BITWISE OPERATIONS (PART 4)

① Shift-and-Add Multiplication

1. Decompose the multiplier into a sum of powers of 2
2. Multiply by powers of 2 by shifting
3. Sum the results

Ex
$$
\begin{aligned}
3 \cdot \underline{21} &= 3 \cdot 10101_2 \\
&= 3 \cdot (2^4 + 2^2 + 2^0) \\
&= 3 \cdot 2^4 + 3 \cdot 2^2 + 3 \cdot 2^0 \\
&= (3 \ll 4) + (3 \ll 2) + (3 \ll 0) \\
&= 110000_2 + 1100_2 + 11_2 \\
&= 111111_2 \\
&= 63
\end{aligned}
$$

② Zeroing a Register

Fact: $a \oplus a = 0$

xor eax, eax sets EAX to 0 ← Why?

Smaller encoding
mov eax, 0 B8 00 00 00 00
xor eax, eax 33 C0

③ Swap Without a Temporary

Fact: $a \oplus b \oplus a = b$

($a \oplus a = 0$
$0 \oplus b = b$
$a \oplus a \oplus b = b$
$a \oplus b \oplus a = b$ since $\oplus$ is commutative)

Can swap EAX & EBX w/ a sequence of 3 XOR's:

```
; Assume n1 in EAX, n2 in EBX

xor eax, ebx    ; EAX = n1 ⊕ n2           EBX = n2
xor ebx, eax    ;    "                    EBX = n2 ⊕ (n1 ⊕ n2) = n1
xor eax, ebx    ; EAX = (n1 ⊕ n2) ⊕ n1 = n2
```

In real life:

```
xchg eax, ebx
```

④ Absolute Value w/o a Conditional (32-bit integer)

DEF. $abs(x) = \begin{cases} -x & \text{if } x < 0 \\ x & \text{if } x \geq 0 \end{cases}$

PF. • Recall Two's Complement: $-x = \underbrace{\neg x + 1}_{\text{Flip Bits \& Add 1}} = \neg x - (-1)$

• Can flip bits using XOR $\quad x \oplus -1 = \neg x$ ①

" retain " " " $\quad x \oplus 0 = x$

• $x \gg^s 31 = \begin{cases} -1 & \text{if } x < 0 \\ 0 & \text{if } x \geq 0 \end{cases}$ ②

combining ①+②,

• So $x \oplus (x \gg^s 31) = \begin{cases} \neg x & \text{if } x < 0 \\ x & \text{if } x \geq 0 \end{cases}$

• Thus, $x \oplus (x \gg^s 31) - (x \gg^s 31) = \begin{cases} \neg x - (-1) & \text{if } x < 0 \\ x & \text{if } x \geq 0 \end{cases}$

THM. • $abs(x) = x \oplus (x \gg^s 31) - (x \gg^s 31)$ ☆

(5) Minimum of Two w/o a Conditional

Def. $$\min(a,b) = \begin{cases} a & \text{if } a < b \\ b & \text{if } a \geq b \end{cases}$$

Thm. $$\min(a,b) = b \oplus \big((a \oplus b) \mathbin{\&} ((a-b) \gg^{s} 31)\big) \qquad (\circledast)$$

Pf. $a - b < 0$ when $a < b$

So $$(a-b) \gg^{s} 31 = \begin{cases} -1 & \text{if } a<b \\ 0 & \text{if } a \geq b \end{cases}$$

$$(a \oplus b) \mathbin{\&} ((a-b) \gg^{s} 31) = \begin{cases} a \oplus b & \text{if } a<b \\ 0 & \text{if } a \geq b \end{cases}$$

So formula $\circledast$ gives $$\begin{cases} b \oplus a \oplus b & \text{if } a<b \\ b \oplus 0 & \text{if } a \geq b \end{cases} = \begin{cases} a & \text{if } a<b \\ b & \text{if } a \geq b. \end{cases} \quad \blacksquare$$

ACTIVITY 15

Algebraic Properties of Bitwise Operations

Commutativity
- a | b = b | a
- a ⊕ b = b ⊕ a
- a & b = b & a

Associativity
- (a | b) | c =a | (b | c)
- (a ⊕ b) ⊕ c = a ⊕ (b ⊕ c)
- (a & b) & c = a & (b & c)

Distributivity
- a & (b | c) = (a & b) | (a & c)
- a & (b ⊕ c) = (a & b) ⊕ (a & c)
- a | (b & c) = (a | b) & (a | c)

Identities
- a | 0 = a
- a ⊕ 0 = a
- a & −1 = a

Inverse
- a ⊕ a = 0

Annihilator
- a & 0 = 0

Cancellation
- ¬(¬a) = a

Complement
- a | ¬a = −1
- a & ¬a = 0

Idempotency
- a & a = a
- a | a = a

Absorption
- a | (a & b) = a
- a & (a | b) = a

DeMorgan's Laws
- ¬(a & b) = ¬a | ¬b
- ¬(a | b) = ¬a & ¬b

Other Properties of 0, −1
- a | −1 = −1
- ¬0 = −1
- ¬−1 = 0

0	00000000
0	00000000
1	00000001
-1	11111111
2	00000010
-2	11111110
3	00000011
-3	11111101
4	00000100
-4	11111100
5	00000101
-5	11111011
6	00000110
-6	11111010
7	00000111
-7	11111001
8	00001000
-8	11111000
9	00001001
-9	11110111
10	00001010
-10	11110110
11	00001011
-11	11110101
12	00001100
-12	11110100
13	00001101
-13	11110011
14	00001110
-14	11110010
15	00001111
-15	11110001
16	00010000
-16	11110000

120	01111000
-120	10001000
121	01111001
-121	10000111
122	01111010
-122	10000110
123	01111011
-123	10000101
124	01111100
-124	10000100
125	01111101
-125	10000011
126	01111110
-126	10000010
127	01111111
-127	10000001

Two's Complement: Flip the bits to the left of the rightmost 1-bit

-127	10000001
-126	10000010
-125	10000011
-124	10000100
-123	10000101
-122	10000110
-121	10000111
-120	10001000
-16	11110000
-15	11110001
-14	11110010
-13	11110011
-12	11110100
-11	11110101
-10	11110110
-9	11110111
-8	11111000
-7	11111001
-6	11111010
-5	11111011
-4	11111100
-3	11111101
-2	11111110
-1	11111111
0	00000000
1	00000001
2	00000010
3	00000011
4	00000100
5	00000101
6	00000110
7	00000111
8	00001000
9	00001001
10	00001010
11	00001011
12	00001100
13	00001101
14	00001110
15	00001111
16	00010000
120	01111000
121	01111001
122	01111010
123	01111011
124	01111100
125	01111101
126	01111110
127	01111111

To add 1: Flip rightmost 0-bit & all bits to its right

To subtract 1: Flip rightmos 1-bit & all bits to its right

Manipulating Rightmost Bits

- Clear the rightmost 1-bit $\quad x \,\&\, (x-1)$

  is 0 if $x=0$ or x is a power of 2

- Set the rightmost 0-bit $\quad x \mid (x+1)$

- Isolate the rightmost 1-bit $\quad x \,\&\, (-x)$