X86_64 Discovery

X86-64 Registers

64-bit	32-bit	16-bit	8-bit	Use
RAX	EAX	AX	AL	
RBX	EBX	BX	BL	
RCX	ECX	CX	CL	
RDX	EDX	DX	DL	
RSI	ESI	SI	SIL	
RDI	EDI	DI	DIL	
RBP	EBP	BP	BPL	Current Stack-Frame Pointer
RSP	ESP	SP	SPL	Stack Pointer
R8	R8D	R8W	R8B	
R9	R9D	R9W	R9B	
R10	R10D	R10W	R10B	
R11	R11D	R11W	R11B	
R12	R12D	R12W	R12B	
R13	R13D	R13W	R13B	
R14	R14D	R14W	R14B	
R15	R15D	R15W	R15B	
RIP				Instruction Pointer

Stages of Compilation:

Code:

```
void six_args(long a, long b, long c, long d, long e, long f);
```

Code:

```
void six_args(long a, long b, long c, long d, long e, long f);

void do_six() {
    six_args(1,2,3,4,5,6);
}
```

Generated Code:

```
00000000004027f1 <do_six>:
  4027f1: 55                            pushq   %rbp
  4027f2: 48 89 e5                      movq    %rsp, %rbp
  4027f5: 41 b9 06 00 00 00             movl    $0x6, %r9d
  4027fb: 41 b8 05 00 00 00             movl    $0x5, %r8d
  402801: b9 04 00 00 00                movl    $0x4, %ecx
  402806: ba 03 00 00 00                movl    $0x3, %edx
  40280b: be 02 00 00 00                movl    $0x2, %esi
  402810: bf 01 00 00 00                movl    $0x1, %edi
  402815: e8 8b ff ff ff                callq   0x4027a5 <six_args>
  40281a: 5d                            popq    %rbp
  40281b: c3                            retq
```

Code:

```
long return42() {
    return 42;
}
```

Generated Code:

```
0000000000402857 <return42>:
  402857: b8 2a 00 00 00                movl    $0x2a, %eax
  40285c: c3                            retq
```

Code:

```
long identity(long v) {
    return v;
}
```

Generated Code:

```
0000000000402895 <identity>:
  402895: 48 89 f8                      movq    %rdi, %rax
  402898: c3                            retq
```

Code:

```
long fetch_ptr(long *p) {
    return *p;
}
```

Generated Code:

```
0000000000402871 <fetch_ptr>:
  402871: 48 8b 07                      movq    (%rdi), %rax
  402874: c3                            retq
```

X86_64 Discovery

Code:

```
void store_ptr(long* p, long v) {
    *p = v;
}
```

Generated Code:

```
000000000040286d <store_ptr>:
  40286d: 48 89 37                      movq    %rsi, (%rdi)
  402870: c3                            retq
```

Code:

```
long fetch_next_ptr(long *p) {
    return *(p+1);
}
```

Generated Code:

```
0000000000402875 <fetch_next_ptr>:
  402875: 48 8b 47 08                   movq    0x8(%rdi), %rax
  402879: c3                            retq
```

Code:

```
void store_next_ptr(long* p, long v) {
    *(p+1) = v;
}
```

Generated Code:

```
000000000040287a <store_next_ptr>:
  40287a: 48 89 77 08                   movq    %rsi, 0x8(%rdi)
  40287e: c3                            retq
```

Code:

```
long fetch_array(long *p, long i) {
    return p[i];
}
```

Generated Code:

```
000000000040287f <fetch_array>:
  40287f: 48 8b 04 f7                   movq    (%rdi,%rsi,8), %rax
  402883: c3                            retq
```

Code:

```
void store_array(long *p, long i, long v) {
    p[i] = v;
}
```

Generated Code:

```
0000000000402884 <store_array>:
  402884: 48 89 14 f7                   movq    %rdx, (%rdi,%rsi,8)
  402888: c3                            retq
```

Code:

```
long var1;

void store_var1(long v) {
    var1 = v;
}

long fetch_var1() {
    return var1;
}
```

Generated Code:

```
000000000040285d <store_var1>:
  40285d: 48 89 3d 0c 42 0a 00          movq    %rdi, 0xa420c(%rip)
                                                        # 0x4a6a70 <var1>
  402864: c3                            retq
0000000000402865 <fetch_var1>:
  402865: 48 8b 05 04 42 0a 00          movq    0xa4204(%rip), %rax
                                                        # 0x4a6a70 <var1>
  40286c: c3                            retq
```

