McMaster University
Department of Computing and Software
Dr. W. Kahl

COMP SCI 1FC3 — Mathematics for Computing

6 February 2012

Substitution and Equality

(1.1) **Inference rule Substitution:** $\dfrac{E}{E[x := R]}$

(1.2) **Axiom, Reflexivity of =:** $a = a$

(1.3) **Axiom, Symmetry of =:** $(a = b) \quad = \quad (b = a)$

(1.4) **Inference rule Transitivity of =:** $\dfrac{X = Y \qquad Y = Z}{X = Z}$

(1.5) **Inference rule Leibniz:** $\dfrac{X = Y}{E[z := X] = E[z := Y]}$

Equivalence

(3.1) **Axiom, Associativity of ≡:** $((p \equiv q) \equiv r) \equiv (p \equiv (q \equiv r))$

(3.2) **Axiom, Symmetry of ≡:** $p \equiv q \equiv q \equiv p$

(3.3) **Axiom, Identity of ≡:** $true \equiv q \equiv q$

(3.4) $true$

(3.5) **Reflexivity of ≡:** $p \equiv p$

(3.7) **Metatheorem:** Any two theorems are equivalent.

Negation

(3.8) **Axiom, Definition of *false*:** $false \equiv \neg true$

(3.9) **Axiom, Distributivity of ¬ over ≡:** $\neg(p \equiv q) \equiv \neg p \equiv q$

(3.10) **Axiom, Definition of ≢:** $(p \not\equiv q) \equiv \neg(p \equiv q)$

(3.11) $\neg p \equiv q \equiv p \equiv \neg q$

(3.12) **Double negation:** $\neg\neg p \equiv p$

(3.13) **Negation of *false*:** $\neg false \equiv true$

(3.14) $(p \not\equiv q) \ \equiv\ \neg p \equiv q$

(3.15) $\neg p \equiv p \equiv false$

(3.16) **Symmetry of ≢:** $(p \not\equiv q) \equiv (q \not\equiv p)$

(3.17) **Associativity of ≢:** $((p \not\equiv q) \not\equiv r) \equiv (p \not\equiv (q \not\equiv r))$

(3.18) **Mutual associativity:** $((p \not\equiv q) \equiv r) \equiv (p \not\equiv (q \equiv r))$

(3.19) **Mutual interchangeability:** $p \not\equiv q \equiv r \quad \equiv \quad p \equiv q \not\equiv r$

Disjunction

(3.24) **Axiom, Symmetry of ∨:** $p \vee q \equiv q \vee p$

(3.25) **Axiom, Associativity of ∨:** $(p \vee q) \vee r \equiv p \vee (q \vee r)$

(3.26) **Axiom, Idempotency of ∨:** $p \vee p \equiv p$

(3.27) **Axiom, Distributivity of ∨ over ≡:** $p \vee (q \equiv r) \equiv p \vee q \equiv p \vee r$

(3.28) **Axiom, Excluded Middle:** $p \vee \neg p$

(3.29) **Zero of ∨:** $p \vee true \equiv true$

(3.30) **Identity of ∨:** $p \vee false \equiv p$

(3.31) **Distributivity of ∨ over ∨:** $p \vee (q \vee r) \equiv (p \vee q) \vee (p \vee r)$

(3.32) $p \vee q \ \equiv\ p \vee \neg q \ \equiv\ p$

Conjunction

(3.35) **Axiom, Golden rule:** $p \wedge q \quad \equiv \quad p \equiv q \quad \equiv \quad p \vee q$

(3.36) **Symmetry of ∧:** $p \wedge q \quad \equiv \quad q \wedge p$

(3.37) **Associativity of ∧:** $(p \wedge q) \wedge r \quad \equiv \quad p \wedge (q \wedge r)$

(3.38) **Idempotency of ∧:** $p \wedge p \quad \equiv \quad p$

(3.39) **Identity of ∧:** $p \wedge true \quad \equiv \quad p$

(3.40) **Zero of ∧:** $p \wedge false \quad \equiv \quad false$

(3.41) **Distributivity of ∧ over ∧:** $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge (p \wedge r)$

