# Announcements

- HW1 DUE OCT 6 (8pm)

- Office hours: today 4-5pm (zoom)
  Wednesday 1:30-2:30 (CS lounge)

# TODAY

- First Order Logic

  Language / Syntax

  Semantics : Models

(pages 18 - 27 of course notes)

# FIRST ORDER LOGIC

Underlying language $\mathcal{L}$ specified by:

1. $\forall n \in \mathbb{N}$ a set of n-ary function symbols (ie.: $f, g, h, +, \cdot$ )

   0-ary function symbols are called constants

2. $\forall n \in \mathbb{N}$ a set of n-ary predicate symbols (i.e. $P, Q, R, <, \leq$ )

Plus:

- Variables: $x, y, z, \ldots a, b, c, \ldots$
- $\neg, \vee, \wedge, \exists, \forall$
- parenthesis ( , )

} Built in symbols

## Example $\mathcal{L}_A$ (Language of arithmetic)

$$\mathcal{L}_A = \{ \underbrace{\overset{\text{0-ary}}{0}, \overset{\text{1-ary}}{s}, \overset{\text{2-ary}}{+}, \overset{\text{2-ary}}{\cdot}}_{\text{function symbols}} ; \underbrace{\overset{\text{2-ary}}{=}}_{\text{relation symbols}} \}$$

$0$ constant (0-ary function symbol)

$s$ unary function symbol

$+, \cdot$ binary function symbols

$=$ binary predicate symbol

# Terms over $\mathcal{L}$

(1) Every variable is a term

(2) If $f$ is an $n$-ary function symbol, and $t_1, \ldots, t_n$ terms, then $f t_1 \ldots t_n$ is a term

# Terms over $\mathcal{L}$

(1) Every variable is a term

(2) If $f$ is an $n$-ary function symbol, and $t_1, \ldots, t_n$ terms, then $f t_1 \ldots t_n$ is a term

## Examples of terms

$(0, s, f, +, \cdot)$

0-ary

unary

binary

$f0sss0$, $+xfyz$, $\cdot + ab\, ss0$

$f(0, sss0)$ $\quad x + f(y, z)$ $\quad (a+b) \cdot ss0$

# FIRST ORDER FORMULAS OVER $\mathcal{L}$

(1) $Pt_1 .. t_n$ is an atomic $\mathcal{L}$-formula, where
$P$ is an $n$-ary predicate in $\mathcal{L}$, and
$t_1 .. t_n$ are terms over $\mathcal{L}$

(2) If $A, B$ are $\mathcal{L}$-formulas, so are
$\neg A$, $(A \wedge B)$, $(A \vee B)$, $\forall x A$, $\exists x A$

# Example : Propositional formulas are FO Formulas

$\mathcal{L}^{prop}$ : (1) No function symbols

(2) 0-ary predicate symbols $P_1, P_2, \ldots$ (are propositional atoms)

<u>plus</u> $\wedge, \vee, \neg$, ), (

Since there are no function symbols, and all predicate symbols have 0-arity, propositional formulas have

no variables, terms, or $\forall, \exists$

## Example: FO Formulas over $\mathcal{L}_A$

(1) Existence of infinitely many primes


$$\forall x\ \exists y\ (y > x \text{ and } y \text{ is prime})$$

# Example: FO Formulas over $\mathcal{L}_A$

(1) Existence of infinitely many primes

Want to say: $\forall x\ \exists y\ (y > x$ and $y$ is prime$)$

y is prime : $\forall z, z'\ (z, z' \geq 2 \Rightarrow z \cdot z' \neq y)$

# Example: FO Formulas over $\mathcal{L}_A$

① Existence of infinitely many primes

want to say: $\forall x\ \exists y\ (\overbrace{y > x}^{(**)}$ and $\overbrace{y \text{ is prime}}^{(*)})$

y is prime: $\forall z, z'\ (z, z' \geq 2 \Rightarrow z \cdot z' \neq y)$

$(*)$ $\forall z \forall z' \Big( \big( \neg(z = 0) \wedge \neg(z = s0) \wedge \neg(z' = 0) \wedge \neg(z' = s0) \big)$
$\rightarrow \neg(z \cdot z' = y) \Big)$

# Example: FO Formulas over $\mathcal{L}_A$

(1) Existence of infinitely many primes

want to say: $\forall x\ \exists y\ (\underbrace{y > x}_{(**)} \text{ and } \underbrace{y \text{ is prime}}_{(*)})$

