

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Mathematics for Computer Science
MIT 6.042J/18.062J

Factoring reduces to SAT

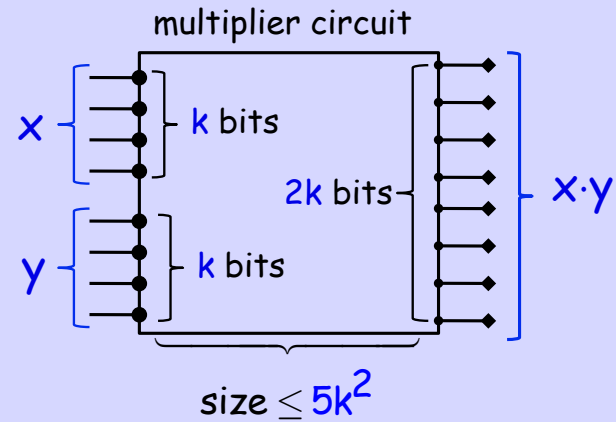


Albert R Meyer March 13, 2013

SATfctr.1

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Why does SAT-solver break it?

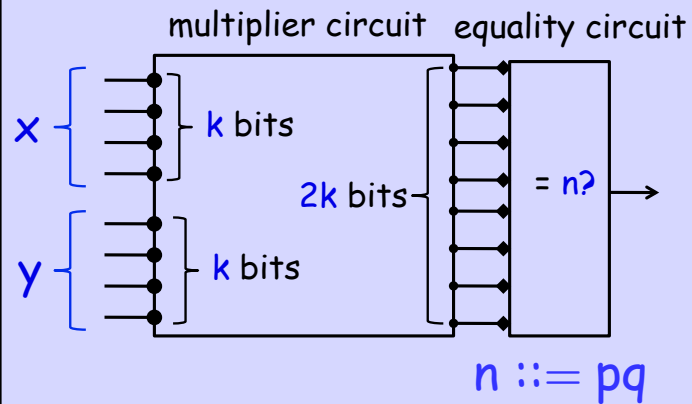


Albert R Meyer March 13, 2013

SATfctr.##

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Why does SAT-solver break it?

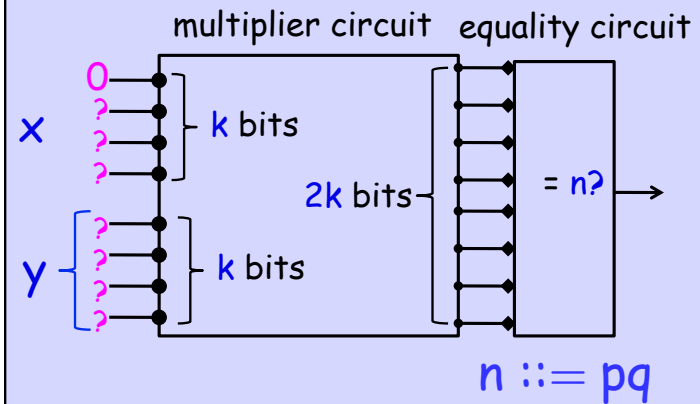


Albert R Meyer March 13, 2013

SATfctr.##

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Why does SAT-solver break it?



Albert R Meyer March 13, 2013

SATfctr.##

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Why does SAT-solver break it?

multiplier circuit

equality circuit

$n ::= pq$

SAT?

Albert R Meyer March 13, 2013 SATfctr.<#>

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Why does SAT-solver break it?

multiplier circuit

equality circuit

$n ::= pq$

SAT?

Albert R Meyer March 13, 2013 SATfctr.<#>

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Why does SAT-solver break it?

multiplier circuit

equality circuit

$n ::= pq$

SAT?

Albert R Meyer March 13, 2013 SATfctr.<#>

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Why does SAT-solver break it?

multiplier circuit

equality circuit

$n ::= pq$

SAT?

Albert R Meyer March 13, 2013 SATfctr.<#>

Why does SAT-solver break it?

multiplier circuit equality circuit

x 0 1 0 ? } k bits

y ? ? ? ? } k bits

2k bits

= n? → SAT?

$n ::= pq$

Albert R Meyer March 13, 2013 SATfctr.<#>

Why does SAT-solver break it?

multiplier circuit equality circuit

x 0 1 0 ? } k bits

y ? ? ? ? } k bits

2k bits

= n? → SAT?

after 2k SAT tests...

Albert R Meyer March 13, 2013 SATfctr.<#>

Why does SAT-solver break it?

multiplier circuit equality circuit

p 0 1 0 1 } k bits

q 1 0 1 0 } k bits

2k bits

= n →

found the factors p, q !

Albert R Meyer March 13, 2013 SATfctr.<#>

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.

Albert R Meyer March 13, 2013 SATfctr.14