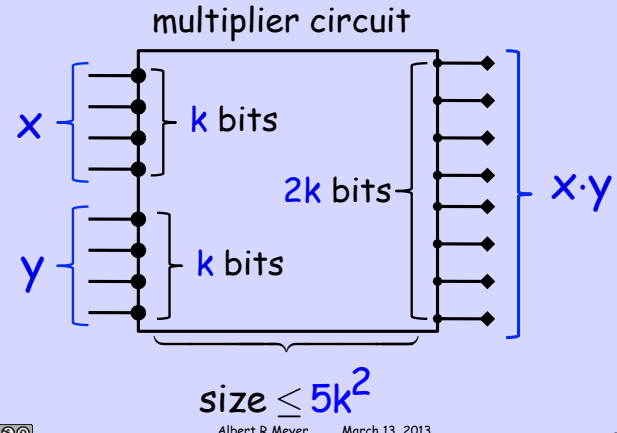
Mathematics for Computer Science
MIT 6.042J/18.062J

Factoring reduces to SAT

Albert R Meyer March 13, 2013

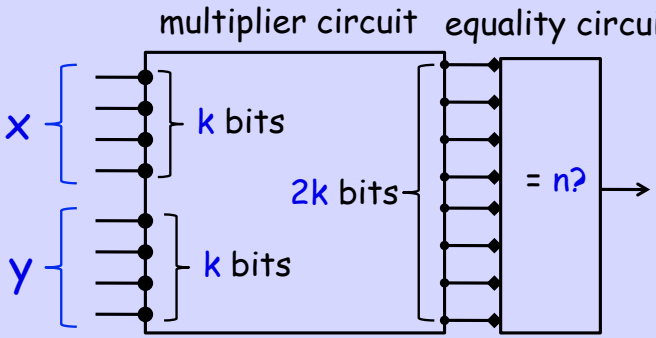
Why does SAT-solver break it?



size $\leq 5k^2$

Albert R Meyer March 13, 2013

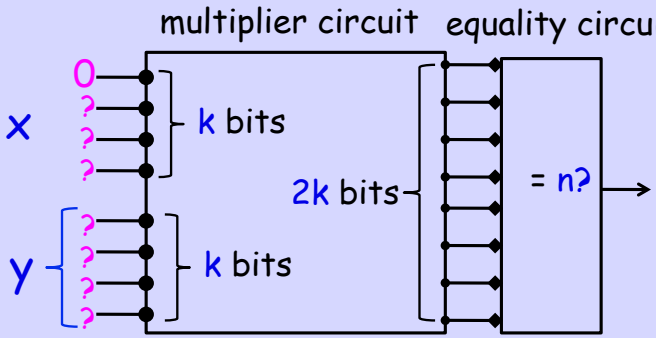
Why does SAT-solver break it?



n ::= pq

Albert R Meyer March 13, 2013

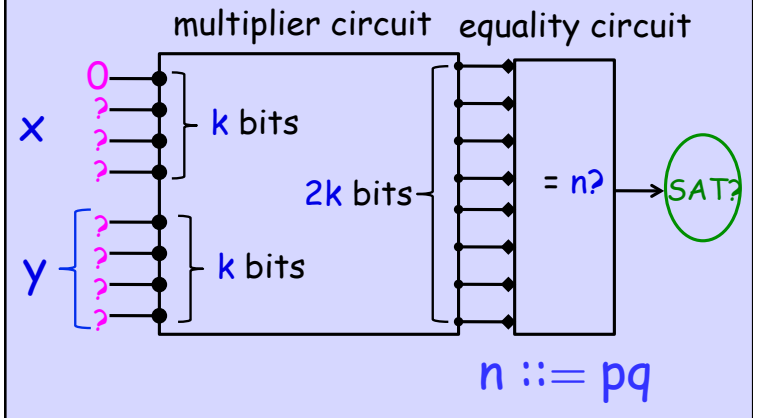
Why does SAT-solver break it?



