Binary Representations of Numbers — a Proof

CSC165 Week 6 - Part ~~1~~ 2

Lindsey Shorser, Winter 2021

Goal for this week

We want to prove: $\forall\ n \in \mathbb{N},\ 0 \leq x \leq 2^n - 1 \iff B(n,x)$

Strategy: Prove the $\Longrightarrow$ direction using induction

Then prove the $\Longleftarrow$ direction using direct proof.

Decimal (Base 10) Numbers

Possible digits: $\boxed{0, 1, 2, 3, 4, 5, 6, 7, 8, \text{ and } 9}$

Where do we get the digits from? $5027_{10} = (5)10^3 + (0)10^2 + (2)10^1 + (7)10^0$

10^7	10^6	10^5	10^4	10^3	10^2	10^1	10^0
0	0	0	0	5	0	2	7

Binary (Base 2) Numbers

Possible digits = {0, 1}

Example: $(46)_{10} = (101110)_2$

$$= (1)2^5 + (0)2^4 + (1)2^3 + (1)2^2 + (1)2^1 + (0)2^0$$

2^7	$2^6 = 64$	$2^5 = 32$	$2^4 = 16$	$2^3 = 8$	$2^2 = 4$	$2^1 = 2$	$2^0 = 1$
0	0	1	0	1	1	1	0

Example: $(46)_{10} = (101110)_2$

$$= \sum_{i=0}^{5} b_i \, 2^i$$

where $b_0 = 0$, $b_1 = 1$, $b_2 = 1$, $b_3 = 1$, $b_4 = 0$, $b_5 = 1$

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
0	0	1	0	1	1	1	0

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

Definition of Predicate B(n,x)

$\forall\, n \in \mathbb{N}, \forall\, x \in \mathbb{N}$, $B(n,x)$ is true if and only if

$\exists\, b_0, b_1, \ldots, b_{n-1} \in \{0,1\}$ such that $x = (b_{n-1}b_{n-2}\ldots b_1b_0)_2$

$= \Sigma\, b_i\, 2^i$

In other words, B(n,x) is true when x can be written in binary using exactly n bits.

True or False?

$$(5)_{10} = \boxed{(101)_2}$$
$$= \boxed{(0101)_2}$$

$B(3,5) =$ True ✓

$B(4,5) =$ True ✓

$$1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$$

$B(2,5) =$ False

B(n,x) is true when x can be written in binary using exactly n bits.

We want to prove that:

$$\forall\ n \in \mathbb{N},\ \boxed{0 \leq x \leq 2^n - 1} \Longleftrightarrow B(n,x)$$

$$\Longrightarrow$$

$$\Longleftarrow$$

We want to prove that:

$\forall\, n \in \mathbb{N}$, $\boxed{0 \le x \le 2^n - 1} \implies B(n,x)$

Base Case: Let $n = 0$, so $\boxed{0 \le x \le 2^0 - 1}$

In other words, $x = 0_{10} = 0_2$ or else $x = 1_{10} = 1_2$

Therefore $B(0,x)$ is true.

$1 \times 10^0 = 1 \times 2^0$

We want to prove that:

$\forall\, n \in \mathbb{N},\ 0 \leq x \leq 2^n - 1 \Longrightarrow B(n,x)$

Hypothesis

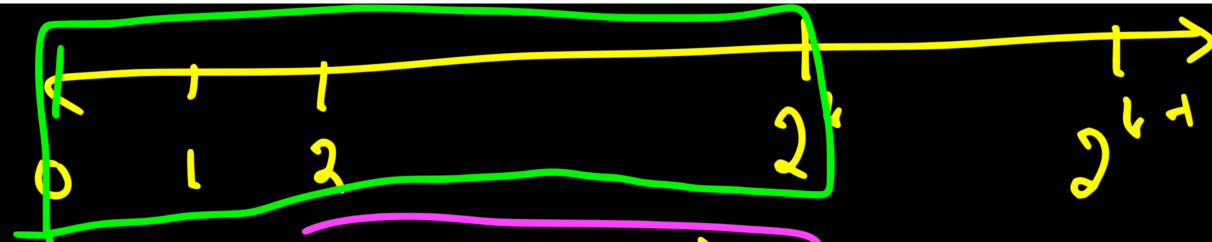
- Induction ~~Step~~: Let $n = k \in \mathbb{N}$

  Assume for some $k \in \mathbb{N}$ $0 \leq x \leq 2^k - 1$
  $\Rightarrow B(k, x)$

- Case of $n = k+1$:

  Want to show that $\forall\, x \in \mathbb{N},\ \boxed{0 \leq x \leq 2^{k+1}-1} \Longrightarrow \boxed{B(k+1,x)}$

Case of n = k+1:



Want to show that $\forall x \in \mathbb{N}$, $\boxed{0 \le x \le 2^{k+1}-1} \Longrightarrow B(k+1,x)$

B(k+1,x) is true when x can be written in binary using exactly k+1 bits.

