: `mov`

Berechnungen auf Registern, Zugriff mittels `mov`-**Instruktion**

Register ← Konstante `mov rax, 42`

Assembler: `mov`

Berechnungen auf Registern, Zugriff mittels `mov`-**Instruktion**

Register ← Konstante	`mov rax, 42`
Register ← Register	`mov rax, rcx`

Assembler: `mov`

Berechnungen auf Registern, Zugriff mittels **`mov`-Instruktion**

Register ← Konstante	`mov rax, 42`
Register ← Register	`mov rax, rcx`
Register ↔ Speicher	`mov rax, [0xb8000]`
	`mov [0xb8000 + 4], rax`
	`mov rax, [rcx + rdx]`
	`mov rax, [rsp]`
	~~`mov [0xb8000], [0xb8002]`~~

Besonderheiten bei `mov`

Besonderheiten bei `mov`

`mov eax, XX` `eax` wird gesetzt, obere Hälfte **genullt**

Besonderheiten bei `mov`

`mov eax, XX` `eax` wird gesetzt, obere Hälfte **genullt**

`mov ax, XX` `ax` wird gesetzt, **Rest unverändert**

`mov al, XX` `al` wird gesetzt, **Rest unverändert**

Falls Rest gesetzt werden muss: `movzx`, `movsx`

Details zur Performance bei partiellem Schreiben: → StackOverflow

Operationen mit dem Stack

Stack ← Register `push rax`

Zur Erinnerung – für den Stack auf x64 gilt

- Der Stack „wächst“ von *oben* (hohe Adresse) nach *unten* (niedrige Adresse)
- Der Stackzeiger (`rsp`) zeigt auf das zuletzt hinzugefügte Datum

`push X` verringert zuerst den Wert von `rsp` um 8 Byte und legt dann `X` an die resultierende Adresse

`pop X` liest den Inhalt des Speichers, auf das `rsp` zeigt, in `X` und erhöht anschließend den Wert von `rsp` um 8 Byte.

Zur Erinnerung – für den Stack auf x64 gilt

- Der Stack „wächst“ von *oben* (hohe Adresse) nach *unten* (niedrige Adresse)
- Der Stackzeiger (`rsp`) zeigt auf das zuletzt hinzugefügte Datum

  `push X` verringert zuerst den Wert von `rsp` um 8 Byte und legt dann `X` an die resultierende Adresse

  `pop X` liest den Inhalt des Speichers, auf das `rsp` zeigt, in `X` und erhöht anschließend den Wert von `rsp` um 8 Byte.

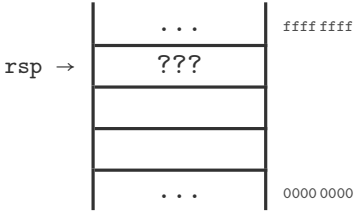
- Bei Funktionsaufrufen muss der Stack an 16 Byte ausgerichtet sein

Operationen mit dem Stack

Stack ← Register `push rax`

Operationen mit dem Stack

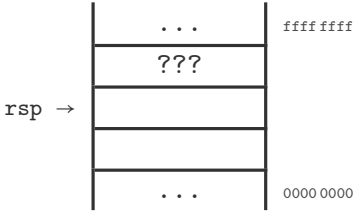
Stack ← Register `push rax`



Operationen mit dem Stack

Stack ← Register

```
push rax
sub rsp, 8
```

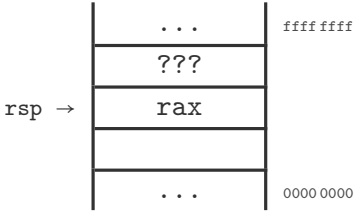


Operationen mit dem Stack

Stack ← Register

```
push rax
```

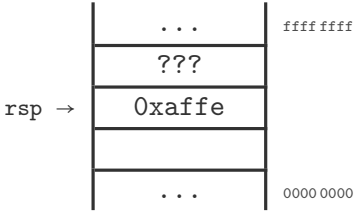
```
sub rsp, 8
mov [rsp], rax
```



Operationen mit dem Stack

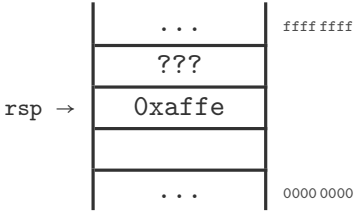
Stack ← Register

```
mov eax, 0xaffe
push rax
sub rsp, 8
mov [rsp], rax
```



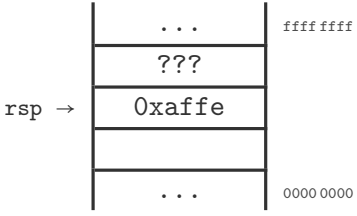
Operationen mit dem Stack

```
                    mov eax, 0xaffe
Stack ← Register    push rax
                    sub rsp, 8
                    mov [rsp], rax
Register ← Stack    pop rcx
```



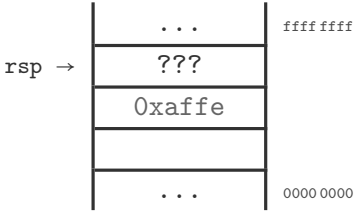
Operationen mit dem Stack

```
                    mov eax, 0xaffe
Stack ← Register    push rax
                    sub rsp, 8
                    mov [rsp], rax
Register ← Stack    pop rcx
                    mov rcx, [rsp]
```



Operationen mit dem Stack

```
                    mov eax, 0xaffe
Stack ← Register    push rax
                    sub rsp, 8
                    mov [rsp], rax
Register ← Stack    pop rcx
                    mov rcx, [rsp]
                    add rsp, 8
```



Mathematische Operationen

Addition/Subtraktion	`add rax, 4`	`x += 4;`
	`sub QWORD [rax], rcx`	`*x -= rcx;`
	`inc rax`	`x++;`
	`dec rax`	`x--;`
Bit-Operationen	`and rax, 0xff`	`x &= 0xff;`
	`or rax, [rcx]`	`x |= *rcx;`
	`xor rax, 0xaa`	`x ^= 0xaa;`
	`not rax`	`x = !x;`
	`neg rcx`	`x = ~x;`
	`shl rax, 1`	`x <<= 1;`
	`shr rax, 1`	`x >>= 1;`

Kontrollfluss-Beeinflussung

Sprungmarke	`LABEL:` `<...>`
Einfache Sprünge	`jmp LABEL`
Bedingte Sprünge	`je/jne/jg/jge/jl/jle/jz LABEL`

Letztere sind abhängig von den Flags im Statusregister (`rflags`)

Kontrollfluss-Beeinflussung

Sprungmarke

```
LABEL:
    <...>
```

Einfache Sprünge

```
jmp LABEL
```

Bedingte Sprünge

```
je/jne/jg/jge/jl/jle/jz LABEL
```

Letztere sind abhängig von den Flags im Statusregister (`rflags`)

Mathematische Operationen und Vergleiche setzen *carry*, *zero* & *sign flag* (Bit 0, 6 & 7 im Statusregister):

Vergleiche

```
cmp rax, rdx
cmp rax, 0x10
≅ sub rax, 0x10
```

(aber `rax` unverändert)

Funktionsaufrufe

Funktionsaufruf

```
call function
```

```
push <next RIP>
jmp function
```

Rückkehr aus Funktion

```
ret
```

```
pop rip
```

Rückkehr aus Interrupt

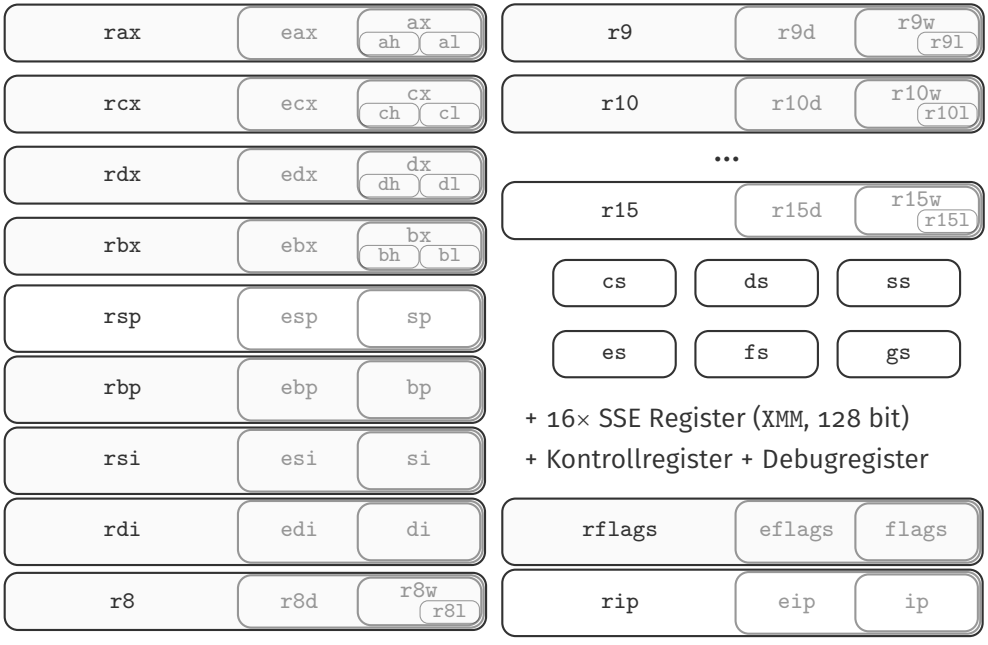
```
iretq
```

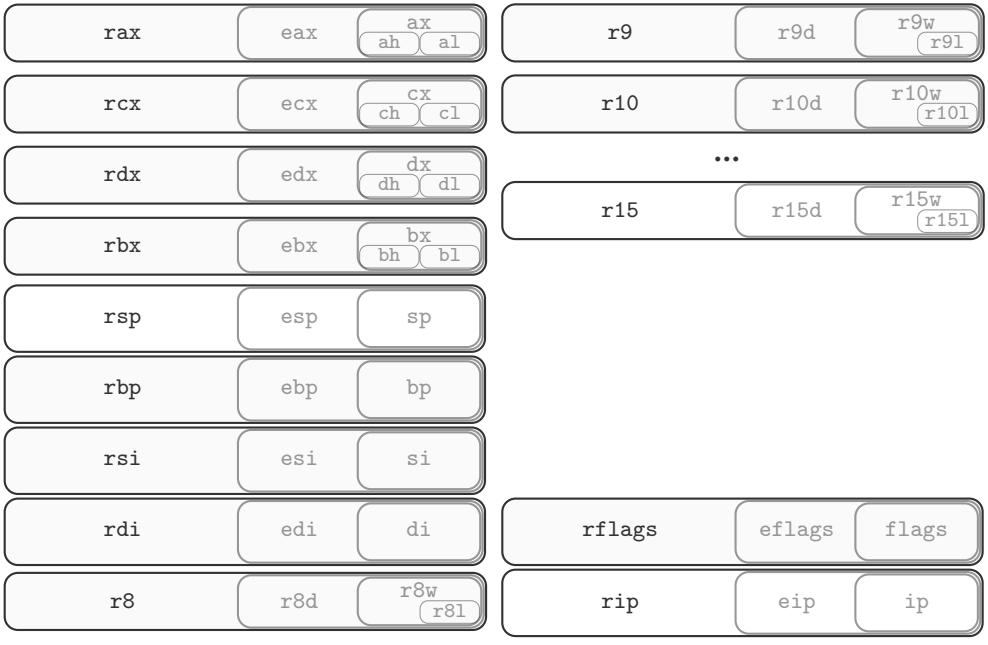
Stellt Hardware-Kontext (`rip`, `cs`, `rflags`) wieder her

