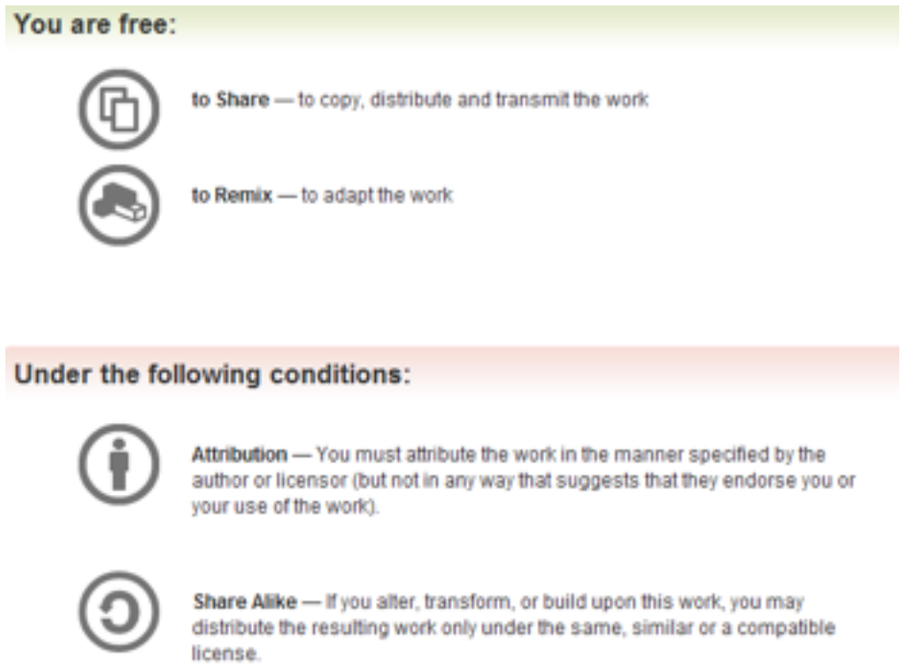
Introduction to Intel x86-64 Assembly, Architecture, Applications, & Alliteration

Xeno Kovah – 2014-2015
xeno@legbacore.com

All materials is licensed under a Creative Commons “Share Alike” license.

- http://creativecommons.org/licenses/by-sa/3.0/



Attribution condition: You must indicate that derivative work
"Is derived from Xeno Kovah's 'Intro x86-64' class, available at http://OpenSecurityTraining.info/IntroX86-64.html"

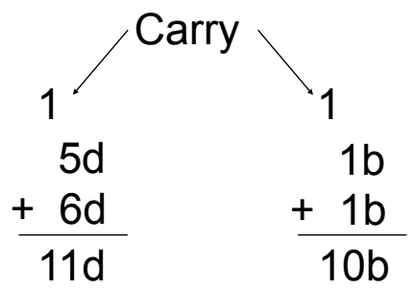
Attribution condition: You must indicate that derivative work

"Is derived from Xeno Kovah's ‘Intro x86-64’ class, available at http://OpenSecurityTraining.info/IntroX86-64.html"

Digression – Why Two's Compliment?

- Alternative methods of representing negative numbers (signed magnitude, or just ones compliment), as well as their problems presented on page 166-167 of the 32 bit book.
  - Note to self: show on board quick
- The benefit of two's compliment is due to having only one representation of zero, and being able to reuse the same hardware for addition/subtraction
- Dave Keppler suggested expanding on this

Why Two's Compliment? 2

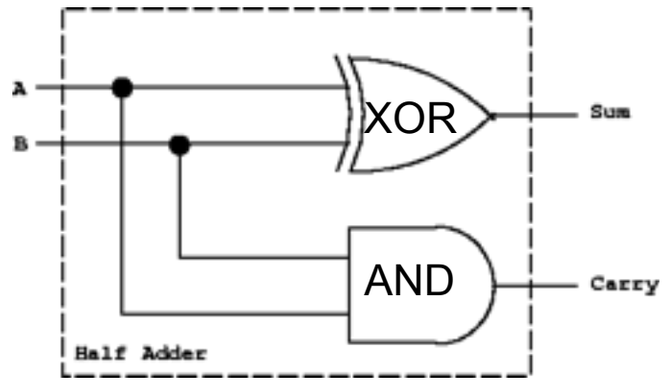


Binary/Decimal Inputs		Decimal Result	Binary Result
A	B	D	$Y_1\ Y_0$
0	0	0	0 0
0	1	1	0 1
1	0	1	0 1
1	1	2	1 0

Table taken from
http://thalia.spec.gmu.edu/~pparis/classes/notes_101/node110.html