$y$ is prime : $\forall z, z'\ (z, z' \geq 2 \Rightarrow z \cdot z' \neq y)$

(*) $\forall z \forall z' \Big( \big(\neg(z=0) \wedge \neg(z=s0) \wedge \neg(z'=0) \wedge \neg(z'=s0)\big) \rightarrow \neg(z \cdot z' = y) \Big)$

(**) $y > x$ : $\neg(x=y) \wedge \exists w\ (x+w=y)$

# Example: FO Formulas over $\mathcal{L}_A$

① Existence of infinitely many primes

Want to say: $\forall x\ \exists y\ (y > x$ and $y$ is prime$)$

y is prime : $\forall z, z'\ (z, z' \geq 2 \Rightarrow z \cdot z' \neq y)$

(*) $\forall z \forall z' \Big( \big( \neg(z = 0) \wedge \neg(z = S0) \wedge \neg(z' = 0) \wedge \neg(z' = S0) \big) \rightarrow \neg(z \cdot z' = y) \Big)$

(**) y > x : $\neg(x = y) \wedge \exists w\ (x + w = y)$

Whole thing: $\forall x \exists y\ (*) \wedge (**)$

# Example: FO Formulas over $\mathcal{L}_A$

(2) Twin Prime Conjecture

There exists infinitely many pairs of numbers, $(x, x')$ such that $x' = x + 2$ and both $x$ and $x'$ are prime

# Example : FO Formulas in $\mathcal{L}_A$

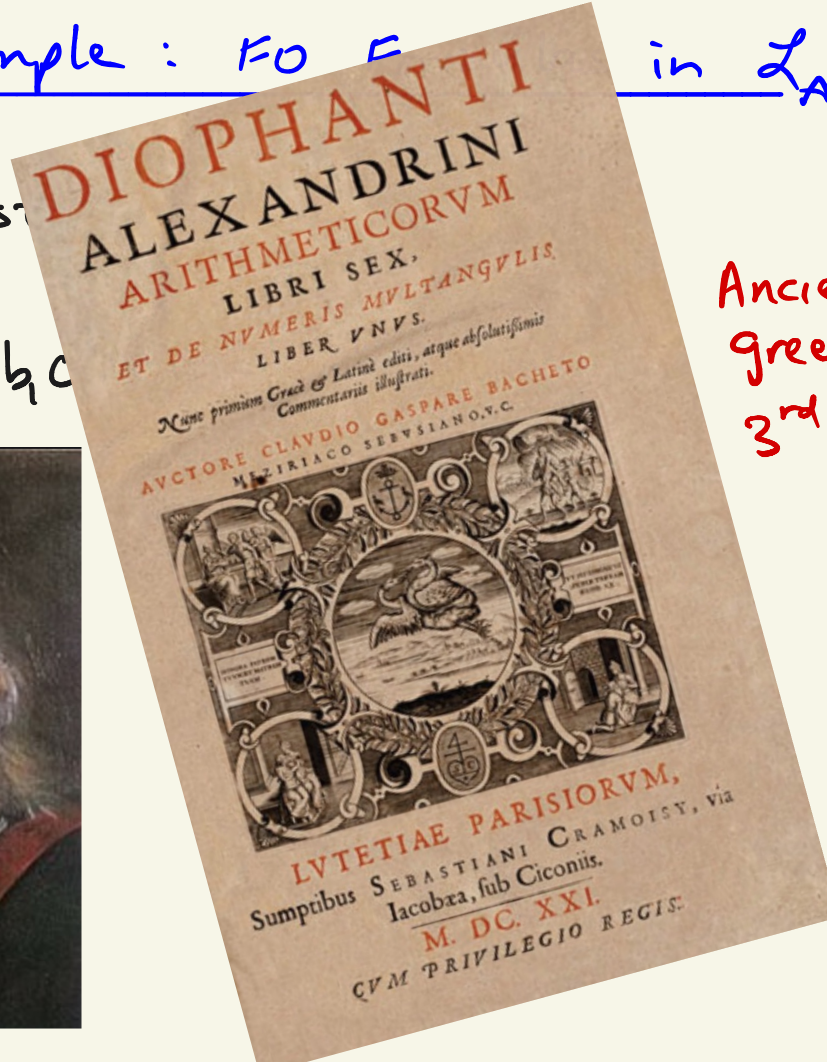
(3) Fermat's Last Theorem

$$\forall n \geq 3 \; \forall a,b,c \; (n>2 \rightarrow a^n + b^n \neq c^n)$$

## Example : FO F in $\mathcal{L}_A$

③ Fermat's Last

$\forall n \geq 3 \ \forall a, b, c$



DIOPHANTI ALEXANDRINI ARITHMETICORVM LIBRI SEX, ET DE NVMERIS MVLTANGVLIS LIBER VNVS.