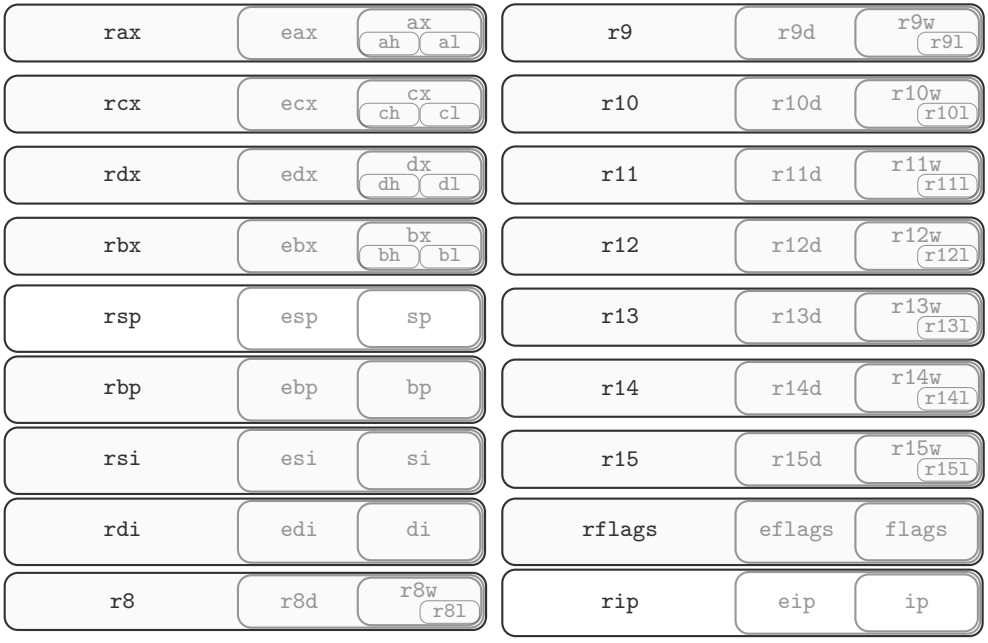
Kontextsicherung gemäß Konvention

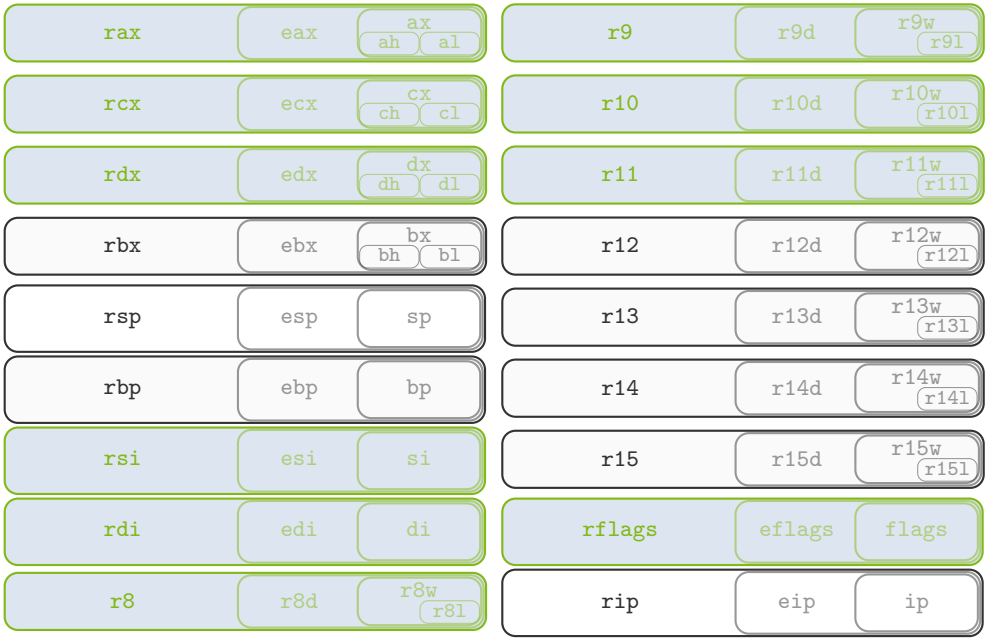
```
1  void baz(){
2    ...
3
4    // flüchtige Register
5    // sichern
6
7    func();
8
9    // flüchtige Register
10   // wiederherstellen
11
12   ...
13 }
```

```
1  void func(){
2    // nicht-flüchtige
3    // Register
4    // sichern
5
6    ...
7
8    // nicht-flüchtige
9    // Register
10   // wiederherstellen
11
12   return;
13 }
```

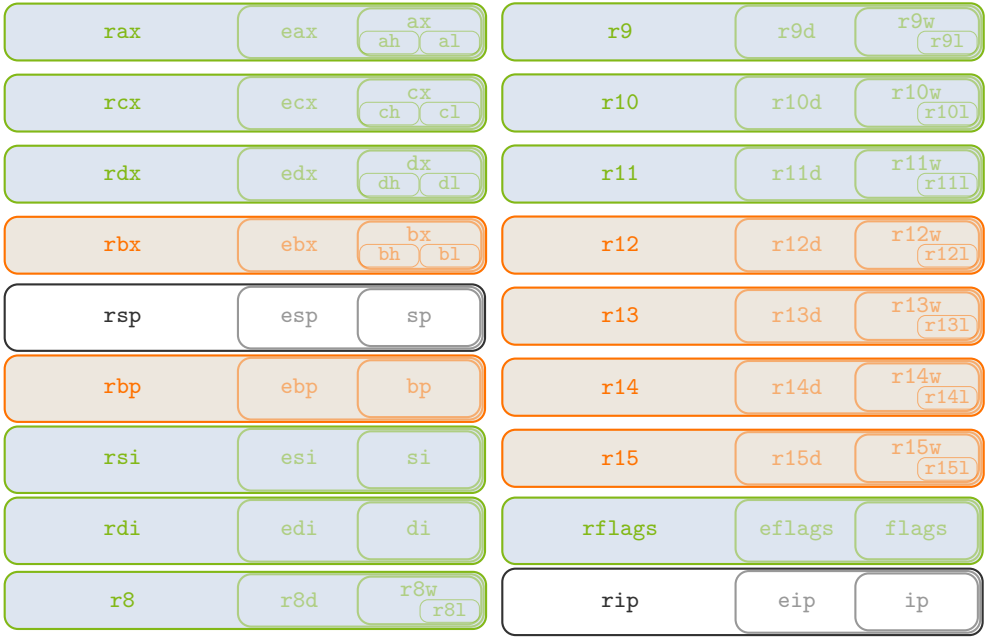

rax
eax
ax
ah
al
rcx
ecx
cx
ch
cl
rdx
edx
dx
dh
dl
rbx
ebx
bx
bh
bl
rsp
esp
sp
rbp
ebp
bp
rsi
esi
si
rdi
edi
di
r8
r8d
r8w
r8l
r9
r9d
r9w
r9l
r10
r10d
r10w
r10l
...
r15
r15d
r15w
r15l
cs
ds
ss
es
fs
gs
+ 16× SSE Register (XMM, 128 bit)
+ Kontrollregister + Debugregister
rflags
eflags
flags
rip
eip
ip


rax
eax
ax
ah
al
rcx
ecx
cx
ch
cl
rdx
edx
dx
dh
dl
rbx
ebx
bx
bh
bl
rsp
esp
sp
rbp
ebp
bp
rsi
esi
si
rdi
edi
di
r8
r8d
r8w
r8l
r9
r9d
r9w
r9l
r10
r10d
r10w
r10l
...
r15
r15d
r15w
r15l
rflags
eflags
flags
rip
eip
ip


rax
eax
ax
ah
al
rcx
ecx
cx
ch
cl
rdx
edx
dx
dh
dl
rbx
ebx
bx
bh
bl
rsp
esp
sp
rbp
ebp
bp
rsi
esi
si
rdi
edi
di
r8
r8d
r8w
r8l
r9
r9d
r9w
r9l
r10
r10d
r10w
r10l
r11
r11d
r11w
r11l
r12
r12d
r12w
r12l
r13
r13d
r13w
r13l
r14
r14d
r14w
r14l
r15
r15d
r15w
r15l
rflags
eflags
flags
rip
eip
ip

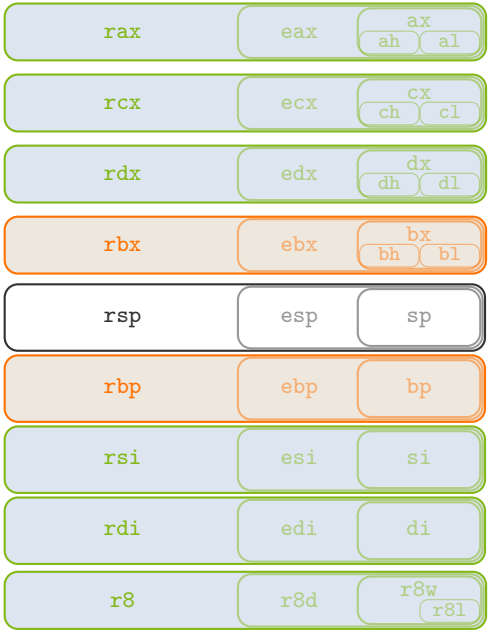


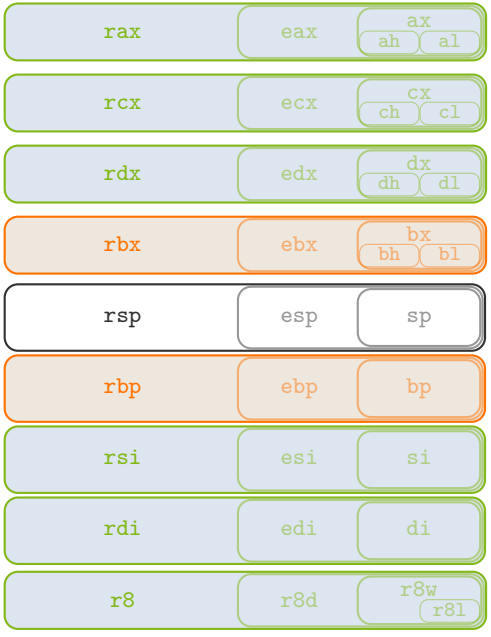
flüchtige (*scratch* / *caller-save*) Register


rax
eax
ax
ah
al
rcx
ecx
cx
ch
cl
rdx
edx
dx
dh
dl
rbx
ebx
bx
bh
bl
rsp
esp
sp
rbp
ebp
bp
rsi
esi
si
rdi
edi
di
r8
r8d
r8w
r8l
r9
r9d
r9w
r9l
r10
r10d
r10w
r10l
r11
r11d
r11w
r11l
r12
r12d
r12w
r12l
r13
r13d
r13w
r13l
r14
r14d
r14w
r14l
r15
r15d
r15w
r15l
rflags
eflags
flags
rip
eip
ip
flüchtige (scratch / caller-save) Register
nicht-flüchtig (non-scratch / callee-save)

Wieso nicht gleich die **flüchtigen Register** beim Funktionsaufruf nutzen?

