Derivation of Algorithms

Lecture 2
Predicate Calculus

COMP H 4018
Lecturer: Stephen Sheridan

Predicate Calculus

The Predicate calculus is concerned with relative truths - not absolute as in propositional calculus. It is concerned with statements like:

‘ x < 10 ‘

This assertion only becomes true or false when a value is substituted for x.

Ex:
x < 10
≡ { x:=7}
7 < 10
≡ {arithmetic}
true

Exercise Show that x =7 ≡ false

Statements of this type are called predicates

Exercise

Write predicates for each of the following:

1. x is a positive value less than 100
2. x is a positive even value
3. x is an odd number greater than 100 and less than 1000

Notation

P(X1,X2,.....Xn) stands for a predicate with n arguments
e.g. x + y = z might be represented by s(x,y,x)

Universe of Discourse (U)

This is the universe from which the values of variables in predicates are drawn.
Typical examples might be N,Z,R

Predicates as Propositions

Predicates become propositions(& hence,true or false) by binding their variables. This can be done in one of two ways.

1. Substitute values from a given domain of discourse for the variables
   e.g. Let P(x,y) be x + y = 3. Then
   P(1,2) = true , P(3,1) = false

2. Quantify the variables
The two most common forms are universal and existential quantification.

Universal Quantification : States that “ for all values of x in a given domain P(x) is true ”. It is written as : ∀x P(x).

Ex: Let U = Z,
$\forall x[x < x + 1] \equiv \underline{\text{true}}$
$\forall x[x = 3] \equiv \underline{\text{false}}$

Notes :

1. $\forall x P(x) \Rightarrow P(c)$, where $c \in U$.
2. The truth or falsity of $\forall x P(x)$ depends on U
   e.g. given $\forall x \forall y[x+y>x]$
   $U=N \Rightarrow \forall x \forall y[x+y>x] \equiv \underline{\text{true}}$
   $U= Z \Rightarrow \forall x \forall y[x+y>x] \equiv \underline{\text{false}}$
   Why ?

Existential Quantification: states that "there exists at least one x in U, such that P(x) is true. Written as - $\exists x P(x)$.

Ex Suppose U = Z
$\exists x[x<x+1] \equiv \underline{\text{true}}$
$\exists x[x=3] \equiv \underline{\text{true}}$
$\exists x[x=x+1] \equiv \underline{\text{false}}$

Note:
It is possible to have capture the notion of uniqueness with what is termed the Unique existential quantifier. This is written - $\exists! x P(x)$
Ex : Suppose U = N
$\exists! x[x<1] \equiv \underline{\text{true}}$
$\exists! x[x<4] \equiv \underline{\text{false}}$

Relationship between Quantifiers and Propositions

Suppose $U = \{ x_1, x_2, x_3, \ldots\ldots x_n\}$

$$\forall x P(x) \equiv P(x_1) \wedge P(x_2) \wedge P(x_3) \wedge \ldots\ldots \wedge P(x_n)$$

$$\exists x P(x) \equiv P(x_1) \vee P(x_2) \vee P(x_3) \vee \ldots\ldots \vee P(x_n)$$

Scope of Quantifier : The scope of a quantifier extends to the smallest well formed formula that follows the quantifier
e.g. **$\underline{\forall x P(x)}$** $\wedge$ Q(x)
$\underline{\forall x(P(x) \wedge Q(x))}$

Bound and Free Variables

Definition of Bound
Variables are bound when they occur within the scope of a quantifier
e.g. $\forall x(P(x))$ - x is bound
Definition of Free
Variables that are not bound are free.
e.g. $\forall x\, P(x) \wedge Q(\mathbf{y})$
In this expression x is bound and y is free.

Restriction Rule

All variables in a formula should be either free or bound but not both, and a given variable in a formula, if bound, should be bound, only to one quantifier.
e.g. $\forall x(P(x) \wedge \exists x Q(x))$ violates the restriction rule and is not a valid predicate.

Interpretation

An interpretation of a predicate P consists of a choice of domain and an assignment of relations to the predicate symbols.
e.g. $\forall x P(x)$ is given an interpretation when $U = Z$ and $P(x) = x>0 \wedge x < 100$.

Definition of Valid

A predicate is valid if it is true for all interpretations.

