# CS245 Midterm Reference Sheets

(3 pages)

## Essential laws of propositional logic

Commutativity

$$p \land q \;\models\!\!\!\!\!\models\; q \land p$$

$$p \lor q \;\models\!\!\!\!\!\models\; q \lor p$$

$$p \leftrightarrow q \;\models\!\!\!\!\!\models\; q \leftrightarrow p$$

Associativity

$$p \land (q \land r) \;\models\!\!\!\!\!\models\; (p \land q) \land r$$

$$p \lor (q \lor r) \;\models\!\!\!\!\!\models\; (p \lor q) \lor r$$

Distributivity

$$p \lor (q \land r) \;\models\!\!\!\!\!\models\; (p \lor q) \land (p \lor r)$$

$$p \land (q \lor r) \;\models\!\!\!\!\!\models\; (p \land q) \lor (p \land r)$$

De Morgan

$$\neg(p \land q) \;\models\!\!\!\!\!\models\; \neg p \lor \neg q$$

$$\neg(p \lor q) \;\models\!\!\!\!\!\models\; \neg p \land \neg q$$

Double Negation

$$\neg(\neg p) \;\models\!\!\!\!\!\models\; p$$

Excluded Middle

$$p \lor \neg p \;\models\!\!\!\!\!\models\; 1$$

Contradiction

$$p \land \neg p \;\models\!\!\!\!\!\models\; 0$$

Implication

$$p \to q \;\models\!\!\!\!\!\models\; \neg p \lor q$$

Contrapositive

$$p \to q \;\models\!\!\!\!\!\models\; \neg q \to \neg p$$

Equivalence

$$p \leftrightarrow q \;\models\!\!\!\!\!\models\; (p \to q) \land (q \to p)$$

Idempotence

$$p \lor p \;\models\!\!\!\!\!\models\; p$$

$$p \land p \;\models\!\!\!\!\!\models\; p$$

Identity

$$p \land 1 \;\models\!\!\!\!\!\models\; p$$

$$p \lor 0 \;\models\!\!\!\!\!\models\; p$$

Domination

$$p \land 0 \;\models\!\!\!\!\!\models\; 0$$

$$p \lor 1 \;\models\!\!\!\!\!\models\; 1$$

Absorption I

$$p \lor (p \land q) \;\models\!\!\!\!\!\models\; p$$

$$p \land (p \lor q) \;\models\!\!\!\!\!\models\; p$$

Absorption II

$$(p \land q) \lor (\neg p \land q) \;\models\!\!\!\!\!\models\; q$$

$$(p \lor q) \land (\neg p \lor q) \;\models\!\!\!\!\!\models\; q$$

EQ subs

**Theorem(EQSubs).** Let $r(u)$ be a term that contains $u$ as a free variable, and let $t_1, t_2$ be terms. Let $r(t_i)$ denote $r$ where all instances of $u$ have been replaced by $t_i$. For any set $\Sigma$ of first-order logic formulas, we have that $\Sigma \vdash t_1 \approx t_2$ implies $\Sigma \vdash r(t_1) \approx r(t_2)$.

EQtrans

**Theorem (EQTrans(k)).** Let $k \geq 1$ be a natural number, $\Sigma$ be a set of first-order logic formulas, and $t_1, t_2, \ldots, t_{k+1}$ be terms. If $\Sigma \vdash t_i \approx t_{i+1}$ for all $1 \leq i \leq k$, then $\Sigma \vdash t_1 \approx t_{k+1}$.

**PA1** : $\forall x(\neg(s(x) = 0))$
**PA2** : $\forall x \forall y(s(x) = s(y) \to x = y)$
**PA3** : $\forall x(x + 0 = x)$
**PA4** : $\forall x \forall y(x + s(y) = s(x + y))$
**PA5** : $\forall x(x \cdot 0 = 0)$
**PA6** : $\forall x \forall y(x \cdot s(y) = x \cdot y + x)$
**PA7** : $(A(0) \land \forall x(A(x) \to A(s(x)))) \to \forall x A(x)$,
for each formula $A(u)$ with free variable $u$.

*Continued on next page*

Theorem (Transitivity of deducibility, (Tr.)) Let $\Sigma, \Sigma' \subseteq \mathrm{Form}(\mathcal{L}^p)$. If $\Sigma \vdash \Sigma'$ and $\Sigma' \vdash A$, then $\Sigma \vdash A$.

Theorem. (Finiteness of premise set) If $\Sigma \vdash A$, then there exists a finite $\Sigma^0 \subseteq \Sigma$ such that $\Sigma^0 \vdash A$.

