TABLE I. Rewrite rules.

Class	Rewrite Rule	Instruction
Logical Operations	(And ?a (Or ?a ?b)) → ?a	$A \wedge (A \vee B) = A$
	(And ?b (Or ?a ?b)) → ?b	$B \wedge (A \vee B) = B$
	(Or ?a (And ?a ?b)) → ?a	$A \vee (A \wedge B) = A$
	(Or ?b (And ?a ?b)) → ?b	$B \vee (A \wedge B) = B$
	(Or ?a ?a) → ?a	$A \vee A = A$
	(And ?a ?a) → ?a	$A \wedge A = A$
	(Not (Not ?a)) → ?a	$\neg(\neg A) = A$
	(Or ?a ?b) → (Or ?b ?a)	$A \vee B = B \vee A$
	(And ?a ?b) → (And ?b ?a)	$A \wedge B = B \wedge A$
	(Or ?a (Not ?a)) → true	$A \vee \neg A = true$
	(Or ?a true) → true	$A \vee true = true$
	(Or ?a false) → ?a	$A \vee false = A$
	(And ?a true) → ?a	$A \wedge true = A$
	(And ?a false) → false	$A \wedge false = false$
	(And (Not ?a) ?a) → false	$\neg A \wedge A = false$
Arithmetic Operations	(Add ?a ?b) → (Add ?b ?a)	$A + B = B + A$
	(Add ?a (Add ?b ?c)) → (Add (Add ?a ?c) ?b)	$A + (B + C) = (A + C) + B$
	(Mul ?a ?b) → (Mul ?b ?a)	$A \times B = B \times A$
	(Mul ?a (Mul ?b ?c)) → (Mul (Mul ?a ?b) ?c)	$A \times (B \times C) = (A \times B) \times C$
	(Add (Mul ?a ?b) (Mul ?a ?c)) → (Mul ?a (Add ?b ?c))	$A \times B + A \times C = A \times (B + C)$
	(Add (Mul ?a ?c) (Mul ?b ?c)) → (Mul ?c (Add ?a ?b))	$A \times C + B \times C = C \times (A + B)$
	(Add ?a (Sub (Atom (Int 0)) ?b)) → (Sub ?a ?b)	$A + (0 - B) = A - B$
	(Div (Div ?a ?b) ?c) → (Div (Div ?a ?c) ?b)	$(A \div B) \div C = (A \div C) \div B$
	(Div ?a ?b) → (Mul ?a (Div (Atom (Int 1)) ?b))	$A \div B = A \times (1 \div B)$
	(Div ?a (Mul ?b ?c)) → (Div (Div ?a ?b) ?c)	$A \div (B \times C) = (A \div B) \div C$
	(Mod (Add ?a ?b) ?c) → (Mod (Add (Mod ?a ?c) (Mod ?b ?c)) ?c)	$(A + B) \mod C = ((A \mod C) + (B \mod C)) \mod C$
	(Mod (Sub ?a ?b) ?c) → (Mod (Sub (Mod ?a ?c) (Mod ?b ?c)) ?c)	$(A - B) \mod C = ((A \mod C) - (B \mod C)) \mod C$
	(Mod (Mul ?a ?b) ?c) → (Mod (Mul (Mod ?a ?c) (Mod ?b ?c)) ?c)	$(A \times B) \mod C = ((A \mod C) \times (B \mod C)) \mod C$
	(Mod (Power ?a ?b) ?c) → (Mod (Power (Mod ?a ?c) (Mod ?b ?c)) ?c)	$(A^B) \mod C = ((A \mod C)^{B \mod C}) \mod C$
	(Mod (Add (Mod (Add ?a ?b) ?c) ?d) ?c) → (Mod (Add ?a (Mod (Add ?b ?d) ?c) ?c))	$(((A + B) \mod C) + D) \mod C = (A + ((B + D) \mod C)) \mod C$
	(Mod (Mul (Mod (Mul ?a ?b) ?c) ?d) ?c) → (Mod (Mul ?a (Mod (Mul ?b ?d) ?c) ?c))	$(((A \times B) \mod C) \times D) \mod C = (A \times ((B \times D) \mod C)) \mod C$
	(Mod (Mul (Mod (Add ?a ?b) ?c) ?d) ?c) → (Mod (Add (Mod (Mul ?a ?d) ?c) (Mod (Mul ?b ?d) ?c) ?c))	$((A + B) \mod C \times D) \mod C = ((A \times D \mod C) + (B \times D \mod C)) \mod C$
	(Add ?a ?a) → (Mul ?a (Atom (Int 2)))	$A + A = A \times 2$
	(Mul ?a ?a) → (Power ?a (Atom (Int 2)))	$A \times A = A^2$
	(Add ?a (Atom (Int 0))) → ?a	$A + 0 = A$
	(Sub ?a (Atom (Int 0))) → ?a	$A - 0 = A$
	(Sub (Atom (Int 0)) ?a) → (Subone ?a)	$0 - A = -A$
	(Mul ?a (Atom (Int 0))) → (Atom (Int 0))	$A \times 0 = 0$
