Module 5

Quantifier scope

$$\underbrace{\forall x \in D,\ (\underbrace{\exists y \in E,\ Q(x,y) \to \underbrace{\forall z \in F,\ R(y,z)}})\ \wedge\ P(x)}$$

$$(\underbrace{\forall x \in \mathbb{Z},\ (\underbrace{\exists y \in \mathbb{Z},\ x < y \wedge Even(y)})})$$

$$\sim\underbrace{(\exists x \in \mathbb{Z}^+,\ (\underbrace{\forall y \in \mathbb{Z}^+,\ x < y \wedge Even(y)}))}$$

Module 5 Predicate Logic

Fundamental difference between a proposition and a predicate.

Example 1: $\underbrace{\text{Alice } \underbrace{\text{is an instructor at UBC}}_{①}}_{②}$

① is a predicate / proposition ?

② is a predicate / proposition ?

Example 2: Let $P(x, y)$ be $x < y$.

$$\underbrace{\forall x \in \mathbb{Z},\ \underbrace{\exists y \in \mathbb{Z},\ \underbrace{P(x, y)}_{①}}_{②}}_{③}$$

① is a predicate / proposition ?

② is a predicate / proposition ?

③ is a predicate / proposition ?

Module 5. Predicate Logic
The Lions Example

① $\forall x \in D,\ L(x) \rightarrow F(x) \equiv \forall x \in D,\ \sim L(x) \vee (L(x) \wedge F(x))$

- Every lion is fierce.
- Every creature is either not a lion or is a fierce lion.

② $\forall x \in D,\ L(x) \wedge F(x)$

- All creatures are fierce lions.
- Every creature is a fierce lion.

③ $\exists x \in D,\ L(x) \wedge \sim C(x)$

- Some lions do not drink coffee
- There exists a creature which is a lion and doesn't drink coffee

④ $\exists x \in D,\ L(x) \rightarrow \sim C(x) \equiv \exists x \in D,\ \sim L(x) \vee (L(x) \wedge \sim C(x))$

- There exists a creature which is not a lion or is a lion and doesn't drink coffee

---

① versus ② : ② can only be true when all creatures are lions. whereas ① can be true even if some creatures are not lions

if $D = \{\text{tiger}\}$, then ① $\equiv T$ but ② $\equiv F$.

---

③ versus ④ : ④ is true as long as there is a creature that is not a lion. whereas ③ can only be true if there is at least one lion.

if $D = \{\text{tiger}\}$, then ④ $\equiv T$ but ③ $\equiv F$

Module 5

The Alice in Wonderland example

F: set of foods, $E(x)$: Alice eats food x.
g: Alice grows s: Alice shrinks.

① Eating food causes Alice to grow or shrink.

$\forall x \in F,\ E(x) \to (g \vee s)$ (strictly speaking, it's more accurate to have $g \oplus s$.)

② Alice shrank when she ate some food.

$\exists x \in F,\ E(x) \wedge s$

Other related quantified statements:

① $\exists x \in F,\ E(x) \to s$.

This statement is true as long as there is one food which Alice does not eat. For example, if carrot $\in F$ and Alice does not eat carrots (i.e. $E(x)$ is false), then this statement is true. So this may say nothing about whether there exists a food which causes Alice to shrink if she ate the food.

② $\forall x \in F,\ E(x) \wedge (g \vee s)$

Alice eats every food and she grows or shrinks.

$\forall x \in F,\ E(x) \to (g \vee s)$

If Alice eats a food, she grows or shrinks.

Module 5 The Lions Example

D: domain of creatures

$L(x)$: x is a lion.
$F(x)$: x is fierce.

① $\forall x \in D, \quad L(x) \to F(x)$.

Every lion is fierce. (Not every creature has to be a lion for this proposition to be true.)

② $\forall x \in D, \quad L(x) \wedge F(x)$.

Every creature is a fierce lion.

Examples: $D = \{\text{rabbit}\}$ ① $\equiv T$ ② $\equiv F$
$D = \{\text{fierce lion 1, fierce lion 2}\}$ ① $\equiv T$ ② $\equiv T$.
$D = \{\text{rabbit, non-fierce lion}\}$ ① $\equiv F$ ② $\equiv F$.

③ $\exists x \in D, \quad L(x) \wedge F(x)$.

There is a fierce lion.

④ $\exists x \in D, \quad L(x) \to F(x)$.

If there is a lion, it must be fierce.

Examples: $D = \{\text{rabbit}\}$ ① $\equiv F$ ② $\equiv T$
$D = \{\text{rabbit, non-fierce lion}\}$ ① $\equiv F$ ② $\equiv T$
$D = \{\text{rabbit, fierce lion}\}$ ① $\equiv T$ ② $\equiv T$

About ④, as soon as we find a creature in D which is not a lion, ④ is true. This says nothing about whether there exists a fierce lion.

D: set of creatures $\qquad$ $L(x)$: x is a lion.

① There is at least one lion.

$$\exists x \in D,\ L(x)$$

② There is at most one lion.

ⓐ $\forall x \in D,\ \forall y \in D,\ (L(x) \wedge L(y)) \rightarrow x = y.$

ⓑ $\sim(\exists x \in D,\ \exists y \in D,\ L(x) \wedge L(y) \wedge\ x \neq y)$

ⓒ $(\forall x \in D, \sim L(x)) \vee (\exists x \in D,\ L(x) \wedge \forall y \in D,\ L(y) \rightarrow x = y)$

ⓐ If I can find 2 lions, x and y, they must be the same.

ⓑ It's not the case that there exist 2 different lions.

ⓒ Either there is no lion or there is exactly one lion.

③ There is exactly one lion.

ⓐ $(\exists x \in D,\ L(x)) \wedge (\forall x \in D,\ \forall y \in D,\ (L(x) \wedge L(y)) \rightarrow x = y)$

ⓑ $\exists x \in D,\ L(x) \wedge \forall y \in D,\ L(y) \rightarrow x = y.$

④ There are at least two lions.

$$\sim(\forall x \in D,\ \forall y \in D,\ L(x) \wedge L(y) \rightarrow x = y).$$

$$\exists x \in D,\ \exists y \in D,\ L(x) \wedge L(y) \wedge x \neq y.$$

The challenge method.

Example 1: $\exists x \in \mathbb{Z}, \forall n \in \mathbb{Z}^+, 2^x < n$.

Proof: Choose $x = -1$. Then $2^x = 2^{-1} = \frac{1}{2}$

Consider any unspecified positive integer n.

$n \geq 1$ since n is a positive integer.

So $n \geq 1 > \frac{1}{2} = 2^x$. $\Rightarrow n > 2^x$. ▨

Example 2: $\forall n \in \mathbb{N}, \exists x \in \mathbb{N}, n < 2^x$. (Assume $\mathbb{N} = \{1, 2, 3, \ldots, \}$)

Proof: Consider any unspecified natural number n.

Choose $x = \log_2(n+1)$.

Then $2^x = 2^{\log_2(n+1)} = n+1$.

So $n < n+1 = 2^x$. ▨

Example 3: $\exists x \in \mathbb{N}, \forall n \in \mathbb{N}, n < 2^x$.

This statement is false.

Proof: We prove that $\forall x \in \mathbb{N}, \exists n \in \mathbb{N}, n \geq 2^x$.

Consider any unspecified natural number x.

Choose $n = 2^x$.

It must be that $n \geq 2^x$. ▨

Theorem: For any integer n, $n(n-1)+3$ is odd.

In predicate logic: $\forall n \in \mathbb{Z}, \text{Odd}(n(n-1)+3)$

$\equiv \forall n \in \mathbb{Z}, \exists k \in \mathbb{Z}, n(n-1)+3 = 2k+1$.

Proof:

Consider an unspecified integer n.

Let's consider two cases.

Case 1: n is even.

$n = 2x$ for some integer x.

$n-1 = 2x-1$

$n(n-1)+3 = 2x(2x-1)+3 = 2x(2x-1)+2+1$

$= 2(x(2x-1)+1)+1$

Thus, $n(n-1)+3$ is odd because $x(2x-1)+1$ is an integer.

