| galois |

Exercise 1:

add.saw:

```
m <- llvm_load_module "add.bc";

let add_spec = do {
    x <- llvm_fresh_var "x" (llvm_int 32);
    y <- llvm_fresh_var "y" (llvm_int 32);

    llvm_execute_func [llvm_term x, llvm_term y];

    ret <- llvm_fresh_var "ret" (llvm_int 32);
    llvm_return (llvm_term ret);
};

add_ov <- llvm_verify m "add" [] true add_spec z3;
```

running add.saw:

```
saw add.saw
[16:22:28.263] Loading file
"<path-to-add.saw>/add.saw"
[16:22:28.334] Verifying add ...
[16:22:28.336] Simulating add ...
[16:22:28.339] Checking proof obligations add ...
[16:22:28.406] Proof succeeded! add
```

Exercise 2:

add_ptr.saw:

```
m <- llvm_load_module "add_in.bc";

let ptr_to_fresh(name : String) (type : LLVMType) = do {
    x <- llvm_fresh_var name type;
    p <- llvm_alloc type;
    llvm_points_to p (llvm_term x);
    return (x, p);
};

let add_in_spec = do {
    (x,p) <- ptr_to_fresh "x" (llvm_int 32);
    y <- llvm_fresh_var "y" (llvm_int 32);
    llvm_execute_func [p, llvm_term y];
    llvm_return (llvm_term {{ x+y : [32]}});
};

add_in_ov <- llvm_verify m "add_in" [] true add_in_spec z3;
```

running add.saw:

```
saw add_ptr.saw
[20:21:06.429] <path-to-add_ptr.saw>/add_ptr.saw"
[20:21:06.501] Verifying add_ptr ...
[20:21:06.503] Simulating add_ptr ...
```

[20:21:06.506] Checking proof obligations add_ptr ...
[20:21:06.512] Proof succeeded! add_ptr

Exercise 3:

Exercise 4:

Exercise 5:

Exercise 6:

Exercise 7:

Exercise 8:

Exercise 9:

Example 10: