A Calculational Deductive System for Linear Temporal Logic

J. STANLEY WARFORD, Pepperdine University, USA
DAVID VEGA, The Aerospace Corporation, USA
SCOTT M. STALEY, Ford Motor Company Research Labs (retired), USA

This article surveys the linear temporal logic (LTL) literature and presents all the LTL theorems from the survey, plus many new ones, in a calculational deductive system. Calculational deductive systems, developed by Dijkstra and Scholten and extended by Gries and Schneider, are based on only four inference rules—Substitution, Leibniz, Equanimity, and Transitivity. Inference rules in the older Hilbert-style systems, notably modus ponens, appear as theorems in this calculational deductive system. This article extends the calculational deductive system of Gries and Schneider to LTL, using only the same four inference rules. Although space limitations preclude giving a proof of every theorem in this article, every theorem has been proved with calculational logic.

CCS Concepts: • **Theory of computation → Modal and temporal logics**;

Additional Key Words and Phrases: Calculational logic, equational logic, linear temporal logic

ACM Reference format:
J. Stanley Warford, David Vega, and Scott M. Staley. 2020. A Calculational Deductive System for Linear Temporal Logic. *ACM Comput. Surv.* 53, 3, Article 53 (June 2020), 38 pages.
https://doi.org/10.1145/3387109

1 INTRODUCTION

Linear temporal logic (LTL) has application to proof of correctness for concurrent programs. Many concurrent programs, such as operating systems and embedded systems that control physical equipment, are nonterminating by design. Consequently, proof techniques that depend on proving the correctness of postconditions on program termination do not apply. LTL, however, can be used to prove desirable program traits such as freedom from deadlock.

Most treatments of LTL consist of cursory introductions in one or two chapters of graduate-level textbooks [2, 20, 21, 24]. While many LTL theorems are common in the different treatments, each treatment has theorems that are unique to it. This survey is a comprehensive collection of all the LTL theorems that we have found in the literature, together with many new theorems, all of which are presented in an axiomatic logic system. It serves as an introduction to LTL and should be accessible with a prerequisite only of the standard propositional and predicate logic at the undergraduate level.

The Tooma Undergraduate Research Fellowship Program, Pepperdine University, supported the second author in summer 2009 and academic year 2009–'10.
Authors' addresses: J. S. Warford, Pepperdine University, Malibu, CA, 90263; email: Stan.Warford@pepperdine.edu; D. Vega, The Aerospace Corporation, El Segundo, CA, 90245; email: davega8@gmail.com; S. M. Staley, Ford Motor Company Research Labs (retired), Dearborn, MI, 48124; email: smstaley@icloud.com.

0360-0300/2020/06-ART53
https://doi.org/10.1145/3387109

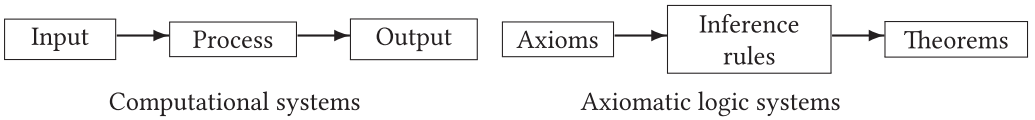

Fig. 1. Computational systems and axiomatic logic systems.

1.1 Axiomatic Logic Systems

All axiomatic logic systems have three components: inference rules, axioms, and theorems. Both inference rules and axioms are assumed. Theorems are proved from axioms using inference rules. From a computational systems perspective, the inference rules process axioms as input and produce theorems as output. Figure 1 shows the parallel between traditional computational systems and axiomatic logic systems. In the same way that a processor executes program statements with input to produce output, a proof uses inference rules with axioms to produce theorems.

In a conventional computational system, placement of the hardware/software boundary is a design decision. Any given computational task can be implemented either in hardware or in software. The tradeoff in such systems is usually between speed of execution and flexibility. Usually, a task implemented in hardware executes faster than if it is implemented in software. However, once implemented in hardware a task is more difficult to modify or extend than if it is implemented in software. One goal of RISC design is to simplify the hardware by moving tasks from hardware to software. For example, CISC machines provide complex addressing modes with hardware circuits to compute array cell addresses. The equivalent address computation is done in software in a RISC machine.