Bild: twemoji


rax
eax
ax
ah
al
rcx
ecx
cx
ch
cl
rdx
edx
dx
dh
dl
rbx
ebx
bx
bh
bl
rsp
esp
sp
rbp
ebp
bp
rsi
esi
si
rdi
edi
di
r8
r8d
r8w
r8l



Rückgabewert

4. Parameter

3. Parameter

2. Parameter

1. Parameter

5. Parameter

Parameterübergabe gemäß Konvention

```
int i = func(23, 42);
```

Parameterübergabe gemäß Konvention

```
int i = func(23, 42);
```

```
; ggf. Register Sicherung
push r9
; 2. Parameter in Register rsi
mov esi, 0x2a
; 1. Parameter in Register rdi
mov edi, 0x17
; Funktionsaufruf
call func
```

Parameterübergabe gemäß Konvention

```
int i = func(23, 42);
```

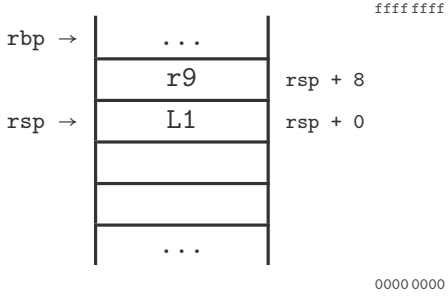
```
  ; ggf. Register Sicherung
  push r9
  ; 2. Parameter in Register rsi
  mov esi, 0x2a
  ; 1. Parameter in Register rdi
  mov edi, 0x17
  ; Funktionsaufruf
  call func
  ; pushed implizit die
  ; Rücksprungadresse
L1:
```

Parameterübergabe gemäß Konvention

```
int i = func(23, 42);
```

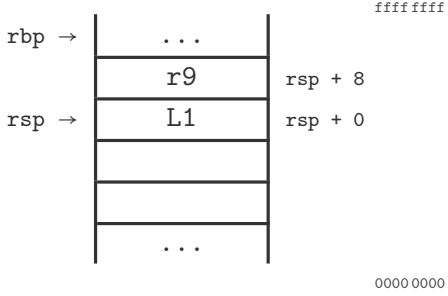
```
  ; ggf. Register Sicherung
  push r9
  ; 2. Parameter in Register rsi
  mov esi, 0x2a
  ; 1. Parameter in Register rdi
  mov edi, 0x17
  ; Funktionsaufruf
  call func
  ; pushed implizit die
  ; Rücksprungadresse
L1:
```

Stack beim Funktionsaufruf:



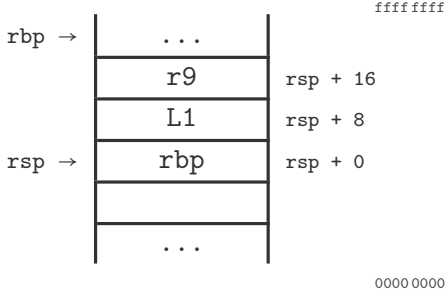
Parameterübergabe gemäß Konvention

```
func:
```



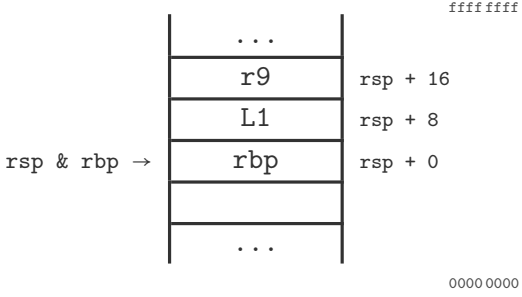
Parameterübergabe gemäß Konvention

```
func:

  ; alten Rahmenzeiger sichern
  push rbp
```



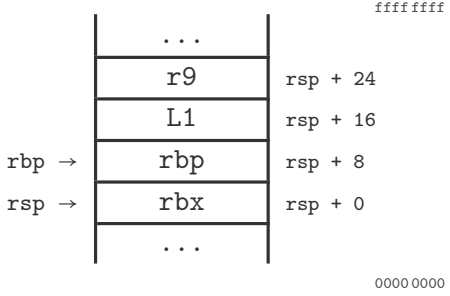
Parameterübergabe gemäß Konvention

```
func:

  ; alten Rahmenzeiger sichern
  push rbp
  ; aktuellen Rahmenzeiger setzen
  mov rbp, rsp
```



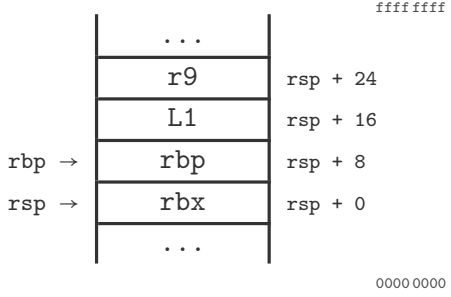
Parameterübergabe gemäß Konvention

```
func:

  ; alten Rahmenzeiger sichern
  push rbp
  ; aktuellen Rahmenzeiger setzen
  mov rbp, rsp
  ; ggf. weitere Register sichern
  push rbx
```



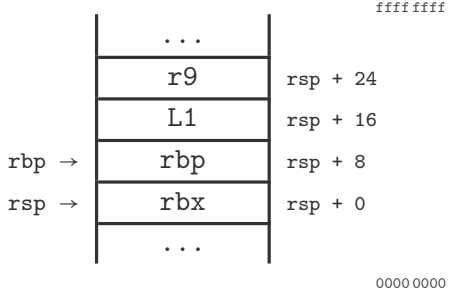
Parameterübergabe gemäß Konvention

```
func:

  ; alten Rahmenzeiger sichern
  push rbp
  ; aktuellen Rahmenzeiger setzen
  mov rbp, rsp
  ; ggf. weitere Register sichern
  push rbx

  ...
```



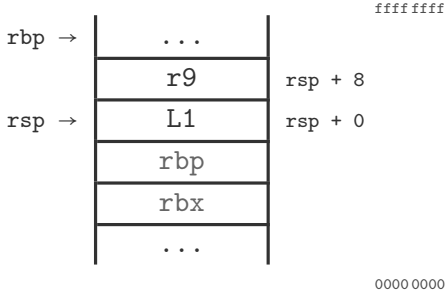
Parameterübergabe gemäß Konvention

```
func:

  ; alten Rahmenzeiger sichern
  push rbp
  ; aktuellen Rahmenzeiger setzen
  mov rbp, rsp
  ; ggf. weitere Register sichern
  push rbx

  ...

  ; Rückgabewert nach rax
  mov eax, 0xd
```



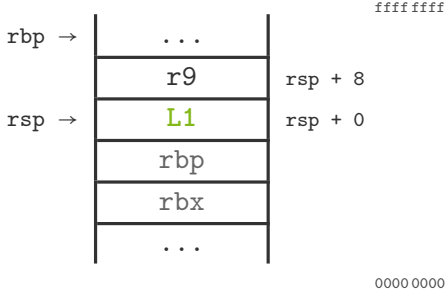
Parameterübergabe gemäß Konvention

```
func:

  ; alten Rahmenzeiger sichern
  push rbp
  ; aktuellen Rahmenzeiger setzen
  mov rbp, rsp
  ; ggf. weitere Register sichern
  push rbx

  ...

  ; Rückgabewert nach rax
  mov eax, 0xd
  ; Register wiederherstellen
  pop rbx
  pop rbp
```



Parameterübergabe gemäß Konvention

```
func:

  ; alten Rahmenzeiger sichern
  push rbp
  ; aktuellen Rahmenzeiger setzen
  mov rbp, rsp
  ; ggf. weitere Register sichern
  push rbx

  ...

  ; Rückgabewert nach rax
  mov eax, 0xd
  ; Register wiederherstellen
  pop rbx
  pop rbp
  ; Rücksprung
  ret
```

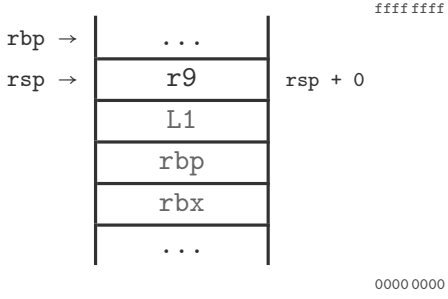


Parameterübergabe gemäß Konvention

```
int i = func(23, 42);
```

```
  ; ggf. Register Sicherung
  push r9
  ; 2. Parameter in Register rsi
  mov esi, 0x2a
  ; 1. Parameter in Register rdi
  mov edi, 0x17
  ; Funktionsaufruf
  call func
  ; pushed implizit die
  ; Rücksprungadresse
L1:
```

Stack nach Funktionsaufruf:

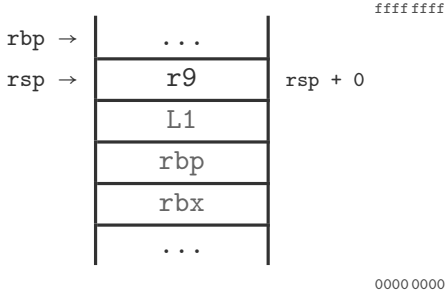


Parameterübergabe gemäß Konvention

```
int i = func(23, 42);
```

```
  ; ggf. Register Sicherung
  push r9
  ; 2. Parameter in Register rsi
  mov esi, 0x2a
  ; 1. Parameter in Register rdi
  mov edi, 0x17
  ; Funktionsaufruf
  call func
  ; pushed implizit die
  ; Rücksprungadresse
L1:
  ; Rückgabewert in rax
  mov rsi, rax
```

Stack nach Funktionsaufruf:

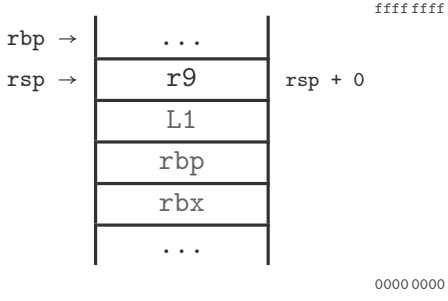


Parameterübergabe gemäß Konvention

```
int i = func(23, 42);
```

```
  ; ggf. Register Sicherung
  push r9
  ; 2. Parameter in Register rsi
  mov esi, 0x2a
  ; 1. Parameter in Register rdi
  mov edi, 0x17
  ; Funktionsaufruf
  call func
  ; pushed implizit die
  ; Rücksprungadresse
L1:
  ; Rückgabewert in rax
  mov rsi, rax
  ; ggf. Register wiederherstellen
  pop r9
```

Stack nach Funktionsaufruf:



Umschaltung

```
1  void foo(){
2    int f = 42;
3
4    while (f--){
5      kout << "foo"
6           << f
7           << endl;
8      context_switch(
9          &stack_foo,
10         &stack_bar
11       );
12   }
13 }
```

```
1  void bar(){
2    int b = 23;
3
4    while (b--){
5      kout << "bar"
6           << b
7           << endl;
8      context_switch(
9          &stack_bar,
10         &stack_foo
11       );
12   }
13 }
```

Umschaltung im Detail

Kontrollflusszustand sichern & laden

Notwendige **Schritte** in `context_switch`:

Umschaltung im Detail

Kontrollflusszustand sichern & laden

Notwendige **Schritte** in `context_switch`:

1. Register sichern

Umschaltung im Detail

Kontrollflusszustand sichern & laden

Notwendige **Schritte** in `context_switch`:

1. Register sichern (*via Stack*)

Umschaltung im Detail

Kontrollflusszustand sichern & laden

Notwendige **Schritte** in `context_switch`:

1. Register sichern (*via Stack*)
2. Stackpointer (`rsp`) sichern

Umschaltung im Detail

Kontrollflusszustand sichern & laden

Notwendige **Schritte** in `context_switch`:

