Verificação Formal

Exercícios sobre Model Checking

nuXmv Verifique que algoritmo de exclusão mútua de Peterson para 2 processos realmente garante exclusão mútua e o progresso para ambos os processos.

TLA+ Verifique que a versão generalizada deste algoritmo para N processos garante também essas propriedades.

nuXmv Verifique que algoritmo de exclusão mútua de Dekker para 2 processos realmente garante exclusão mútua e o progresso para ambos os processos.

NuXmv Verifique que o algoritmo *self stabilising* de Dijkstra garante a convergência para um estado correcto (onde apenas um nó possui o *token*) e a estabilidade deste estado num anel com 4 nós.

TLA+ Verifique que a versão generalizada deste algoritmo para um anel de N nós garante também essas propriedades.

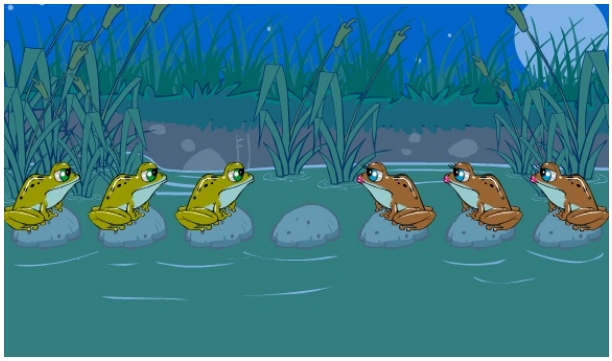
nuXmv O jogo `Lights Out` consiste numa grelha quadrada de lâmpadas. Quando o jogo começa um sub-conjunto aleatório das lâmpadas está acesa. Ao pressionar uma das lâmpadas o seu estado, assim como o das adjacentes, muda (uma lâmpada acesa fica apagada e uma apagada fica acessa). O objectivo do jogo é desligar todas as lâmpadas. Mais informação em

`http://www.logicgamesonline.com/lightsout/`

1. Mostre como poderia resolver o seguinte puzzle (quadrados brancos são luzes ligadas)?

2. Como poderia modificar o modelo anterior para verificar também que o número mínimo de acções para resolver o puzzle é 4?
3. É possível verificar que todos os puzzles 3×3 tem solução? Em caso afirmativo, explique como.

TLA+ Mostre como poderia resolver o conhecido puzzle das rãs ilustrado pela seguinte imagem, mas generalizado para um número arbitrário N (par) de rãs.



Num charco temos uma sequência de $N+1$ pedras alinhadas, $N/2$ rãs verdes encostadas ao lado esquerdo e $N/2$ rãs castanhas encostadas ao lado direito. Em cada pedra pode estar no máximo uma rã. Cada rã pode mover-se para a próxima pedra ou saltar por cima de uma rã de cor diferente que esteja imediatamente à sua frente. O objectivo do puzzle é trocar a posição das rãs verdes com as castanhas.

TLA+ Especifique e verifique o protocolo de eleição de líder de Chang e Roberts para um anel com um número arbitrário de nós.

TLA+ Especifique o seguinte protocolo centralizado para controlo de transações para um número aribtrário de trabalhadores. Todos os nós trabalhadores começam num estado "Working". Os nós trabalhadores podem a qualquer momento terminar a sua tarefa, ficando no estado "Prepared" e informando o nó coordenador desse facto, ou abortar espontaneamente, ficando no estado "Aborted". Depois de o nó coordenador receber mensagens de todos os trabalhadores a informar que estão "Prepared" pode enviar uma mensagem a solicitar o *commit*, terminando a execução. Pode também espontaneamente decidir abortar, enviando uma mensagem a todos os trabalhadores a solicitar o *abort* e terminando a execução. Quando um trabalhador recebe uma mensagem de *commit* passa para o estado "Committed". Quando recebe uma mensagem de *abort* passa para o estado "Aborted". Verifique que este protocolo garante as seguintes propriedades:

- *Consistência*: não pode haver nós com decisões finais ("Committed" ou "Aborted") inconsistentes.
- *Estabilidade*: quando um nó fica "Committed" permanece nesse estado para sempre e idem para o estado "Aborted".
- *Progresso*: assumindo *weak fairness* para ação de *commit* dos trabalhores, se um dos nós fica no estado "Committed" então inevitavelmente todos ficarão nesse estado.