CS6320: Formal Methods for Distributed Systems
Sample Mid-term Exam

1. (2 marks) Show $\{q \Rightarrow r\} \models (p \wedge q) \Rightarrow r$

2. ($2\frac{1}{2}$ marks) Show $\{q \Rightarrow r\} \vdash (p \wedge q) \Rightarrow r$ using the rules of the natural deduction system given in the appendix.

3. (5 marks) Prove $\vdash (\neg\neg p \vee (p \wedge q)) \Rightarrow (p \vee q)$ using the rules of the natural deduction system given in the appendix.

4. ($2\frac{1}{2}$ marks) Determine the weakest precondition P that satisfies the following. Simplify your answers as much as you can.

   (a) $(\!| P |\!)\; y := x^2 \;(\!| y = x^2 |\!)$

   (b) $(\!| P |\!)\; x := x + x; x := x \operatorname{div} 2 \;(\!| y = x^2 |\!)$

5. (3 marks) Prove that $\vdash_{\text{par}} (\!| x \neq 0 |\!)\; \mathit{ProgA}\; (\!| \operatorname{abs}(y) > \operatorname{abs}(x) |\!)$ where *ProgA* is below. Here, abs evaluates to the absolute value of its argument, e.g. $\operatorname{abs}(3) = 3$ and $\operatorname{abs}(-3) = 3$.

```
y := x;
if x > 0
{   x := x − 1;
}
else
{   x := x + 1;
}
```

6. (5 marks) Prove that $\vdash_{\text{par}} (\!| z \mod 2 = 0 |\!)\; \mathit{ProgB}\; (\!| z = 2x |\!)$ where *ProgB* is below. Use $z = x + y$ as the *loop invariant*.

```
x := z;
y := 0;
while x ≠ y
{   x := x − 1;
    y := y + 1;
}
```

Laws of the Algebra of Propositions

Commutativity of $\wedge$ and $\vee$

$$W_1 \wedge W_2 \equiv W_2 \wedge W_1$$
$$W_1 \vee W_2 \equiv W_2 \vee W_1$$

Associativity of $\wedge$ and $\vee$

$$(W_1 \wedge W_2) \wedge W_3 \equiv W_1 \wedge (W_2 \wedge W_3)$$
$$(W_1 \vee W_2) \vee W_3 \equiv W_1 \vee (W_2 \vee W_3)$$

Distributivity of $\wedge$ over $\vee$ and $\vee$ over $\wedge$

$$W_1 \wedge (W_2 \vee W_3) \equiv (W_1 \wedge W_2) \vee (W_1 \wedge W_3)$$
$$W_1 \vee (W_2 \wedge W_3) \equiv (W_1 \vee W_2) \wedge (W_1 \vee W_3)$$

Absorption

$$W_1 \wedge (W_1 \vee W_2) \equiv W_1$$
$$W_1 \vee (W_1 \wedge W_2) \equiv W_1$$

De Morgan's laws

$$\neg(W_1 \wedge W_2) \equiv \neg W_1 \vee \neg W_2$$
$$\neg(W_1 \vee W_2) \equiv \neg W_1 \wedge \neg W_2$$

Idempotence of $\wedge$ and $\vee$

$$W \wedge W \equiv W$$
$$W \vee W \equiv W$$

true-false laws

$$\mathbf{True} \wedge W \equiv W$$
$$\mathbf{False} \wedge W \equiv \mathbf{False}$$

true-false laws, continued

$$\mathbf{True} \vee W \equiv \mathbf{True}$$
$$\mathbf{False} \vee W \equiv W$$
$$W \Rightarrow \mathbf{True} \equiv \mathbf{True}$$
$$\mathbf{True} \Rightarrow W \equiv W$$
$$W \Rightarrow \mathbf{False} \equiv \neg W$$
$$\mathbf{False} \Rightarrow W \equiv \mathbf{True}$$
$$W \Rightarrow W \equiv \mathbf{True}$$

Involution

$$\neg\neg W \equiv W$$

Complement laws

$$W \wedge \neg W \equiv \mathbf{False}$$
$$W \vee \neg W \equiv \mathbf{True}$$
$$\neg\mathbf{True} \equiv \mathbf{False}$$
$$\neg\mathbf{False} \equiv \mathbf{True}$$