Nunc primùm Græcè & Latinè editi, atque absolutissimis Commentariis illustrati.

AVCTORE CLAVDIO GASPARE BACHETO MEZIRIACO SEBVSIANO, V.C.

LVTETIAE PARISIORVM, Sumptibus SEBASTIANI CRAMOISY, via Iacobæa, sub Ciconiis.

M. DC. XXI.

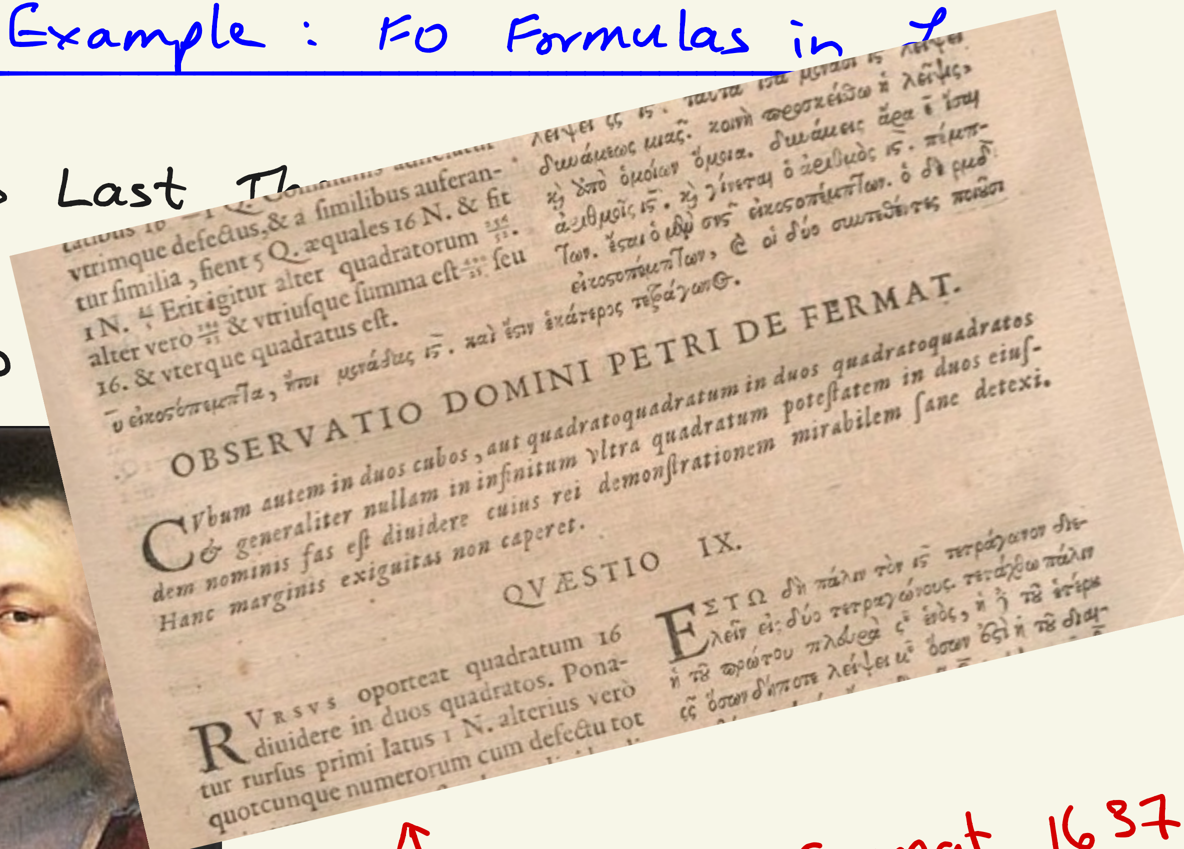
CVM PRIVILEGIO REGIS.