Definition of Satisfiable

A predicate is satisfiable if it holds for some interpretations.

Definition of Unsatisfiable

Predicate is not true for any universe or interpretation.

Note : These are the analogs of tautologies, contingencies and contradictions of propositional calculus.

Definition of Equivalence

Two assertions P and Q are said to be logically equivalent if and only if for every universe of discourse and every interpretation of the predicate variables P is true if and only if Q is true.

This definition can be used to construct proofs involving assertions.

Laws of Predicate Calculus

1. Negation
   (i) $\forall x \neg P(x) \equiv \neg \exists x P(x)$
   (ii) $\exists x \neg P(x) \equiv \neg \forall P(x)$
   (iii) $\exists x P(x) \equiv \neg(\forall x \neg P(x))$

2. **And** Distribution
   (i) $\forall x [P(x) \wedge Q(x)] \equiv \forall x P(x) \wedge \forall x Q(x)$
   (ii) $\forall x [P(x) \wedge R] \equiv \forall x P(x) \wedge R$, x not free in R
   (iii) $\exists x [P(x) \wedge R] \equiv \exists x P(x) \wedge R$, x not free in R
   (iv) $\exists x [P(x) \wedge Q(x)] \equiv \exists x P(x) \wedge \exists x Q(x)$

3. **Or** Distribution
   (i) $\forall x[p(x) \vee R] \equiv \forall x P(x) \vee R$, x not free in R

(ii) $[\forall x\ Px) \vee \forall x\ Q(x)\ ] \Rightarrow \forall x\ [\ P(x) \vee Q\ (x)\ ]$
(iii) $\exists x\ [\ P(x) \vee R\ ] \equiv \exists x\ P(x) \vee R$, x not free in R
(iv) $\exists x\ [P(x) \vee Q(x)\ ] \equiv \exists x\ P(x) \vee \exists x\ Q(x)$

4. $\forall x\ P(x) \Rightarrow P(c)$, where $c \in U$
$P(c) \Rightarrow \exists x P(x)$, where $c \in U$
$\forall x\ P(x) \Rightarrow \exists x\ P(x)$.

Comments
1. Negation

These equivalences can be used to propogate negation through a sequence of quantifiers. For example,

$\neg\ \exists x\ \forall y\ \forall z\ P(x,y,z)$
$\equiv\ \{\neg\ \}$
$\forall x\ \neg \forall y\ \forall\ P(x,y,z)$
$\equiv\ \{\neg\ \}$
$\forall x\ \exists y\ \neg\ \forall z\ P(x,y,z)$
$\equiv\ \{\ \neg\ \}$
$\forall x\ \exists y\ \exists z\ \neg P(x,y,z)$

2: **and** Distribution

Note that $\exists$ does not distribute over .This means that
$\exists x\ [\ P(x)\ \wedge Q(x)\ ] \neq \exists x P(x) \wedge \exists x Q(x)$
The l.h.s requires that some value of x satisfy both whereas the r.h.s may be satisfied by different values of x. As an example, consider U = Z and P(x) ≡ 'x even', Q(x) ='x odd'.

$\exists x\ [\ P(x) \wedge Q(x)\ ] \equiv$ false
$\exists x\ P(x) \wedge \exists x\ Q(x) \equiv$ true

3: **Or** distribution
Note that $\forall$ does not distribute over $\vee$.

Example Proofs

Ex1 : Prove that $\exists x\ [P(x) \Rightarrow Q(x)] \equiv [\forall x P(x) \Rightarrow \exists x\ Q(x)]$

Proof $\exists x\ [P(x) \Rightarrow Q(x)]$
$\equiv \{ \Rightarrow \}$
$\exists x\ [\neg P(x) \vee Q(x)]$
$\equiv$ { or dist }
$\exists x\ \neg P(x) \vee \exists x Q(x)$

$\equiv \{ \neg \}$
$\neg \forall x\ P(x) \vee \exists x Q(x)$
$\equiv \{ \Rightarrow \}$
$\forall x\ P(x) \Rightarrow \exists x\ Q(x)$

Transcribing Mathematical Statements

Ex. Let N (x) denote " x is a non negative integer "
Let E (x) denote " x is even "
Let O (x) denote " x is odd "
Let P (x) denote " x is prime "