A similar design decision exists in axiomatic logic systems with the placement of the inference rule/axiom boundary. It is possible to have two different logic systems produce equivalent sets of theorems but with different sets of inference rules and axioms. What is an inference rule in one system might be a corresponding theorem or axiom in the other. The tradeoff is more subjective in logic systems, as there is apparently no metric of goodness that can be quantified as objectively as can the speed of execution in computational systems. It can be harder to prove that an inference rule is sound than it is to prove that an axiom is sound. Deductive systems often arrange for fewer inference rules to make the soundness proof easier.

This article presents a logic system that places the boundary between inference rules and axioms to minimize the number of inference rules. We maintain that the primary advantage of such a system is a human one. That is, manual proofs in such systems are easier to understand and to design than in other systems.

1.2 Propositional Logic Systems

Propositional calculus is a formal system of logic based on the unary operator negation $\neg$, the binary operators conjunction $\wedge$, disjunction $\vee$, implies $\Rightarrow$ (also written $\rightarrow$), and equivalence $\equiv$ (also written $\leftrightarrow$), variables (lowercase letters p, q, . . .), and the constants *true* and *false*. Hilbert-style logic systems, $\mathcal{H}$, are the deductive logic systems traditionally used in mathematics to describe the propositional calculus. Typical of such descriptions with applications to computer science is the text by Ben-Ari [4]. A key feature of such systems is their multiplicity of inference rules and the importance of modus ponens as one of them.

In the late 1980s, Dijkstra and Scholten [7], and Feijen [11] developed a method of proving program correctness with a new logic based on an equational style. This equational deductive system, $\mathcal{E}$, is the basis of books by Kaldewaij [19] and Cohen [5]. In contrast to $\mathcal{H}$ systems, $\mathcal{E}$ has only four inference rules: Substitution, Leibniz, Equanimity, and Transitivity. In $\mathcal{E}$, modus ponens

plays a secondary role. It is not an inference rule, nor is it assumed as an axiom, but instead is proved as a theorem from the axioms using the inference rules.

Gries and Schneider [12, 14] show that $\mathcal{E}$, also known as a *calculational* system, has several advantages over traditional logic systems. The primary advantage of $\mathcal{E}$ over $\mathcal{H}$ systems is that the calculational system has only four proof rules, with inference rule Leibniz as the primary one. Roughly speaking, Leibniz is "substituting equals for equals," hence the moniker *equational* deductive system. In contrast, $\mathcal{H}$ systems rely on a more extensive set of inference rules. We find proofs in $\mathcal{E}$ easy to understand and to teach, because the substitution of equals for equals is common in elementary algebraic manipulations.

Another major advantage of $\mathcal{E}$ over $\mathcal{H}$ systems is the sequential format of its proof syntax. Proofs in $\mathcal{H}$ systems have a bottom-up tree structure, which is sequentialized with multiple references to previously numbered lines. For example, a proof of formula f_2 might begin by establishing the validity of a formula f_1 on lines 1 through 4. Then, on lines 5 through 9, it might establish the validity of $f_1 \Rightarrow f_2$. Then, on line 10, it would refer back to lines 4 and 9 and invoke modus ponens to establish the validity of f_2.

In contrast, proofs in $\mathcal{E}$ have a top-down structure and proceed sequentially with each step self-contained. There is no need to number the lines in a proof in $\mathcal{E}$, because reference is never made to a previous intermediate step of the proof. Instead, each line depends only on the immediately preceding line by invoking a previously proved theorem or an axiom.

There is an analogy between the proof style of $\mathcal{H}$ systems versus the proof style of $\mathcal{E}$, and the unstructured goto style of programming versus structured programming. In the same way that the goto statement can produce spaghetti code that is more difficult to understand than structured code, proofs in $\mathcal{H}$ systems are more difficult to understand than proofs in $\mathcal{E}$. It is perhaps not coincidental that Dijkstra, who ignited the goto controversy with his famous CACM letter [6], was the prime developer of $\mathcal{E}$.

Proof syntax is no guarantee of clarity. In the same way that a well-written assembly language program can be easier to understand than a poorly written program in a structured high-order language, a well-written proof in $\mathcal{H}$ can be easier to understand than a poorly written proof in $\mathcal{E}$.

We agree with Gries and Schneider [13] that, "We need a style of logic that can be used as a tool in every-day work. In our experience, an equational logic, which is based on equality and Leibniz's rule for substitution of equals for equals, is best suited for this purpose." These advantages of $\mathcal{E}$ over $\mathcal{H}$ systems are primarily *human* advantages, not necessarily machine advantages. That is, the motivation behind this work is based on teaching and human understanding, as opposed to machine theorem provers or proof assistants.

In 1994, Gries and Schneider published *A Logical Approach to Discrete Math* (LADM) [13], in which they first develop $\mathcal{E}$ for propositional and predicate calculus, and then extend it to a theory of sets, a theory of sequences, relations and functions, a theory of integers, recurrence relations, modern algebra, and a theory of graphs. Using calculational logic as a tool, LADM brings all the advantages of $\mathcal{E}$ to these additional knowledge domains. The treatment is in marked contrast to the traditional one exemplified by the classic undergraduate text by Rosen [23].

1.3 Linear Temporal Logic Systems

Linear temporal logic describes how the truth values of propositions change over time. It extends the propositional operators with the unary operators *next* $\bigcirc$, *eventually* $\Diamond$, and *always* $\Box$, and the binary operators *until* $\mathcal{U}$ and *wait* $\mathcal{W}$. Most treatments of linear temporal logic use $\mathcal{H}$ systems instead of $\mathcal{E}$. Typical are Ben-Ari [3], Emerson [10], Kröger and Merz [20], and Manna and Pnueli [21]. Each of these authors describes the semantics of the above temporal operators and provides an axiomatization for linear temporal logic. One characteristic of these $\mathcal{H}$ systems is the introduction

of temporal inference rules along with temporal axioms from which temporal theorems are proved. Section 4 summarizes these systems and compares them with this work.

Our institution has used LADM at the introductory undergraduate level since its publication, and the calculational proof style has consequently permeated the computer science curriculum. A problem arises, however, when those who are schooled in $\mathcal{E}$ study concurrency and need the correctness proof tools of linear temporal logic. Schneider [24] appears to be the only treatment of linear temporal logic that uses $\mathcal{E}$. Although this graduate-level text presents a calculational deductive system, the only appearance of a calculational proof of a temporal logic theorem is a single example. Likewise, Baier and Katoen [2] have a single calculational proof of a linear temporal logic theorem in their chapter on linear temporal logic.

To solve the problem of teaching linear temporal logic at the undergraduate level, this article presents a comprehensive linear temporal logic system suitable for those versed in the calculational deductive system of LADM. In the same way that LADM brings the advantages of $\mathcal{E}$ to set theory and other mathematical domains, this article brings the advantages of $\mathcal{E}$ to linear temporal logic.

This axiomatization follows the spirit of $\mathcal{E}$ in its design to minimize the number of inference rules. A unique characteristic of this system is the absence of temporal inference rules. It extends the propositional calculus of LADM using only the same four inference rules of $\mathcal{E}$ along with additional temporal axioms. In our judgment, the absence of temporal inference rules brings the same clarity to linear temporal logic that $\mathcal{E}$ brings to the propositional calculus.

The article also adds to the linear temporal logic literature by proving many previously unpublished theorems. It is comprehensive, as we have tried to include all known linear temporal theorems described in the literature. Although space limitations preclude giving a proof of every theorem in this article, we have proved every theorem with $\mathcal{E}$.

Section 2 describes the deductive axioms and the proof rules for $\mathcal{E}$. It also defines the syntax and semantics of linear temporal logic. Section 3 presents the calculational deductive system for linear temporal logic. Section 4 summarizes previous linear temporal logic axiomatization systems and compares them with the current work.

2 BACKGROUND

The first section below summarizes the calculational system $\mathcal{E}$ from LADM [13]. The summary is minimal and assumes the reader is familiar with the propositional and predicate calculus. The second section introduces temporal logic and assumes no prior familiarity with it. The article can serve as an introduction to linear temporal logic.

2.1 Calculational Deductive Systems

2.1.1 Propositional and Temporal Operators. Expressions are the basis of propositional calculus in the calculational system. Propositional theorems are simply Boolean expressions that are true in all states. The definition of an expression has four parts:

- A constant or variable is an expression.
- If E is an expression, then (E) is an expression.
- If $\triangleright$ is a unary prefix operator and E is an expression, then $\triangleright E$ is an expression with operand E.
- If $\star$ is a binary infix operator and D and E are expressions, then $D \star E$ is an expression with operands D and E.

By convention, upper-case letters (e.g., X, Y, ...) represent expressions and lower-case letters (e.g., x, y, ...) represent variables. In the propositional calculus, the constants are *true* and *false*.

$[x := e]$ (textual substitution)	Highest precedence
$\neg \quad \circ \quad \Diamond \quad \Box$	
$\mathcal{U} \quad \mathcal{W}$	
$=$ (conjunctional)	
$\vee \quad \wedge$	
$\Rightarrow \quad \Leftarrow$	
$\equiv$ (associative)	Lowest precedence

Fig. 2. Precedence of the propositional and temporal logic operators.

Figure 2 is the table of precedences. Textual substitution has the highest precedence. All the unary operators have the next highest precedence. They are necessarily right associative. For example, $\neg \circ \neg p$ means $\neg(\circ(\neg p))$. In this system, two binary operators that have the same precedence require parentheses to disambiguate. As in LADM, conjunction $\wedge$ and disjunction $\vee$ have the same precedence so that $p \wedge q \vee r$ must be disambiguated as either $(p \wedge q) \vee r$ or $p \wedge (q \vee r)$. This contrasts with many systems in which conjunction has higher precedence than disjunction.

Also consistent with the calculational system of LADM but different from most other deductive logic systems is the difference between operators equals $=$ and equivales $\equiv$. Equals applies to any mathematical type including, e.g., Boolean, natural number, and set. Equivales applies only to Boolean and is commonly denoted $\leftrightarrow$ in other systems. Another difference is that equals is conjunctive, while equivales is associative. For example, the expression $p = q = r$ has conjunctive meaning $(p = q) \wedge (q = r)$, while the expression $p \equiv q \equiv r$ can be taken as either $(p \equiv q) \equiv r$ or $p \equiv (q \equiv r)$. Associativity of equivales is the first axiom in the calculational deductive system of LADM.

2.1.2 Inference Rules. The inference rules for the calculational deductive system are Substitution, Leibniz, Equanimity, and Transitivity:

(I1) **Substitution**: $$\frac{E}{E[z := F]},$$

(I2) **Leibniz**: $$\frac{X = Y}{E[z := X] = E[z := Y]},$$

(I3) **Equanimity**: $$\frac{X, \quad X = Y}{Y},$$

(I4) **Transitivity**: $$\frac{X = Y, \quad Y = Z}{X = Z},$$

where the square bracket in $E[z := F]$ indicates textual substitution of expression F for variable z everywhere z occurs in expression E. In a typical proof, Substitution and Leibniz are explicit, while Equanimity and Transitivity are implicit.

Substitution allows the generalization of a single theorem to represent an infinite number of theorems. For example, because $p \Rightarrow \mathit{false} \equiv \neg p$ is a theorem, then, with $p := p \wedge q$, the expression $(p \wedge q) \Rightarrow \mathit{false} \equiv \neg(p \wedge q)$ is also a theorem.

Roughly speaking, Leibniz allows for the substitution of equals for equals in a proof step. The general form of a proof step is

$$\begin{array}{ll} & E[z := X] \\ = & \quad \langle X = Y \rangle \\ & E[z := Y], \end{array}$$

where the expression enclosed in angle brackets ⟨ ⟩, called the "hint," is the justification for the step.