Case 2: n is odd.

$n = 2x+1$ for some integer x.

$n-1 = 2x+1-1 = 2x$

$n(n-1)+3 = (2x+1)(2x)+3 = 2x(2x+1)+2+1$

$= 2(x(2x+1)+1)+1$

Thus, $n(n-1)+3$ is odd because $x(2x+1)+1$ is an integer.

QED

Theorem: The product of three consecutive integers is divisible by 6.

In predicate logic: $\forall n \in \mathbb{Z}$, DivisibleBy6$(n(n+1)(n+2))$.

$\equiv \forall n \in \mathbb{Z},\ 6 \mid n(n+1)(n+2)$.

$\equiv \forall n \in \mathbb{Z},\ \exists k \in \mathbb{Z},\ n(n+1)(n+2) = 6k$.

Proof:

Consider an unspecified integer n.

First, I will show that $n(n+1)(n+2)$ is divisible by 2.

Case 1: n is even.

$n = 2x$ for some integer x.

$n(n+1)(n+2) = 2x(2x+1)(2x+2)$

$n(n+1)(n+2)$ is divisible by 2 because $x(2x+1)(2x+2)$ is an integer.

Case 2: n is odd.

$n = 2x+1$ for some integer x.

$n(n+1)(n+2) = (2x+1)(2x+2)(2x+3) = (2x+1)2(x+1)(2x+3)$
$= 2(2x+1)(x+1)(2x+3)$

$n(n+1)(n+2)$ is divisible by 2 because $(2x+1)(x+1)(2x+3)$ is an integer.

(continued on the next page).

Proof (continued)

Next, I will show that $n(n+1)(n+2)$ is divisible by 3.

case 1: $n = 3x$ for some integer x.

$n(n+1)(n+2) = 3x(3x+1)(3x+2)$

$n(n+1)(n+2)$ is divisible by 3 since $x(3x+1)(3x+2)$ is an integer.

case 2: $n = 3x+1$ for some integer x.

$n(n+1)(n+2) = (3x+1)(3x+2)(3x+3) = 3(3x+1)(3x+2)(x+1)$

$n(n+1)(n+2)$ is divisible by 3 since $(3x+1)(3x+2)(x+1)$ is an integer.

case 3: $n = 3x+2$ for some integer x.

$n(n+1)(n+2) = (3x+2)(3x+3)(3x+4) = 3(3x+2)(x+1)(3x+4)$.

$n(n+1)(n+2)$ is divisible by 3 since $(3x+2)(x+1)(3x+4)$ is an integer.

Since $n(n+1)(n+3)$ is divisible by 2 and 3, it must be divisible by 6.

QED.

Theorem: For any integer n, $4(n^2+n+1)-3n^2$ is a perfect square.

In predicate logic: $\forall n \in \mathbb{Z}$, PerfectSquare$(4(n^2+n+1)-3n^2)$

$\equiv \forall n \in \mathbb{Z}, \exists k \in \mathbb{Z}, 4(n^2+n+1)-3n^2 = k^2$.

Proof:

Consider an unspecified integer n.

$$4(n^2+n+1)-3n^2 = 4n^2+4n+4-3n^2 = n^2+4n+4$$
$$= (n+2)^2$$

Thus, $4(n^2+n+1)-3n^2$ is a perfect square because $(n+2)$ is an integer.

QED.

Theorem 1: For any integer n, if $n \geq 1$, then $6n^2 + 2n + 8 \leq 16n^2$.

$\forall n \in \mathbb{Z},\ n \geq 1 \rightarrow 6n^2 + 2n + 8 \leq 16n^2$.

Scratch work:

$6n^2 + 2n + 8 \leq 16n^2$

$2n + 8 \leq 16n^2 - 6n^2 = 10n^2$

$2n + 8 \leq 2n^2 + 8n^2$

$2n \leq 2n^2$? $\quad 8 \leq 8n^2$?

$1 \leq n \Rightarrow 2n \leq 2n^2$ ✓

$1 \leq n \Rightarrow 1 \leq n^2 \Rightarrow 8 \leq 8n^2$ ✓

^_^

① Proof: Consider an unspecified integer n. Assume that $n \geq 1$.
We want to prove that $6n^2 + 2n + 8 \leq 16n^2$ is true.
To do this, we need to show that $2n + 8 \leq 10n^2$ is true. Then adding $6n^2$ on both sides, we get $6n^2 + 2n + 8 \leq 16n^2$.

Since $1 \leq n$, multiplying $2n$ on both sides, we have $2n \leq 2n^2$. ① because $2n$ is positive.

Since $1 \leq n$, we have that $1 \leq n^2$. Multiplying 8 on both sides, we get $8 \leq 8n^2$. ②

Adding ① and ②, we have $2n + 8 \leq 2n^2 + 8n^2 = 10n^2$, which is what we wanted to prove.

QED.

Be sure to check out two alternative proofs of this theorem on the next page!

Theorem 1: For any integer n, if $n \geq 1$, then $6n^2+2n+8 \leq 16n^2$.

$\forall n \in \mathbb{Z},\ n \geq 1 \rightarrow 6n^2+2n+8 \leq 16n^2$.

② Proof: Consider an unspecified integer n. Assume that $n \geq 1$.
Since $n \geq 1$, multiplying $2n$ on both sides, we get

$2n^2 \geq 2n$ ① because $2n$ is positive.

Since $n \geq 1$, we know that $n^2 \geq 1$. Multiplying by 8 on both sides, we have $8n^2 \geq 8$ ②

Adding ① and ②, we have $2n^2 + 8n^2 \geq 2n + 8$.

$$10n^2 \geq 2n+8.$$

Add $6n^2$ to both sides, we get

$$10n^2 + 6n^2 \geq 2n+8+6n^2$$

$$16n^2 \geq 6n^2+2n+8.$$

QED.

③ Proof: Consider an unspecified integer n. Assume that $n \geq 1$.
left hand side of the inequality is

$$\begin{aligned} & 6n^2+2n+8 \\ \leq\ & 6n^2+2n^2+8 && 2n \leq 2n^2 \text{ because } n \geq 1. \\ \leq\ & 6n^2+2n^2+8n && 8 \leq 8n \text{ because } n \geq 1. \\ \leq\ & 6n^2+2n^2+8n^2 && 8n \leq 8n^2 \text{ because } n \geq 1. \\ =\ & 16n^2. \end{aligned}$$

which is equal to the right hand side of the inequality.

QED.

Theorem 2: For any integer n, if $n \geq 2$, then $6n^2 + 2n + 8 \leq 9n^2$.

$\forall n \in \mathbb{Z},\ n \geq 2 \rightarrow 6n^2 + 2n + 8 \leq 9n^2$.

Proof: Consider an unspecified integer n. Assume that $n \geq 2$.

The left-hand side of the inequality is

$$
\begin{aligned}
& 6n^2 + 2n + 8 & \\
\leq\ & 6n^2 + n^2 + 8 & 2n \leq n^2 \text{ because } n \geq 2. \\
\leq\ & 6n^2 + n^2 + 4n & 8 \leq 4n \text{ because } n \geq 2. \\
\leq\ & 6n^2 + n^2 + 2n^2 & 4n \leq 2n^2 \text{ because } n \geq 2. \\
=\ & 9n^2. &
\end{aligned}
$$

which is equal to the right-hand side of the inequality.

QED.

Strategies to prove an inequality.

for example: $\forall n \in N,\ n \geq 20 \rightarrow 10n \leq n^2$.

① Start from one side, transform the expression until it becomes the other side.
If you start from the smaller side, you are allowed to make the expression bigger but not smaller.

$$LHS = 10n \underset{\substack{\uparrow \\ 10 \leq 20}}{\leq} 20n \underset{\substack{\uparrow \\ 20 \leq n}}{\leq} n^2 = RHS$$

② Start from an inequality. Multiply or add the same expression on both sides until it becomes the desired inequality.

Since $n \geq 20$, we know that $n \geq 10$.
Multiply n on both sides, the direction of the inequality does not change. Thus, $n^2 \geq 10n$. or $10n \leq n^2$.

