Predicate logic: Formal language

CS242 Formal Specification and Verification

University of Warwick

Autumn term 2007

Terms

Constants:

$$c \in \mathcal{C}$$

Functions:

$$f \in \mathcal{F}$$

Each function has some arity $n \geq 0$.
Terms:

$$t \ ::= \ x \mid c \mid f(t, \ldots, t)$$

$\mathcal{C} = \{f \in \mathcal{F} \mid f \text{ has arity } 0\}$.

Exercise 2.2.1.(a): d constant, f function with arity 3, g function with arity 2.

iv. $g(x, h(y, z), d)$

v. $f(f(g(d, x), f(g(d, x), y, g(y, d)), g(d, d)), g(f(d, d, x), d), z)$

Formulas

Predicates:

$$P \in \mathcal{P}$$

Each predicate has some arity $n \geq 0$.

$$\begin{array}{rcl} \phi & ::= & P(t_1, t_2, \ldots, t_n) \mid (\neg \phi) \mid \\ & & (\phi \wedge \phi) \mid (\phi \vee \phi) \mid (\phi \rightarrow \phi) \mid \\ & & (\forall x\, \phi) \mid (\exists x\, \phi) \end{array}$$

Binding priorities: $\forall y$ and $\exists y$ bind like $\neg$.

Example formula:

$$\forall x((P(x) \rightarrow Q(x)) \wedge S(x, y))$$

Exercise 2.2.3.(a): m constant, f function with one argument, S and B predicates with two arguments.

ii. $B(m, f(m))$

iii. $f(m)$

v. $S(B(m), z)$

vii. $(S(x, y) \rightarrow S(y, f(f(x))))$

Exercise 2.1.3:

(c) No animal is both a cat and a dog.

(d) Every prize was won by a boy.

(e) A boy won every prize.

Exercise 2.1.5:

(a) An attacker can persuade a server that a successful login has occurred, even if it hasn't.

(e) Credentials MUST NOT be forced by the protocol to be present in cleartext at any device other than the end user's.

(h) Different end user devices MAY be used to download, upload, or manage the same set of credentials.

Free and bound occurrences

An occurrence of x in ϕ is *free* if it is a leaf node in the parse tree of ϕ such that there is no path upwards from that node x to a node $\forall x$ or $\exists x$.

Otherwise, that occurrence of x is called *bound*.

For $\forall x\, \psi$, or $\exists x\, \psi$, we say that ψ — minus any of its subformulas $\exists x\, \chi$, or $\forall x\, \chi$ — is the *scope* of $\forall x$, respectively $\exists x$.

Examples:

$$\forall x((P(x) \to Q(x)) \wedge S(x, y))$$

$$(\forall x(P(x) \wedge Q(x))) \to (\neg P(x) \vee Q(y))$$

Substitution

Given a variable x, a term t and a formula ϕ, we define

$$\phi[t/x]$$

to be the formula obtained by replacing each *free* occurrence of variable x in ϕ with t.

Examples:

$$(\forall x((P(x) \to Q(x)) \wedge S(x, y)))[f(x, y)/x]$$

$$((\forall x(P(x) \wedge Q(x))) \to (\neg P(x) \vee Q(y)))[f(x, y)/x]$$

Avoiding variable capture

Given a term t, a variable x and a formula ϕ, we say that t *is free for* x in ϕ if no free x leaf in ϕ occurs in the scope of $\forall y$ or $\exists y$ for any variable y occurring in t.

Example:

$$(S(x) \wedge \forall y(P(x) \rightarrow Q(y)))[f(y, y)/x]$$