COMP1600/6260 Complete Exam Guide - Mock & Final 2024

Q1: Prop Logic Relations (6m)

Mock: $R(A,B) \Leftrightarrow \exists C.(A \wedge C \equiv B)$
Circle true: (a) $R(A,A)$ all A? (b) $\exists A,B$ both $R(A,B)$ & $R(B,A)$? (c) $R(A,B)$ when $B \models A$? (d) $R(\top,B)$ some B? (e) $R(\bot,B)$ all B?

Answers: (a),(b),(d)
(a)✓: $C=\top$, then $A \wedge \top \equiv A$
(b)✓: $A=B$ works, pick $C=\top$ for both
(c)×: Cex: $A=p\wedge q, B=p$. $B \models A$ but no C s.t. $A \wedge C \equiv p$
(d)✓: Pick $B=\top, C=\top$: $\top \wedge \top \equiv \top$
(e)×: $\bot \wedge C \equiv \bot$ only if $B=\bot$

Final: $R(A,B) \Leftrightarrow \exists C.(A \vee C \equiv B)$
Circle true: (a) $R(A,B)$ when $A \equiv B$? (b) $R(A,B) \Rightarrow R(B,A)$? (c) $\exists A,B$ both false? (d) $R(A,B)$ when $A \models B$? (e) $R(A,\top)$ all A? (f) $R(A,\top)$ some A?

Answers: (a),(c),(e),(f)
(a)✓: $C=\bot$, then $A \vee \bot \equiv A \equiv B$
(b)×: $R(p,\top)$ true ($C=\neg p$) but $R(\top,p)$ false
(c)✓: $A=p, B=q$ different atoms. No C works
(d)×: Cex: $A=p\wedge q, B=p$. $A \models B$ but can't get p from $p \wedge q \vee C$
(e)✓: $C=\neg A$, then $A \vee \neg A \equiv \top$
(f)✓: By (e)

Q2: Eliminate $\rightarrow$ (3+3m)

Mock: $H=[p \rightarrow (q \wedge \neg r)] \vee [\neg p \rightarrow (\neg q \vee r)]$
(a) Eliminate $\rightarrow$ (b) Tautology/Contradiction/Contingency?

(a) Use $A \rightarrow B \equiv \neg A \vee B$:
$H \equiv [\neg p \vee (q \wedge \neg r)] \vee [p \vee (\neg q \vee r)]$
Simplify: $[\neg p \vee (q \wedge \neg r)] \vee [p \vee \neg q \vee r]$
(b) Truth table: $p=T, q=T, r=T$: $[\neg T \vee F] \vee [T \vee F] = T$
$p=T, q=T, r=F$: $[\neg T \vee T] \vee [T \vee T] = T$
All 8 rows give T $\rightarrow$ **Tautology**

Final: $G=\neg(p \rightarrow q) \vee (q \wedge \neg r)$
(a) Eliminate $\rightarrow$ (b) Type?

(a) $\neg(p \rightarrow q) = \neg(\neg p \vee q) = p \wedge \neg q$ (De Morgan)
$G \equiv (p \wedge \neg q) \vee (q \wedge \neg r)$
(b) Test: $p=T, q=T, r=T$: $(T \wedge F) \vee (T \wedge F) = F$
$p=T, q=F, r=T$: $(T \wedge T) \vee (F \wedge F) = T$
Mixed T/F $\rightarrow$ **Contingency**

Q3: Free/Bound Vars (3+3m)

Mock (a): $\forall x.R(x,y) \rightarrow \exists y.R(x,y)$
Free? Bound? Equiv if intersect?

Left: $\forall x.R(x,y)$: x bound by $\forall x$, y free
Right: $\exists y.R(x,y)$: y bound by $\exists y$, x free
Free=$\{x,y\}$, Bound=$\{x,y\}$ **INTERSECT**
Equiv: $\forall z.R(z,y) \rightarrow \exists w.R(x,w)$
Now Free=$\{x,y\}$, Bound=$\{z,w\}$ ✓

Mock (b): $\exists x.\exists x.R(x,y) \vee \forall x.R(x,x)$

$\exists x.\exists x.R(x,y)$: Inner $\exists x$ shadows outer, x bound
$\forall x.R(x,x)$: x bound by this $\forall x$
Only y is free. Free=$\{y\}$, Bound=$\{x\}$ ✓