Ancient greek text, 3rd century AD

# Example : FO Formulas in $\mathcal{L}$

③ Fermat's Last Th

$\forall n \geq 3$



... latus 16 – 1 Q. Communis adiiciatur vtrimque defectus, & a similibus auferantur similia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{16}{5}$ Erit igitur alter quadratorum $\frac{256}{25}$. alter vero $\frac{144}{25}$ & vtriusque summa est $\frac{400}{25}$ seu 16. & vterque quadratus est.

OBSERVATIO DOMINI PETRI DE FERMAT.

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

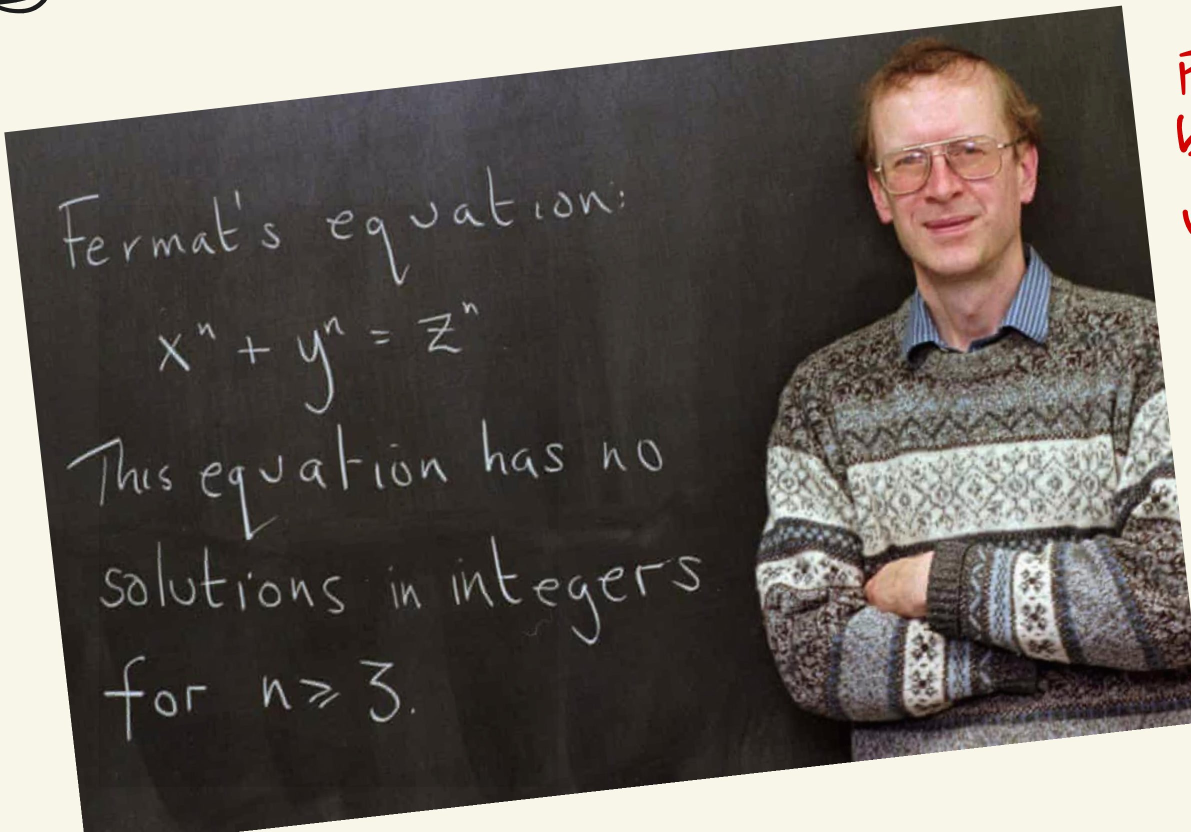
QVÆSTIO IX.

RVRSVS oporteat quadratum 16 diuidere in duos quadratos. Ponatur rursus primi latus 1 N. alterius verò quotcunque numerorum cum defectu tot ...

conjectured by Fermat 1637 in margin of his copy of Arithmetica

# Example: FO Formulas in $\mathcal{L}_A$

③ Fermat's Last Theorem




Finally proven by Andrew Wiles

# Example : FO Formulas in $\mathcal{L}_A$

③ Fermat's Last Theorem (actually Andrew Wiles' theorem)

$$\forall n \geq 3 \left( \forall a, b, c \quad a^n + b^n \neq c^n \right)$$

**Problem**: How to say $a^n$ ?

(we'll see later how to do this!)

