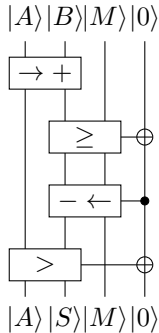


Add first register to second

Compare sum $A+B$ to M

Conditionally subtract M from $A+B$

Compare A to $A+B \bmod M$



$|A\rangle |A+B\rangle |M\rangle |0\rangle$

$|A\rangle |A+B\rangle |M\rangle |?(A+B \geq M)\rangle$

$|A\rangle |A+B \bmod M\rangle |M\rangle |?(A+B \geq M)\rangle$

$|A\rangle |A+B \bmod M\rangle |M\rangle |0\rangle$