Substitution: Recall in propositional logic: $A(B/p_i)$

First-order: If $B = C$, $A^C$ is $A$ with $B$ replaced with $C$, then $A \equiv A^C$.

Substitution of terms for variables $x_i$:

Example: $\exists x_2 (x_2 + x_2 = x_1)$, "$x_1$ is even".

To say $x_3 + x_4$ is even: $\exists x_2 (x_2 + x_2 = x_3 + x_4)$

Notation $A[x_i]$ is $\exists x_2 (x_2 + x_2 = x_i)$

$A(x_3 + x_4 / x_i) = \exists x_2 (x_2 + x_2 = x_3 + x_4)$

Model uses $A_{x_i}[x_3 + x_4]$.

Warning: What if want to say $x_2 + x_3$ is even?

$A(x_2 + x_3 / x_i) = \exists x_2 (x_2 + x_2 = x_2 + x_3)$

does not say "$x_i + x_3$" is even.

$= \exists x_2 (x_2 + x_2 = x_2 + x_3)$

Fix #1: Use an "algebraic variant" like $\exists x_5 (x_5 + x_5 = x)$

Fix #2: Define "substitutable for" - OK to substitute.
Notation: \[ A \left( t_1, \ldots, t_k / x_i, \ldots, x_k \right) \] means substitute \( \overline{t} \) parallel each \( t_j \) for each free occurrence of \( x_j \).

\[ A(t/x) \] - shorthand notation.

Definition of substitution. Let \( s \) be a formula. Let \( t_1, \ldots, t_k, x_i, \ldots, x_k \)

Then \( s(t/x) \) is recursively defined by:

1. If \( s \) is \( x_i j \), then \( s(t/x) \) is \( t_j \).
2. If \( s \) is \( x_i \), \( \epsilon \{ i_1, \ldots, i_k \} \) or \( s \) is a constant symbol \( c \), then \( s(t/x) \) is \( s \).
3. If \( s \) is \( f(v_1, \ldots, v_r) \) - \( f \) is any function,
   \( s(t/x) \) is \( f(v_1(t/x), \ldots, v_r(t/x)) \).

Let \( A \) be a formula.
4. If \( A \) is atomic, i.e. \( A \) is \( v_i = v_j \) or \( P(v_1, \ldots, v_k) \), \( P \) is any
   then \( A(t/x) \) is \( v_i(t/x) = v_j(t/x) \), or \( P(v_1(t/x), \ldots, v_k(t/x)) \).
5. If \( A \) is \( \neg \ B \) or \( A \lor C \) or \( Qx_i : B \) \( i \in \{ i_1, \ldots, i_m \} \) \( Qx_i : A \) or \( \exists x_i \),
   then \( A(t/x) \) is \( \neg B(t/x) \) or \( B(t/x) \lor C(t/x) \) or \( Qx_i (B(t/x)) \).
6. If \( A \) is \( Qx_i : B \) then \( A(t/x) \) is

\[ Qx_i : B \left( t_1, \ldots, t_{j-1}, t_j + \overline{t} / x_i; x_{j-1}, x_j, x_{j+1}, \ldots, x_k \right) \]
Def \( t \) is substitutable for \( x_i \) in \( A \) is inductively defined by:

1. If \( A \) is atomic, \( t \) is substitutable for \( x_i \) in \( A \).
2. If \( A \) is \( \neg B \) or \( B \lor C \), \( t \) is substitutable for \( x_i \) in \( A \) iff \( t \) is substitutable for \( x_i \) in both \( B \) and \( C \).
3. If \( A \) is \( Q x_i : B \), then \( t \) is substitutable for \( x_i \) in \( A \).
4. If \( A \) is \( Q x y : B \), \( y \neq i \), then \( t \) is substitutable for \( x_i \) in \( A \) iff either \( y \) does not occur in \( t \) or \( x_i \) is not free in \( B \) (in \( A \)).

Informally, \( t \) is substitutable for \( x_i \) in \( A \) iff there is no free occurrence of \( x_i \) in \( A \), in the scope of a quantifier \( Q y \) such that \( y \) occurs in \( t \).