# FREE / BOUND VARIABLES

- An occurrence of $x$ in $A$ is bound if $x$ is in a subformula of $A$ of the form $\forall x B$, or $\exists x B$ (otherwise $x$ is free in $A$)

<u>Example</u> $\exists y (x = y + y)$

$$Px \wedge \forall x (\neg(x + Sx = x))$$

- A formula/term is closed if it contains no free variables
- A closed formula is called a sentence

# SEMANTICS OF FO LOGIC

An $\mathcal{L}$-structure $\mathfrak{M}$ (or model) consists of:

1. A nonempty set $M$ called the universe
   (variables range over $M$)

2. For every $n$-ary function symbol $f$ in $\mathcal{L}$,
   an associated function $f^{\mathfrak{M}} : M^n \to M$

3. For each $n$-ary relation symbol $P$ in $\mathcal{L}$,
   an associated relation $P^{\mathfrak{M}} \subseteq M^n$

* Equality predicate $=$ is always <u>true</u> equality
relation on $M$.

$M = \mathbb{N}$ * $=^{\mathbb{N}} = \{(i,i) \mid i \in \mathbb{N}\}$

# Example

$\mathcal{L}_A = \{0, +, \cdot, S; =\}$

1. $\mathbb{N}$: standard model of $\mathcal{L}_A$

$M = \mathbb{N}$

$0 = 0 \in \mathbb{N}$

$+, \cdot, S$ are usual plus, times, successor functions

Jumping ahead a bit: Evaluation of a formula in $\mathbb{N}$

$$\forall x \, \forall z \left( \exists z' \left( \neg(z'=0) \wedge z+z'=x \right) \rightarrow \exists z'' \left( Sz + z'' = x \right) \right)$$

$\forall x \forall z$ if $x > z$ then $x$ can be written as $z+1$ + (some other number in $\mathbb{N}$)

# Example

$\mathcal{L}_A = \{0, s, +, \cdot\, ; =\}$

① $\mathcal{M} = \underline{\mathbb{N}}$ ,

$0 = 0 \in \mathbb{N}$

s: successor. ie. $s(2) = 3$, . . .

+: plus. ie, $+(0,i) = i$, $+(2,3) = 5$, etc

$\cdot$: times

② $M = \{ ■, ●, ★ \}$ $0 = ■$

$s(■) = ●$
$s(●) = ■$
$s(★) = ★$

| + | ■ | ● | ★ |
|---|---|---|---|
| ■ | ● | ● | ★ |
| ● | ● | ● | ★ |
| ★ | ★ | ★ | ★ |

| • | ■ | ● | ★ |
|---|---|---|---|
| ■ | ■ | ★ | ● |
| ● | ■ | ■ | ★ |
| ★ | ★ | ★ | ■ |

How to evaluate formulas that contain free variables?

**Defn** An object assignment $\sigma$ for a model $\mathfrak{M}$ is a mapping from variables to $M$

## Definition: Evaluation of terms/formulas over $\mathfrak{M}, \sigma$

Let $\mathfrak{M}$ be an $\mathcal{L}$-structure,

$\sigma$ an object assignment for $\mathfrak{M}$

### Evaluation of terms over $\mathfrak{M}, \sigma$

(a) $x^{\mathfrak{M}}[\sigma]$ is $\sigma(x)$ for all variables $x$

(b) $(f t_1 .. t_n)^{\mathfrak{M}}[\sigma] = f^{\mathfrak{M}}(t_1^{\mathfrak{M}}[\sigma], \ldots, t_n^{\mathfrak{M}}[\sigma])$

Example $\sigma$: $x_1 \to 5$ $x_2 \to 7$

$S(x_1 + x_2)[\sigma] = 13$

# Evaluation of formulas over $\mathfrak{M}, \sigma$

Let $A$ be an $\mathcal{L}$-formula. $\mathfrak{M} \models A[\sigma]$
($\mathfrak{M}$ satisfies $A$ under $\sigma$) iff

(a) $\mathfrak{M} \models Pt_1 \ldots t_n[\sigma]$ iff $\langle t_1^{\mathfrak{M}}[\sigma], \ldots, t_n^{\mathfrak{M}}[\sigma] \rangle \in P^{\mathfrak{M}}$

