CS705 Assignment 2

Q1.) Model-checking LTL properties using SPIN

Uses only 3 process, because of state space explosion (N=4, States=1e+06).

ltl properties:

```
/* Safety Property: Multiple processes cannot enter the critical section
simultaneously. */
ltl safety { [](ncrit <= 1) }

/* Liveness Property: If a process is waiting, it will eventually enter
the critical section. */
ltl liveness1_pN {[](pos[_pid] > 0 -> <> (ncrit == 1))}
/* Always, if the process is in the waiting state (flag[_pid] > 0), then
eventually (<>) it will reach the critical section (ncrit == 1) */

/* Liveness Property: Any process not in the critical section will
eventually enter it. */
ltl liveness2_pN {[](pos[_pid] == 0 -> <> (ncrit == 1))}
/* Always, if a process is not in crit sect (flag[_pid] == 0), then
eventually (<>) it will enter the critical section (ncrit == 1) */
```

ltl property for each process as `_pid` is not defined outside of the model.

Results:

safety:

```
admin@debian:~/repo/cs705_assignments/cs705_as2/Q1$ ./pan -a -f -N safety
pan: ltl formula safety

(Spin Version 6.5.2 -- 6 December 2019)
        + Partial Order Reduction

Full statespace search for:
        never claim             + (safety)
        assertion violations    + (if within scope of claim)
        acceptance   cycles     + (fairness enabled)
        invalid end states      - (disabled by never claim)

State-vector 56 byte, depth reached 7289, errors: 0
```

```
    12734 states, stored
     9974 states, matched
    22708 transitions (= stored+matched)
        0 atomic steps
hash conflicts:         8 (resolved)

Stats on memory usage (in Megabytes):
    1.020       equivalent memory usage for states (stored*(State-vector +
overhead))
    0.963       actual memory usage for states (compression: 94.44%)
                state-vector as stored = 51 byte + 28 byte overhead
  128.000       memory used for hash table (-w24)
    0.534       memory used for DFS stack (-m10000)
  129.413       total actual memory usage


unreached in proctype user
        petersons_n_muetx.pml:46, state 40, "-end-"
        (1 of 40 states)
unreached in claim safety
        _spin_nvr.tmp:8, state 10, "-end-"
        (1 of 10 states)

pan: elapsed time 0.02 seconds
pan: rate    636700 states/second
```

There were no errors from the `safety` ltl property, meaning that at no point in the execution was the safety property violated.
The model is cyclic and continuously executes the processes with `goto again`, hence `-end-` is never reached.

liveness1:

```
admin@debian:~/repo/cs705_assignments/cs705_as2/Q1$ ./pan -a -f -N
liveness1_p2
pan: ltl formula liveness1_p2

(Spin Version 6.5.2 -- 6 December 2019)
        + Partial Order Reduction

Full statespace search for:
        never claim             + (liveness1_p2)
        assertion violations    + (if within scope of claim)
        acceptance   cycles     + (fairness enabled)
        invalid end states      - (disabled by never claim)

State-vector 56 byte, depth reached 7289, errors: 0
```

```
    18214 states, stored (32741 visited)
    24905 states, matched
    57646 transitions (= visited+matched)
        0 atomic steps
hash conflicts:        13 (resolved)

Stats on memory usage (in Megabytes):
    1.459       equivalent memory usage for states (stored*(State-vector +
overhead))
    1.354       actual memory usage for states (compression: 92.80%)
                state-vector as stored = 50 byte + 28 byte overhead
  128.000       memory used for hash table (-w24)
    0.534       memory used for DFS stack (-m10000)
  129.804       total actual memory usage


unreached in proctype user
        petersons_n_muetx.pml:46, state 40, "-end-"
        (1 of 40 states)
unreached in claim liveness1_p2
        _spin_nvr.tmp:41, state 13, "-end-"
        (1 of 13 states)

pan: elapsed time 0.04 seconds
pan: rate    818525 states/second
```

No errors (`errors: 0`) from `liveness1_p2`, meaning process 2 is guaranteed to eventually enter the critical section when it attempts to.
State Space Search:

```
22825 states, stored (51125 visited)
46604 states, matched
97729 transitions (= visited+matched)
```

These values indicate that a larger portion of the state space was explored for this property, showing that the verification examined a wide range of paths to ensure process 2 isn't starved.