Definition of biconditional

$$W_1 \Leftrightarrow W_2 \equiv (W_1 \Rightarrow W_2) \wedge (W_2 \Rightarrow W_1)$$

Definition of conditional

$$W_1 \Rightarrow W_2 \equiv \neg W_1 \vee W_2$$

Contrapositive law

$$W_1 \Rightarrow W_2 \equiv \neg W_2 \Rightarrow \neg W_1$$

A Natural Deduction System

REPETITION

$$\frac{W}{W}$$

$\wedge$-INTRODUCTION

$$\frac{W_1, W_2}{W_1 \wedge W_2}$$

$\wedge$-ELIMINATION-LEFT

$$\frac{W_1 \wedge W_2}{W_1}$$

$\wedge$-ELIMINATION-RIGHT

$$\frac{W_1 \wedge W_2}{W_2}$$

$\vee$-INTRODUCTION-RIGHT

$$\frac{W_1}{W_1 \vee W_2}$$

$\vee$-INTRODUCTION-LEFT

$$\frac{W_2}{W_1 \vee W_2}$$

$\vee$-ELIMINATION

$$\frac{W_1 \vee W_2, \frac{W_1}{W_3}, \frac{W_2}{W_3}}{W_3}$$

$\neg$-INTRODUCTION

$$\frac{\frac{W_1}{W_2 \wedge \neg W_2}}{\neg W_1}$$

$\neg$-ELIMINATION

$$\frac{\neg\neg W}{W}$$

$\Rightarrow$-INTRODUCTION

$$\frac{\frac{W_1}{W_2}}{W_1 \Rightarrow W_2}$$

$\Rightarrow$-ELIMINATION

$$\frac{W_1, W_1 \Rightarrow W_2}{W_2}$$

$\Leftrightarrow$-INTRODUCTION

$$\frac{\frac{W_1}{W_2}, \frac{W_2}{W_1}}{W_1 \Leftrightarrow W_2}$$

$\Leftrightarrow$-ELIMINATION-LEFT

$$\frac{W_1 \Leftrightarrow W_2, W_1}{W_2}$$

$\Leftrightarrow$-ELIMINATION-RIGHT

$$\frac{W_1 \Leftrightarrow W_2, W_2}{W_1}$$

Floyd-Hoare Deduction System for Partial Correctness

Assignment

$$\frac{}{(\!|\, Q[V \mapsto E] \,|\!)\; V := E \;(\!|\, Q \,|\!)}$$

Sequencing

$$\frac{(\!|\, P \,|\!)\; C_1 \;(\!|\, R \,|\!), \quad (\!|\, R \,|\!)\; C_2 \;(\!|\, Q \,|\!)}{(\!|\, P \,|\!)\; C_1 ; C_2 \;(\!|\, Q \,|\!)}$$

One-armed-conditional

$$\frac{(\!|\, B \wedge P \,|\!)\; C \;(\!|\, Q \,|\!), \quad (\neg B \wedge P) \Rightarrow Q}{(\!|\, P \,|\!)\; \textbf{if}\ B\ C \;(\!|\, Q \,|\!)}$$

Two-armed-conditional

$$\frac{(\!|\, B \wedge P \,|\!)\; C_1 \;(\!|\, Q \,|\!), \quad (\!|\, \neg B \wedge P \,|\!)\; C_2 \;(\!|\, Q \,|\!)}{(\!|\, P \,|\!)\; \textbf{if}\ B\ C_1\ \textbf{else}\ C_2 \;(\!|\, Q \,|\!)}$$

While

$$\frac{(\!|\, Inv \wedge B \,|\!)\; C \;(\!|\, Inv \,|\!)}{(\!|\, Inv \,|\!)\; \textbf{while}\ B\ C \;(\!|\, Inv \wedge \neg B \,|\!)}$$

Consequence

$$\frac{P \Rightarrow P', \quad (\!|\, P' \,|\!)\; C \;(\!|\, Q' \,|\!), \quad Q' \Rightarrow Q}{(\!|\, P \,|\!)\; C \;(\!|\, Q \,|\!)}$$