Beware, the inequality changes direction if you multiply it by a negative number on both sides.

③ An invalid way to prove an inequality.
Proof: Consider an unspecified natural number n.
Assume that $n \geq 20$.
$$10n \leq n^2$$
Divide by n on both sides, we have
$$10 \leq n$$
This is true because we assumed that $n \geq 20$.
QED.

Theorem: $\forall n \in \mathbb{N},\ n \geqslant 20 \rightarrow 10n \leq n^2$.

An invalid proof:

Proof: Consider an unspecified natural number n.
Assume that $n \geqslant 20$.

$$10n \leqslant n^2.$$

Divide by n on both sides, we have

$$10 \leqslant n$$

This is true because we assumed that $n \geqslant 20$.
QED.

What's wrong with this proof?

- By writing down $10n \leq n^2$, we are assuming that it is true instead of proving that it is true
- We are allowed to divide by n on both sides because n is positive
- The direction of the inequality doesn't change because n is positive.

This proof is trying to work backwards from the conclusion.
This is completely valid scratch work, but not an acceptable proof.

A revised and valid proof:

Proof: Consider an unspecified natural number n.
Assume that $n \geqslant 20$. Thus, we have

$$10 \leq n \quad (\text{because } n \geqslant 20)$$
$$10n \leq n^2 \quad (\text{because } n \text{ is positive})$$

QED.

Proving a statement with mixed quantifiers

Theorem: Every even square can be written as the sum of two consecutive odd integers.

In predicate logic: $\forall x \in N$, $Even(x) \wedge Square(x) \rightarrow SumOfTwoConsOdd(x)$.

$Even(x)$: $\exists a \in Z, x = 2a$. $Square(x)$: $\exists b \in Z, x = b^2$.
$SumOfTwoConsOdd(x)$: $\exists c \in Z, x = (2c-1) + (2c+1) = 4c$.

Theorem: $\forall x \in N, (\exists a \in Z, x = 2a) \wedge (\exists b \in Z, x = b^2)$
$\rightarrow (\exists c \in Z, x = 4c)$.

Proof: Consider an unspecified natural number x.
Assume that x is an even square.
We need to show that x can be written as the sum of two consecutive odd integers. (We need to choose c so that $x = 4c$.)

x is a square. So $x = b^2$ for some integer b.
We will show that if b^2 is even, then b is even. We prove the contrapositive: if b is odd, then b^2 is odd.
Assume that b is odd. Then $b = 2k+1$ for an integer k.
$b^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.
b^2 is odd because $2k^2 + 2k$ is an integer.

$x = b^2$ is even, so b is even. Let $b = 2j$ for an integer j.
$x = b^2 = (2j)^2 = 4j^2$.

Choose $c = j^2$.
$x = 4j^2 = 4c = (2c-1) + (2c+1)$

Thus, x can be written as the sum of two consecutive odd integers.

QED

Proving a statement with mixed quantifiers.

Theorem: $\forall x \in A, \exists y \in B, \forall z \in C, P(x,y,z) \rightarrow Q(x,y,z)$.

Write as much of the proof as possible without knowing the sets A, B and C, and the predicates P and Q. Whenever you choose a specific value for a variable, specify what (if anything) this choice can depend on.

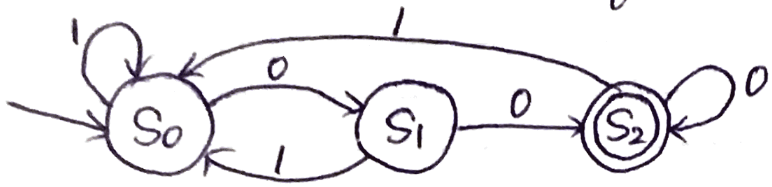
Proof: Consider an unspecified element x of A.
Choose y to be an element of B. This choice can depend on the value of x.
Consider an unspecified element z of C.
Assume that $P(x,y,z)$ is true.
...
Therefore $Q(x,y,z)$ is true.

QED.

Some useful tips:

- If a variable is existentially quantified, we get to choose its value
- If a variable is universally quantified, we cannot choose its value. We need to pick an unspecified element of its domain.
- For a statement with multiple quantifiers, we need to consider the variables from left to right in order.
- Whenever we choose a value for an existentially quantified variable, our choice can depend on the values of all variable to its left, regardless of whether the previous variables are universally or existentially quantified.

Convert the DFA to a sequential circuit.



(D flip-flops)

① How many bits do we need to represent all the states?

1 bit can represent up to $2^1 = 2$ states.
2 bit can represent up to $2^2 = 4$ states.
We need 2 bits (D flip-flops).

② How many bits do we need to represent all possible inputs?

There are 2 possible inputs: 0 and 1.
We need 1 bit. $(2^1 = 2)$

③ Design the next-state circuits.

Let's represent S_0, S_1, S_2 by 00, 01 and 10 (in binary).

Current State b_1	Current State b_0	Input	Next State b_1	Next State b_0	
0	0	0	0	1	$b_1 \equiv 0,\ b_0 \equiv \sim$input
0	0	1	0	0	
0	1	0	1	0	$b_1 \equiv \sim$input, $b_0 \equiv 0$
0	1	1	0	0	
1	0	0	1	0	$b_1 \equiv \sim$input, $b_0 \equiv 0$
1	0	1	0	0	

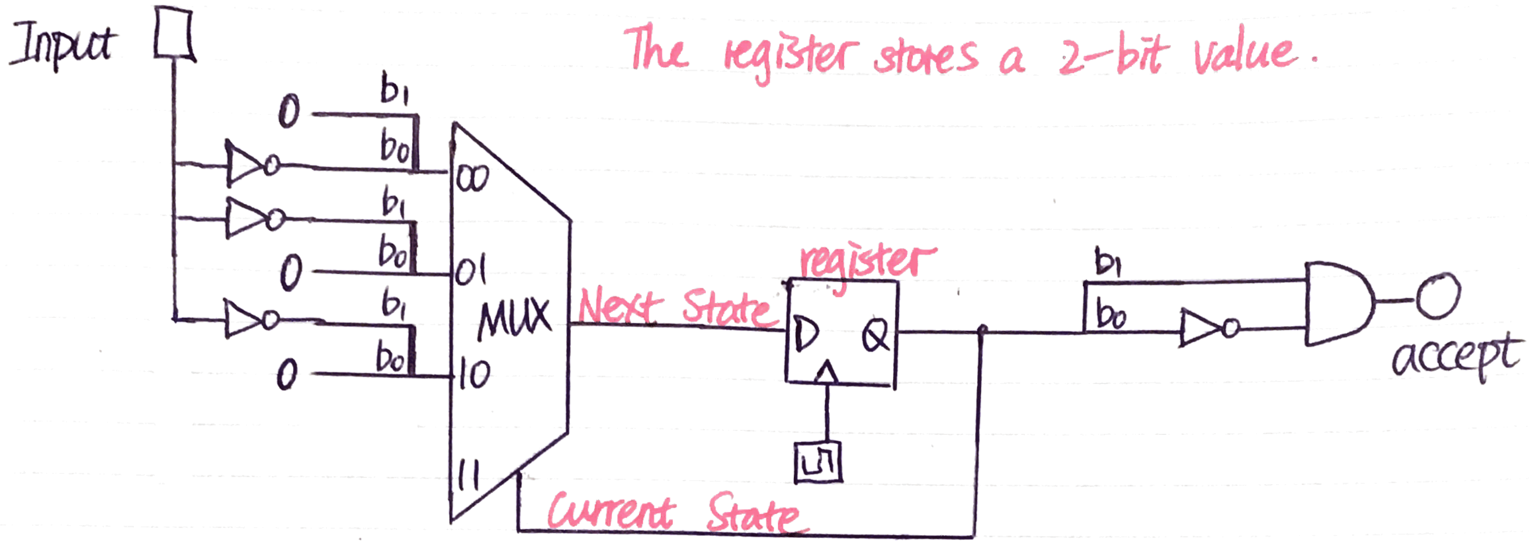
④ Design the circuit producing the output.

