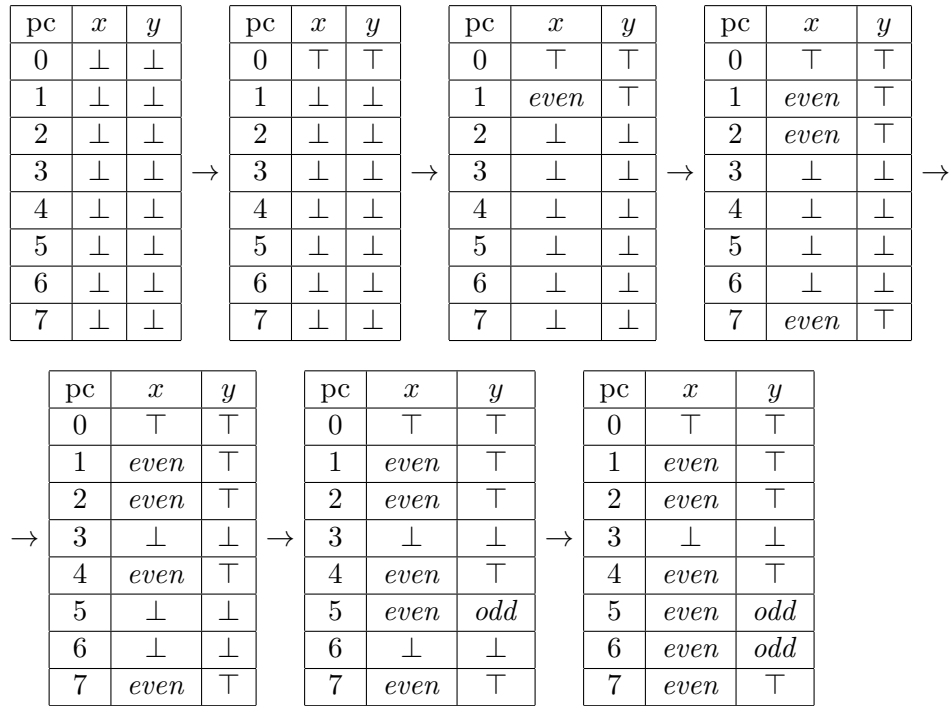


Assignment 8: Solution

Exercise 1



Exercise 2

The domains Sign and Interval are comparable. Parity is not comparable with both Sign and Interval.

1. The Interval domain is more precise than Sign. This is because any state expressed with the Sign domain can be expressed with the Interval domain. The converse does not hold, there are states expressed using the Interval domain that cannot be expressed using the Sign domain.
2. The following program can be verified using the Interval domain, but it cannot be verified with the Parity domain:

```
int x = 1;
assert x > 0;
```

The following program can be verified using the Parity domain, but it cannot be verified with the Interval domain:

```
foo(int i) {
    x := 2*i;
    assert x is even;
}
```

Exercise 3

```
int x = 1;
int z = 0;
if (x!=1) {
    int y,t,u;
    y=9;      // Unreachable code for the Interval domain
    t=19;     // but reachable under the Sign domain.
    u=199;
}
assert(z == 0);
```

Exercise 4

```
int x = 5;
int y = 7;
while (i >= 0) {
    y = y + 1; // Sign domain iterates here once
    i = i - 1; // Interval domain with widening - twice
}
assert(x >= 0);
```

Exercise 5

Yes. For example, let the domain be intervals of the type $[a, b]$, and we restrict $a, b \in \{-\infty, 5, 7, \infty\}$.