liveness2:

```
admin@debian:~/repo/cs705_assignments/cs705_as2/Q1$ ./pan -a -f -N
liveness2_p2
pan: ltl formula liveness2_p2

(Spin Version 6.5.2 -- 6 December 2019)
        + Partial Order Reduction
```

```
Full statespace search for:
        never claim             + (liveness2_p2)
        assertion violations    + (if within scope of claim)
        acceptance   cycles     + (fairness enabled)
        invalid end states      - (disabled by never claim)

State-vector 56 byte, depth reached 7289, errors: 0
    22825 states, stored (51125 visited)
    46604 states, matched
    97729 transitions (= visited+matched)
        0 atomic steps
hash conflicts:        15 (resolved)

Stats on memory usage (in Megabytes):
    1.828       equivalent memory usage for states (stored*(State-vector +
overhead))
    1.647       actual memory usage for states (compression: 90.08%)
                state-vector as stored = 48 byte + 28 byte overhead
  128.000       memory used for hash table (-w24)
    0.534       memory used for DFS stack (-m10000)
  130.097       total actual memory usage


unreached in proctype user
        petersons_n_muetx.pml:46, state 40, "-end-"
        (1 of 40 states)
unreached in claim liveness2_p2
        _spin_nvr.tmp:74, state 13, "-end-"
        (1 of 13 states)

pan: elapsed time 0.08 seconds
pan: rate  639062.5 states/second
```

No errors (`errors: 0`) from `liveness2_p2`, meaning process 2 is guaranteed to eventually enter the critical section, even if it isn't actively trying to at the moment.
State Space Search:

```
22825 states, stored (51125 visited)
46604 states, matched
97729 transitions (= visited+matched)
```

These values indicate that a larger portion of the state space was explored for this property, showing that the verification examined a wide range of paths to ensure process 2 isn't starved.

General

No atomic steps: The model doesn't include any atomic operations, as we are using control structures.

Unreached states in `user` process: The implicit termination state (`-end-` state) is never reached. This is due to the process loops using goto again indefinitely.