Final (a): $R(x) \rightarrow \forall x.\forall x.R(y) \vee \exists y.R(y)$

$R(x)$: x free
$\forall x.\forall x.R(y)$: both $\forall x$ bind (outer shadowed), y free
$\exists y.R(y)$: y bound
Free=$\{x,y\}$, Bound=$\{x,y\}$ **INTERSECT**
Equiv: $R(z) \rightarrow \forall u.\forall v.R(y) \vee \exists w.R(w)$

Final (b): $\neg\exists x.(R(y,x) \vee \exists x.R(x,y))$

$R(y,x)$: outer $\exists x$ binds x, y free
$\exists x.R(x,y)$: inner $\exists x$ binds x, y free
Free=$\{y\}$, Bound=$\{x\}$ ✓

Q4: Induction Base/Step (varies)

Mock (a): sum[]=0, sum$(x:xs)$ = x+sumxs
$P(l)$ =sum$(l) \geq 1$. Why step $\forall x.P(l) \rightarrow P(x:l)$ true?

If $P(l)$, i.e., sum$(l) \geq 1$, then:
sum$(x:l) = x+$sum$(l) \geq x+1 \geq 0+1=1$
since $x \in \mathbb{N}$ means $x \geq 0$. So $P(x:l)$ holds.

Mock (b): Why not prove $\forall l.P(l)$?

Base case fails: $P([])$ requires sum$[]=0 \geq 1$, which is false. Without base case, can't complete induction.

Final (a): Give $P(n)$ where step holds but base fails.

$P(n)=(n \geq 1)$. Step: If $n \geq 1$ then $n+1 \geq 2 > 1$, so $P(n) \rightarrow P(n+1)$ ✓. Base: $P(0)=0 \geq 1$ is false ×

Final (b): Given $P(k)$ true for $k>0$ and step holds. Prove $\forall n \geq k.P(n)$?

Define $Q(m)=P(m+k)$. Base: $Q(0)=P(k)$ true (given). Step: Assume $Q(m)=P(m+k)$. Then $P(m+k) \rightarrow P(m+k+1)$ by P's step, so $Q(m) \rightarrow Q(m+1)$. By induction, $\forall m.Q(m)$, hence $\forall m.P(m+k)$, i.e., $\forall n \geq k.P(n)$.

Q5: Generalization (2+1+3m)

Mock: $e(0,a)=a; e(n+1,a)=e(n,2a)$
$P(n) \equiv e(2n,1)=e(n,1) \times e(n,1)$
(a) What does e compute? What is P?
(b) Why induction hard? (c) Generalize?

(a) $e(n,a)=2^n \times a$. P expresses $2^{2n}=(2^n)^2$.
(b) IH: $e(2n,1)=e(n,1)^2$. Need: $e(2(n+1),1)$.
But $e(2n+2,1)=e(2n+1,2)=e(2n,4)$. IH only has $e(2n,\mathbf{1})$ not $e(2n,\mathbf{4})$. Parameter mismatch!
(c) **Generalize:** $Q(n,a) \equiv e(2n,a)=e(n,a)^2$.
$Q \Rightarrow P$: Set $a=1$. Why easier: IH $Q(n,a)$ for all a, so use $Q(n,2a)$: $e(2n,2a)=e(n,2a)^2$. Matches recursion!

Final: $m(0,x,a)=a; m(n+1,x,a)=m(n,x,a+x)$
$P(n,x) \equiv m(n,x,0)=m(x,n,0)$
Same questions.

(a) $m(n,x,a)=a+n \times x$. P expresses $n \times x = x \times n$ (commutativity).
(b) IH: $m(n,x,0)=m(x,n,0)$. Need: $m(n+1,x,0)$.
But $m(n+1,x,0)=m(n,x,x)$. IH only has $m(n,x,\mathbf{0})$ not $m(n,x,\mathbf{x})$. Parameter mismatch!
(c) **Generalize:** $Q(n,x,a) \equiv m(n,x,a)=m(x,n,a)$.
$Q \Rightarrow P$: Set $a=0$. Why easier: IH $Q(n,x,a)$ for all a, so use $Q(n,x,a{+}x)$: $m(n,x,a{+}x)=m(x,n,a+x)$. Matches recursion!

