



## Exercise 1:

### ffs\_imp.c:

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

typedef unsigned int uint32_t;

uint32_t ffs_imp(uint32_t word) {
    char n = 1;
    if (!(word & 0xffff)) { n += 16; word >>= 16; }
    if (!(word & 0x00ff)) { n += 8; word >>= 8; }
    if (!(word & 0x000f)) { n += 4; word >>= 4; }
    if (!(word & 0x0003)) { n += 2; word >>= 2; }
    return (word) ? (n+((word+1) & 0x01)) : 0;
}

int main (int argc, char **argv) {
    if (argc != 2) {
        printf("Usage: %s <number>\n", argv[0]);
        exit(0);
    }
    uint32_t n = atol(argv[1]);
    printf("ffs_imp: first 1 at %d\n", ffs_imp(n));
}
```

## Exercise 2:

### ffs\_ref.bc:

```
clang -g -O0 -c -emit-llvm ffs_ref.c -o ffs_ref.bc
```

### ffs\_imp.bc:

```
clang -g -O0 -c -emit-llvm ffs_imp.c -o ffs_imp.bc
```

### ffs\_imp.saw:

```
m1 <- llvm_load_module "ffs_ref.bc";
ffs_ref <- llvm_extract m1 "ffs_ref";

m2 <- llvm_load_module "ffs_imp.bc";
ffs_imp <- llvm_extract m2 "ffs_imp";

let thm1 = [{ \x -> ffs_ref x == ffs_imp x }];
result <- prove z3 thm1;
print result;
```

### running ffs\_imp.saw:

```
saw ffs_imp.saw
[19:05:02.280] Loading file "<path-to-ffs_imp.saw>/ffs_imp.saw"
[19:05:02.439] Valid
```

### Exercise 3:

#### ffs\_mus.c:

```
uint32_t ffs_mus (uint32_t word) {
    static const char debruijn32[32] = {
        0,  1, 23,  2, 29, 24, 19,  3, 30, 27, 25, 11, 20,  8,  4, 13,
        31, 22, 28, 18, 26, 10,  7, 12, 21, 17,  9,  6, 16,  5, 15, 14
    };
    return word ? debruijn32[(word & -word)*0x076be629 >> 27]+1 : 0;
}

int main (int argc, char **argv) {
    if (argc != 2) {
        printf("Usage: %s <number>\n", argv[0]);
        exit(0);
    }
    uint32_t n = atol(argv[1]);
    printf("ffs_mus: first 1 at %d\n", ffs_mus(n));
}
```

#### ffs\_mus.bc:

```
clang -g -O0 -c -emit-llvm ffs_mus.c -o ffs_mus.bc
```

#### ffs\_imp.saw:

```
m1 <- llvm_load_module "ffs_ref.bc";
ffs_ref <- llvm_extract m1 "ffs_ref";

m2 <- llvm_load_module "ffs_mus.bc";
ffs_mus <- llvm_extract m2 "ffs_mus";

let thm2 = [{ \x -> ffs_ref x == ffs_mus x }];
result <- prove z3 thm2;
print result;
```

#### running ffs\_imp.saw:

```
saw ffs_mus.saw
[17:40:08.109] Loading file
"<path-to-ffs_mus.saw>/ffs_mus.saw"
[17:40:08.280] Valid
```

### Exercise 4:

#### ffs\_bug.c:

```
uint32_t ffs_bug(uint32_t word) {
    int i = 0;
    int cnt = 0;
    if (!word) return 0;

    /* injected bug: */
    if (word == 1052688) return 4; /* instead of 5 (in hex: 0x101010) */

    for (cnt = 0; cnt < 32; cnt++)
        if (((1 << i++) & word) != 0) return i;
    return 0;
}
```

```

int main (int argc, char **argv) {
    if (argc != 2) {
        printf("Usage: %s <number>\n", argv[0]);
        exit(0);
    }
    uint32_t n = atol(argv[1]);
    printf("ffs_bug: first 1 at %d\n", ffs_bug(n));
}

```

#### **ffs\_bug.bc:**

```
clang -g -O0 -c -emit-llvm ffs_bug.c -o ffs_bug.bc
```

#### **ffs\_bug.saw:**

```

m1 <- llvm_load_module "ffs_ref.bc";
ffs_ref <- llvm_extract m1 "ffs_ref";

m2 <- llvm_load_module "ffs_bug.bc";
ffs_bug <- llvm_extract m2 "ffs_bug";

let thm3 = {{ \x -> ffs_ref x == ffs_bug x }};
result <- prove z3 thm3;
print result;

```

#### **running ffs\_bug.saw:**

```

saw ffs_bug.saw
[17:57:41.672] Loading file
"<path-to-ffs_bug.saw>/ffs_bug.saw"
[17:57:41.835] Sat: [x = 1052688]

```