An example of a proof step from the proof of theorem (166) in Section 3.8 is

$$\begin{array}{ll} & \Box(\Box p \wedge \Diamond q) \Rightarrow \Box\Diamond(p \wedge q) \\ = & \quad \langle (99) \text{ Distributivity of } \Box \text{ over } \wedge \rangle \\ & \Box\Box p \wedge \Box\Diamond q \Rightarrow \Box\Diamond(p \wedge q). \end{array}$$

This proof step uses the previously proved theorem (99) Distributivity of $\Box$ over $\wedge$, which is $\Box(p \wedge q) \equiv \Box p \wedge \Box q$. The justification in the hint $X = Y$ comes from inference rule Substitution, with the textual substitution of $\Box p$ for p and $\Diamond q$ for q in (99) as follows:

$$(\Box(p \wedge q) \equiv \Box p \wedge \Box q)[p, q := \Box p, \Diamond q] : \quad \Box(\Box p \wedge \Diamond q) \equiv \Box\Box p \wedge \Box\Diamond q.$$

The expressions in Leibniz for the step are

$$\begin{array}{ll} E: & z \Rightarrow \Box\Diamond(p \wedge q), \\ X: & \Box(\Box p \wedge \Diamond q), \\ Y: & \Box\Box p \wedge \Box\Diamond q. \end{array}$$

The textual substitutions are

$$\begin{array}{ll} E[z := X]: & \Box(\Box p \wedge \Diamond q) \Rightarrow \Box\Diamond(p \wedge q), \\ E[z := Y]: & \Box\Box p \wedge \Box\Diamond q \Rightarrow \Box\Diamond(p \wedge q). \end{array}$$

The proof of a theorem consists of showing the equivalence of that theorem to a previously proved theorem through a sequence of the proof steps. For example, here is a one-step proof of (3) $\circ p \equiv \neg\circ\neg p$ in Section 3.1.

Proof:

$$\begin{array}{ll} & \circ p \equiv \neg\circ\neg p \\ = & \quad \langle (3.11)\ \neg p \equiv q \equiv p \equiv \neg q \text{ with } p, q := \circ\neg p, \circ p, \\ & \quad\ \neg\circ\neg p \equiv \circ p \equiv \circ\neg p \equiv \neg\circ p \rangle \\ & \neg\circ p \equiv \circ\neg p \quad -(1) \text{ Self-dual} \quad \blacksquare \end{array}$$

In a proof hint, numeric references that contain a decimal point, such as (3.11) above, refer to a theorem in $\mathcal{E}$ from LADM. Equanimity is implicit in the proof. Because $\neg\circ p \equiv \circ\neg p$ (i.e., X) is a previous theorem, and $\neg\circ p \equiv \circ\neg p$ is equivalent to $\circ p \equiv \neg\circ\neg p$ (i.e., $X = Y$), by equanimity $\circ p \equiv \neg\circ\neg p$ (i.e., Y) is proved.

Transitivity of equality allows a derivation to be given as a sequence of equivalent expressions, which, at the end, proves the equivalence of the first expression in the sequence with the last expression in the sequence. For example, here is a two-step proof of (22) Idempotency of $\mathcal{U}$, $p\,\mathcal{U}\,p \equiv p$ in Section 3.2.

Proof:

$$\begin{array}{ll} & p\ \mathcal{U}\ p \equiv p \\ = & \quad \langle (10) \text{ Expansion of } \mathcal{U} \rangle \\ & p \vee (p \wedge \circ(p\ \mathcal{U}\ p)) \equiv p \\ = & \quad \langle (3.43b) \text{ Absorption, } p \vee (p \wedge q) \equiv p \text{ with } q := \circ(p\ \mathcal{U}\ p) \rangle \\ & p \equiv p \quad -(3.5) \text{ Reflexivity of } \equiv \quad \blacksquare \end{array}$$

Transitivity of equality is implicit in the proof. Because $p \mathcal{U} p \equiv p$ is equivalent to $p \vee (p \wedge \circ (p \mathcal{U} p)) \equiv p$ (i.e., $X = Y$), and $p \vee (p \wedge \circ (p \mathcal{U} p)) \equiv p$ is equivalent to $p \equiv p$ (i.e., $Y = Z$), by transitivity $p \mathcal{U} p \equiv p$ is equivalent to $p \equiv p$ (i.e., $X = Z$).