(3.42) **Contradiction:** $p \wedge \neg p \quad \equiv \quad false$

(3.43) **Absorption:** $p \wedge (p \vee q) \quad \equiv \quad p$
$p \vee (p \wedge q) \quad \equiv \quad p$

(3.44) **Absorption:** $p \wedge (\neg p \vee q) \quad \equiv \quad p \wedge q$
$p \vee (\neg p \wedge q) \quad \equiv \quad p \vee q$

(3.45) **Distributivity of ∨ over ∧:** $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

(3.46) **Distributivity of ∧ over ∨:** $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

(3.47) **De Morgan:** $\neg(p \wedge q) \quad \equiv \quad \neg p \vee \neg q$
$\neg(p \vee q) \quad \equiv \quad \neg p \wedge \neg q$

(3.48) $p \wedge q \quad \equiv \quad p \wedge \neg q \quad \equiv \quad \neg p$

(3.49) $p \wedge (q \equiv r) \quad \equiv \quad p \wedge q \quad \equiv \quad p \wedge r \quad \equiv \quad p$

(3.50) $p \wedge (q \equiv p) \quad \equiv \quad p \wedge q$

(3.51) **Replacement:** $(p \equiv q) \wedge (r \equiv p) \quad \equiv \quad (p \equiv q) \wedge (r \equiv q)$

(3.52) **Definition of ≡:** $p \equiv q \quad \equiv \quad (p \wedge q) \vee (\neg p \wedge \neg q)$

(3.53) **Definition of ≢ (Exclusive or):** $p \not\equiv q \quad \equiv \quad (\neg p \wedge q) \vee (p \wedge \neg q)$

Implication

(3.57) **Axiom, Definition of Implication:** $p \Rightarrow q \quad \equiv \quad p \vee q \quad \equiv \quad q$

(3.58) **Axiom, Consequence:** $p \Leftarrow q \quad \equiv \quad q \Rightarrow p$

(3.59) **(Alternative) Definition of Implication:** $p \Rightarrow q \ \equiv\ \neg p \vee q$

(3.60) **(Dual) Definition of Implication:** $p \Rightarrow q \ \equiv\ p \wedge q \ \equiv\ p$

(3.61) **Contrapositive:** $p \Rightarrow q \quad \equiv \quad \neg q \Rightarrow \neg p$

Ex. 3.45 $p \Rightarrow q \quad \equiv \quad \neg p \vee \neg q \quad \equiv \quad \neg p$

Ex. 3.46 $p \Rightarrow q \quad \equiv \quad \neg p \wedge \neg q \quad \equiv \quad \neg q$

(3.62) $p \Rightarrow (q \equiv r) \quad \equiv \quad p \wedge q \quad \equiv \quad p \wedge r$

(3.63) **Distributivity of ⇒ over ≡:** $p \Rightarrow (q \equiv r) \quad \equiv \quad p \Rightarrow q \quad \equiv \quad p \Rightarrow r$

(3.64) **Self-distributivity of ⇒:** $p \Rightarrow (q \Rightarrow r) \quad \equiv \quad (p \Rightarrow q) \Rightarrow (p \Rightarrow r)$

(3.65) **Shunting:** $p \wedge q \Rightarrow r \quad \equiv \quad p \Rightarrow (q \Rightarrow r)$

(3.66) $p \wedge (p \Rightarrow q) \quad \equiv \quad p \wedge q$

(3.67) $p \wedge (q \Rightarrow p) \quad \equiv \quad p$

(3.68) $p \vee (p \Rightarrow q) \quad \equiv \quad true$

(3.69) $p \vee (q \Rightarrow p) \quad \equiv \quad q \Rightarrow p$

(3.70) $p \vee q \Rightarrow p \wedge q \quad \equiv \quad p \equiv q$

(3.71) **Reflexivity of ⇒:** $p \Rightarrow p \quad \equiv \quad true$

(3.72) **Right zero of $\Rightarrow$:** $p \Rightarrow true \quad \equiv \quad true$

(3.73) **Left identity of $\Rightarrow$:** $true \Rightarrow p \quad \equiv \quad p$