(i) There exists an even integer $\exists x E(x)$
(ii) Every integer is even or odd $\forall x\ (E(x) \vee O(x))$
(iii) All primes are non negative $\forall x\ [P(x) \Rightarrow N(x)]$
(iv) The only even prime is two $\forall x\ [(\exists (x) \wedge P(x)) \Rightarrow x = 2]$
(v) There is one and only one even prime $\exists!\ x[P(x) \wedge E(x)]$
(vi) Not all integers are odd $\neg \forall x O(x)$ or $\exists x \neg O(x)$
(vii) If an integer is not odd then its even $\forall x[\neg O(x) \Rightarrow E(x)]$

Quantifying over Ranges

Def of sequence
A sequence is an ordered collection of elements, each of which has an associated index value indicating its position in the sequence.

Notation

f[0..N), denotes a sequence f of N elements whose indices are 0..N-1.

Assertions over Sequences

Ex1: State that every element of any array f[0..N) is positive.

Solution : $\forall i : 0 \leq i < N : f.i > 0$

Ex2 : State that f.k is the max element in array f.[0..N)

Solution $\forall i : 0 \leq i < n : f.k \geq f.i$

Ex3 : State that the elements in f.[0..N) are sorted in ascending order

Solution $\forall i : 0 \leq i < n : f.(i-1) \leq f.i$
or
$\forall i : 0 \leq i < n-1 : f.i < f.(i+1)$
or

$$\forall i,j : 0 \le i < n \wedge i \le j < n : f.i \le f.j$$

Ex4 : There is an element of the array f which has the value x'

Solution $\exists i : 0 \le i < N : f.i = x$

Ex5: There exists an element of array f which is greater than 5.

Solution $\exists i : 0 \le i < N : f.i > 5$

Ex6 : At least one element of f is greater than all elements of b.

Solution $\exists i : 0 \le i < N : \forall j : 0 \le j < N : f.i > b.j$

Ex7 Every element of b is a copy of some element of f.

Solution $\forall i : 0 \le i < N : \exists j : 0 \le j < M : b.i = f.j$

Laws

Universal Quantification over Ranges

$[\forall i : R : P \equiv \forall i : \neg R \vee P]$ Trading
$[\forall i : \underline{\text{false}} : P \equiv \underline{\text{true}}]$
$[\forall i : i = x : P \equiv P(i := x)]$ One-point rule
$[(\forall i : R : P) \wedge (\forall i : R : Q) \equiv (\forall i : R : P \wedge Q)]$
$[(\forall i : R : P) \wedge (\forall i : S : P) \equiv (\forall i : R \vee S : P)]$
$[(\forall i : R : P) \vee (\forall i : R : Q) \Rightarrow (\forall i : R : P \vee Q)]$
$[Q \vee (\forall i : R : P) \equiv (\forall i : R : Q \vee P)]$
$[Q \wedge (\forall i : R : P) \equiv (\forall i : R : Q \wedge P)]$

Existential Quantification over Ranges

$[\exists i : R : P \equiv \exists i : R \wedge P]$ Trading
$[\exists i : \underline{\text{false}} : P \equiv \underline{\text{false}}]$
$[\exists i : i = x : P \equiv P(i := x)]$ One-point rule
$[(\exists i : R : P \wedge Q) \Rightarrow (\exists i : R : P) \wedge (\exists i : R : Q)]$
$[(\exists i : R : P) \vee (\exists i : R : Q) \equiv (\exists i : R : P \vee Q)]$
$[Q \vee (\exists i : R : P) \equiv (\exists i : R : Q \vee P)]$
$[Q \wedge (\exists i : R : P) \equiv (\exists i : R : Q \wedge P)]$
$[(\exists i : R : P) \equiv \neg(\forall i : R : \neg P)]$

Reasoning with the Laws

Ex1: Prove $\forall j : \underline{false} : P \equiv \underline{true}$

Proof

$\forall j : \underline{false} : P$
$\equiv$ { trading }
$\forall j : \neg \underline{false} \vee P$
$\equiv$ { constant }
$\forall j : \underline{true} \vee P$
$\equiv$ { constant }
$\underline{true}$

Ex2: Prove $\neg(\exists j : m \leq j < n : P.j) \equiv \forall j : m \leq j < n : \neg P.j$