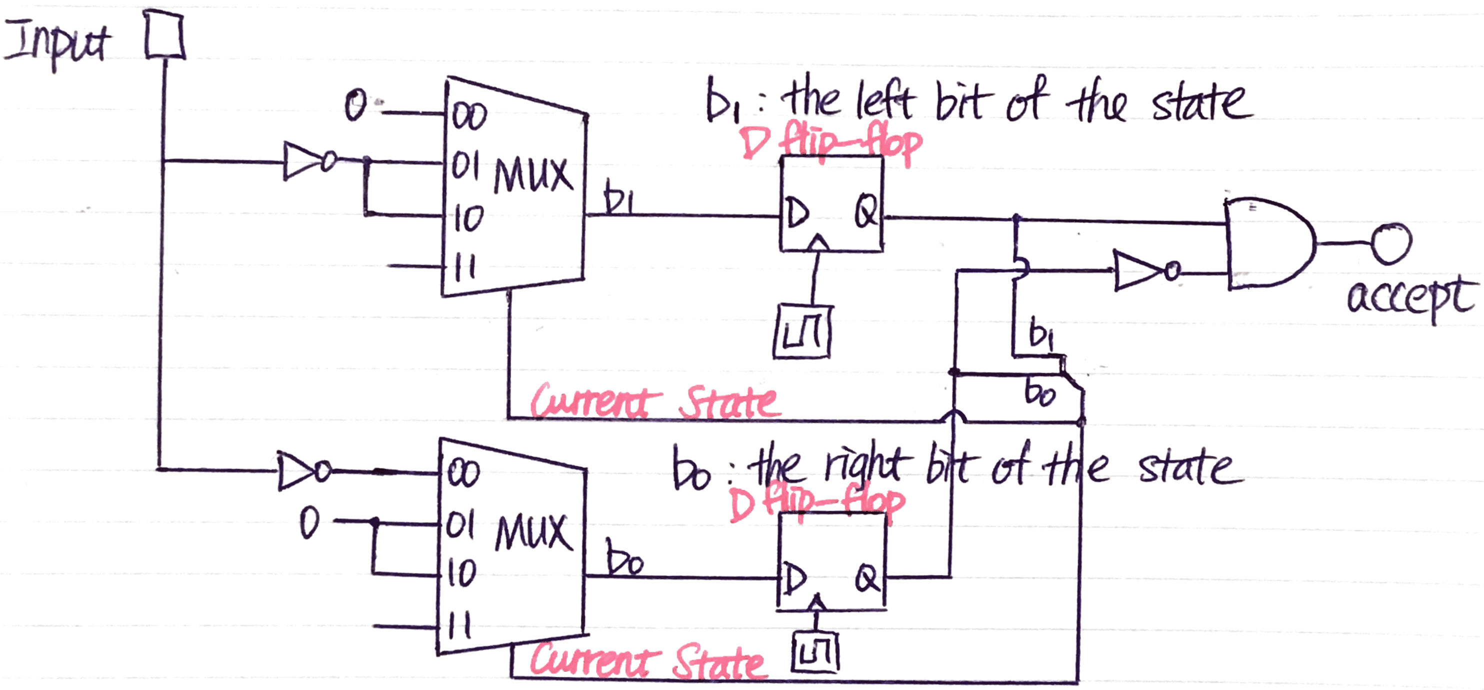
Current State b_1	Current State b_0	Output
0	0	0
0	1	0
1	0	1 ←
1	1	0

The output should be true when the current state is S_2 (10). (the accepting state)

output $\equiv b_1 \wedge \sim b_0$

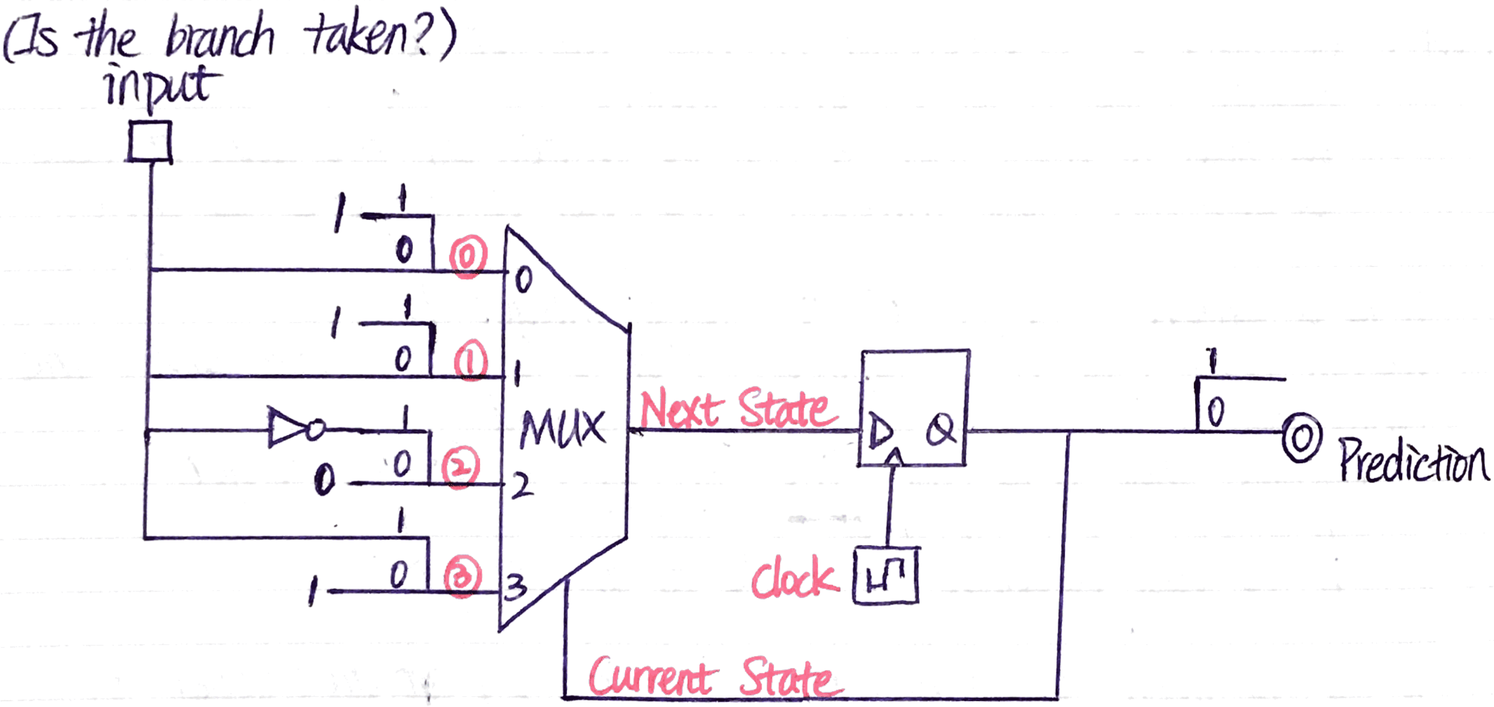
Convert the DFA to a sequential circuit.





The Sequential Circuit for Branch Prediction.