Full results

Results for the other processes:

```
admin@debian:~/repo/cs705_assignments/cs705_as2/Q1$ ./pan -a -f -N
liveness1_p0
pan: ltl formula liveness1_p0

(Spin Version 6.5.2 -- 6 December 2019)
        + Partial Order Reduction

Full statespace search for:
        never claim             + (liveness1_p0)
        assertion violations    + (if within scope of claim)
        acceptance   cycles     + (fairness enabled)
        invalid end states      - (disabled by never claim)

State-vector 56 byte, depth reached 7289, errors: 0
    18093 states, stored (33223 visited)
    24963 states, matched
    58186 transitions (= visited+matched)
        0 atomic steps
hash conflicts:        51 (resolved)

Stats on memory usage (in Megabytes):
    1.449       equivalent memory usage for states (stored*(State-vector +
overhead))
    1.354       actual memory usage for states (compression: 93.42%)
                state-vector as stored = 50 byte + 28 byte overhead
  128.000       memory used for hash table (-w24)
    0.534       memory used for DFS stack (-m10000)
  129.804       total actual memory usage

unreached in proctype user
        petersons_n_muetx.pml:46, state 40, "-end-"
        (1 of 40 states)
unreached in claim liveness1_p0
        _spin_nvr.tmp:19, state 13, "-end-"
        (1 of 13 states)
```

```
pan: elapsed time 0.05 seconds
pan: rate    664460 states/second

admin@debian:~/repo/cs705_assignments/cs705_as2/Q1$ ./pan -a -f -N
liveness1_p1
pan: ltl formula liveness1_p1

(Spin Version 6.5.2 -- 6 December 2019)
        + Partial Order Reduction

Full statespace search for:
        never claim             + (liveness1_p1)
        assertion violations    + (if within scope of claim)
        acceptance   cycles     + (fairness enabled)
        invalid end states      - (disabled by never claim)

State-vector 56 byte, depth reached 7289, errors: 0
    18327 states, stored (33422 visited)
    25341 states, matched
    58763 transitions (= visited+matched)
        0 atomic steps
hash conflicts:        68 (resolved)

Stats on memory usage (in Megabytes):
    1.468       equivalent memory usage for states (stored*(State-vector +
overhead))
    1.354       actual memory usage for states (compression: 92.23%)
                state-vector as stored = 49 byte + 28 byte overhead
  128.000       memory used for hash table (-w24)
    0.534       memory used for DFS stack (-m10000)
  129.804       total actual memory usage

unreached in proctype user
        petersons_n_muetx.pml:46, state 40, "-end-"
        (1 of 40 states)
unreached in claim liveness1_p1
        _spin_nvr.tmp:30, state 13, "-end-"
        (1 of 13 states)

pan: elapsed time 0.05 seconds
pan: rate    668440 states/second

admin@debian:~/repo/cs705_assignments/cs705_as2/Q1$ ./pan -a -f -N
liveness2_p0
pan: ltl formula liveness2_p0

(Spin Version 6.5.2 -- 6 December 2019)
        + Partial Order Reduction

Full statespace search for:
```

```
        never claim             + (liveness2_p0)
        assertion violations    + (if within scope of claim)
        acceptance   cycles     + (fairness enabled)
        invalid end states      - (disabled by never claim)

State-vector 56 byte, depth reached 7289, errors: 0
    23007 states, stored (50400 visited)
    46281 states, matched
    96681 transitions (= visited+matched)
        0 atomic steps
hash conflicts:        38 (resolved)

Stats on memory usage (in Megabytes):
    1.843       equivalent memory usage for states (stored*(State-vector +
overhead))
    1.647       actual memory usage for states (compression: 89.36%)
                state-vector as stored = 47 byte + 28 byte overhead
  128.000       memory used for hash table (-w24)
    0.534       memory used for DFS stack (-m10000)
  130.097       total actual memory usage


unreached in proctype user
        petersons_n_muetx.pml:46, state 40, "-end-"
        (1 of 40 states)
unreached in claim liveness2_p0
        _spin_nvr.tmp:52, state 13, "-end-"
        (1 of 13 states)

pan: elapsed time 0.08 seconds
pan: rate    630000 states/second

admin@debian:~/repo/cs705_assignments/cs705_as2/Q1$ ./pan -a -f -N
liveness2_p1
pan: ltl formula liveness2_p1

(Spin Version 6.5.2 -- 6 December 2019)
        + Partial Order Reduction

Full statespace search for:
        never claim             + (liveness2_p1)
        assertion violations    + (if within scope of claim)
        acceptance   cycles     + (fairness enabled)
        invalid end states      - (disabled by never claim)

State-vector 56 byte, depth reached 7289, errors: 0
    22720 states, stored (50283 visited)
    45928 states, matched
    96211 transitions (= visited+matched)
        0 atomic steps
```

```
hash conflicts:         10 (resolved)

Stats on memory usage (in Megabytes):
    1.820       equivalent memory usage for states (stored*(State-vector +
overhead))
    1.647       actual memory usage for states (compression: 90.49%)
                state-vector as stored = 48 byte + 28 byte overhead
  128.000       memory used for hash table (-w24)
    0.534       memory used for DFS stack (-m10000)
  130.097       total actual memory usage


unreached in proctype user
        petersons_n_muetx.pml:46, state 40, "-end-"
        (1 of 40 states)
unreached in claim liveness2_p1
        _spin_nvr.tmp:63, state 13, "-end-"
        (1 of 13 states)

pan: elapsed time 0.07 seconds
pan: rate 718328.57 states/second
```

Q2.) SMT solvers for hardware verification

Majority voter equation:

```
Y = (!ABC) + (A!BC) + (AB!C) + (ABC)
```

Equation:

```
Y' = AB + BC + AC
```

Result:

```
admin@debian:~/repo/cs705_assignments$ python -u
"/home/admin/repo/cs705_assignments/cs705_as2/Q2/smt_sovler.py"
Equations are equivalent
```

Simplification steps to prove `!ABC + A!BC + AB!C + ABC == BC + AB + AC`:

Majority voter equation: `(!ABC) + (A!BC) + (AB!C) + (ABC)`

1. distributive law: `ABC + !ABC = BC(!A + A)`

`BC(!A + A) + A!BC + AB!C`

2. complement law: `(!A + A) = 1`

`BC + A!BC + AB!C`

3. distributive law: `BC + A!BC = C(A!B + B)`

`C(A!B + B) + AB!C`

4. absorption law: `A!B + B = A + B`

`C(A + B) + AB!C`

5. expand: `C(A + B) = AC + BC`

`AC + BC + AB!C`

6. distributive law: `AC + AB!C = A(B!C + C)`

`BC + A(B!C + C)`

7. absorption law: `A(B!C + C) = A(B + C)`

`BC + A(B + C)`

8. expand: `A(B + C) = AB + AC`

`BC + AB + AC`