(3.74) $p \Rightarrow false \quad \equiv \quad \neg p$

(3.75) $false \Rightarrow p \quad \equiv \quad true$

(3.76a) **Weakening**/strengthening: $p \Rightarrow p \vee q$

(3.76b) **Weakening**/strengthening: $p \wedge q \Rightarrow p$

(3.76c) **Weakening**/strengthening: $p \wedge q \Rightarrow p \vee q$

(3.76d) **Weakening**/strengthening: $p \vee (q \wedge r) \Rightarrow p \vee q$

(3.76e) **Weakening**/strengthening: $p \wedge q \Rightarrow p \wedge (q \vee r)$

(3.77) **Modus ponens:** $p \wedge (p \Rightarrow q) \Rightarrow q$

(3.78) **Case analysis:** $(p \Rightarrow r) \wedge (q \Rightarrow r) \;\equiv\; (p \vee q \Rightarrow r)$

(3.79) **Case analysis:** $(p \Rightarrow r) \wedge (\neg p \Rightarrow r) \;\equiv\; r$

(3.80) **Mutual implication:** $(p \Rightarrow q) \wedge (q \Rightarrow p) \;\equiv\; p \equiv q$

(3.80b) **Reflexivity wrt. Equivalence:** $(p \equiv q) \Rightarrow (p \Rightarrow q)$ — (not in the textbook)

(3.81) **Antisymmetry:** $(p \Rightarrow q) \wedge (q \Rightarrow p) \;\Rightarrow\; (p \equiv q)$

(3.82a) **Transitivity:** $(p \Rightarrow q) \wedge (q \Rightarrow r) \;\Rightarrow\; (p \Rightarrow r)$

(3.82b) **Transitivity:** $(p \equiv q) \wedge (q \Rightarrow r) \;\Rightarrow\; (p \Rightarrow r)$

(3.82c) **Transitivity:** $(p \Rightarrow q) \wedge (q \equiv r) \;\Rightarrow\; (p \Rightarrow r)$

(4.1) $p \Rightarrow (q \Rightarrow p)$

(4.2) **Monotonicity of $\vee$:** $(p \Rightarrow q) \;\Rightarrow\; (p \vee r \Rightarrow q \vee r)$

(4.3) **Monotonicity of $\wedge$:** $(p \Rightarrow q) \;\Rightarrow\; p \wedge r \;\Rightarrow\; q \wedge r$

(4.4) **(Extended) Deduction Theorem:** Suppose adding $P_1, \ldots, P_n$ as axioms to propositional logic **E**, with the variables of the P_i considered to be constants, allows Q to be proved.
Then $P_1 \wedge \ldots \wedge P_n \Rightarrow Q$ is a theorem.

(4.6) $(p \vee q \vee r) \wedge (p \Rightarrow s) \wedge (q \Rightarrow s) \wedge (r \Rightarrow s) \;\Rightarrow\; s$

Integers

(15.1) **Axiom, Associativity:** $(a+b)+c = a+(b+c)$
$(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(15.2) **Axiom, Symmetry:** $a+b = b+a$
$a \cdot b = b \cdot a$

(15.3) **Axiom, Additive identity:** $0+a = a$
$a+0 = a$

(15.4) **Axiom, Multiplicative identity:** $1 \cdot a = a$
$a \cdot 1 = a$

(15.5) **Axiom, Distributivity:** $a \cdot (b+c) = a \cdot b + a \cdot c$
$(b+c) \cdot a = b \cdot a + c \cdot a$

(15.7) **Cancellation of $\cdot$:** $c \neq 0 \Rightarrow (c \cdot a = c \cdot b \;\equiv\; a = b)$
$c \neq 0 \Rightarrow (a \cdot c = b \cdot c \;\equiv\; a = b)$

(15.8) **Cancellation of $+$:** $a+b = a+c \quad \equiv \quad b = c$

(15.13) **Axiom, Unary minus:** $a + (-a) = 0$

(15.14) **Axiom, Subtraction:** $a - b = a + (-b)$

(15.9) **Zero of Multiplication:** $a \cdot 0 = 0$

(15.10a) $a + z = a \quad \equiv \quad z = 0$

(15.10b) $a \neq 0 \quad \Rightarrow \quad (a \cdot z = a \quad \equiv \quad z = 1)$