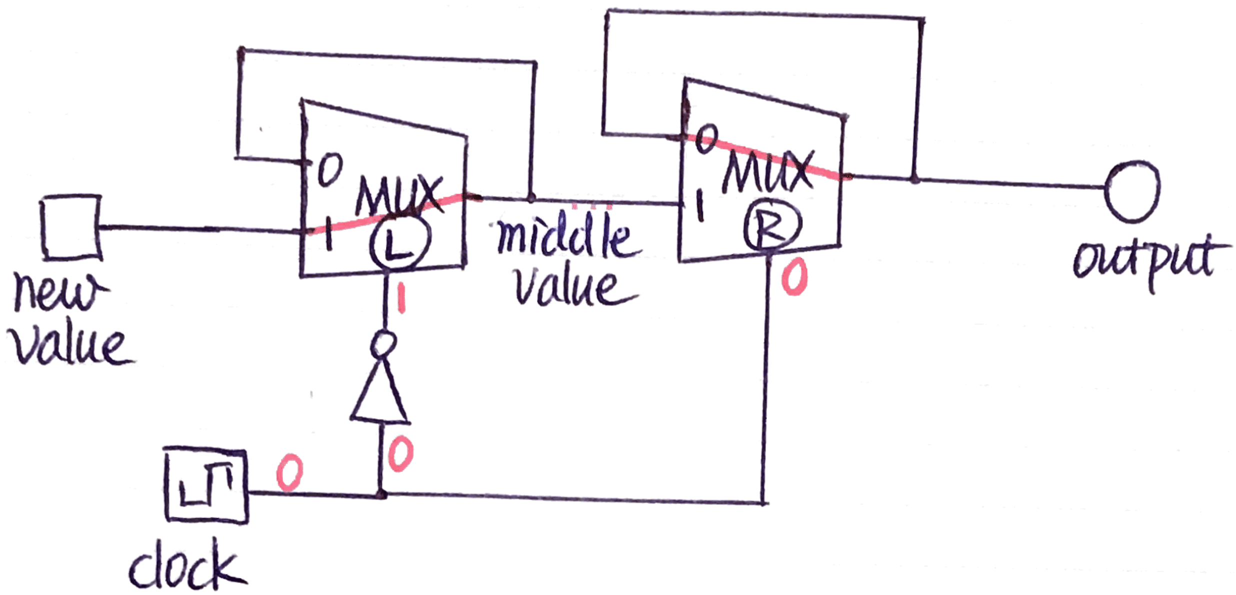
Current State Confidence	Current State Prediction	(input) Is the branch taken?	Next State Confidence	Next State Prediction	
0	0	0	1	0	Conf ≡ 1
0	0	1	1	1	Pred ≡ input
0	1	0	1	0	Conf ≡ 1
0	1	1	1	1	Pred ≡ input
1	0	0	1	0	Conf ≡ ~ input
1	0	1	0	0	Pred ≡ 0
1	1	0	0	1	Conf ≡ input
1	1	1	1	1	Pred ≡ 1



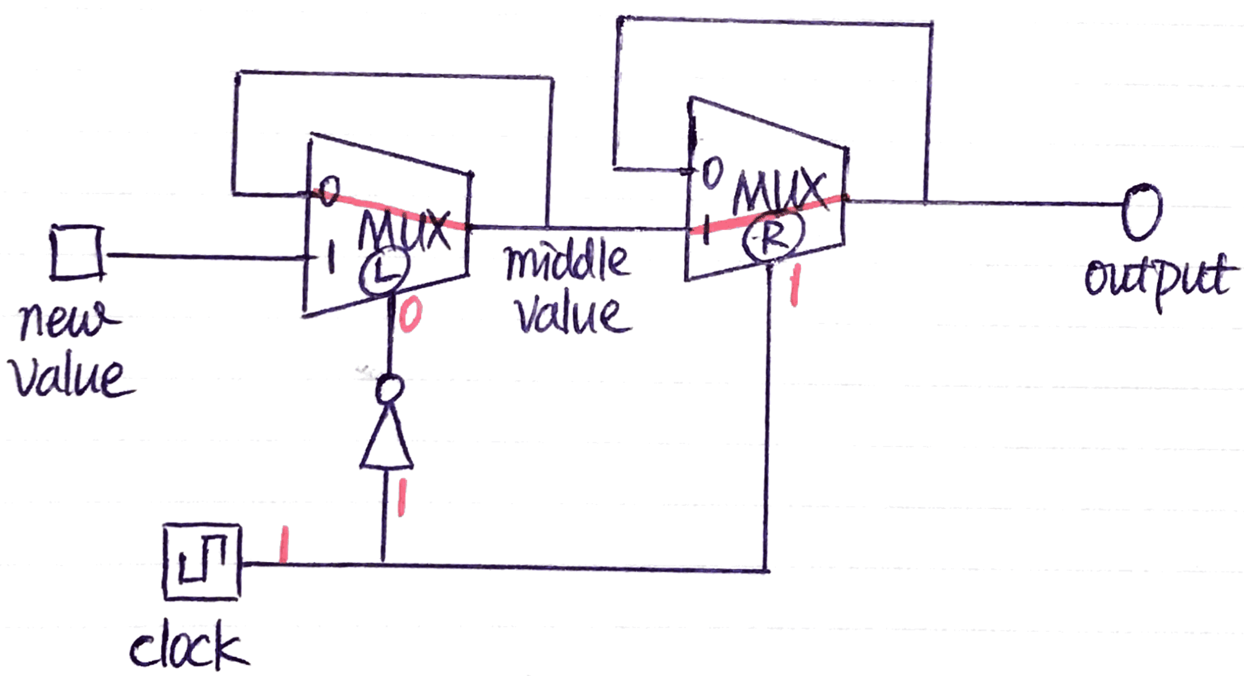
The "next-state" circuits :

⓪ : The next state if the current state is 00.
① : The next state if the current state is 01.
② : The next state if the current state is 10.
③ : The next state if the current state is 11.

Understanding how a D flip-flop works.



When clock = 0, MUX (L) is open. middle value = new value.
MUX (R) is closed.



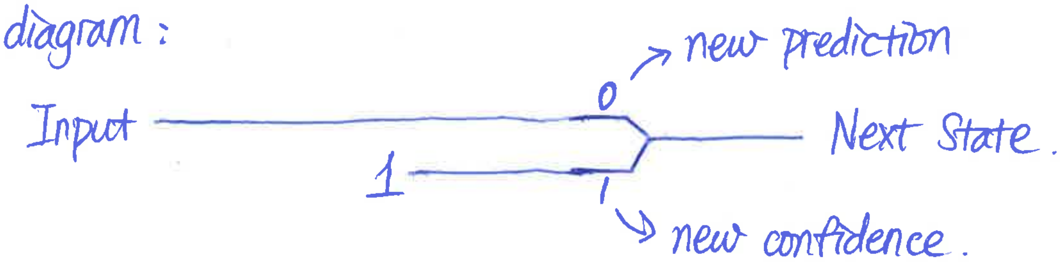
When clock = 1, MUX (L) is closed.
MUX (R) is open. output = middle value.

Suppose current state is Confidence $= 0$ Prediction $= 0$

Current State		Input	Next State	
Confidence	Prediction		Confidence	Prediction
0	0	0	1	0
0	0	1	1	1

New prediction = input.
New confidence = 1

Circuit diagram:

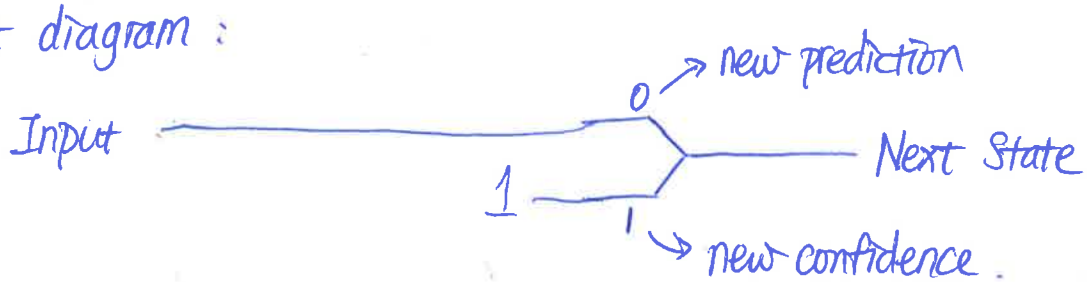


Suppose current state is Confidence $= 0$ Prediction $= 1$.