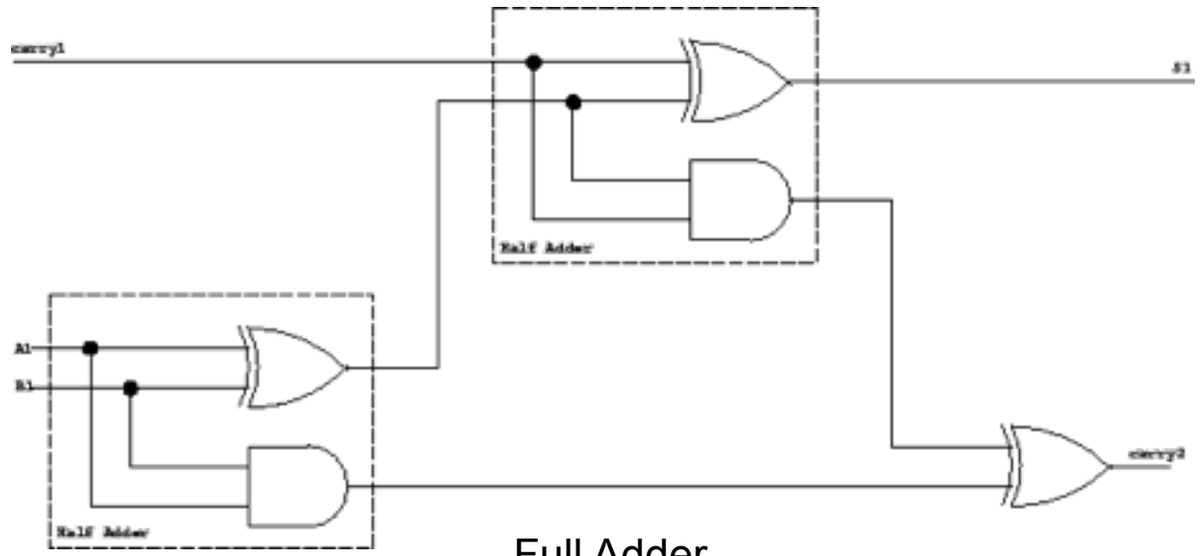
Why Two's Compliment? 3

A half adder circuit suffices for one bit addition



Picture taken from
http://thalia.spec.gmu.edu/~pparis/classes/notes_101/node110.html

Why Two's Compliment? 4



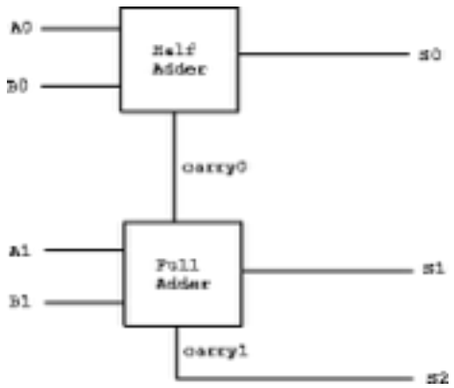
Full Adder

You can't just chain the one bit half adders together to get multi-bit adders. To see why, see the truth table at the link.

Picture taken from
http://thalia.spec.gmu.edu/~pparis/classes/notes_101/node111.html

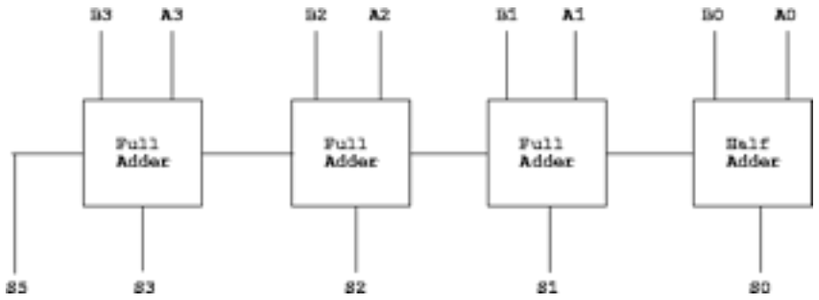
Why Two's Compliment? 5

2 bit adder



Note: we start with a half adder because a full adder would need a carry input at the start. However, if we wanted to use this for subtraction we could use a full adder to start. More on this on next slide.

4 bit adder
(continue to make n bit adder)



Pictures taken from
http://thalia.spec.gmu.edu/~pparis/classes/notes_101/node112.html
http://thalia.spec.gmu.edu/~pparis/classes/notes_101/node113.html

Why Two's Compliment? 6

- So you have these physical adder circuits in the Arithmetic Logic Unit (ALU), and you can feed both add and subtract to the same circuit. But for this to work, you need to start with a full adder, and then run one the one subtract operand bits through not gates, and then set carry to one on the first full adder.
- Keppler's example of x-y == x+(-y)
  - Cause it was right there in my email and I'm lazy ;)

```
  00001010   00001010 (10d) ==  00001010 (10d)
+ 00000101  -00000101 (5d)     +11111011 (-5d)
----------  ---------          ---------
  00001111   00000101         1 00000101
```