Q6: Termination (varies)

Mock: sub$(n,0) = n$; sub(n,m) =sub$(n-1, m-1)$
(a) When terminate? Why yes/no for each?
(b) Why not all despite both decrease?

(a) **Terminates:** $m \geq 0$ (any n).
Proof: If $m = 0$, returns n (base). If $m > 0$, calls sub$(n-1, m-1)$ where new m is $m-1 < m$. Measure: m. After m steps, reaches $m = 0$, terminates.
Not terminate: $m < 0$.
Proof: Each call $m \to m-1$ becomes more negative: $-1, -2, -3, \ldots$ Never reaches base $m = 0$. Infinite recursion.
(b) $\mathbb{Z}$ has no minimum element. Though $n-1 < n$ and $m-1 < m$, when $m < 0$, can decrease forever. Termination needs well-founded measure (maps to $\mathbb{N}$, which has min 0). $\mathbb{Z}$ not well-founded.

Final: gcd$(a,0) = a$; gcd(a,b) =gcd$(b, a\%b)$
(a) Why terminate for $a, b \geq 0$?
(b) Define measure, justify decrease.

(a) Base: $b = 0$ returns a directly. Recursive: $b > 0$ calls gcd$(b, a\%b)$. Key: $0 \leq a\%b < b$ (remainder property). So second parameter strictly decreases: $b \to a\%b$ where $a\%b < b$. Since $b \in \mathbb{N}$ and decreases, must reach 0 in finite steps. Terminates.
(b) **Measure:** Second parameter b.
Justification: In recursive call gcd$(b, a\%b)$, new measure is $a\%b$. By modulo definition, $a\%b < b$ when $b > 0$. So measure strictly decreases: $b \to a\%b < b$. Since $b \geq 0$ and decreases to 0, terminates.

Q7: Hoare Triples (4m)

Mock: Circle valid:
(a) $\{x > 3\}$ y:=x*2 $\{y > 7\}$
(b) $\{x > -3\}$ y:=x*(-2) $\{y > 6\}$
(c) $\{a = 3 \wedge b = 4\}$ while a¿0 do a:=a+1 $\{a \leq 0\}$
(d) $\{a = 9\}$ while a=0 do a:=-1 $\{a = -1\}$

Valid: (a),(c)
(a)✓: Pre: $x > 3$, assume int so $x \geq 4$. Execute: $y := x \times 2$, so $y \geq 8$. Post: $y \geq 8 > 7$ ✓
(b)×: Cex: $x = 0$ satisfies $0 > -3$. Execute: $y := 0 \times (-2) = 0$. Check: $0 \not> 6$ ×
(c)✓: Pre: $a = 3 > 0$, enter loop. Body: $a := a + 1$ increases a. Condition $a > 0$ remains true forever. Loop never exits. Partial correctness vacuously true (doesn't terminate).
(d)×: Pre: $a = 9$. Condition: $a = 0$ is $9 = 0$, false. Loop body never executes. Post: a still 9, not -1 ×

Final: Circle valid (all int):
(a) $\{x = 3 \wedge y = x\}$ x:=x-1; y:=x-1 $\{y = x\}$
(b) $\{x = 3 \wedge y = x\}$ y:=x-1; x:=x-1 $\{y = x\}$
(c) $\{m > 0 \wedge n > m\}$ if m¿n then x:=0 else y:=0 $\{n > x\}$
(d) $\{m = n \wedge m < n\}$ if x¡3 then y:=4 else z:=5 $\{z \times y = 20\}$

Valid: (b),(d)
(a)×: $x = 3, y = 3$. After x:=x-1: $x = 2, y = 3$. After y:=x-1: $x = 2, y = 1$. Check: $y \neq x$ ×
(b)✓: $x = 3, y = 3$. After y:=x-1: $x = 3, y = 2$. After x:=x-1: $x = 2, y = 2$. Check: $y = x$ ✓
(c)×: Pre: $m > 0 \wedge n > m$ so $m \not> n$. Else branch: y:=0. But x undefined or unchanged. Can't guarantee $n > x$ ×
(d)✓: Pre: $m = n \wedge m < n$ is contradiction (impossible). Vacuously true (false precondition implies anything).

Q8: Partial vs Total (2m)

Mock: Example where $\{P\}S\{Q\}$ valid but $[P]S[Q]$ not? Or explain impossible.