Theorem (Replaceability of syntactically equivalent formulas, (Repl.)) Let $B \vdash\dashv C$. For any $A$, let $A'$ be constructed from $A$ by replacing some (not necessarily all) occurrences of $B$ by $C$. Then $A \vdash\dashv A'$.

Theorem (exercise)
$A_1, A_2, \ldots, A_n \vdash A$ iff $\emptyset \vdash A_1 \wedge \ldots \wedge A_n \to A$.

Theorem (exercise)
$A_1, \ldots, A_n \vdash A$ iff $\emptyset \vdash A_1 \to (\ldots(A_n \to A)\ldots)$.

# The 11 rules of formal deduction ($\vdash$) for propositional logic

Theorem. (Church, 1936) There is no algorithm for deciding the (universal) validity or satisfiability of formulas in first-order logic.

↑ undecidable

Satisfiability of propositional logic is decidable.

| | | | |
|---|---|---|---|
| (1) | (Ref) | $A \vdash A$ | Reflexivity |
| (2) | (+) | If $\Sigma \vdash A$,<br>then $\Sigma, \Sigma' \vdash A$. | Addition of premises |
| (3) | $(\neg -)$ | If $\Sigma, \neg A \vdash B$,<br>$\Sigma, \neg A \vdash \neg B$,<br>then $\Sigma \vdash A$. | $\neg$ elimination |
| (4) | $(\to -)$ | If $\Sigma \vdash A \to B$,<br>$\Sigma \vdash A$,<br>then $\Sigma \vdash B$. | $\to$ elimination |
| (5) | $(\to +)$ | If $\Sigma, A \vdash B$,<br>then $\Sigma \vdash A \to B$. | $\to$ introduction |
| (6) | $(\wedge -)$ | If $\Sigma \vdash A \wedge B$,<br>then $\Sigma \vdash A$,<br>$\Sigma \vdash B$. | $\wedge$ elimination |
| (7) | $(\wedge +)$ | If $\Sigma \vdash A$,<br>$\Sigma \vdash B$,<br>then $\Sigma \vdash A \wedge B$. | $\wedge$ introduction |
| (8) | $(\vee -)$ | If $\Sigma, A \vdash C$,<br>$\Sigma, B \vdash C$,<br>then $\Sigma, A \vee B \vdash C$. | $\vee$ elimination |
| (9) | $(\vee +)$ | If $\Sigma \vdash A$,<br>then $\Sigma \vdash A \vee B$,<br>$\Sigma \vdash B \vee A$. | $\vee$ introduction |
| (10) | $(\leftrightarrow -)$ | If $\Sigma \vdash A \leftrightarrow B$,<br>$\Sigma \vdash A$,<br>then $\Sigma \vdash B$. | |
| | | If $\Sigma \vdash A \leftrightarrow B$,<br>$\Sigma \vdash B$,<br>then $\Sigma \vdash A$. | $\leftrightarrow$ elimination |
| (11) | $(\leftrightarrow +)$ | If $\Sigma, A \vdash B$,<br>$\Sigma, B \vdash A$,<br>then $\Sigma \vdash A \leftrightarrow B$. | $\leftrightarrow$ introduction |

$(\in)$ If $A \in \Sigma$
then $\Sigma \vdash A$.

partial / Total correctness is undecidable.

$\emptyset \vdash \neg G(y) \vee G(y)$

$\emptyset \vdash \forall y(\neg G(y) \vee G(y))$

$\emptyset \vdash \exists x \forall y(\neg G(x) \vee G(y))$

$\emptyset \vdash \exists x \forall y(\neg G(x) \to G(y))$

---

$\emptyset \vdash \exists x(\neg G(x) \to \forall y G(y))$

$M_1 \subseteq M_2 \Rightarrow$ Halt

$M_1 \not\subseteq M_2 \Rightarrow$ not halt.

- (Reflexivity of Equality) $\forall x(x = x)$
- (Symmetry of Equality) $\forall x \forall y((x = y) \to (y = x))$
- (Transitivity of Equality) $\forall x \forall y \forall z((x = y) \wedge (y = z) \to (x = z))$

(12) $(\forall -)$ **If** $\Sigma \vdash \forall x A(x)$ is a theorem
**then** $\Sigma \vdash A(t)$, where $t$ is any term, is a theorem.

(13) $(\forall +)$ If $\Sigma \vdash A(u)$ is a theorem and $u$ does not occur in $\Sigma$
**then** $\Sigma \vdash \forall x A(x)$ is a theorem.

(14) $(\exists -)$ **If** $\Sigma, A(u) \vdash B$ is a theorem,
and $u$ does not occur in $\Sigma$ or in $B$
**then** $\Sigma, \exists x A(x) \vdash B$ is a theorem.

