substitutions in propositional logic

Canonical name	SubstitutionsInPropositionalLogic
Date of creation	2013-03-22 19:32:41
Last modified on	2013-03-22 19:32:41
Owner	CWoo (3771)
Last modified by	CWoo (3771)
Numerical id	22
Author	CWoo (3771)
Entry type	Definition
Classification	msc 03B99
Synonym	instance
Synonym	US
Related topic	Substitutability
Defines	simultaneous substitution
Defines	uniform substitution
Defines	schema
Defines	substitution instance

Uniform Substitution

One area of mathematics where substitution plays a prominent role is mathematical logic. In this entry, we are mainly interested in propositional logic. Recall that a substitution is a function $s : \Sigma_1^* \to P(\Sigma_2^*)$ preserving the empty word and concatenation. In a propositional logic, s has the following additional characteristics:

- only one alphabet Σ, often infinite, consisting of all propositional variables, logical connectives, and parentheses, is involved;
- s maps to singletons, so we might as well think of s as mapping into Σ^*;
- s fixes the logical connectives and parentheses;
- $s(\Sigma^*)$ is a set of well-formed formulas (rather than a set of words over Σ).

s is also called a *uniform substitution* because for any propositional variable p that occurs in A, s replaces each and every occurrence of p in A by $s(p)$. In practice, we write

$$A[B/p]$$

to mean change all occurrences of p in A by B, and leave all other variables fixed. This includes the case when p does not occur in A, in which case $A[B/p] = A$. $A[B/p]$ corresponds to a substitution that sends p to B and fixes all variables in A not equal to p. This is called an *individual substitution*. More generally,

$$A[B_1/p_1, \dots, B_n/p_n]$$

means: change all occurrences of p_i in A to B_i, for each $i = 1, \dots, n$, and leave all other variables fixed. This is called a *simultaneous substitution*, and corresponds to a substitution that sends p_i to B_i and fixes all other variables in A. Simultaneous substitutions are not the same as iterated individual substitutions:

$$A[B_1/p_1, \dots, B_n/p_n] \neq A[B_1/p_1] \cdots [B_n/p_n].$$

For example, if $A = p \vee q$, then $A[q/p, p/q] = q \vee p \neq p \vee p = A[q/p][p/q]$.

Recursive Definition of Substitution

Substitutions can also be defined inducitvely, starting from propositional variables. For the sake of simplicity, we only define uniform substitutions on one variable.

Definition. Suppose A and B are wff's, and p a propositional variable. Then

1. A is a propositional variable. If A is p, then $A[B/p] := B$. Otherwise, $A[B/p] := A$.
2. $\perp [B/p] := \perp$
3. If A is $C \to D$, then $A[B/p] := C[B/p] \to D[B/p]$.
4. If A is $C \wedge D$, then $A[B/p] := C[B/p] \wedge D[B/p]$.
5. If A is $C \vee D$, then $A[B/p] := C[B/p] \vee D[B/p]$.

Since $\neg A$ is $A \to \perp$, we see that $(\neg A)[B/p]$ is $\neg(A[B/p])$. In addition, if the language of the logic contains a modal connective, say $\Box$, we have

6. If A is $\Box C$, then $A[B/p] := \Box C[B/p]$.

Sets Closed under Uniform Substitution

A set Λ of wff's is said to be closed under uniform substitution if for any $A \in \Lambda$, $s(A) \in \Lambda$ for any (uniform) substitution s. We also say the set is closed under US (for uniform substitution), or obeys the rule of US. The smallest set containing a wff A that is closed under US is called a *schema* based on A, and is denoted by $\mathbf{A}$, the bold face version of A. An element of $\mathbf{A}$ is called a *substitution instance*, or simply an *instance* of A. For example, if A is $p \to (q \to p)$, where p and q are propositional variables, then

$$(D \to B) \to (((D \to B) \to C) \to (D \to B))$$

is a substitution instance of A, where p is replaced by $D \to B$ and q by $(D \to B) \to C$.