1. Register sichern (*via Stack*)
2. Stackpointer (`rsp`) sichern
3. Stackpointer (`rsp`) laden

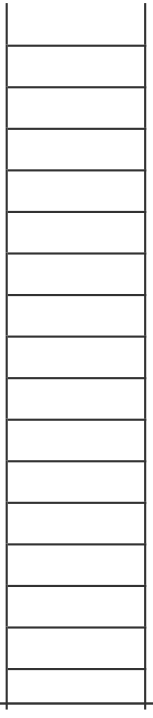
Umschaltung im Detail

Kontrollflusszustand sichern & laden

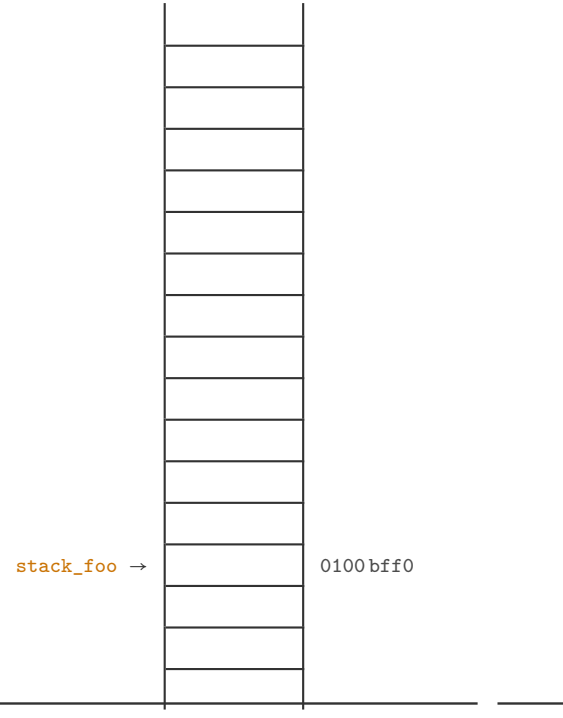
Notwendige **Schritte** in `context_switch`:

1. Register sichern (*via Stack*)
2. Stackpointer (`rsp`) sichern
3. Stackpointer (`rsp`) laden
4. Register wiederherstellen

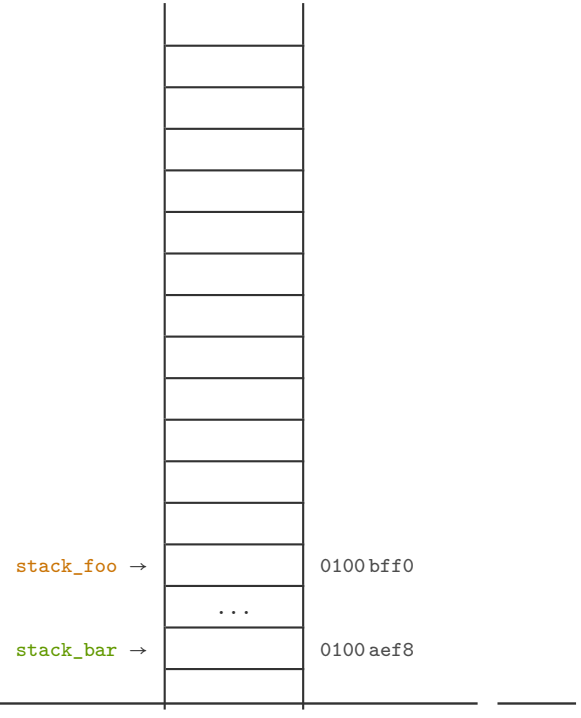
```
// Global sichtbar:

struct StackPointer {
  void *kernel;

  // Später auch User-
  // Stackpointer (in BST)
};
```



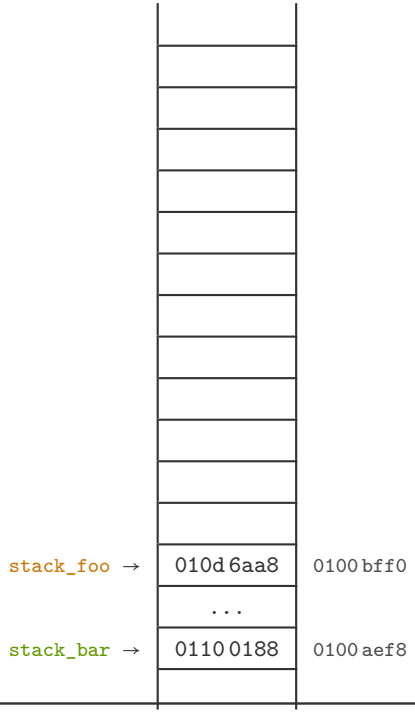
```
// Global sichtbar:

struct StackPointer {
  void *kernel;

  // Später auch User-
  // Stackpointer (in BST)
};

StackPointer stack_foo;
```



```
// Global sichtbar:

struct StackPointer {
  void *kernel;

  // Später auch User-
  // Stackpointer (in BST)
};

StackPointer stack_foo;

StackPointer stack_bar;
```



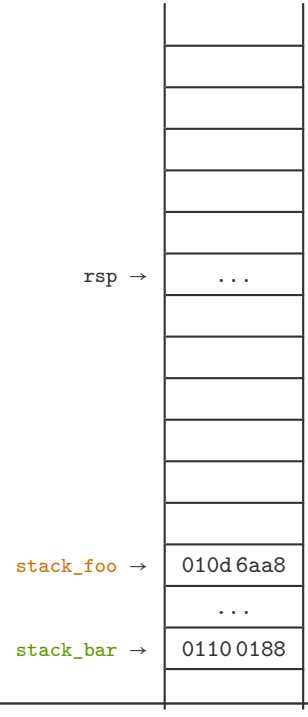
```
// Global sichtbar:

struct StackPointer {
  void *kernel;

  // Später auch User-
  // Stackpointer (in BST)
};

StackPointer stack_foo;

StackPointer stack_bar;

// Sinnvoll initialisieren
// (mehr dazu später...)
```



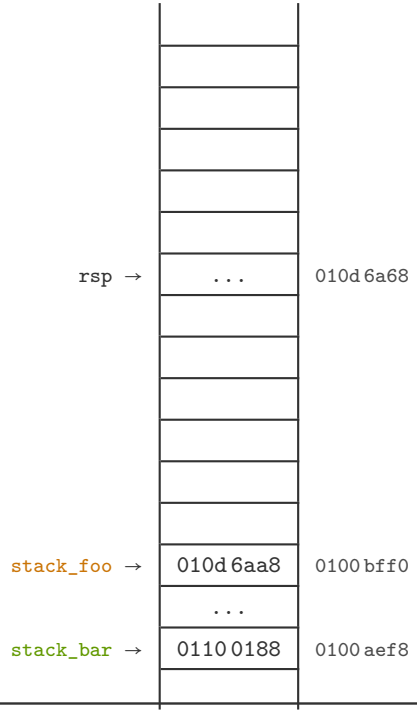
```
void foo(){
  ...
```

```
  context_switch(
      &stack_foo,
      &stack_bar
    );
```

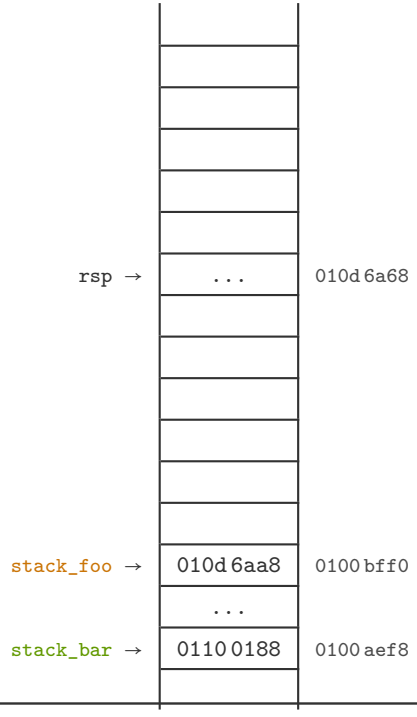
```
  ...
```



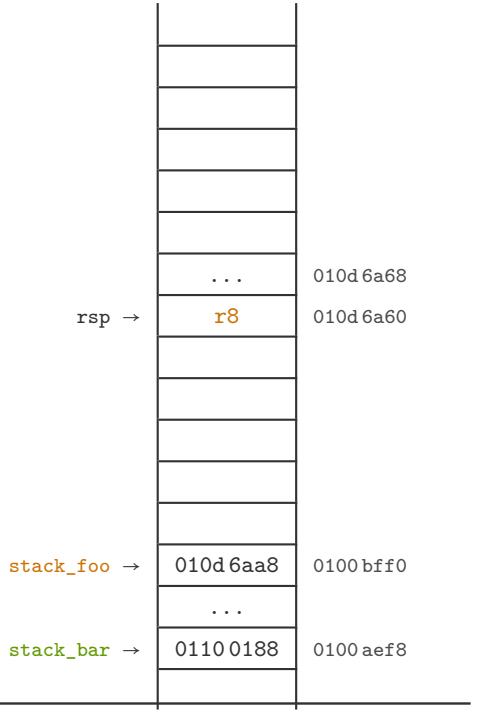
```
void foo(){
  ...

  // Sicherung der
  // flüchtigen Register
  // von Kontext foo



  context_switch(
      &stack_foo,
      &stack_bar
    );


  ...
```



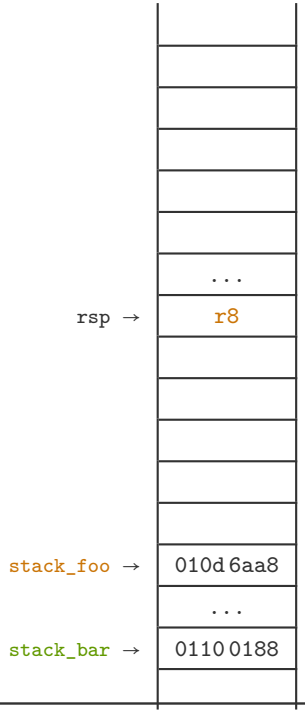
```
void foo(){
  ...

  // Sicherung der
  // flüchtigen Register
  // von Kontext foo
  // durch Übersetzer


  context_switch(
      &stack_foo,
      &stack_bar
    );


  ...
```



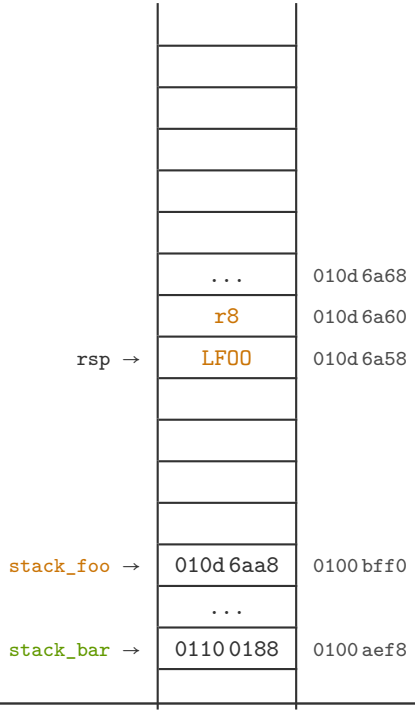
```
void foo(){
  ...

  // Sicherung der
  // flüchtigen Register
  // von Kontext foo
  // durch Übersetzer
  // (z.B. r8)

  context_switch(
      &stack_foo,
      &stack_bar
    );


  ...
```