(15) $(\exists +)$ **If** $\Sigma \vdash A(t)$ is a theorem
**then** $\Sigma \vdash \exists x A(x)$ is a theorem,
where $A(x)$ results from $A(t)$ by replacing some (not necessarily all) occurrences of $t$ by $x$.

(16) $(\approx -)$ **If** $\Sigma \vdash A(t_1)$ is a theorem
and $\Sigma \vdash t_1 \approx t_2$ is a theorem
**then** $\Sigma \vdash A(t_2)$ is a theorem,
where $A(t_2)$ results from $A(t_1)$ by replacing some (not necessarily all) occurrences of $t_1$ by $t_2$.

(17) $(\approx +)$ $\emptyset \vdash u \approx u$ is a theorem.

The additional rules of formal deduction for first-order logic are called:

- $\forall$-*elimination* for $(\forall -)$; $\forall$-*introduction* for $(\forall +)$;
- $\exists$-*elimination* for $(\exists -)$; $\exists$-*introduction* for $(\exists +)$;
- $\approx$-*elimination* for $(\approx -)$; $\approx$-*introduction* for $(\approx +)$.

Note: $\approx$ is just another notation for equality, "=".

*Continued on next page*

Lemma. If $A \vdash\dashv A'$ and $B \vdash\dashv B'$ then
(1) $\neg A \vdash\dashv \neg A'$.
(2) $A \wedge B \vdash\dashv A' \wedge B'$.
(3) $A \vee B \vdash\dashv A' \vee B'$.
(4) $A \to B \vdash\dashv A' \to B'$.
(5) $A \leftrightarrow B \vdash\dashv A' \leftrightarrow B'$.

$\neg\forall x P(x) \models\!\!\mid \exists x \neg P(x)$.

$\neg\exists x P(x) \models\!\!\mid \forall x \neg P(x)$.

Theorem (Soundness Theorem). If $\Sigma \vdash A$ then $\Sigma \models A$, where $\vdash$ means the formal deduction based on the 11 given rules.

Theorem (Completeness Theorem). If $\Sigma \models A$ then $\Sigma \vdash A$, where $\vdash$ means the formal deduction based on the 11 given rules.

Lemma. Let $A$ be a formula with atoms $p_1, p_2, \ldots, p_n$, and let $t$ be a truth valuation. Then

- if $A^t = 1$ then $p_1', p_2', \ldots, p_n' \vdash A$, and
- if $A^t = 0$ then $p_1', p_2', \ldots, p_n' \vdash \neg A$

Lemma. A set $\Sigma$ of formulas is satisfiable iff $\Sigma$ is consistent.

# Formally proved theorems of propositional logic

(proved in Logic06, or "Hints & Answers")

($\in$): If $A \in \Sigma$ then $\Sigma \vdash A$.

(Tr.): Let $\Sigma \subseteq \mathrm{Form}(\mathcal{L}^p)$, $n \geq 1$, and $A_1, \ldots, A_n$ be formulas in $\mathrm{Form}(\mathcal{L}^p)$.
If $\Sigma \vdash A_i$ for all $i = 1, \ldots n$, and $A_1, \ldots, A_n \vdash A$, then $\Sigma \vdash A$.

($\neg+$): If $\Sigma, A \vdash B$ and $\Sigma, A \vdash \neg B$, then $\Sigma \vdash \neg A$.

(Repl.): If $B \vdash\dashv C$ and $A'$ results from $A$ by replacing some (not necessarily all) occurrences of $B$ in $A$ by $C$, then $A \vdash\dashv A'$.

(Hypothetical Syllogism): $A \to B,\ B \to C \vdash A \to C$.

$\emptyset \vdash G(y) \vee \neg G(y)$

$\emptyset \vdash \exists x (\neg G(x) \vee G(y))$

$\emptyset \vdash \exists x (\neg G(x) \vee \forall y (G(y))$

(Double-negation): $\neg\neg A \vdash\dashv A$.

(Disjunctive Syllogism): $A \vee B, \neg B \vdash A$.

(Contrapositive): $A \to B \vdash\dashv \neg B \to \neg A$.

(Excluded Middle): $\emptyset \vdash A \vee \neg A$.

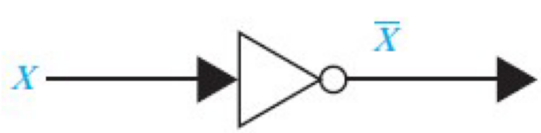
(Non-Contradiction): $\emptyset \vdash \neg(A \wedge \neg A)$.

(Inconsistency Rule): $A, \neg A \vdash B$.