	(Mul ?a (Atom (Int 1))) → ?a	$A \times 1 = A$
	(Div (Atom (Int 0)) ?a) → (Atom (Int 0))	$0 \div A = 0$
	(Div ?a (Atom (Int 1))) → ?a	$A \div 1 = A$
	(Mod ?a (Atom (Int 1))) → (Atom (Int 0))	$A \mod 1 = 0$
	(Power ?a (Atom (Int 0))) → (Atom (Int 1))	$A^0 = 1$
	(Power ?a (Atom (Int 1))) → ?a	$A^1 = A$
Bitwise Operations	(BitAnd ?a (BitOr ?a ?b)) → ?a	$A \& (A \mid B) = A$
	(BitAnd ?b (BitOr ?a ?b)) → ?b	$B \& (A \mid B) = B$
	(BitOr ?a (BitAnd ?a ?b)) → ?a	$A \mid (A \& B) = A$
	(BitOr ?b (BitAnd ?a ?b)) → ?b	$B \mid (A \& B) = B$
	(BitOr ?a ?a) → ?a	$A \mid A = A$
	(BitAnd ?a ?a) → ?a	$A \& A = A$
	(BitOr ?a ?b) → (BitOr ?b ?a)	$A \mid B = B \mid A$
	(BitAnd ?a ?b) → (BitAnd ?b ?a)	$A \& B = B \& A$
	(BitXor ?a ?b) → (BitXor ?b ?a)	$A \oplus B = B \oplus A$
Associative/ Distributive	(BitOr (BitOr ?a ?b) ?c) → (BitOr ?a (BitOr ?b ?c))	$(A \mid B) \mid C = A \mid (B \mid C)$
	(BitAnd (BitAnd ?a ?b) ?c) → (BitAnd ?a (BitAnd ?b ?c))	$(A \& B) \& C = A \& (B \& C)$
	(BitAnd ?a (BitOr ?b ?c)) → (BitOr (BitAnd ?a ?b) (BitAnd ?a ?c))	$A \& (B \mid C) = (A \& B) \mid (A \& C)$
	(BitOr ?a (BitAnd ?b ?c)) → (BitAnd (BitOr ?a ?b) (BitOr ?a ?c))	$A \mid (B \& C) = (A \mid B) \& (A \mid C)$
Shift Operations	(Mul (Power (Atom (Int 2)) ?b) ?a) → (ShiftLeft ?a ?b)	$2^B * A = A \ll B$
	(ShiftLeft ?a (Add ?b ?c)) → (ShiftLeft (ShiftLeft ?a ?b) ?c)	$A \ll (B + C) = (A \ll B) \ll C$
	(Mul ?a 2) → (shiftLeft ?a (Atom (Int 1)))	$A * 2 = A \ll 1$
	(ShiftLeft (Mul ?a ?b) ?c) → (Mul (ShiftLeft ?a ?c) ?b)	$(A \times B) \ll C = (A \ll C) \times B$
	(AshiftLeft (Mul ?a ?b) ?c) → (Mul (AshiftLeft ?a ?c) ?b)	$(A \times B) \lll C = (A \lll C) \times B$
	(Mul (Power (Atom (Int 2)) ?b) ?a) → (AshiftLeft ?a ?b)	$A \times 2^B = A \lll B$
	(AshiftLeft ?a (Add ?b ?c)) → (AshiftLeft (AshiftLeft ?a ?b) ?c)	$A \lll (B + C) = (A \lll B) \lll C$
	(Mul ?a (Atom (Int 2))) → (AshiftLeft ?a (Atom (Int 1)))	$A \times 2 = A \lll 1$
	(Mul (ShiftLeft ?a ?c) ?b) → (ShiftLeft (Mul ?a ?b) ?c)	$(A \ll C) \times B = (A \times B) \ll C$
	(Mul (AshiftLeft ?a ?c) ?b) → (AshiftLeft (Mul ?a ?b) ?c)	$(A \lll C) \times B = (A \times B) \lll C$
	(Div ?a (Power 2 ?b)) → (ShiftRight ?a ?b)	$A \div 2^B = A \gg B$
	(ShiftRight (ShiftRight ?a ?b) ?c) → (ShiftRight ?a (Add ?b ?c))	$(A \gg B) \gg C = A \gg (B + C)$
	(Mul ?a (Power 2 ?b)) → (ShiftLeft ?a ?b)	$A \times 2^B = A \ll B$
	(AshiftRight ?a (Add ?b ?c)) → (AshiftRight (AshiftRight ?a ?b) ?c)	$(A \ggg B) \ggg C = A \ggg (B + C)$
	(Div ?a (Atom (Int 2))) → (ShiftRight ?a (Atom (Int 1)))	$A \div 2 = A \gg 1$
	(BitAnd (ShiftRight ?a ?b) (Atom (Int 1))) → (BitIndex ?a ?b)	$(A \gg B) \& 1 = A[B]$
	(Mul (ShiftRight ?a ?c) ?b) → (ShiftRight (Mul ?a ?b) ?c)	$(A \gg C) \times B = (A \times B) \gg C$
	(Mul (AshiftRight ?a ?c) ?b) → (AshiftRight (Mul ?a ?b) ?c)	$(A \ggg C) \times B = (A \times B) \ggg C$