Current State		Input	Next State	
Confidence	Prediction		Confidence	Prediction
0	1	0	1	0
0	1	1	1	1

New prediction = input
New confidence = 1

Circuit diagram:



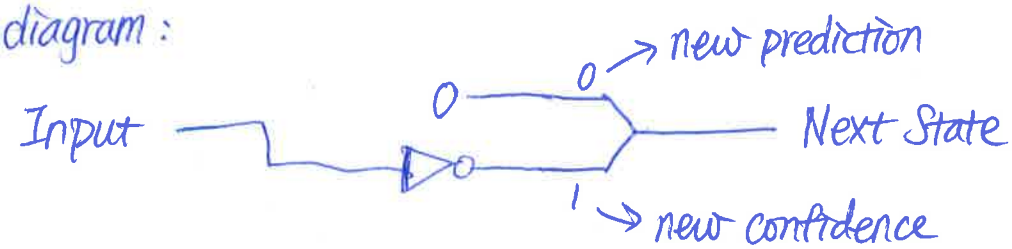
Suppose current state is Confidence = 1 Prediction = 0

Current State		Input	Next State	
Confidence	Prediction		Confidence	Prediction.
1	0	0	1	0
1	0	1	0	0

New prediction = 0

New confidence = ~input.

Circuit diagram:



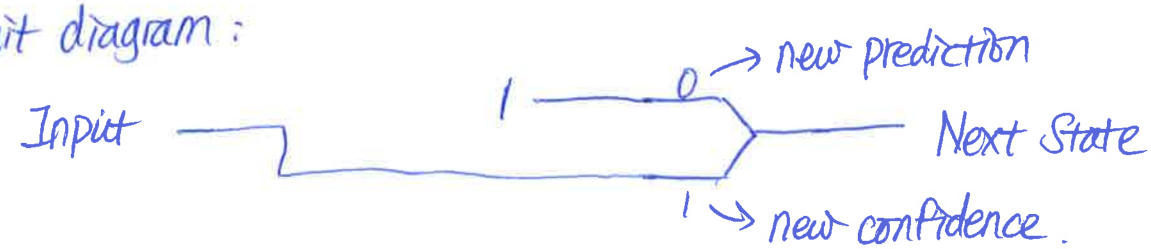
Suppose current state is Confidence = 1 Prediction = 1.

Current State		Input	Next State	
Confidence	Prediction		Confidence	Prediction
1	1	0	0	1
1	1	1	1	1

New prediction = 1

New confidence = input.

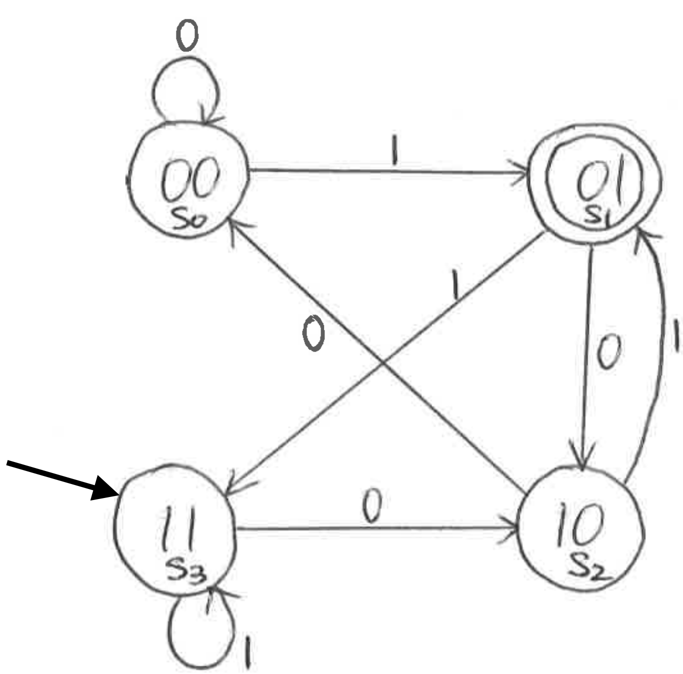
Circuit diagram:



Design a DFA which accepts any string of bits which ends with 01.

The DFA only needs to keep track of the last 2 bits of the string. So we have 4 states, corresponding to the last 2 bits being 00, 01, 10, 11.

	current state		next bit seen ↓ input	next state		
S_0	0	0	0	0	0	S_0
S_0	0	0	1	0	1	S_1
S_1	0	1	0	1	0	S_2
S_1	0	1	1	1	1	S_3
S_2	1	0	0	0	0	S_0
S_2	1	0	1	0	1	S_1
S_3	1	1	0	1	0	S_2
S_3	1	1	1	1	1	S_3



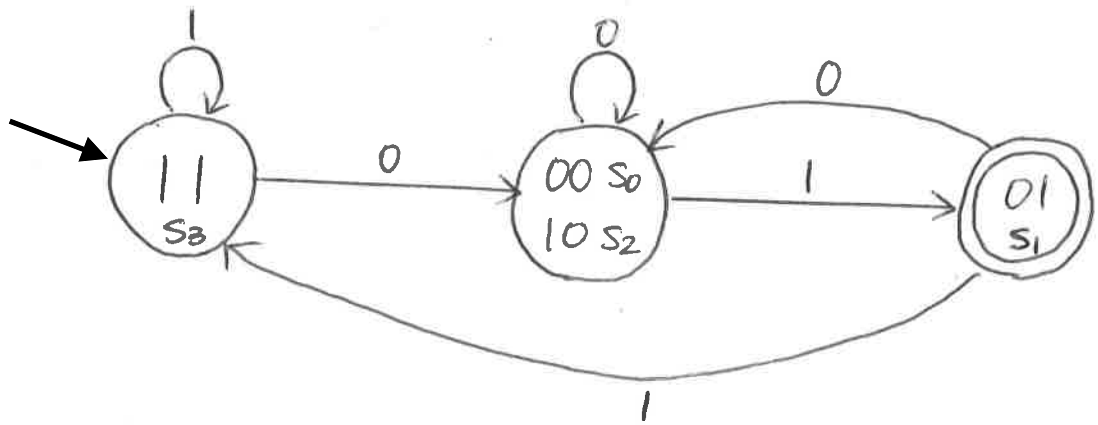
s1 cannot be the initial state because the empty string should not be accepted.

s0 or s2 cannot be the initial state because the string “1” should not be accepted.

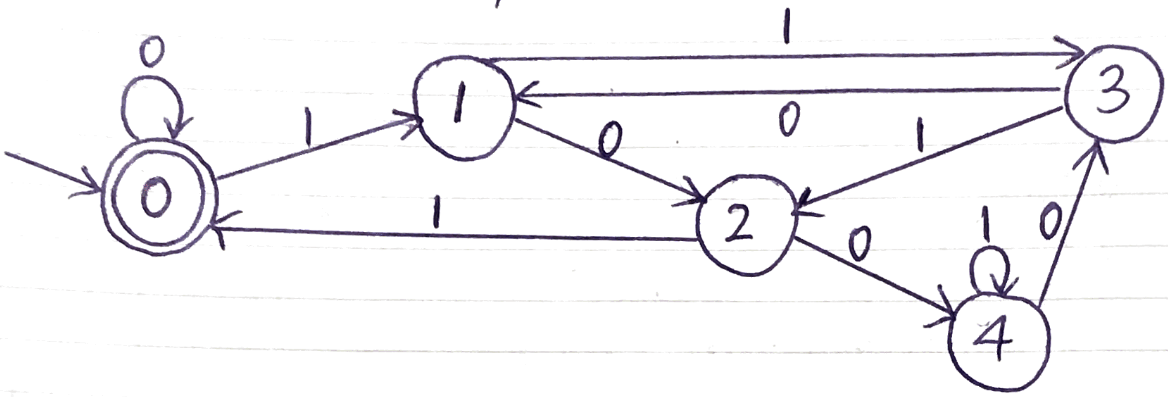
Therefore, the initial state has to be s3.

Designing a DFA (continued)

The 4-state DFA we designed is equivalent to the 3-state DFA below.



A Fun Induction Example



Given any string of bits, the DFA will read the bits from left to right.

Theorem: The DFA ends up in state r after reading string s if and only if $\exists q \in \mathbb{Z},\ s = 5q + r$.

Proof: We prove the theorem by induction on the length n of the string s.

Base case: $n=1$. There are 2 possible strings with 1 bit.
If $s =$ "0", the DFA should end in state 0 and it does.
If $s =$ "1", the DFA should end in state 1 and it does.