Proof

$\neg(\exists j : m \leq j < n : P.j)$
$\equiv$ { trading }
$\neg \exists j : (m \leq j < n \wedge P.j)$
$\equiv$ { $\neg\exists \equiv \forall\neg$ }
$\forall j : \neg(m \leq j < n \wedge P.j)$
$\equiv$ { de Morgan }
$\forall j : \neg(m \leq j < n) \vee \neg P.j)$
$\equiv$ { trading }
$\forall j : m \leq j < n : \neg P.j)$

Ex3 : Prove $(\forall x : R.x : f.x) \wedge (\forall x : R.x : g.x) \equiv (\forall x : R.x : f.x \wedge g.x)$

Proof

$(\forall x : R.x : f.x) \wedge (\forall x : R.x : g.x)$
$\equiv$ { trading twice }
$(\forall x : \neg R.x \vee f.x) \wedge (\forall x : \neg R.x \vee g.x)$
$\equiv$ { $\forall$ distributes over $\wedge$ }
$\forall x : (\neg R.x \vee f.x) \wedge (\neg R.x \vee g.x)$
$\equiv$ { $\vee$ distribution }
$\forall x : \neg R.x \vee (f.x \wedge g.x)$
$\equiv$ { trading }
$\forall x : R.x : (f.x \wedge g.x)$

Sum and Product

In programs we often need to find the sum or product of a sequence of numbers. To formalise this process we introduce the + and * quantifiers as follows:

Given $f[0..N)$ of numeric data

$+j: 0 \le j < N: f.j$ = sum of the elements in f
$*j: 0 \le j < N: f.j$ = product of the elements in f

Ex
$+j: 0 \le j < 3 : f.j = f.0 + f.1 + f.2$
$(+j: 0 \le j < t: f.j) + (+j: t \le i < N : f.j) = (f.0+f1+.. +f.t-1)+(f.t+f.t+1+ .. + f.N-1)$

Note: the identity elements for addition and multiplication are 0 and 1, respectively. That is, $a + 0 = a$ and $a*1 = a$.

Cardinality

Cardinality means the frequency of occurrence of some thing or event. In programming we often wish to count the frequency of occurrence of some value or condition. To formalise this process we define the cardinality- # - quantifier as follows:

$\#(true) = 1$ and $\#(false) = 0$

Given $f[0..N)$ of data and some predicate P

$\#j: 0 \le j < N: P(f.j)$ = the number of elements in f satisfying P.

For example, the frequency of even elements in an integer array f is given by

$\#j: 0 \le j < N: f.j \bmod 2 = 0$

Min and Max

We often compare two values to find the bigger or smaller of the two. Again we specify two binary operators called min and max as follows:

$a \min b = c \equiv (a = c \vee b = c) \wedge a \ge c \wedge b \ge c$
$a \max b = c \equiv (a = c \vee b = c) \wedge a \le c \wedge b \le c$

Note: the identity elements for min and max are $+Inf$ and $-Inf$. That is,
$a \min +inf = a$ and $a \max -Inf = a$.

Exercise

Q1. Given an array f[0..N), N ≥ 0, write down assertions for each of the following:

(a) t equals the sum of the elements in f;
(b) t equals the sum of the even elements in f;
(c) p equals the product of all multiples of 3 in f;
(d) k equals the frequency of the number 5 in f;
(e) the number of multiples of 5 in f is 10;
(f) all the elements in f are negative;
(use the cardinality quantifier to write this assertion)
(g) k is the smallest value in f

Problem Sheet 3 : Predicate Calculus

Q1 : Let U = {2,4,6} and let P(x) ≡ x mod 2 = 0
Evaluate ∀xP(x) , ∃xP(x).

