Binary Representations of Numbers — a Proof

CSC165 Week 6 - Part 1

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 ____________________

Decimal (Base 10) Numbers

Possible digits: 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9

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

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

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	2^5	2^4	2^3	2^2	2^1	2^0
0	0	1	0	1	1	1	0

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

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

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 $x = (b_{n-1}b_{n-2}\ldots b_1 b_0)_2$

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

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

True or False?

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

$B(3,5) =$ True

$B(4,5) =$ True

$B(2,5) =$ False

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

We want to prove that:

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

We want to prove that:

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

Base Case: Let $n = 0$, so $0 \leq x \leq 2^0 - 1$

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

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

We want to prove that:

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

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

Assume

Case of $n = k+1$:

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

Case of $n = k+1$:

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

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

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

Case 1: Assume $x \leq 2^k - 1$

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

Subtract 2k from all parts to get:

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

$0 \leq x - 2^k \leq 2^k(2-1) - 1$

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

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

Therefore,

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

Now we want to show the other direction:

$$\forall\ x \in \mathbb{N},\ 0 \leq x \leq 2^{k+1}\text{-}1 \Longleftarrow B(k+1,x)$$

[redacted]

Modular Arithmetic

Example: n (mod 3)

		-1
0	1	2
3		

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

$$a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \implies ac \equiv bd \pmod{m}$$

Proof: We want to show:

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

Base case: Let $n = 0$

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 $x \equiv y \pmod{m}$

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