Induction step:
Consider an unspecified integer $n \geq 1$.
Induction hypothesis:
Assume that the DFA behaves correctly for any string with n bits.
We need to show that the DFA behaves correctly for any string with $n+1$ bits.

Consider a string of $(n+1)$ bits: $b_1 b_2 b_3 \cdots b_n b_{n+1}$.
Suppose that after reading the first n bits $b_1 b_2 \cdots b_n$, the DFA ends up in state r.
By our induction hypothesis, it must be that

$$b_1 b_2 \cdots b_n = 5q + r \text{ for some integer } q.$$

A Fun Induction Example

Proof (continued):

If the DFA reads the next bit b_{n+1}, what state should it end up in (which depends on r)?

If $b_{n+1} = 0$.

$b_1 b_2 \cdots b_n 0$ → adding a zero to the right is multiplying the binary number by 2.

$= 2 * b_1 b_2 \cdots b_n$

$= 2 * (5q + r)$ → by our induction hypothesis

$= \underbrace{10q}_{\text{divisible by 5}} + 2r$

The next state should be the remainder when we divide $2r$ by 5.

If $b_{n+1} = 1$

$b_1 b_2 \cdots b_n 1$

$= b_1 b_2 \cdots b_n 0 + 1$

$= 2 * b_1 b_2 \cdots b_n + 1$

$= 2(5q + r) + 1$ → by our induction hypothesis.

$= \underbrace{10q}_{\text{divisible by 5}} + 2r + 1$

The next state should be the remainder when we divide $2r+1$ by 5.

r (current state)	b_{n+1}	$2r$	next state
0	0	0	0
1	0	2	2
2	0	4	4
3	0	6	1
4	0	8	3

r (current state)	b_{n+1}	$2r+1$	next state
0	1	1	1
1	1	3	3
2	1	5	0
3	1	7	2
4	1	9	4

The DFA should behave according to these two tables. All we need to do is to verify that it does.

QED

NOTE: The induction step shows you the process we would have followed to design this DFA. So now you should be able to design a DFA which accepts any integer that is divisible by k for any integer $k \geq 2$. :)

Induction

Define $P(n) \equiv \sum_{i=0}^{n-1} i = \frac{n(n-1)}{2}$.

Theorem : $\forall n \in \mathbb{Z}^+, \sum_{i=0}^{n-1} i = \frac{n(n-1)}{2}$

$\equiv \forall n \in \mathbb{Z}^+, P(n) \equiv P(1) \land P(2) \land P(3) \land \cdots$

Proof ① : Base case : $P(1)$ is true.
Induction step : $P(1) \to P(2) \land P(2) \to P(3) \land P(3) \to P(4) \land \cdots$ is true.

Is proof ① valid? Yes.
The $n=1$ case is covered by the base case. The other cases $n=2,3,\ldots$ are covered by combining the base case with the induction step.

Proof ② : Base cases : $P(1)$ and $P(2)$ are true.
Induction step : $P(2) \to P(3) \land P(3) \to P(4) \land \cdots$ is true.

Is proof ② valid? Yes.
The $n=1,2$ cases are covered by the base cases. The other cases $n=3,4,\ldots$ are covered by combining the base cases with the induction step.

Proof ③ : Base case : $P(1)$ is true.
Induction step : $P(2) \to P(3) \land P(3) \to P(4) \land \cdots$ is true.

Is proof ③ valid? No.
We never proved that $P(2)$ is true.

What do we need to prove in the induction step?

✓ (a) $\forall n \in \mathbb{Z}^+, \left(\sum_{i=0}^{n-1} i = \frac{n(n-1)}{2} \to \sum_{i=0}^{n} i = \frac{(n+1)n}{2}\right)$

$\equiv (P(1) \to P(2)) \land (P(2) \to P(3)) \land (P(3) \to P(4)) \land \cdots$

X (b) $\left(\forall n \in \mathbb{Z}^+ \sum_{i=0}^{n-1} i = \frac{n(n-1)}{2}\right) \to \left(\forall n \in \mathbb{Z}^+, \sum_{i=0}^{n} i = \frac{(n+1)n}{2}\right)$

$\equiv (\underbrace{P(1) \land P(2) \land P(3) \land \cdots}) \to (P(2) \land P(3) \land P(4) \land \cdots)$

If we assume this is true, we already assumed that the theorem is true.

Induction (geometric series)

Theorem 2: $\forall t \in N, \sum_{i=0}^{t} 5^i = \frac{5^{t+1}-1}{5-1}$.

Proof: We prove the theorem by induction on n.

Base case: $t=0$ $\sum_{i=0}^{0} 5^i = 5^0 = 1$, $\frac{5^{0+1}-1}{5-1} = \frac{5-1}{5-1} = 1$, $\sum_{i=0}^{0} 5^i = \frac{5^{0+1}-1}{5-1}$.

Induction step:

We need to prove that $\forall t \in N, \sum_{i=0}^{t} 5^i = \frac{5^{t+1}-1}{5-1} \rightarrow \sum_{i=0}^{t+1} 5^i = \frac{5^{t+2}-1}{5-1}$

Consider an unspecified natural number t.

Assume that $\sum_{i=0}^{t} 5^i = \frac{5^{t+1}-1}{5-1}$ or $5^0+5^1+\cdots+5^{t-1}+5^t = \frac{5^{t+1}-1}{5-1}$.

(induction hypothesis)

We need to show that $\sum_{i=0}^{t+1} 5^i = \frac{5^{t+2}-1}{5-1}$.

$$\sum_{i=0}^{t+1} 5^i = (5^0+5^1+\cdots+5^{t-1}+5^t) + 5^{t+1}$$

$$= \sum_{i=0}^{t} 5^i + 5^{t+1}$$

$$= \frac{5^{t+1}-1}{5-1} + 5^{t+1}$$ by our induction hypothesis.

$$= \frac{5^{t+1}+(5-1)5^{t+1}-1}{5-1}$$

$$= \frac{5*5^{t+1}-1}{5-1}$$

$$= \frac{5^{t+2}-1}{5-1}$$

QED

Induction

Define $P(n) \equiv \sum_{i=0}^{n-1} i = \frac{n(n-1)}{2}$.

Theorem : $\forall n \in \mathbb{Z}^+, \sum_{i=0}^{n-1} i = \frac{n(n-1)}{2}$

$\equiv \forall n \in \mathbb{Z}^+, P(n) \equiv P(1) \land P(2) \land P(3) \land \cdots$

Proof ① : Base case : $P(1)$ is true.
Induction step : $P(1) \to P(2) \land P(2) \to P(3) \land P(3) \to P(4) \land \cdots$ is true.

Is proof ① valid? Yes.
The $n=1$ case is covered by the base case. The other cases $n = 2, 3, \ldots$ are covered by combining the base case with the induction step.

Proof ② : Base cases : $P(1)$ and $P(2)$ are true.
Induction step : $P(2) \to P(3) \land P(3) \to P(4) \land \cdots$ is true.

Is proof ② valid? Yes.
The $n = 1, 2$ cases are covered by the base cases. The other cases $n = 3, 4, \ldots$ are covered by combining the base cases with the induction step.

Proof ③ : Base case : $P(1)$ is true.
Induction step : $P(2) \to P(3) \land P(3) \to P(4) \land \cdots$ is true.

Is proof ③ valid? No.
We never proved that $P(2)$ is true.

What do we need to prove in the induction step?

√ (a) $\forall n \in \mathbb{Z}^+, \left(\sum_{i=0}^{n-1} i = \frac{n(n-1)}{2} \to \sum_{i=0}^{n} i = \frac{(n+1)n}{2}\right)$

$\equiv (P(1) \to P(2)) \land (P(2) \to P(3)) \land (P(3) \to P(4)) \land \cdots$

X (b) $\left(\forall n \in \mathbb{Z}^+ \sum_{i=0}^{n-1} i = \frac{n(n-1)}{2}\right) \to \left(\forall n \in \mathbb{Z}^+, \sum_{i=0}^{n} i = \frac{(n+1)n}{2}\right)$

$\equiv (\underbrace{P(1) \land P(2) \land P(3) \land \cdots}) \to (P(2) \land P(3) \land P(4) \land \cdots)$

If we assume this is true, we already assumed that the theorem is true.