Either $\boxed{0 \le x \le 2^{k}-1}$ or $\boxed{2^{k} \le x \le 2^{k+1}-1}$

$05_{10} = 5_{10} = 101_2 = 0101_2 = 00101_2$

Case 1: Assume $x \le 2^k - 1$ $0 \le x \le 2^k - 1$

By Induction Hypothesis, we know that $B(k,x)$ is true.
Therefore:

$\exists\, b_0, b_1, \ldots, b_{k-1} \in \{0,1\}$ such that $x = (b_{k-1}b_{k-2}\ldots b_1b_0)_2$

$= \Sigma\, b_i\, 2^i$

We can append a 0 to the left side of the number without changing its value. So $x = (0b_{k-1}b_{k-2}\ldots b_1b_0)_2$

$= (0)\, 2^k + \Sigma\, b_i\, 2^i$

Thus $B(k+1, x)$ is true. ✓

Case 2: Assume $x > 2^k - 1$

Then, $\boxed{2^k \leq x \leq 2^{k+1} - 1}$

Subtract 2^k from all parts to get:

$$2^k - 2^k \leq x - 2^k \leq 2^{k+1} - 1 - 2^k$$

$$0 \leq x - 2^k \leq 2^k(2-1) - 1 \qquad 0 \leq \boxed{x - 2^k} \leq 2^k - 1$$

By the Induction hypothesis, we know $B(k, x-2^k)$

$\exists\ b_0, b_1, \ldots, b_{k-1} \in \{0,1\}$ such that

$$x - 2^k = (b_{k-1}b_{k-2}\ldots b_1 b_0)_2 = \Sigma\ b_i\ 2^i$$

$$\begin{array}{r} 56_{10} \\ -32 \\ \hline 24 \\ -16 \\ \hline 8 \end{array}$$

111000_2

$$x - 2^k + \boxed{2^k}$$

Therefore,

$$0 \le x - 2^k \le 2^k - 1$$

$\exists\ b_0, b_1, \ldots, b_{k-1} \in \{0,1\}$ such that

$x = (1b_{k-1}b_{k-2}\ldots b_1b_0)_2 = (1)2^k + \Sigma\ b_i\ 2^i$

B(k+1, x) is true.

$B(k, x-2^k)$

2^k	2^{k-1}	...	2^2	2^1	2^0
1	b_{k-1}		b_2	b_1	b_0

Now we want to show the other direction:

$$\forall x \in \mathbb{N},\ \boxed{0 \le x \le 2^{\cancel{k+1}\ n}-1} \Longleftarrow \boxed{B(\cancel{k+1}\ n,x)}$$

For a direct proof: Let $n, x \in \mathbb{N}$

Assume $B(n,x)$ is true.

$0\ldots000_2$

- n-zeros is the smallest n-digit binary number
- n-ones " " biggest " " "

$$\underbrace{11\ldots1}_{n \text{ times}} = \boxed{1\times2^0 + 1\times2^1 + 1\times2^2 + \ldots + 1\times2^{n-1}} = 2^n - 1$$

by Lemma

QED

$$\boxed{\sum_{k=0}^{n-1} 2^k \stackrel{?}{=} 2^{n} - 1}$$ ← Lemma

Proof: by induction on n $(\forall n \in \mathbb{N})$

Base Case: $2^0 = 2^1 - 1$ $(n=1)$

($n=0$ is not well-defined)

When $n=k$ assume for $k \in \mathbb{N}$, $2^0 + \ldots + 2^{k-1} = 2^k - 1$

Let $n = k+1$, $\underbrace{2^0 + 2^1 + \ldots + 2^{k-1}}$ $+ 2^k = 2^k - 1 + 2^k$

$= 2(2^k) - 1 = 2^{k+1} - 1$

$1 + 2 + 4 = 7 = 2^3 - 1$

$1 + 2 + 4 + 8 = 15 = 2^4 - 1$

$0 \leq x \leq 2^n - 1$

Modular Arithmetic

Example: n (mod 3) = remainder after calculating $n \div 3$

$x \equiv n \pmod{3}$

$\exists k \in \mathbb{N}$

$x = 3k + n$

-6	-5	-4
-3	-2	-1
0	1	2
3	4	5
6	7	8
9	10	11

$3 \mid$ (numbers that are $\equiv 0 \bmod 3$)

Lemma: $\forall\, a,b,c,d \in \mathbb{Z}$, $m \in \mathbb{Z}$

$$a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \implies \underbrace{ac}_{\substack{\text{rs} \\ \equiv}} \equiv \underbrace{bd}_{\substack{\text{rs} \\ \equiv}} \pmod{m}$$

Let $a = a_1 m + r$ $\qquad c = c_1 m + s$

$b = b_1 m + r$ $\qquad d = d_1 m + s$

Proof: We want to show: *Example 3.4*

$\forall x,y,m \in \mathbb{N}, \forall n \in \mathbb{N}, \boxed{x \equiv y \pmod{m}} \Longrightarrow x^n \equiv y^n \pmod{m}$

Base case: Let n = 0

$$x^k \equiv y^k \pmod{m}$$

$$\Longrightarrow x \cdot x^k \equiv y \cdot y^k \pmod{m} \text{ by Lemma}$$

Induction Hypothesis:

Assume that for some $k \in \mathbb{N}$,

$x,y,m \in \mathbb{N}$, $x \equiv y \pmod{m} \implies x^k \equiv y^k \pmod{m}$

Now let $n = k+1$:

We want to show that $x \equiv y \pmod{m}$

$$\implies x^{k+1} \equiv y^{k+1} \pmod{m}$$

[redacted]