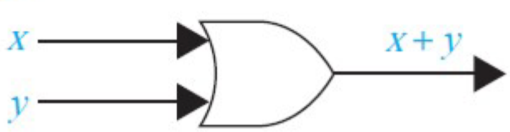
(De Morgan): $\neg(A \wedge B) \vdash\dashv (\neg A \vee \neg B)$ and $\neg(A \vee B) \vdash\dashv (\neg A \wedge \neg B)$.

(Implication Rule): $A \to B \vdash\dashv (\neg A \vee B)$.

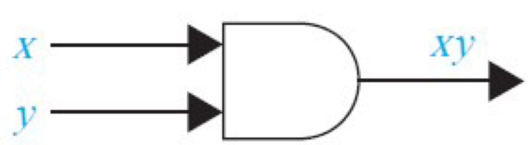
(Flip-Flop): If $A \vdash B$ then $\neg B \vdash \neg A$.




(a) Inverter




(b) OR gate




(c) AND gate

Annotated program template for `if-then-else`:

| | |
|---|---|
| $(\!\vert P\vert\!)$ | |
| if ( $B$ ) { | |
| $\quad(\!\vert P \wedge B\vert\!)$ | if-then-else |
| $\quad C_1$ | |
| $\quad(\!\vert Q\vert\!)$ | *(justify depending on $C_1$—a "subproof")* |
| } else { | |
| $\quad(\!\vert P \wedge \neg B\vert\!)$ | if-then-else |
| $\quad C_2$ | |
| $\quad(\!\vert Q\vert\!)$ | *(justify depending on $C_2$—a "subproof")* |
| } | |
| $(\!\vert Q\vert\!)$ | if-then-else [*justifies this $Q$, given the previous two $Q$*] |

Annotated program template for `if-then`:

| | |
|---|---|
| $(\!\vert P\vert\!)$ | |
| if ( $B$ ) { | |
| $\quad(\!\vert P \wedge B\vert\!)$ | if-then |
| $\quad C$ | |
| $\quad(\!\vert Q\vert\!)$ | [*add justification based on $C$*] |
| } | |
| $(\!\vert Q\vert\!)$ | if-then<br>Implied: Proof of $P \wedge \neg B \rightarrow Q$ |

## Annotations for partial-`while`

| | |
|---|---|
| $(\!\vert P\vert\!)$ | |
| $(\!\vert I\vert\!)$ | Implied (a) |
| while ( $B$ ) { | |
| $\quad(\!\vert I \wedge B\vert\!)$ | partial-`while` |
| $\quad C$ | |
| $\quad(\!\vert I\vert\!)$ | $\longleftarrow$ *to be justified, based on $C$* |
| $\quad$} | |
| $(\!\vert I \wedge \neg B\vert\!)$ | partial-`while` |
| $(\!\vert Q\vert\!)$ | Implied (b) |

(a) Prove $P \rightarrow I$ (precondition $P$ implies the loop invariant)
(b) Prove $(I \wedge \neg B) \rightarrow Q$ (exit condition implies postcondition)

We need to determine/find the loop invariant $I$!!

prenex normal form

1. $\forall x A(x) \wedge \forall x B(x) \vDash\dashv \forall x(A(x) \wedge B(x))$. ☆
2. $\exists x A(x) \vee \exists x B(x) \vDash\dashv \exists x(A(x) \vee B(x))$.
3. $\forall x \forall y A(x, y) \vDash\dashv \forall y \forall x A(x, y)$.
4. $\exists x \exists y A(x, y) \vDash\dashv \exists y \exists x A(x, y)$.
5. $Q_1 x A(x) \wedge Q_2 y B(y) \vDash\dashv Q_1 x Q_2 y(A(x) \wedge B(y))$,
   ($x$ not occurring in $B(y)$, and $y$ not occuring in $A(x)$).
6. $Q_1 x A(x) \vee Q_2 y B(y) \vDash\dashv Q_1 x Q_2 y(A(x) \vee B(y))$,
   ($x$ not occurring in $B(y)$, and $y$ not occuring in $A(x)$).

where $Q_1, Q_2 \in \{\forall, \exists\}$, and $\vDash\dashv$ can be replaced by $\vdash\dashv$.

To examplify item (5) above, if $Q_1 = \forall$ and $Q_2 = \exists$, we have
$\forall x A(x) \wedge \exists y B(y) \vDash\dashv \forall x \exists y(A(x) \wedge B(y)) \vDash\dashv$
$\exists y B(y) \wedge \forall x A(x) \vDash\dashv \exists y \forall x(B(y) \wedge A(x))$.
This only holds if $x$ does not occur in $B(y)$, $y$ does not occur in $A(x)$.