Induction

Theorem 3: $\forall n \geq 4,\ 2^n < n!$

Proof: We prove this theorem by induction on n.

Base case: $n = 4$

$2^4 = 16$ $\quad 4! = 4*3*2*1 = 24$ $\quad 2^4 < 4!$

Induction step:

We need to prove that $\forall n \geq 4,\ 2^n < n! \rightarrow 2^{n+1} < (n+1)!$

Consider an unspecified integer $n \geq 4$.

Assume that $2^n < n!$ (induction hypothesis)

We need to show that $2^{n+1} < (n+1)!$.

$2^{n+1} = 2 * 2^n$

$< 2 * n!$ by our induction hypothesis.

$< (n+1) * n!$ because $n \geq 4$ so $n+1 \geq 5 > 2$.

$= (n+1)!$

QED

Another version of the induction step:

We need to prove that $\forall n \geq 5,\ 2^{n-1} < (n-1)! \rightarrow 2^n < n!$

Consider an unspecified integer $n \geq 5$.

Assume that $2^{n-1} < (n-1)!$ (induction hypothesis)

We need to show that $2^n < n!$

$2^n = 2 * 2^{n-1}$

$< 2 * (n-1)!$ by our induction hypothesis

$< n * (n-1)!$ because $n \geq 5 > 2$.

$= n!$

QED

Induction

Theorem 4: $\forall n \geq 1 \ \sum_{i=1}^{n} \frac{1}{i^2} \leq 2 - \frac{1}{n}$.

Proof: We prove this theorem by induction on n.

Base case: $n=1$ $\quad \sum_{i=1}^{1} \frac{1}{i^2} = \frac{1}{1^2} = 1 \quad 2 - \frac{1}{1} = 2-1 = 1 \quad 1 \leq 1$.

Induction step:

We need to prove that $\forall n \geq 1, \ \sum_{i=1}^{n} \frac{1}{i^2} \leq 2 - \frac{1}{n} \rightarrow \sum_{i=1}^{n+1} \frac{1}{i^2} \leq 2 - \frac{1}{n+1}$.

Consider an unspecified integer $n \geq 1$.

Induction hypothesis: assume that $\sum_{i=1}^{n} \frac{1}{i^2} \leq 2 - \frac{1}{n}$.

We need to show that $\sum_{i=1}^{n+1} \frac{1}{i^2} \leq 2 - \frac{1}{n+1}$.

$$
\begin{aligned}
\sum_{i=1}^{n+1} \frac{1}{i^2} &= \left(\frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{n^2}\right) + \frac{1}{(n+1)^2} \\
&= \sum_{i=1}^{n} \frac{1}{i^2} + \frac{1}{(n+1)^2} \\
&\leq 2 - \frac{1}{n} + \frac{1}{(n+1)^2} && \text{by our induction hypothesis.} \\
&= 2 + \frac{-n^2-n-1}{n(n+1)^2} \\
&= 2 + \frac{-n^2-n}{n(n+1)^2} - \frac{1}{n(n+1)^2} \\
&\leq 2 + \frac{-n^2-n}{n(n+1)^2} && \text{because } \frac{1}{n(n+1)^2} > 0 \\
&= 2 - \frac{1}{n+1}
\end{aligned}
$$

I figured out how to do these steps by first doing scratch work on the next page.

QED

Induction

Theorem 4: $\forall n \geq 1, \sum_{i=1}^{n} \frac{1}{i^2} \leq 2 - \frac{1}{n}$.

Scratch work:

After applying the induction hypothesis, I need to show that $2 - \frac{1}{n} + \frac{1}{(n+1)^2} \leq 2 - \frac{1}{n+1}$. How do I prove this?

$$\cancel{2} - \frac{1}{n} + \frac{1}{(n+1)^2} \leq \cancel{2} - \frac{1}{n+1}$$

$$① \; -\frac{1}{n} + \frac{1}{(n+1)^2} \leq -\frac{1}{n+1} \; ⑤$$

$$\frac{-(n+1)^2 + n}{n(n+1)^2} \leq \frac{-n(n+1)}{n(n+1)^2}$$

$$\frac{-n^2 - 2n - 1 + n}{n(n+1)^2} \leq \frac{-n^2 - n}{n(n+1)^2}$$

$$② \; \frac{-n^2 - n - 1}{n(n+1)^2} \leq \frac{-n^2 - n}{n(n+1)^2}$$

$$③ \; \frac{-n^2 - n}{n(n+1)^2} - \frac{1}{n(n+1)^2} \leq \frac{-n^2 - n}{n(n+1)^2} \; ④$$

Then I wrote down the quantities in the order specified by the numbers above.

$$\begin{aligned}
& -\frac{1}{n} + \frac{1}{(n+1)^2} \\
&= \frac{-n^2 - n - 1}{n(n+1)^2} \\
&= \frac{-n^2 - n}{n(n+1)^2} - \frac{1}{n(n+1)^2} \\
&\leq \frac{-n^2 - n}{n(n+1)^2} \\
&= -\frac{1}{n+1}
\end{aligned}$$

Induction

Theorem 3: $\forall n \geq 4,\ 2^n < n!$

Proof: We prove the theorem by induction.

Base case: $n=4$ ...

Induction step: Consider an unspecified integer $n \geq 4$.
Assume $2^n < n!$ (induction hypothesis)
We need to show that $2^{n+1} < (n+1)!$.

First, let's do some scratch work to figure out how to prove this.

Version ①

$$2^{n+1} < (n+1)!$$
$$2 * 2^n < (n+1) * n!$$

All I need to show are $2 < (n+1)$ and $2^n < n!$

$2 < (n+1)$ means $n > 1$, this is true because we know $n \geq 4$

$2^n < n!$ is true because we assumed it's true in our induction hypothesis.

Ha, we are done.

Version ②

$2^{n+1} < (n+1)!$ Let's divide by 2 on both sides

$2^n < \frac{1}{2}(n+1)!$ Let's separate $n!$ on the right-hand side.

$2^n < \frac{1}{2}(n+1) * n!$

All I need to show are $1 < \frac{1}{2}(n+1)$ and $2^n < n!$

$1 < \frac{1}{2}(n+1) \Rightarrow 2 < n+1 \Rightarrow n > 1$ true because $n \geq 4$.

$2^n < n!$ is true by our induction hypothesis.

We are done.

"Okay, now I know how to prove $2^{n+1} < (n+1)!$, I need to write it up properly."

Please see the next page for 4 versions of the proper write up.

Proper writeups for the induction step.

Version 1 : (write our scratch work in reverse)

$2^n < n!$ is true by our induction hypothesis.

$1 < \frac{1}{2}(n+1)$ because $n \geq 4$.

Multiplying the two inequalities, we have

$$2^n < n! * \frac{1}{2}(n+1)$$
$$2^n < \frac{1}{2}(n+1) * n!$$
$$2^n < \frac{1}{2}(n+1)!$$
$$2^{n+1} < (n+1)! \qquad \text{multiplying by 2 on both sides.}$$

Version 2 : (start from the left-hand side of the inequality and transform it or make it bigger until we get to the right-hand side).

$$2^{n+1} = 2 * 2^n \underset{①}{<} 2 * n! \underset{②}{<} (n+1) * n! = (n+1)!$$

① is by our induction hypothesis.

② is because $n \geq 4$ so $(n+1) > 2$.

Version 3 : (another way of writing version 2).

$$2^{n+1} = 2 * 2^n$$
$$2 * 2^n < 2 * n! \qquad \text{by our induction hypothesis.}$$
$$2 * n! < (n+1) * n! \qquad \text{because } n \geq 4.$$
$$(n+1) * n! = (n+1)!$$

Version 4 : (yet another way of writing versions 2 and 3)

$$\begin{aligned} 2^{n+1} &= 2 * 2^n \\ &< 2 * n! && \text{by our induction hypothesis} \\ &< (n+1) * n! && \text{because } n \geq 4. \\ &= (n+1)! \end{aligned}$$