Example: \( x_3 + x_4 \) is substitutable for \( x_i \) in \( \exists x_2 (x_2 + x_2 = x_i) \) \( x_2 \neq x_3 \) is not substitutable.
Theorem: 2 Let $s$ be a term, $t_j$'s terms, $x_{ij}$'s variables

\[ x_1 = t_1 \land \ldots \land x_k = t_k \rightarrow s = s(\bar{t}/\bar{x}) \]

(6) If each $t_j$ is substitutable for $x_{ij}$ in $A$, then

\[ x_1 = t_1 \land \ldots \land x_k = t_k \rightarrow (A \leftrightarrow A(\bar{t}/\bar{x})) \]

Proof - omitted

Examples 1

\[ \vdash x = y \rightarrow x + z = y + z \]

Take $s$ to be $x + z$, $s(y/x)$ is $y + z$.

2

\[ \vdash x = y \rightarrow u = u \rightarrow x + u = y + u \]

Take $s$ to be $x + u$, $s(y, u/x, u)$ is $y + u$.

3 For $f$ - $k$-ary,

\[ y_1 = z_1 \rightarrow y_2 = z_2 \rightarrow \ldots \rightarrow y_k = z_k \rightarrow f(y_1, \ldots, y_k) = f(z_1, \ldots, z_k) \]

Take $s$ to be $f(y_1, \ldots, y_k)$, $s(\bar{z}/\bar{y})$. Equality Axiom

4

\[ x = y \rightarrow (x \leq z \leftrightarrow y \leq z) \]

Take $A$ to be $x \leq z$, $A(y/x)$ is $y \leq z$.

5

\[ x = y \rightarrow u = v \rightarrow (x \leq u \leftrightarrow y \leq v) \]

Take $A$ to be $x \leq u$.
6) \[ y_1 = z_1 \rightarrow y_2 = z_2 \rightarrow \ldots \rightarrow y_k = z_k \rightarrow (P(y_1, y_k) \rightarrow P(z_1, \ldots, z_k)) \]

when \( P \) is \( k \)-ary

Equality Axiom.

Alphabetic Variant

\[ \exists x \exists z (x_2 + x_2 = x_1) \Leftrightarrow \exists x_3 (x_3 + x_3 = x_1) \]

Theorem

Let \( \exists x \, B \) be a formula.

Suppose \( y \) is substitutable for \( x \) in \( B \) and \( y \) does not appear free in \( P \).

Then

\[ \exists x \, B \vdash \exists y \, B(y/x). \]

Example

\[ B \iff x_2 + x_2 = x_1; \quad x_1, x_3, y = \bar{x}_5 \]

Proof:

\[ \vdash x = y \rightarrow (B \leftrightarrow B(y/x)) \] by Previous Theorem.

\[ \Omega \vdash \exists x \, B[\sigma] \iff \Omega \vdash B[\tau] \] for some \( x \)-variant \( \tau \) of \( \sigma \).

\[ \iff \Omega \vdash B[\tau] \] for the \( y \)-variant \( \tau \) of \( \tau \) with \( \tau(y) = \tau(x) \) since \( y \) not free in \( B \).

\[ \iff \Omega \vdash B(y/x)[\tau] \] since \( \tau(y) = \tau(x) \).

\[ \iff \Omega \vdash \exists y \, B(y/x)[\tau] \] since \( \sigma, \tau \) differ only on \( x \) and \( y \) and \( x, y \) not free in \( \exists y \, B(y/x) \).
Informal notation for substitution.

Often write $A(x)$ and then later $A(t)$
to mean $A$ is a formula (with free variable $x$
that occurs only as indicated)
and $A(t) = A(t/x)$.
Understood that $t$ substitutable for $x$ in $A$
and there are no "extra" occurrences of $x$ in $A$.

In structures, if $\mathcal{O}$ is a structure and $a \in \Omega_1$,
then $\mathcal{O} \models A(a)$ means

$\mathcal{O} \models A[\sigma]$ for any $\sigma$ s.t. $\sigma(x) = a$.

If $A \equiv A(x_1, \ldots, x_k)$

$\mathcal{O} \models A[a_1, \ldots, a_k]$ means $\mathcal{O} \models A[\sigma]$

for any $\sigma$ s.t. $\sigma(x_i) = a_i$ for all $i$.

Understood - use an alphahebic variant if necessary