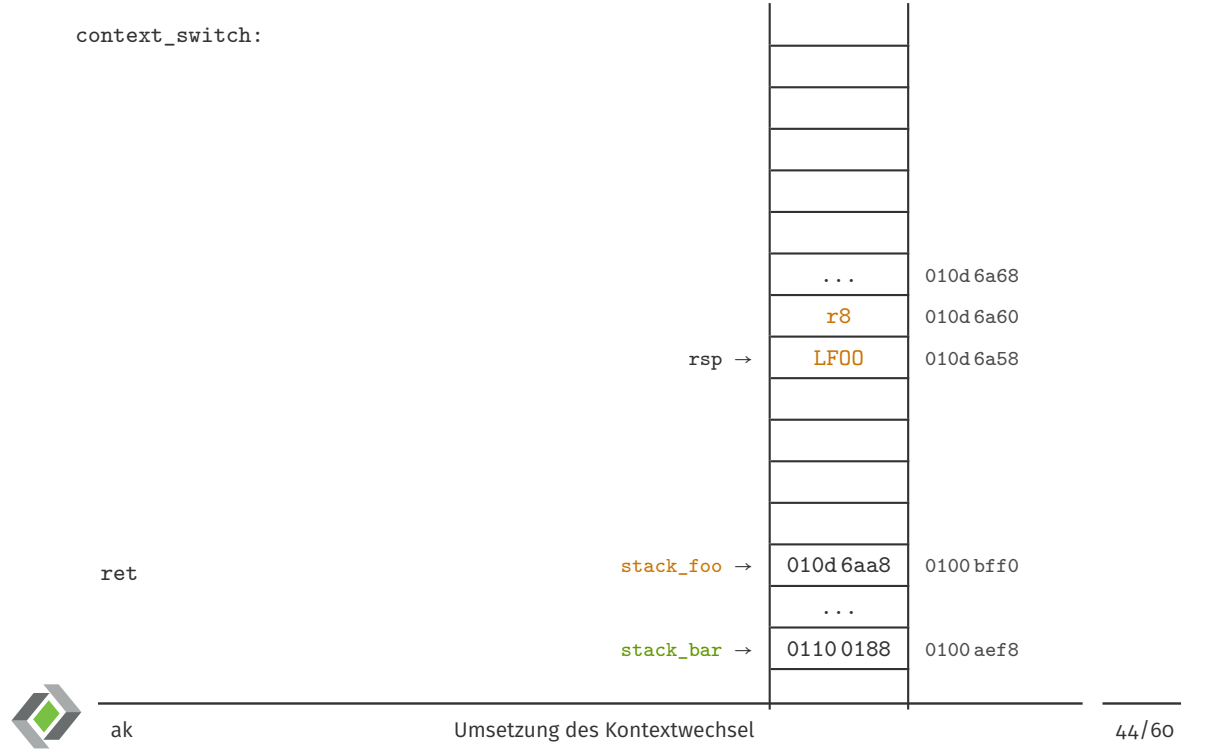


```
void foo(){
  ...

  // Sicherung der
  // flüchtigen Register
  // von Kontext foo
  // durch Übersetzer
  // (z.B. r8)

  context_switch(
      &stack_foo,
      &stack_bar
    );


  ...
```

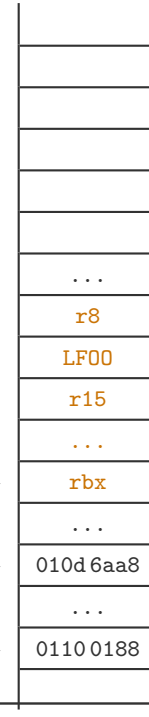


```
void foo(){
  ...

  // Sicherung der
  // flüchtigen Register
  // von Kontext foo
  // durch Übersetzer
  // (z.B. r8)

  context_switch(
      &stack_foo,
      &stack_bar
    );
LFOO:

  ...
```




context_switch:
...
010d6a68
r8
010d6a60
rsp →
LF00
010d6a58
ret
stack_foo →
010d6aa8
0100bff0
...
stack_bar →
0110 0188
0100aef8

```
context_switch:

  ;; nicht-flüchtige
  ;; Register von
  ;; foo sichern

  ret
```



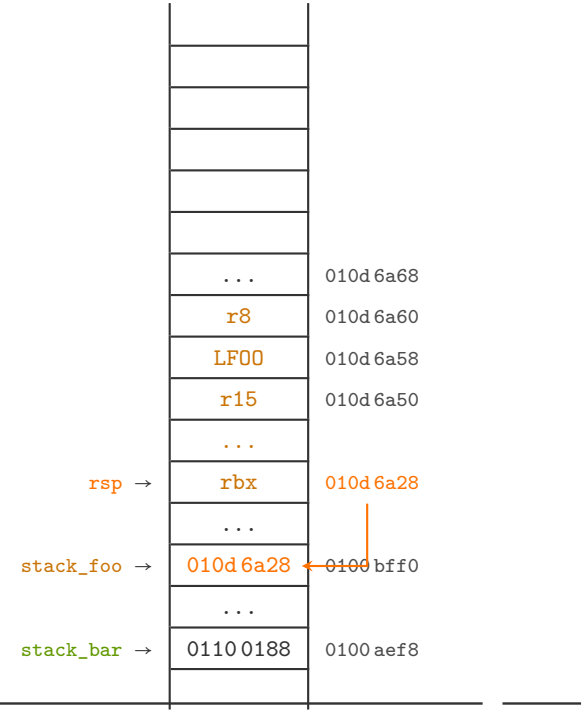
rsp →

stack_foo →

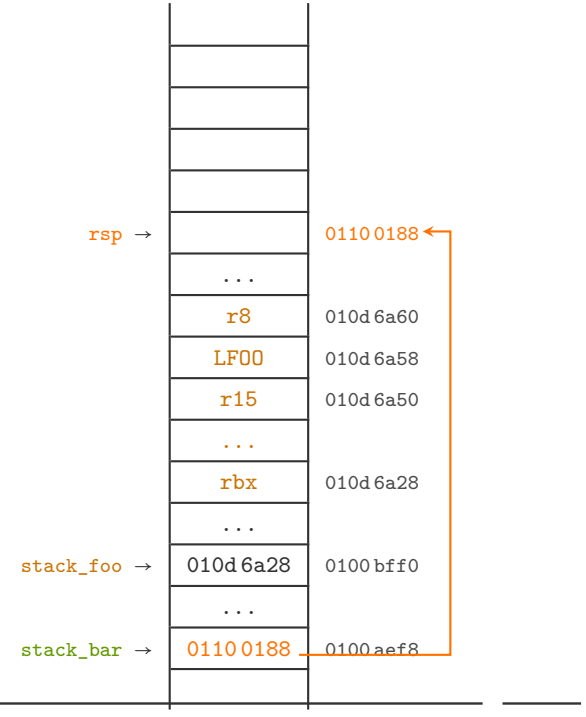
stack_bar →

...	010d6a68
r8	010d6a60
LF00	010d6a58
r15	010d6a50
...	
rbx	010d6a28
...	
010d6aa8	0100bff0
...	
0110 0188	0100aef8

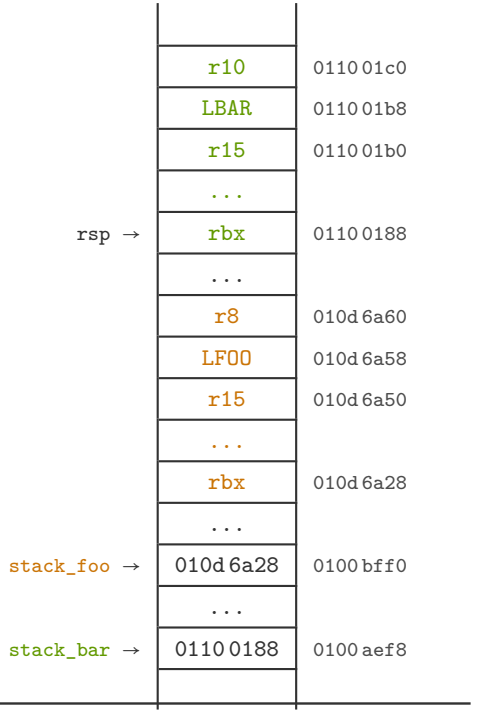
```
context_switch:

  ;; nicht-flüchtige
  ;; Register von
  ;; foo sichern

  ;; Stackzeiger von
  ;; foo sichern

  ret
```



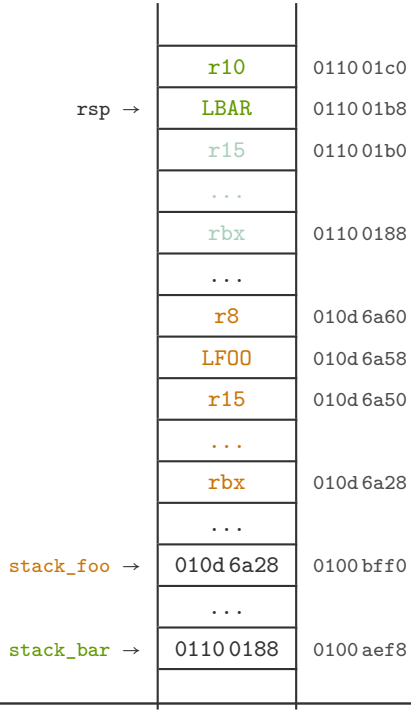
```
context_switch:

  ;; nicht-flüchtige
  ;; Register von
  ;; foo sichern

  ;; Stackzeiger von
  ;; foo sichern

  ;; Stackzeiger von
  ;; bar laden

  ret
```



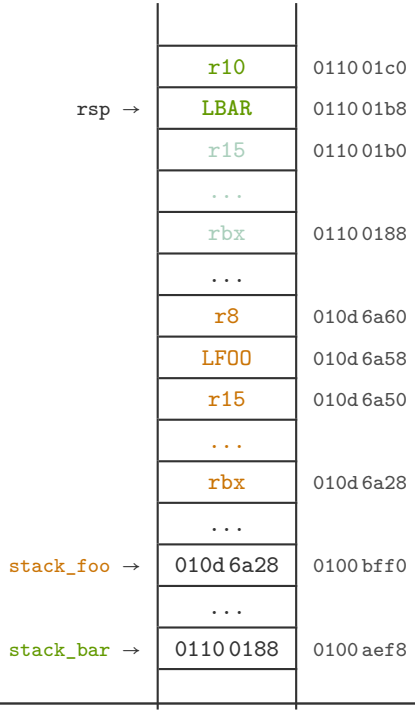
```
context_switch:

  ;; nicht-flüchtige
  ;; Register von
  ;; foo sichern

  ;; Stackzeiger von
  ;; foo sichern

  ;; Stackzeiger von
  ;; bar laden

  ret
```



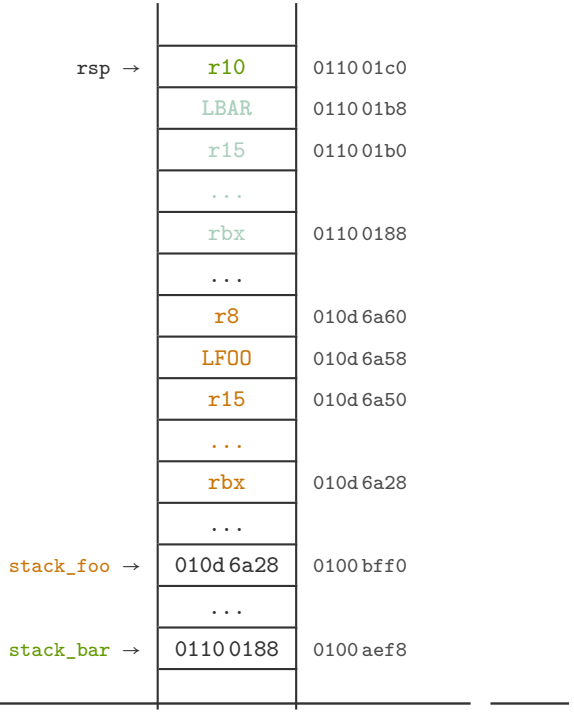
```
context_switch:

  ;; nicht-flüchtige
  ;; Register von
  ;; foo sichern

  ;; Stackzeiger von
  ;; foo sichern

  ;; Stackzeiger von
  ;; bar laden

  ;; nicht-flüchtige
  ;; Register von
  ;; bar laden

  ret
```



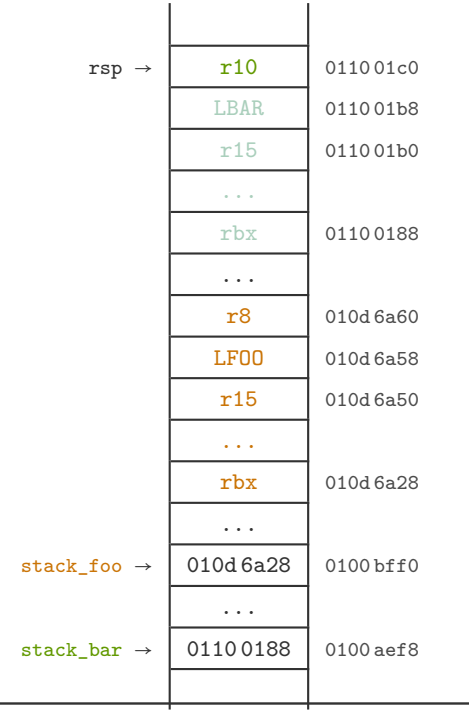
```
context_switch:

  ;; nicht-flüchtige
  ;; Register von
  ;; foo sichern

  ;; Stackzeiger von
  ;; foo sichern

  ;; Stackzeiger von
  ;; bar laden

  ;; nicht-flüchtige
  ;; Register von
  ;; bar laden

  ret
```



```
void bar(){
  ...

  context_switch(
      &stack_bar,
      &stack_foo
    );
LBAR:

  ...
```



```
void bar(){
  ...

  context_switch(
      &stack_bar,
      &stack_foo
    );
LBAR:

  // Wiederhestellen der
  // flüchtigen Register
  // von Kontext bar
  // durch Übersetzer
  // (z.B. r10)

  ...
```



Koroutine (erstmalig) starten

Wie rufe ich die Koroutine erstmalig auf?

Ziel: Instruktionszeiger `rip` ändern

Koroutine (erstmalig) starten

Wie rufe ich die Koroutine erstmalig auf?

Ziel: Instruktionszeiger `rip` ändern

Problem: Register `rip` kann nicht direkt beschrieben werden

Koroutine (erstmalig) starten

Wie rufe ich die Koroutine erstmalig auf?

Ziel: Instruktionszeiger `rip` ändern

Problem: Register `rip` kann nicht direkt beschrieben werden

Lösung: Zieladresse auf Stack und `ret` ändert `rip`

Koroutine (erstmalig) starten

Wie rufe ich die Koroutine erstmalig auf?

Ziel: Instruktionszeiger `rip` ändern

Problem: Register `rip` kann nicht direkt beschrieben werden

Lösung: Zieladresse auf Stack und `ret` ändert `rip`

→ `context_switch` mit entsprechenden Stack

Koroutine (erstmalig) starten

Wie rufe ich die Koroutine erstmalig auf?

Ziel: Instruktionszeiger `rip` ändern

Problem: Register `rip` kann nicht direkt beschrieben werden

Lösung: Zieladresse auf Stack und `ret` ändert `rip`

→ `context_switch` mit entsprechenden Stack

Wie rufe ich die aller erste Koroutine auf?

Koroutine (erstmalig) starten

Wie rufe ich die Koroutine erstmalig auf?

Ziel: Instruktionszeiger `rip` ändern

Problem: Register `rip` kann nicht direkt beschrieben werden

Lösung: Zieladresse auf Stack und `ret` ändert `rip`
→ `context_switch` mit entsprechenden Stack

Wie rufe ich die aller erste Koroutine auf?

- `context_go` mit nur einem Parameter

Koroutine (erstmalig) starten

Wie rufe ich die Koroutine erstmalig auf?

Ziel: Instruktionszeiger `rip` ändern

Problem: Register `rip` kann nicht direkt beschrieben werden

Lösung: Zieladresse auf Stack und `ret` ändert `rip`
→ `context_switch` mit entsprechenden Stack

Wie rufe ich die aller erste Koroutine auf?

- `context_go` mit nur einem Parameter

Was wird für jede Koroutine gebraucht?

Koroutine (erstmalig) starten

Wie rufe ich die Koroutine erstmalig auf?

Ziel: Instruktionszeiger `rip` ändern

Problem: Register `rip` kann nicht direkt beschrieben werden

Lösung: Zieladresse auf Stack und `ret` ändert `rip`
→ `context_switch` mit entsprechenden Stack

Wie rufe ich die aller erste Koroutine auf?

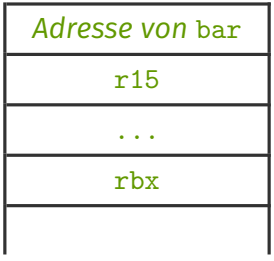
- `context_go` mit nur einem Parameter

Was wird für jede Koroutine gebraucht?

- eigener, präparierter Stack
- Speicher für Stackzeiger (`struct StackPointer`)

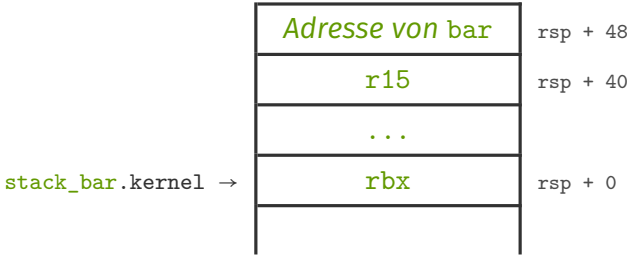
Stack aufsetzen

Stack für Einsprung in Koroutine `void bar()`



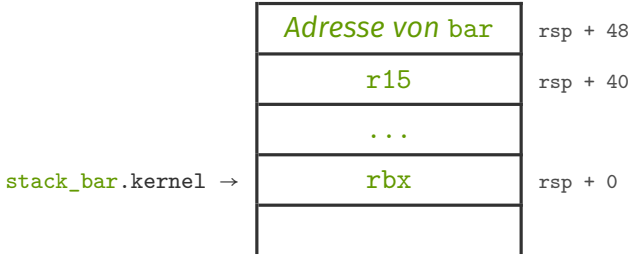
Stack aufsetzen

Stack für Einsprung in Koroutine `void bar()`



Stack aufsetzen

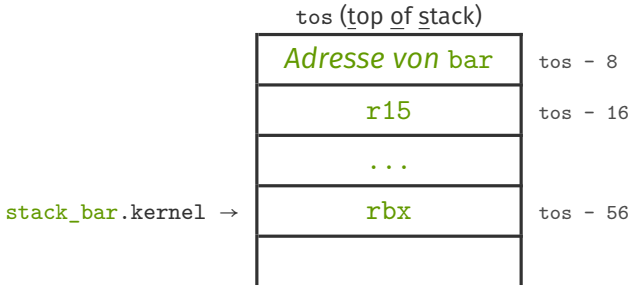
Stack für Einsprung in Koroutine `void bar()`




```
1 #define STACKSIZE 4096
2 char stackBar[STACKSIZE];
3 void* tos = stackFoo + STACKSIZE;
```

Stack aufsetzen

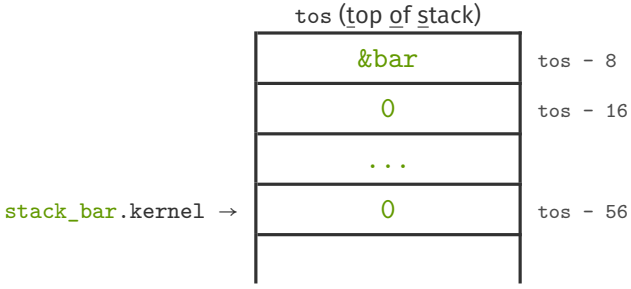
Stack für Einsprung in Koroutine `void bar()`




```
1 #define STACKSIZE 4096
2 char stackBar[STACKSIZE];
3 void* tos = stackFoo + STACKSIZE;
```

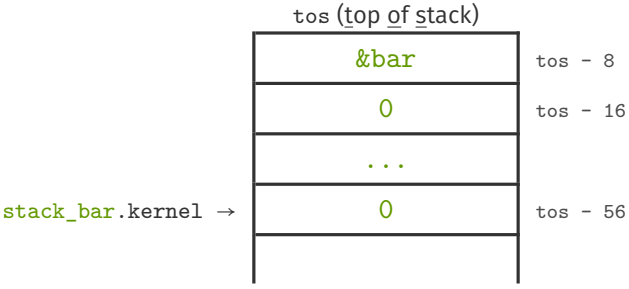
Stack aufsetzen

Stack für Einsprung in Koroutine `void bar()`



Stack aufsetzen

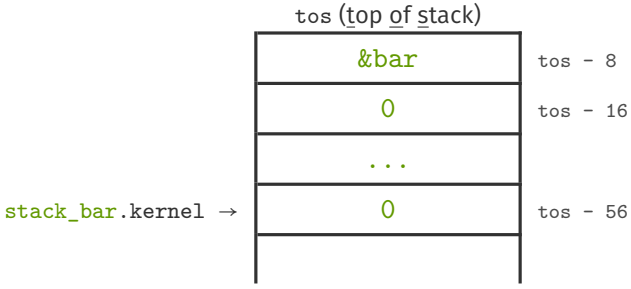
Stack für Einsprung in Koroutine `void bar()`



Was passiert nun bei `context_switch`?

Stack aufsetzen

Stack für Einsprung in Koroutine `void bar()`



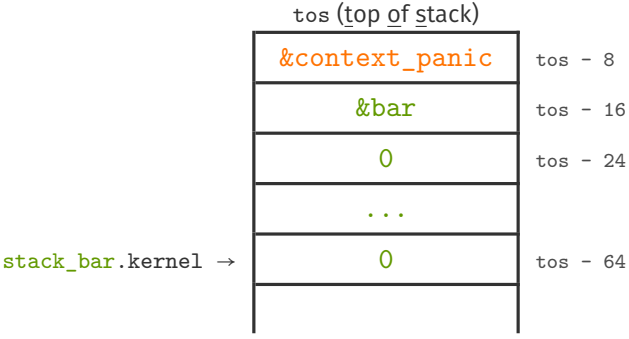
Was passiert, wenn die Koroutine `bar` abgearbeitet ist?

Stack aufsetzen (Robust)

```
1 void panic() {
2   kernelpanic("Application should not return!1!!11");
3 }
```

Stack aufsetzen (Robust)

```
1 void panic() {
2   kernelpanic("Application should not return!1!!11");
3 }
```



Stack aufsetzen mit Funktionsparameter

Stack für Einsprung in Koroutine `void bar(int i)`

Stack aufsetzen mit Funktionsparameter

Stack für Einsprung in Koroutine `void bar(int i)` unter Verwendung einer zusätzlichen Hilfsfunktion – z.B. `bar_wrapper`

Stack aufsetzen mit Funktionsparameter

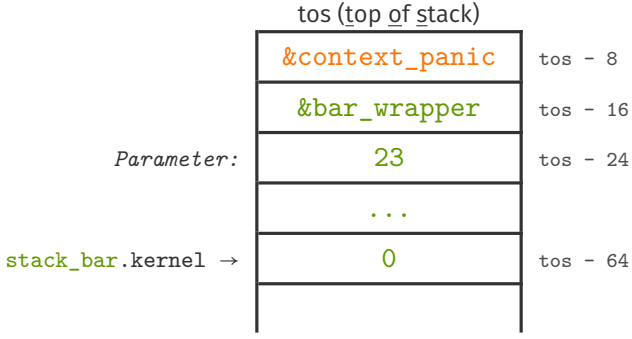
Stack für Einsprung in Koroutine `void bar(int i)` unter Verwendung einer zusätzlichen Hilfsfunktion – z.B. `bar_wrapper`

- liest Parameter aus nicht-flüchtigem Register (`r15`)
- schreibt Wert in flüchtiges Parameterregister (`rdi`)
- springt in eigentliche Funktion (`bar`)