(b) $\mathfrak{M} \models (s = t)[\sigma]$ iff $s^{\mathfrak{M}}[\sigma] = t^{\mathfrak{M}}[\sigma]$

(c) $\mathfrak{M} \models \neg A[\sigma]$ iff not $\mathfrak{M} \models A[\sigma]$

(d) $\mathfrak{M} \models (A \vee B)[\sigma]$ iff $\mathfrak{M} \models A[\sigma]$ or $\mathfrak{M} \models B[\sigma]$

(e) $\mathfrak{M} \models (A \wedge B)[\sigma]$ iff $\mathfrak{M} \models A[\sigma]$ and $\mathfrak{M} \models B(\sigma)$

(f) $\mathfrak{M} \models \forall x A[\sigma]$ iff $\forall m \in M$ $\mathfrak{M} \models A[\sigma(m/x)]$

(g) $\mathfrak{M} \models \exists x A[\sigma]$ iff $\exists m \in M$ $\mathfrak{M} \models A[\sigma(m/x)]$

## Example

$\mathcal{L} = \{ ; R, = \}$

$\mathfrak{M} = (\mathbb{N}, \leq, =)$

$R^{\mathfrak{M}}(m,n)$ iff $m \leq n$

Then

$\mathfrak{M} \overset{?}{\models} \forall x \exists y R(x,y)$ yes

satisfiable by $\mathfrak{M}$

$\mathfrak{M} \overset{?}{\models} \exists y \forall x R(x,y)$ No

but $\exists y \forall x R(x,y)$ is also satisfiable

# IMPORTANT DEFINITIONS

Let $A$ be a f.o. formula over $\mathcal{L}$.

① $A$ is satisfiable iff there exists a model $\mathfrak{M}$ and an object assignment $\sigma$ such that $\mathfrak{M} \models A[\sigma]$

② A set of formulas $\Phi$ is satisfiable iff $\exists \mathfrak{M}, \sigma$ such that $\mathfrak{M} \models \Phi[\sigma]$ [$\mathfrak{M} \models A[\sigma]$ for all $A \in \Phi$]

③ $\Phi \models A$ ($A$ is a logical consequence of $\Phi$) iff $\forall \mathfrak{M}\ \forall \sigma$ if $\mathfrak{M} \models \Phi[\sigma]$ then $\mathfrak{M} \models A[\sigma]$

$\models A$ ($A$ is valid) iff $\forall \mathfrak{M}, \sigma$ $\mathfrak{M} \models A[\sigma]$

④ $A \Leftrightarrow B$ ($A$ and $B$ are logically equivalent)

iff $\forall \mathfrak{M} \, \forall \sigma \quad \mathfrak{M} \models A[\sigma]$ iff $\mathfrak{M} \models B[\sigma]$

$A \models B$ and $B \models A$

# Examples

(1) $(\forall x\, Px \vee \forall x\, Qx) \overset{?}{\models} \forall x\,(Px \vee Qx)$

(2) $\forall x\,(Ax \vee Bx) \overset{?}{\models} \forall x\, Ax \vee \forall x\, Bx$

$\mathcal{L} = \{\, ; \; P, Q, A, B\}$

# Example

Earlier formula A:

$$\forall x \forall z\ (\exists z' (\neg(z'=0) \wedge z+z'=x) \supset \exists z'' (sz + z'' = x))$$

says for every $x, z$ if $x > z$ then we can write $x$ as $(z+1) + z''$ for some $z''$

- true when $\mathcal{M} = \underline{\mathbb{N}}$ so $A$ is satisfiable
- false when $\mathcal{M} = \left( M = \{0,1,2\} \quad \begin{array}{l} s0=1 \\ s1=2 \\ s2=0 \end{array} \quad \begin{array}{l} 0+2=2 \\ \text{all others} \\ x+y=0 \end{array} \right)$

$x=2 \quad z=0 \quad z'=2$

# Example

$$\forall x \forall y\, (fx = fy) \overset{?}{\underset{\text{No}}{\models}} x = y$$

Let $M = \{0, 1\}$

$\mathfrak{M}$: $f(0) = 0$

$f(1) = 0$

then $\mathfrak{M} \models \forall x \forall y\, (fx = fy)$

but $\mathfrak{M} \not\models x = y$ (since $0 \neq 1$)