Q2 : Let U = {5,6,7,11} , P(x) ≡ x < 10
Evaluate ∀x P(x) , ¬ ∃x P(x)

Q3 : Specify a Universe of Discourse for which the following propositions are true. (Try to choose the Universe to be as large a subset of the integers as possible.)

i) ∀x [x > 0] ,
ii) ∀x [x = 3]
iii) ∃y ∀x [x + y < 0]

Q4 : Let U = { 0,1 }. Expand each of the following :

i) ∀x P(0,x),
ii) ∀x ∀y P(x,y),
iii) ∀x ∃y P (x,y)
iv) ∃x ∀y P(x,y) ,
v) ∃y ∃x P(x,y)
vi) ∃x P(x,1) ∨ ∃x P(0,x)

Q5 : Prove that i) ∀x ∀y P(x,y) ≡ ∀y ∀x P(x,y)
ii) ∃x ∃y P(x,y) ≡ ∃y ∃x P(x,y)
[Hint : Expand the expressions to infinite conjunctions in i) and infinite disconjunctions in ii)]

Q6 : Write down quantified predicates for

i) x is a multiple of k
ii) x is a power of 2
iii) x is divisible by 3
iv) x is prime number

Q7 : In each of the following state whether the given predicate is valid or not valid (giving a reason) and in the case of valid predicates name the bound and free variables

i) 2 ≤ m < n ∧ (∀i : 2 ≤ i < m : i mod 2 ≠ 0)
ii) 2 ≤ m < n ∧ (∀n : 2 ≤ n < m : n mod 2 = 0)
iii) (∀m : n < m < n + 6 : (∃n : 2 ≤ n < m : m mod n = 0)
iv) ∃j : 0 ≤ j < n : (∀i : 0 ≤ i < j + 1 : f.i < a.j + 1)
v) x mod 2 = 0 ∧ (∀x : 0 ≤ x < n : f.x > 0)

Q8 : Prove

i) ∃x (P(x) ⇒ Q(x)) ≡ (∀x P(x) ⇒ ∃x Q(x))
ii) ¬∃x ¬ P(x) ≡ ∀x P(x)
iii) ∀x P(x) ∴ Q ≡ ∃x (P(x) ⇒ Q), x not free in Q.

iv) $\forall x\ (\neg P(x) \vee Q(x)) \equiv \neg\exists x\ (P(x) \wedge \neg\ Q(x))$

Q9: Let A[0..N), N ≥1 be an integer array.
Write down formal assertions for each of the following:

i) All elements of A are in the range 1..100
ii) All elements of A[j..k] are zero
iii) A[j..k] contains an even integer value
iv) No values of A[j..k] are zero
v) Max is the largest value in A
vi) All elements of A are equal
vii) All values in A[j..k] are in the range a to b inclusive
viii) j = index of smallest element in A[i..N]
ix) All the elements of A are unique
x) A is not sorted
xi) A.i is the "left most" zero in A, if any
xii) If $x \in A[0..k]$ then $x \in A[k..N]$

Q10: Prove

i) $[\ Q \vee \forall x : R.x : f.x\ ] \equiv [\ \forall x : R.x : Q \vee f.x\ ]$
ii) $[\ \forall x : R.x : f.x \wedge \forall x : S.x : f.x\ ] \equiv [\ \forall x : R.x \vee S.x : f.x\ ]$
iii) $\forall x : \underline{\text{false}} : f.x \equiv \underline{\text{true}}$
iv) $\exists x : \underline{\text{false}} : f.x \equiv \underline{\text{false}}$

Q11: Prove

i) $(\forall i : 0 \le i < k : f.i > 0\ ) \wedge (\ \forall i : k \le i < n : f.i > 0\ ) \equiv \forall i : 0 \le i < n : f.i > 0$
ii) $(\ \exists i : 0 \le i < k : f.i > 0\ ) \vee (\ \exists i : k \le i < n : f.i > 0\ ) \equiv \exists i : 0 \le i < n : f.i > 0$
iii) $x > 0 \vee \forall i : 0 \le i < n : f.i \le x \equiv \forall i : 0 \le i < n : x > 0 \vee f.i \le x$

Q12: Prove

i) $\neg(\ \forall i : 0 \le i < n : b.i = x\ ) \equiv \exists i : 0 \le i < n : b.i \ne x$
ii) $\neg\ (\ \forall i : 0 \le i < n : b.i > 0 \vee b.i < 100\ ) \equiv (\ \exists i : 0 \le i < n : b.i \le 0 \vee b.i > 100)$
iii) $\neg(\ \exists i : 0 \le i < n : b.i = 0\ ) \equiv \forall i : 0 \le i < n : b.i \ne 0$
iv) $\neg\ (\ \forall i : R.i : f.i\ ) \equiv (\ \exists i : R.i : \neg\ f.i\ )$