| galois |

Exercise 1:

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
```

makeaigc.saw:

```
c1 <- llvm_load_module "ffs_ref.bc";
c2 <- llvm_load_module "ffs_imp.bc";

c_ffs_ref <- llvm_extract c1 "ffs_ref";
c_ffs_imp <- llvm_extract c2 "ffs_imp";

write_aig "c_ffs_ref.aig" c_ffs_ref;
write_aig "c_ffs_imp.aig" c_ffs_imp;
```

running makeaigc.saw:

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

running `ls` in directory `lab5C`:

```
c_ffs_imp.aig   ffs_imp.c   ffs_imp.bc   lab.pdf       background.pdf
c_ffs_ref.aig   ffs_ref.c   ffs_ref.bc   solution.odt  synopsis.pdf
```

Exercise 2:

ffs_ref.class:

```
javac ffs_ref.java
```

ffs_imp.class:

```
javac ffs_imp.java
```

makeaigjava.saw:

```
j1 <- java_load_class "ffs_ref";
j2 <- java_load_class "ffs_imp";

java_ffs_ref <- jvm_extract j1 "ffs_ref";
java_ffs_imp <- jvm_extract j2 "ffs_imp";

write_aig "java_ffs_ref.aig" java_ffs_ref;
write_aig "java_ffs_imp.aig" java_ffs_imp;
```

running makeaigjava.saw:

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

aig file statistics:

	size	#and vertices
c_ffs_ref.aig:	4050K	1392
c_ffs_imp.aig:	5287K	1878
java_ffs_ref.aig:	4050K	1392
java_ffs_imp.aig:	5092K	1786

Exercise 3:

makeaigcryptol.saw:

```
c1 <- cryptol_load "ffs.cry";

cry_ffs_ref <- cryptol_extract c1 "ffs_ref";
cry_ffs_imp <- cryptol_extract c1 "ffs_imp";

write_aig "cry_ffs_ref.aig" cry_ffs_ref;
write_aig "cry_ffs_imp.aig" cry_ffs_imp;
```

running makeaigcryptol.saw:

```
saw makeaigcryptol.saw
[10:39:35.646] Loading file "<path-to-makeaigcryptol.saw>/makeaigcryptol.saw"
```

aig file statistics:

	size	#and vertices
c_ffs_ref.aig:	4050	1392
c_ffs_imp.aig:	5287	1878
java_ffs_ref.aig:	4050	1392
java_ffs_imp.aig:	5092	1786
cry_ffs_ref.aig:	25017	8427
cry_ffs_imp.aig:	6117	2151

Exercise 4:

ffs_compare_aig.saw:

```
java_ffs_ref <- read_aig "java_ffs_ref.aig";
java_ffs_imp <- read_aig "java_ffs_imp.aig";

c_ffs_ref <- read_aig "c_ffs_ref.aig";
c_ffs_imp <- read_aig "c_ffs_imp.aig";

cry_ffs_ref <- read_aig "cry_ffs_ref.aig";
cry_ffs_imp <- read_aig "cry_ffs_imp.aig";

print "java ref aig <-> java imp aig";
let thm1 = {{ \x -> java_ffs_ref x == java_ffs_imp x }};
result <- prove z3 thm1;
print result;
print " ";

print "c ref aig <-> c imp aig ";
let thm2 = {{ \x -> c_ffs_ref x == c_ffs_imp x }};
result <- prove z3 thm2;
print result;
print " ";

print "c ref aig <-> java imp aig";
let thm3 = {{ \x -> java_ffs_ref x == c_ffs_imp x }};
result <- prove z3 thm3;
print result;
print " ";

print "java ref aig <-> c imp aig";
let thm4 = {{ \x -> java_ffs_ref x == c_ffs_imp x }};
result <- prove z3 thm4;
print result;
print " ";
```

```
print "java imp aig <-> cryptol ref aig";
let thm5 = {{ \x -> java_ffs_imp x == cry_ffs_ref x }};
result <- prove z3 thm5;
print result;
print " ";

print "java imp aig <-> cryptol imp aig";
let thm6 = {{ \x -> java_ffs_imp x == cry_ffs_imp x }};
result <- prove z3 thm6;
print result;
print " ";

print "cryptol imp aig <-> cryptol ref aig";
let thm7 = {{ \x -> cry_ffs_imp x == cry_ffs_ref x }};
result <- prove z3 thm7;
print result;
print " ";

print "c imp aig <-> cryptol ref aig";
let thm8 = {{ \x -> c_ffs_imp x == cry_ffs_ref x }};
result <- prove z3 thm8;
print result;
```

running `ffs_compare_aig.saw`:

```
saw ffs_compare_aig.saw
[10:52:54.434] java ref aig <-> java imp aig
[10:52:54.547] Valid
[10:52:54.547]
[10:52:54.548] c ref aig <-> c imp aig
[10:52:54.687] Valid
[10:52:54.687]
[10:52:54.687] c ref aig <-> java imp aig
[10:52:54.796] Valid
[10:52:54.796]
[10:52:54.796] java ref aig <-> c imp aig
[10:52:54.933] Valid
[10:52:54.933]
[10:52:54.933] java imp aig <-> cryptol ref aig
[10:52:55.180] Valid
[10:52:55.181]
[10:52:55.181] java imp aig <-> cryptol imp aig
[10:52:55.328] Valid
[10:52:55.328]
[10:52:55.328] cryptol imp aig <-> cryptol ref aig
[10:52:55.575] Valid
[10:52:55.575]
[10:52:55.575] c imp aig <-> cryptol ref aig
[10:52:55.846] Valid
```