Stack aufsetzen mit Funktionsparameter

Stack für Einsprung in Koroutine `void bar(int i)` unter Verwendung einer zusätzlichen Hilfsfunktion – z.B. `bar_wrapper`

- liest Parameter aus nicht-flüchtigem Register (`r15`)
- schreibt Wert in flüchtiges Parameterregister (`rdi`)
- springt in eigentliche Funktion (`bar`)



Threads

```
1 class Thread {
2     StackPointer sp;
3   public:
4     Thread();
5     virtual void action() = 0;
6 };
```

Threads

```
1 class Thread {
2     StackPointer sp;
3   public:
4     Thread();
5     virtual void action() = 0;
6 };
```

Adresse einer virtuellen Member-Funktion nicht (einfach) ermittelbar

Threads

```
1 class Thread {
2     StackPointer sp;
3   public:
4     Thread();
5     virtual void action() = 0;
6 };
```

Adresse einer virtuellen Member-Funktion nicht (einfach) ermittelbar

```
1 Thread * x = &app;
2 x->action(); // Foo::action oder Bar::action ?
```

```
7 class Foo : public Thread {
8   void action() { ... }
9 };
```

```
1 class Bar : public Thread {
2   void action() { ... }
3 };
```

Threads

```
1 class Thread {
2     StackPointer sp;
3   public:
4     Thread();
5     virtual void action() = 0;
6 };
```

Adresse einer virtuellen Member-Funktion nicht (einfach) ermittelbar

```
1 void kickoff(Thread* t){
2   t->action();
3 }
```

Threads: Stack aufsetzen

```
1 void * prepareContext(void * tos,
2                        void (*kickoff)(void*),
3                        void * param);
```

Präpariert einen Stack für den ersten Einsprung

Threads: Stack aufsetzen

```
1 void * prepareContext(void * tos,
2                        void (*kickoff)(void*),
3                        void * param);
```

Präpariert einen Stack für den ersten Einsprung

- statisch reservierten Speicher `tos` als Stack aufsetzen

Threads: Stack aufsetzen

```
1 void * prepareContext(void * tos,
2                        void (*kickoff)(void*),
3                        void * param);
```

Präpariert einen Stack für den ersten Einsprung

- statisch reservierten Speicher `tos` als Stack aufsetzen
- nach dem Einsprung soll `kickoff` mit `param` aufgerufen werden

Threads: Stack aufsetzen

```
1 void * prepareContext(void * tos,
2                        void (*kickoff)(void*),
3                        void * param);
```

Präpariert einen Stack für den ersten Einsprung

- statisch reservierten Speicher `tos` als Stack aufsetzen
- nach dem Einsprung soll `kickoff` mit `param` aufgerufen werden
- Stackpointer `kernel` in Thread entsprechend setzen

Threads: Stack aufsetzen

```
1 void * prepareContext(void * tos,
2                        void (*kickoff)(void*),
3                        void * param);
```

Präpariert einen Stack für den ersten Einsprung

- statisch reservierten Speicher `tos` als Stack aufsetzen
- nach dem Einsprung soll `kickoff` mit `param` aufgerufen werden
- Stackpointer `kernel` in Thread entsprechend setzen
- in C++ (statt Assembler)

Threads: Stack aufsetzen

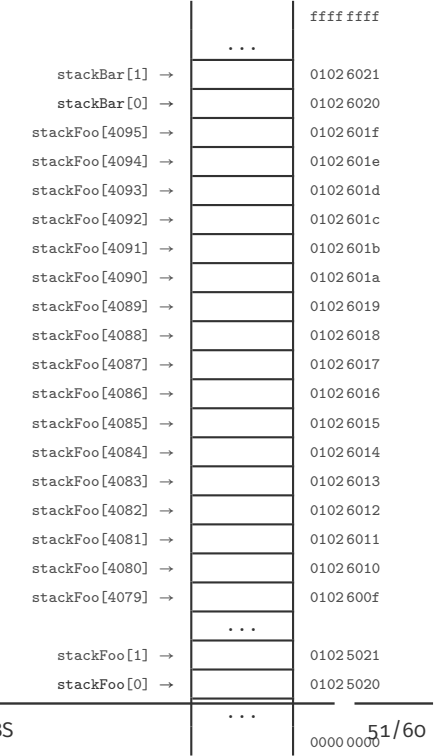
```
1 void * prepareContext(void * tos,
2                        void (*kickoff)(void*),
3                        void * param);
```

Präpariert einen Stack für den ersten Einsprung

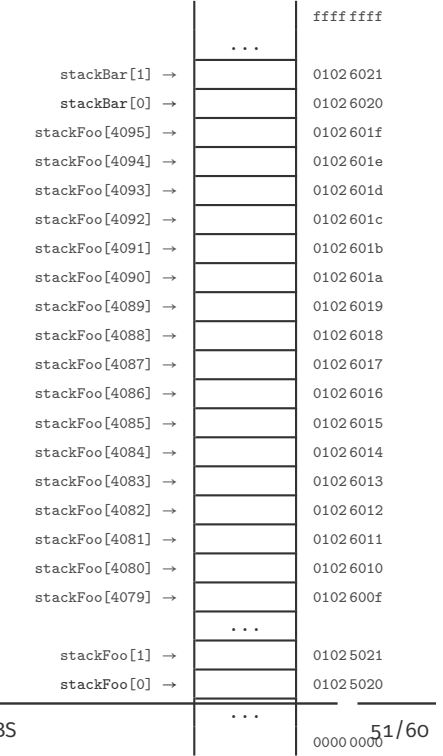
- statisch reservierten Speicher `tos` als Stack aufsetzen
- nach dem Einsprung soll `kickoff` mit `param` aufgerufen werden
- Stackpointer `kernel` in Thread entsprechend setzen
- in C++ (statt Assembler)
- Pointerarithmetik ist hilfreich

```
1 #define STACKSIZE 4096
2 char stackBar[STACKSIZE];
3 char stackFoo[STACKSIZE];
```

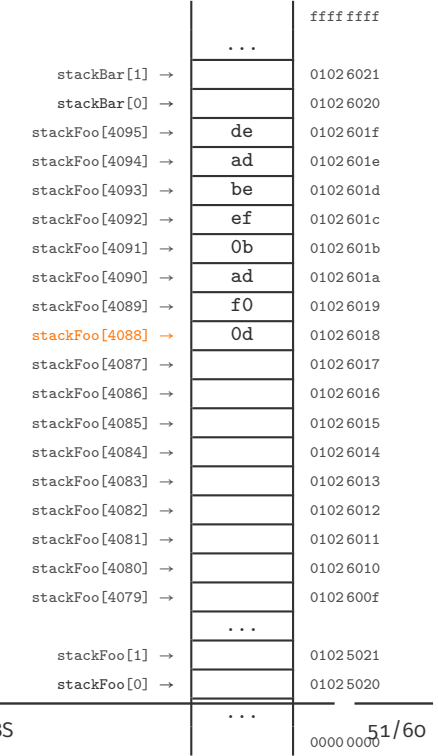
```
1 #define STACKSIZE 4096
2 char stackBar[STACKSIZE];
3 char stackFoo[STACKSIZE];
```



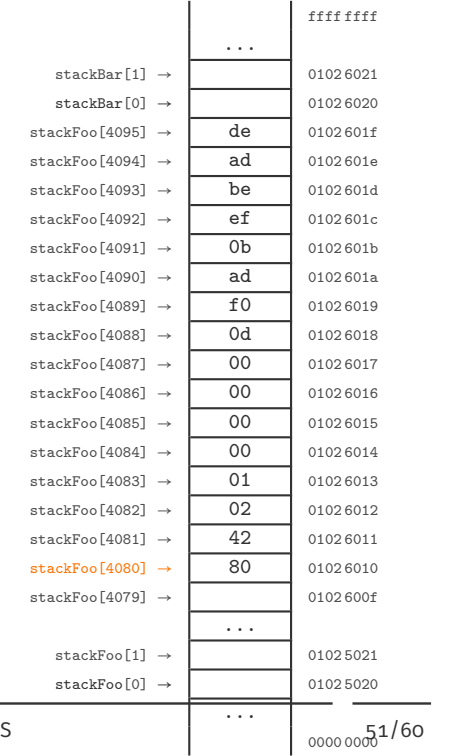
```
1 #define STACKSIZE 4096
2 char stackBar[STACKSIZE];
3 char stackFoo[STACKSIZE];

4 void* tos = stackFoo + STACKSIZE;
5 void** rsp = (void**) tos;
```



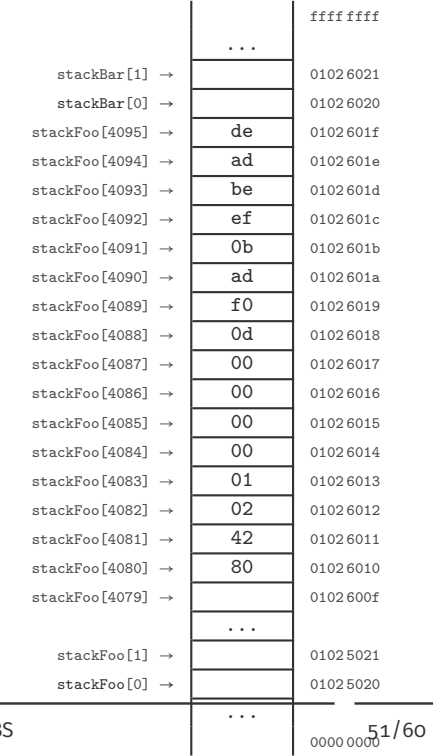
```
1 #define STACKSIZE 4096
2 char stackBar[STACKSIZE];
3 char stackFoo[STACKSIZE];

4 void* tos = stackFoo + STACKSIZE;
5 void** rsp = (void**) tos;

6 rsp--;
7 // rsp = &(stackFoo[4088])
8 *rsp = (void*) 0xdeadbeef0badf00d;
```



```
1  #define STACKSIZE 4096
2  char stackBar[STACKSIZE];
3  char stackFoo[STACKSIZE];

4  void* tos = stackFoo + STACKSIZE;
5  void** rsp = (void**) tos;

6  rsp--;
7  // rsp = &(stackFoo[4088])
8  *rsp = (void*) 0xdeadbeef0badf00d;

10 rsp--;
11 // rsp = &(stackFoo[4080])
12 extern Thread foo;
13 // &foo = 0x102 4280
14 *rsp = (void*) &foo;
```



```
1  #define STACKSIZE 4096
2  char stackBar[STACKSIZE];
3  char stackFoo[STACKSIZE];

4  void* tos = stackFoo + STACKSIZE;
5  void** rsp = (void**) tos;

6  rsp--;
7  // rsp = &(stackFoo[4088])
8  *rsp = (void*) 0xdeadbeef0badf00d;

10 rsp--;
11 // rsp = &(stackFoo[4080])
12 extern Thread foo;
13 // &foo = 0x102 4280
14 *rsp = (void*) &foo;

16 // ...
```