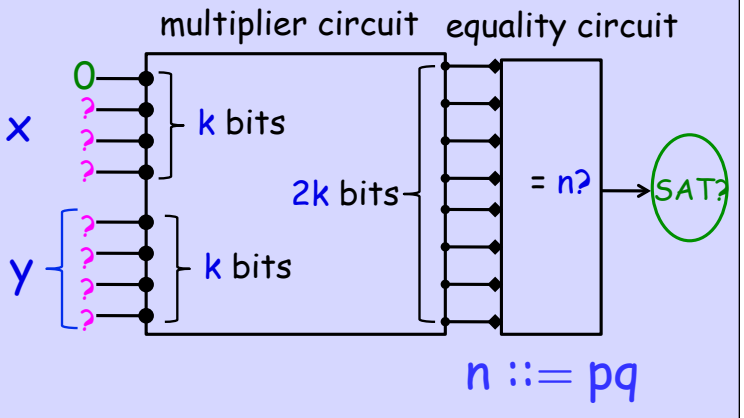
n ::= pq

Albert R Meyer March 13, 2013

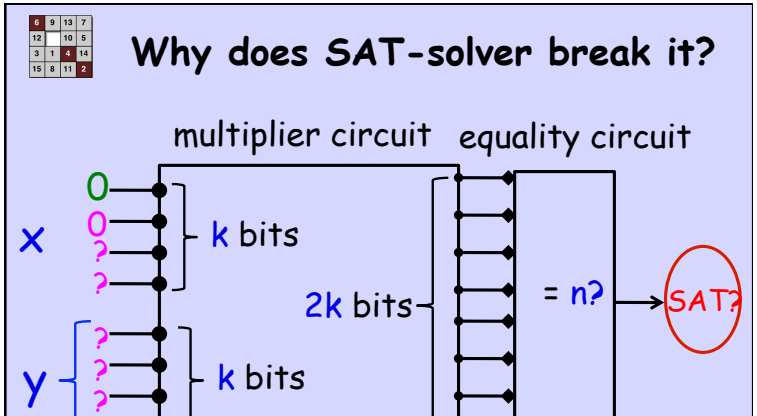
Why does SAT-solver break it?



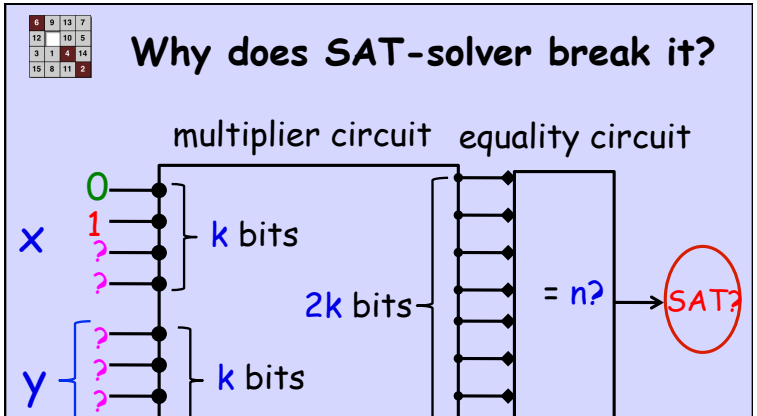
Why does SAT-solver break it?



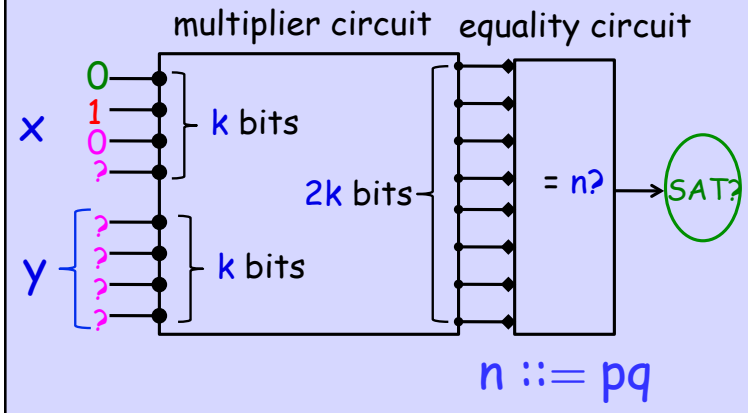
Why does SAT-solver break it?



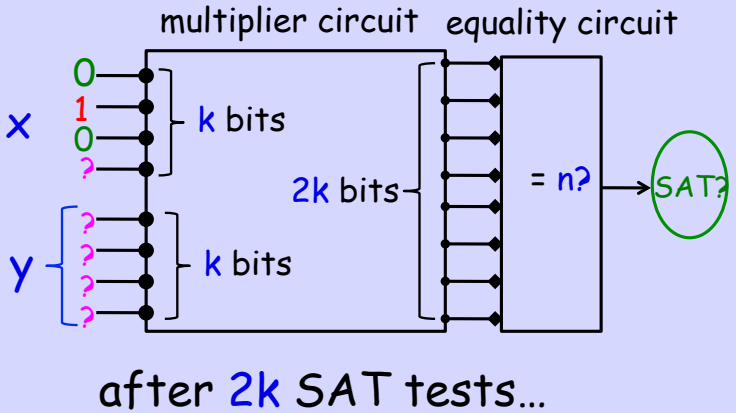
Why does SAT-solver break it?



Why does SAT-solver break it?

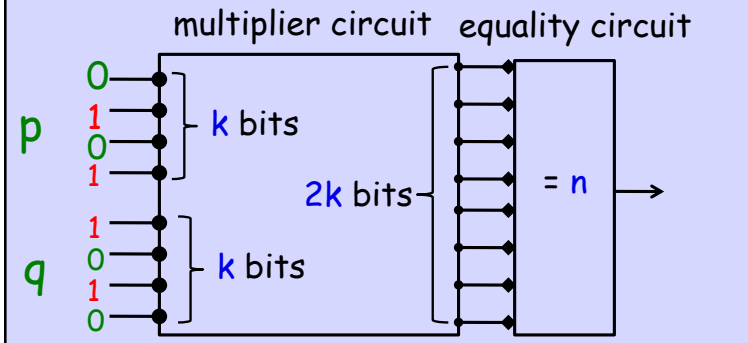


Why does SAT-solver break it?



after 2k SAT tests...

Why does SAT-solver break it?



found the factors p,q !

Why does SAT-solver break it?

SAT-solvers work on formulas.
But there's a simple trick to find
an equi-satisfiable formula
about the same size as circuit.