Code:

```
long formula(long x, long y) {
    return x + 2 * y + 3;
}
```

Generated Code:

```
000000000040288e <formula>:
  40288e: 48 8d 44 77 03                leaq    0x3(%rdi,%rsi,2), %rax
  402893: c3                            retq
```

Code:

```
void six_args(long a, long b, long c, long d, long e, long f) {
    long result = a;
    result += b;
    result += c;
    result += d;
    result += e;
    result += f;
    print_long(result);
}
```

Generated Code:

```
00000000004027a5 <six_args>:
  4027a5: 55                            pushq   %rbp
  4027a6: 48 89 e5                      movq    %rsp, %rbp
  4027a9: 48 01 f7                      addq    %rsi, %rdi
  4027ac: 48 01 d7                      addq    %rdx, %rdi
  4027af: 48 01 cf                      addq    %rcx, %rdi
  4027b2: 4c 01 c7                      addq    %r8, %rdi
  4027b5: 4c 01 cf                      addq    %r9, %rdi
  4027b8: e8 cc 00 00 00                callq   0x402889 <print_long>
  4027bd: 5d                            popq    %rbp
  4027be: c3                            retq
```

X86_64 Discovery

Code:

```
void twelve_args(long a, long b, long c, long d, long e, long f,
                 long g, long h, long i, long j, long k, long l);

void do_twelve() {
    twelve_args(1,2,3,4,5,6,7,8,9,10,11,12);
}
```

Generated Code:

```
000000000040281c <do_twelve>:
  40281c: 55                            pushq   %rbp
  40281d: 48 89 e5                      movq    %rsp, %rbp
  402820: 6a 0c                         pushq   $0xc
  402822: 6a 0b                         pushq   $0xb
  402824: 6a 0a                         pushq   $0xa
  402826: 6a 09                         pushq   $0x9
  402828: 6a 08                         pushq   $0x8
  40282a: 6a 07                         pushq   $0x7
  40282c: 41 b9 06 00 00 00             movl    $0x6, %r9d
  402832: 41 b8 05 00 00 00             movl    $0x5, %r8d
  402838: b9 04 00 00 00                movl    $0x4, %ecx
  40283d: ba 03 00 00 00                movl    $0x3, %edx
  402842: be 02 00 00 00                movl    $0x2, %esi
  402847: bf 01 00 00 00                movl    $0x1, %edi
  40284c: e8 6e ff ff ff                callq   0x4027bf <twelve_args>
  402851: 48 83 c4 30                   addq    $0x30, %rsp
  402855: c9                            leave
  402856: c3                            retq
```

Code:

```
void twelve_args(long a, long b, long c, long d, long e, long f,
                 long g, long h, long i, long j, long k, long l) {
    long result = a;
    result += b;
    result += c;
    result += d;
    result += e;
    result += f;
    result += g;
    result += h;
    result += i;
    result += j;
    result += k;
    result += l;
    print_long(result);
}
```

Generated Code:

```
00000000004027bf <twelve_args>:
  4027bf: 55                            pushq   %rbp
  4027c0: 48 89 e5                      movq    %rsp, %rbp
  4027c3: 48 01 f7                      addq    %rsi, %rdi
  4027c6: 48 01 d7                      addq    %rdx, %rdi
  4027c9: 48 01 cf                      addq    %rcx, %rdi
  4027cc: 4c 01 c7                      addq    %r8, %rdi
  4027cf: 4c 01 cf                      addq    %r9, %rdi
  4027d2: 48 03 7d 10                   addq    0x10(%rbp), %rdi
  4027d6: 48 03 7d 18                   addq    0x18(%rbp), %rdi
  4027da: 48 03 7d 20                   addq    0x20(%rbp), %rdi
  4027de: 48 03 7d 28                   addq    0x28(%rbp), %rdi
  4027e2: 48 03 7d 30                   addq    0x30(%rbp), %rdi
  4027e6: 48 03 7d 38                   addq    0x38(%rbp), %rdi
  4027ea: e8 9a 00 00 00                callq   0x402889 <print_long>
  4027ef: 5d                            popq    %rbp
  4027f0: c3                            retq


0000000000402894 <print_long>:
  402894: c3                            retq
```