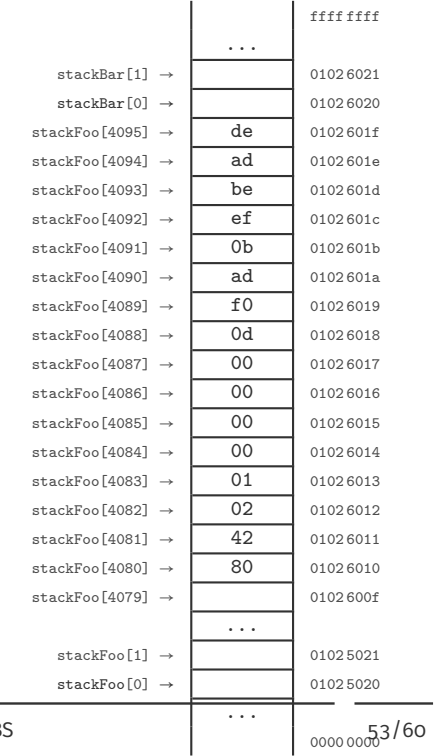


Stapelüberlauf

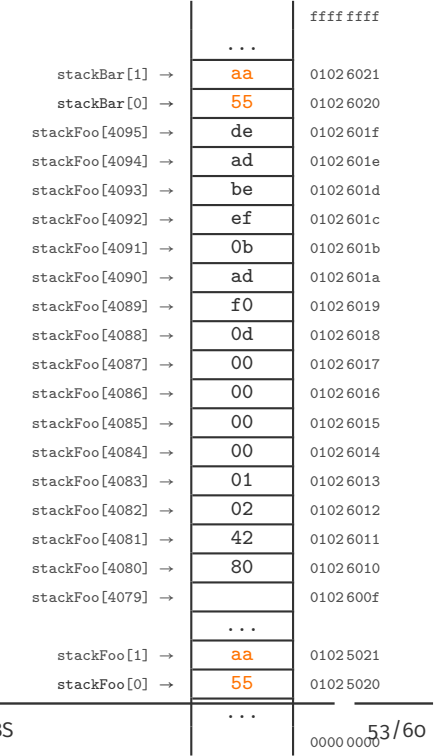
- Die Stacks sind nur 4K groß
- Die Stacks liegen (oft) hintereinander
- Das gilt auch für die initialen Stacks beim Systemstart

➔ Mechanismus zum Erkennen von Überlaufen hilfreich („Stack Canary“)

```
1  #define STACKSIZE 4096
2  char stackBar[STACKSIZE];
3  char stackFoo[STACKSIZE];

4  void* tos = stackFoo + STACKSIZE;
5  void** rsp = (void**) tos;

6  rsp--;
7  // rsp = &(stackFoo[4088])
8  *rsp = (void*) 0xdeadbeef0badf00d;

10 rsp--;
11 // rsp = &(stackFoo[4080])
12 extern Thread foo;
13 // &foo = 0x102 4280
14 *rsp = (void*) &foo;

16 // ...
```



```
1  #define STACKSIZE 4096
2  char stackBar[STACKSIZE];
3  char stackFoo[STACKSIZE];

4  void* tos = stackFoo + STACKSIZE;
5  void** rsp = (void**) tos;

6  rsp--;
7  // rsp = &(stackFoo[4088])
8  *rsp = (void*) 0xdeadbeef0badf00d;

10 rsp--;
11 // rsp = &(stackFoo[4080])
12 extern Thread foo;
13 // &foo = 0x102 4280
14 *rsp = (void*) &foo;

16 // ...
```



Zentrale Verwaltung der Koroutinen (Threads)

```
1 class Scheduler {
2     Queue<Thread> readylist;
3   public:
4     void ready(Thread *);
5     void schedule();
6     void resume();
7     void exit();
8     void kill(Thread *);
9 };
```

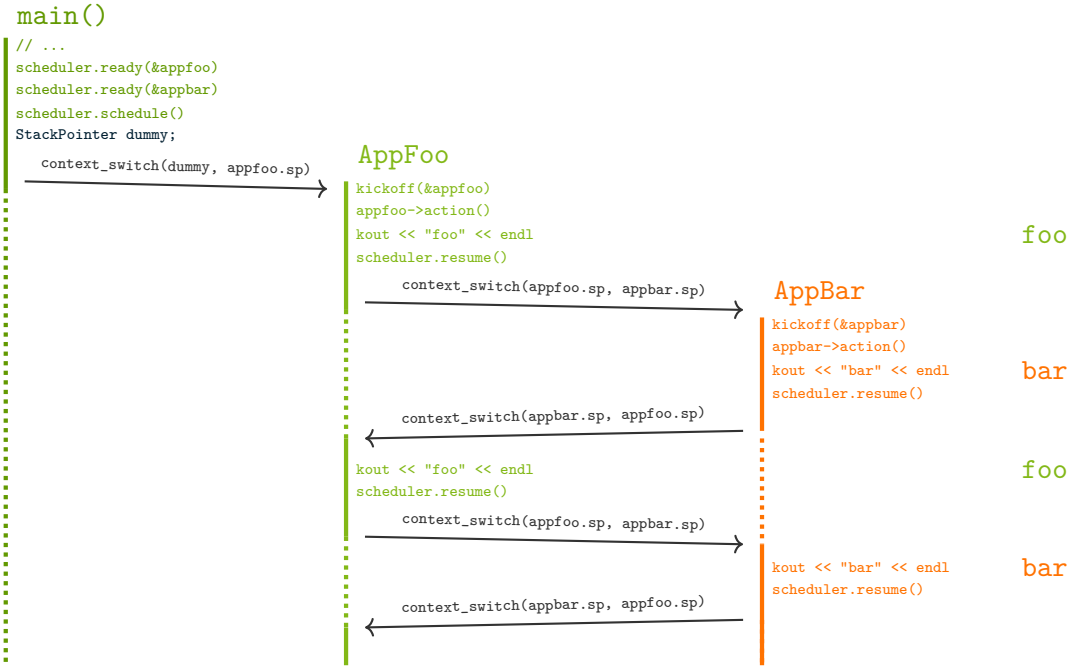
```
// Thread AppFoo
void AppFoo::action(){
  while (1){
    kout << "foo" << endl;
    @scheduler.resume();@
  }
}
```

```
// Thread AppBar
void AppBar::action(){
  while (1){
    kout << "bar" << endl;
    @scheduler.resume();@
  }
}
```

```
// Thread AppFoo
void AppFoo::action(){
  while (1){
    kout << "foo" << endl;
    @scheduler.resume();@
  }
}
```

```
// Thread AppBar
void AppBar::action(){
  while (1){
    kout << "bar" << endl;
    @scheduler.resume();@
  }
}
```

```
// main.cc
AppFoo appfoo;
AppBar appbar;
int main (){
  // ...
  @scheduler.ready(&appfoo);@
  @scheduler.ready(&appbar);@
  @scheduler.schedule();@
}
```


main()
// ...
scheduler.ready(&appfoo)
scheduler.ready(&appbar)
scheduler.schedule()
StackPointer dummy;
context_switch(dummy, appfoo.sp)
AppFoo
kickoff(&appfoo)
appfoo->action()
kout << "foo" << endl
scheduler.resume()
foo
context_switch(appfoo.sp, appbar.sp)
AppBar
kickoff(&appbar)
appbar->action()
kout << "bar" << endl
scheduler.resume()
bar
context_switch(appbar.sp, appfoo.sp)
kout << "foo" << endl
scheduler.resume()
foo
context_switch(appfoo.sp, appbar.sp)
kout << "bar" << endl
scheduler.resume()
bar
context_switch(appbar.sp, appfoo.sp)

E_0 (Anwendung)

$E_{\frac{1}{2}}$ (Epilog)

E_1 (IRQ/Prolog)

E_0 (Anwendung)

$E_{\frac{1}{2}}$ (Epilog)

E_1 (IRQ/Prolog)

OOStuBS immer synchrone Aufrufe
→ Konsistenz gesichert

Scheduler

OOStuBS immer synchrone Aufrufe
→ Konsistenz gesichert

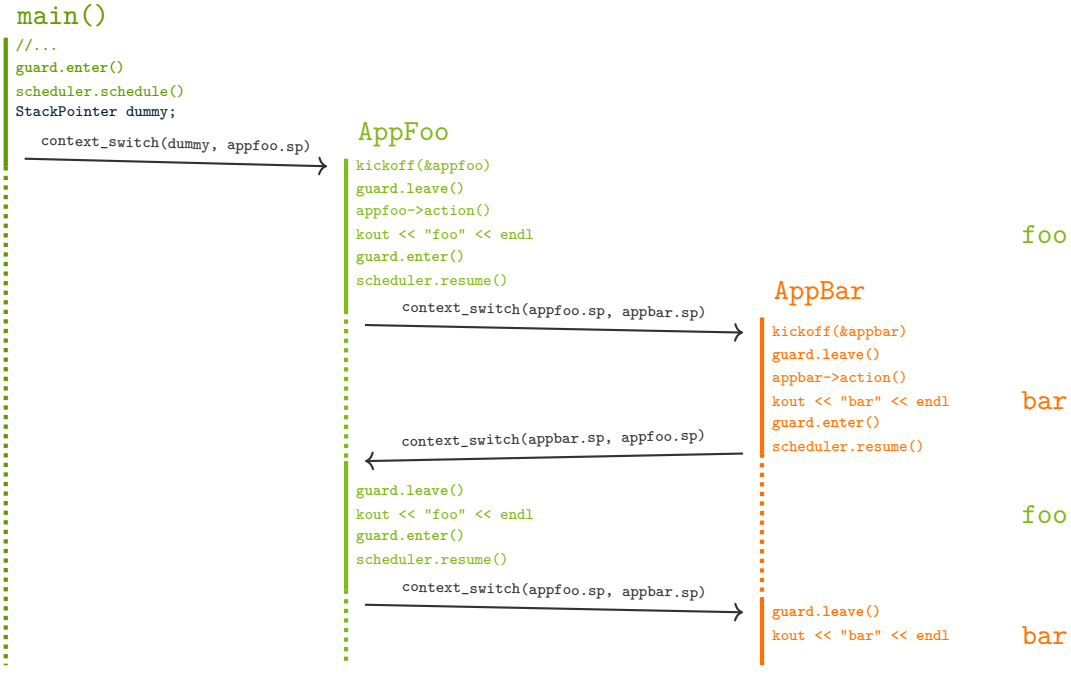
MPStuBS Synchronisation notwendig

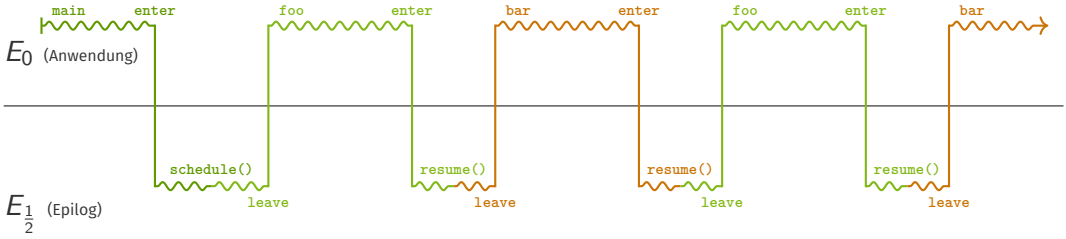
Scheduler

OOStuBS immer synchrone Aufrufe
→ Konsistenz gesichert

MPStuBS Synchronisation notwendig

- Scheduling auf der Epilogebene


main()
//...
guard.enter()
scheduler.schedule()
StackPointer dummy;
context_switch(dummy, appfoo.sp)
AppFoo
kickoff(&appfoo)
guard.leave()
appfoo->action()
kout << "foo" << endl
guard.enter()
scheduler.resume()
foo
context_switch(appfoo.sp, appbar.sp)
AppBar
kickoff(&appbar)
guard.leave()
appbar->action()
kout << "bar" << endl
guard.enter()
scheduler.resume()
bar
context_switch(appbar.sp, appfoo.sp)
guard.leave()
kout << "foo" << endl
guard.enter()
scheduler.resume()
foo
context_switch(appfoo.sp, appbar.sp)
guard.leave()
kout << "bar" << endl
bar


main
enter
foo
enter
bar
enter
foo
enter
bar
E_0 (Anwendung)
schedule()
resume()
resume()
resume()
leave
leave
leave
leave
$E_{\frac{1}{2}}$ (Epilog)
E_1 (IRQ/Prolog)

Fragen?

Abgabe der Aufgabe
bis Mittwoch, den 13. Dezember

Bild: twemoji