(15.12) $x + a = 0 \wedge y + a = 0 \quad \Rightarrow \quad x = y$

(15.15) $x + a = 0 \quad \equiv \quad x = -a$

(15.16) $-a = -b \quad \equiv \quad a = b$

(15.17) $-(-a) = a$

(15.18) $-0 = 0$

(15.19) $-(a+b) = -a + -b$

(15.20) $-a = -1 \cdot a$

(15.21) $(-a) \cdot b = a \cdot (-b)$

(15.22) $a \cdot (-b) = -(a \cdot b)$

(15.23) $(-a) \cdot (-b) = a \cdot b$

(15.24) $a - 0 = a$

(15.25) $(a-b) + (c-d) = (a+c) - (b+d)$

(15.25a) **Mutual associativity of $+$ and $-$:** $a + (b-c) = (a+b) - c$

(15.25b) $a - (b+c) = (a-b) - c$

(15.26) $(a-b) - (c-d) = (a+d) - (b+c)$

(15.27) $(a-b) \cdot (c-d) = (a \cdot c + b \cdot d) - (a \cdot d + b \cdot c)$

(15.28) $a - b = c - d \quad \equiv \quad a + d = b + c$

(15.29) $(a-b) \cdot c = a \cdot c - b \cdot c$

(15.30) **Axiom, Addition in pos:** $\mathsf{pos}.a \wedge \mathsf{pos}.b \;\Rightarrow\; \mathsf{pos}(a+b)$

(15.31) **Axiom, Multiplication in pos:** $\mathsf{pos}.a \wedge \mathsf{pos}.b \;\Rightarrow\; \mathsf{pos}(a \cdot b)$

(15.32) **Axiom:** $\neg \mathsf{pos}.0$

(15.33) **Axiom:** $b \neq 0 \quad \Rightarrow \quad (\mathsf{pos}.b \;\equiv\; \neg \mathsf{pos}(-b))$

(15.34) $b \neq 0 \quad \Rightarrow \quad \mathsf{pos}(b \cdot b)$

(15.35) $\mathsf{pos}.a \quad \Rightarrow \quad (\mathsf{pos}.b \quad \equiv \quad \mathsf{pos}(a \cdot b))$

(15.36) **Axiom, Less:** $a < b \quad \equiv \quad \mathsf{pos}(b-a)$

(15.37) **Axiom, Greater:** $a > b \quad \equiv \quad \mathsf{pos}(a-b)$

(15.38) **Axiom, At most:** $a \leq b \quad \equiv \quad a < b \;\vee\; a = b$

(15.39) **Axiom, At least:** $a \geq b \quad \equiv \quad a > b \;\vee\; a = b$

(15.40) **Positive elements:** $\mathsf{pos}.b \quad \equiv \quad 0 < b$

(15.41) **Transitivity:**
$(a) \quad a < b \;\wedge\; b < c \;\Rightarrow\; a < c$
$(b) \quad a \leq b \;\wedge\; b < c \;\Rightarrow\; a < c$
$(c) \quad a < b \;\wedge\; b \leq c \;\Rightarrow\; a < c$
$(d) \quad a \leq b \;\wedge\; b \leq c \;\Rightarrow\; a \leq c$

(15.42) **Monotonicity of $+$:** $a < b \;\equiv\; a + d < b + d$

(15.43) **Monotonicity of $\cdot$:** $0 < d \Rightarrow (a < b \;\equiv\; a \cdot d < b \cdot d)$

(15.44) **Trichotomy:** $(a < b \quad \equiv \quad a = b \quad \equiv \quad a > b) \wedge$
$\neg(a < b \quad \wedge \quad a = b \quad \wedge \quad a > b)$

(15.45) **Antisymmetry of $\leq$:** $a \leq b \quad \wedge \quad a \geq b \quad \equiv \quad a = b$

(15.46) **Reflexivity of $\leq$:** $a \leq a$

(15.47) $a = b \quad \equiv \quad (\forall z \;\bullet\; z \leq a \quad \equiv \quad z \leq b)$