Exists. Let P =true, S=while true do skip, Q =false.
Partial {true}S{false} valid: S never terminates, so "if S terminates then false" is vacuously true (antecedent false).
Total [true]S[false] invalid: S must terminate, but while true loops forever. Violates termination requirement.

Final: Example where $[P]S[Q]$ valid but $\{P\}S\{Q\}$ not? Or explain impossible.

Impossible. Total correctness $[P]S[Q]$ means: if P holds, then S terminates AND Q holds after. This implies partial correctness $\{P\}S\{Q\}$ (if P and S terminates, then Q), since total guarantees termination. Therefore $[P]S[Q]$ valid $\Rightarrow$ $\{P\}S\{Q\}$ valid. No counterexample exists.

Q9: Loop Total Correctness (8m)

Mock: $[P(x)]$ while $(f(x) > 0)$ $\{x := g(x)\}$ [true]
f, g terminate. Valid for all satisfying:
(a) $g(x) < x\ \forall x$ (b) $g(x) < x < f(x)\ \forall x$
(c) $P(x) \equiv x > 0$ & $g(x) < x$ (d) $f(x) < g(x) < x\ \forall x$

(a)×: Cex: P =true, $g(x) = x - 1$, $f(x) = 1$. Start $x = 5$, $f(5) = 1 > 0$ enter. Loop: $x \to 4 \to 3 \to 2 \to 1 \to 0 \to -1 \to \ldots$ x decreases but $f(x) = 1 > 0$ always. Never exits.
(b)×: Same issue. $x < f(x)$ doesn't help. No lower bound on x.
(c)×: Even $x > 0$ initially, if $f(x) = 1$ constantly, can go negative forever while f stays > 0.
(d)✓: Key: $f(x) < g(x) < x$. Each iteration: $x' = g(x) < x$ and $f(x) < g(x)$. Creates strictly decreasing sequence. Since bounded below (eventually), terminates in finite steps. (More rigorous: $f(x) < g(x)$ creates well-founded ordering.)

Final: $[P(x)]$ while $b(x)$ $\{x := g(x)\}$ [true]
b, g terminate. Valid under:
(a) $P(x) \to b(g(x))\ \forall x$ (b) b constant
(c) $g(x) < x$ & $b(x) = b(g(x))\ \forall x$
(d) $b(x) = \neg b(g(x))$ & $P(x) \to b(x)\ \forall x$

(a)×: Says $b(g(x))$ true but nothing about termination. Cex: P =true, $b(x)$ =true, $g(x) = x$. Never exits.
(b)×: If $b \equiv$true, loop never exits.
(c)×: b value unchanged means loop may not exit. Cex: $b(x)$ =true constant, $g(x) = x - 1$. Loops forever.
(d)✓: b flips each iteration. If $P(x)$ then $b(x)$ =true (enter loop). After one iteration: $x' = g(x)$, $b(x') = b(g(x)) = \neg b(x)$ =false. Exits immediately. Maximum 1 iteration, always terminates.

Quick Reference

Prop Logic: $A \to B \equiv \neg A \vee B$; $\neg(A \wedge B) \equiv \neg A \vee \neg B$; $\neg(A \vee B) \equiv \neg A \wedge \neg B$
FOL: $\neg\forall x.P \equiv \exists x.\neg P$; $\neg\exists x.P \equiv \forall x.\neg P$
Induction: Base + Step $\vdash \forall n$. For lists: $P([])$ + $(\forall x, xs.P(xs) \to P(x : xs)) \vdash \forall l.P(l)$
Hoare: Assign: $\{Q[x \to E]\}$x:=E$\{Q\}$; Seq: $\{P\}$S1$\{R\}\{R\}$S2$\{Q\}$ $\Rightarrow$ $\{P\}$S1;S2$\{Q\}$; If: $\{P \wedge b\}$S1$\{Q\}\{P \wedge \neg b\}$S2$\{Q\} \Rightarrow \{P\}$if b then S1 else S2$\{Q\}$; While: $\{I \wedge b\}$S$\{I\} \Rightarrow \{I\}$while b do S$\{I \wedge \neg b\}$
Partial vs Total: $\{P\}S\{Q\}$=IF P & S terminates THEN Q. $[P]S[Q]$=IF P THEN S terminates AND Q.