It is easy to see that a set is closed under US iff it is closed under individual substitution (IS). Obviously, one direction is clear, as IS is just special case of US. Conversely, suppose $A \in \Lambda$, which is closed under IS. Let

$p_1, \ldots, p_n$ be all the propositional variables in A, and $X_1, \ldots, X_n$ are arbitrary wff's. Let $q_1, \ldots, q_n$ be propositional variables, none of which occur in any of $A, X_1, \ldots, X_n$. Then

$$A[X_1/p_1, \ldots, X_n/p_n] = A[q_1/p_1] \cdots [q_n/p_n][X_1/q_1] \cdots [X_n/q_n] \in \Lambda.$$

There are in general two ways to specify a given axiom system for a propositional logic:

- list wff's $A_1, A_2, \ldots$ as axioms, and $R_1, \ldots$ as inference rules, including US, or
- list schemas $\mathbf{A_1}, \mathbf{A_2}, \ldots$ as axiom schemas, and $R_1, \ldots$ as inference rules, excluding US

Both specifications are equivalent, in that they produce the same set of theorems.

Non-Uniform Substitution

It is also possible to consider substitutions that only replace some, but not all, occurrences of a propositional variable in a formula A, or replace a variable at different locations in A by different formulas. For example, if A is $(p \to q) \vee (q \to p)$, then

- $(B \to q) \vee (B \to p)$ is obtained by replacing the first occurrences of p and q by B;
- $(B \to q) \vee (q \to C)$ is obtained by replacing the first and second occurrences of p by B and C respectively.

Replacements such as these are called *non-uniform substitutions*. Technically, these are no longer substitutions, for they are no longer functions on Σ^*, as individual variables may be mapped to different things depending on their location in the formula. In the first example above, p is mapped to both B and p, depending on whether it is the first or second occurrence in A.

To present a non-uniform substitution, let $\overline{p}$ be the list all the propositional variables $p_1, \ldots, p_n$ in A in order. Note that since a propositional variable p_i may occur multiple times in A, p may occur multiple times in $\overline{p}$.

Suppose each p_i is replaced by B_i. Let $\overline{B}$ be the list $B_1, \dots, B_n$. Then we denote

$$A[\overline{B}/\overline{p}]$$

by this non-uniform substitution. In the two examples above, $A[(B, q, B, p)/(p, q, q, p)]$ is the first wff, while $A[(B, q, q, C)/(p, q, q, p)]$ is the second.

Nevertheless, non-uniform substitution is useful in one respect: preservation of theoremhood. This fact is the famous substitution theorem, which says, if $p_1, \dots, p_n$ are all the propositional variables (not necessarily distinct) in a wff A that are listed in order of appearance in A, then replacing each variable by deductively equivalent formulas produces equivalent result. In short, if $\vdash B_i \leftrightarrow C_i$ for $i = 1, \dots, n$, then

$$\vdash A[\overline{B}/\overline{p}] \leftrightarrow A[\overline{C}/\overline{p}].$$

A set closed under non-uniform substitution (NUS) is defined in the same way as that of uniform substitution. It is easy to see that the smallest set closed under NUS containing the formula A is the schema $\mathbf{A}[\overline{\mathbf{q}}/\overline{\mathbf{p}}]$, where $\overline{q}$ is a list of pairwise distinct propositional variables. For example, the smallest set closed under NUS containing $(p \to q) \vee (q \to p)$ is $(\mathbf{p} \to \mathbf{q}) \vee (\mathbf{r} \to \mathbf{s})$. It is not hard to see that if the NUS closure of a formula is used as an axiom schema for a logic, with modus ponens as a rule of inference, then the logic is inconsistent.

First Order Logic

In a first order logic, substitutions are more complicated. Given a wff A, $A[B/p]$ does not necessarily mean replacing all occurrences of p by B. Here, again, a substitution is no longer a substitution in the sense above. In fact, replacements of symbols, like non-uniform substitutions, are conditional on the locations of the symbols in the wff A. These conditions are collectively known as the *substitutability* of a term B for the variable p, and is discussed in more detail `http://planetmath.org/Substitutability`here.