TP3

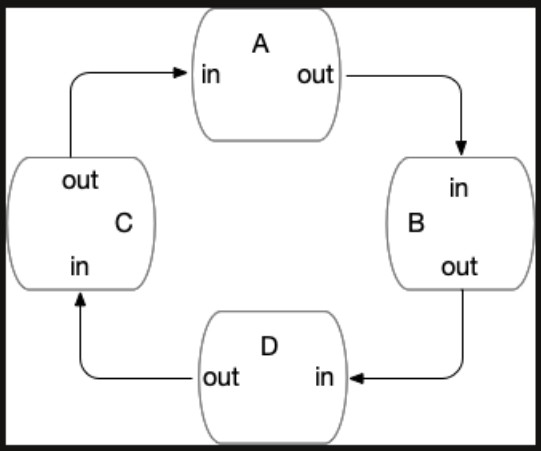
Exercício 3.1

Pretende-se construir uma implementação simplificada do algoritmo "model checking" orientado aos interpolantes seguindo a estrutura apresentada nos apontamentos onde no passo (n, m) na impossibilidade de encontrar um interpolante invariante se dá ao utilizador a possibilidade de incrementar um dos índices n e m à sua escolha.
Pretende-se aplicar este algoritmo ao problema da da multiplicação de inteiros positivos usando Inteiros (apresentado no TP2).

> Aparentemente as SMT's que contém `BitVec` não permitem calcular interpolantes em `z3` ou `msat`. Por isso temos de usar SMT's mais simples que usam apenas inteiros.

Exercício 3.2

O seguinte sistema dinâmico denota 4 *inversores* (A, B, C, D) que lêm um bit num canal input e escrevem num canal output uma transformação desse bit.



i. Cada inversor tem um bit s de estado, inicializado com um valor aleatório.

ii. Cada inversor é regido pelas seguintes transformações

$$\begin{aligned}&\textbf{invert}(in, out)\\ &\quad x \leftarrow \texttt{read}(\texttt{in})\\ &\quad s \leftarrow \neg x \;\;\|\;\; s \leftarrow s \oplus x\\ &\quad \texttt{write}(\texttt{out}, s)\end{aligned}$$

iii. A escolha neste comando é sempre determinística; isto é, em cada inversor a escolha do comando a executar é sempre a mesma. Porém qual é essa escolha é determinada aleatoriamente na inicializarão do sistema.

iii. O estado do sistema é um duplo definido pelos 4 bits s, e é inicializado com um vetor aleatório em $\{0,1\}^4$.

iv. O sistema termina em ERRO quando o estado do sistema for $(0,0,0,0)$.

a. Construa um SFOTS que descreva este sistema e implemente este sistema, numa abordagem BMC ("bouded model checker") num traço com n estados.
b. Verifique se o sistema é seguro usando BMC, k-indução ou model checking com interpolantes.