2.1.3 Proof Technique Metatheorems. The logic system $\mathcal{E}$ of LADM [13] has 13 axioms for the propositional calculus from which theorems are deduced with the above inference rules in the calculational style. The system also contains a number of metatheorems based on properties of equivalence and implication, which allow the proof style to be extended. Here are four of the proof technique metatheorems.

(4.4) **Deduction (assume conjuncts of antecedent):**
To prove $P_1 \wedge P_2 \Rightarrow Q$, assume P_1 and P_2, and prove Q.
You cannot use textual substitution in P_1 or P_2.

(4.7) **Mutual implication:** To prove $P \equiv Q$, prove $P \Rightarrow Q$ and $Q \Rightarrow P$.

(4.7.1) **Truth implication:** To prove P, prove $true \Rightarrow P$.

(4.12) **Contrapositive:** To prove $P \Rightarrow Q$, prove $\neg Q \Rightarrow \neg P$.

The validity of each metatheorem is established from the theorems of the propositional calculus and the inference rules. Deduction is established by showing that any deductive proof has an equivalent calculational proof. Mutual implication is based on (3.80), Truth implication is based on (3.73), and Contrapositive is based on (3.61).

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

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

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

The proof format is extended to the case where the theorem to be proved is of the form $P \equiv Q$. For theorems of this form, the proof may begin with the left-hand side and show equivalence to the right-hand side through a sequence of proof steps. This proof style is established by showing that such a proof is equivalent to a calculational proof and is based on (3.5).

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

For example, the following proof is the preferred style for the previous proof of (22):

Proof:

$$
\begin{array}{ll}
 & p \mathcal{U} p \\
= & \quad \langle (10) \text{ Expansion of } \mathcal{U} \rangle \\
 & p \vee (p \wedge \circ (p \mathcal{U} p)) \\
= & \quad \langle (3.43b) \text{ Absorption, } p \vee (p \wedge q) \equiv p \text{ with } q := \circ (p \mathcal{U} p) \rangle \\
 & p \quad \blacksquare
\end{array}
$$

Gries and Schneider also extend the proof format to incorporate implication using its transitive properties with itself and with equivales. Instead of proving a theorem of the form $P \Rightarrow Q$ to be equivalent to a previously proved theorem, P can be shown to imply Q, or Q can be shown to follow from P. The following mutual transitivity theorems justify this extension:

(3.82) **Transitivity:**
(a) $(p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$,
(b) $(p \equiv q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$,
(c) $(p \Rightarrow q) \wedge (q \equiv r) \Rightarrow (p \Rightarrow r)$.

An example is a proof of (46) $p \Rightarrow \Diamond\, p$ in Section 3.3.

Proof:

$$
\begin{array}{ll}
 & \Diamond\, p \\
= & \quad \langle (45) \text{ Expansion of } \Diamond \rangle \\
 & p \vee \circ \Diamond\, p \\
\Leftarrow & \quad \langle (3.76a) \text{ Weakening } p \Rightarrow p \vee q \text{ with } q := \circ \Diamond\, p \rangle \\
 & p \quad \blacksquare
\end{array}
$$

Because $\Diamond\, p$ equivales $p \vee \circ \Diamond\, p$, and $p \vee \circ \Diamond\, p$ follows from p, it follows by mutual transitivity that $\Diamond\, p$ follows from p.

The following two theorems from LADM provide a further extension to proof steps with implication:

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

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

They are required to justify an implication when the antecedent of the implication is a conjunct or disjunct. For example, here is a proof step where the antecedent $p\ \mathcal{U}\ q$ is a disjunct in the expression $\Box\, p \vee p\ \mathcal{U}\ q$:

$$
\begin{array}{ll}
 & \Box\, p \vee p\ \mathcal{U}\ q \\
\Rightarrow & \quad \langle (42) \text{ Eventuality and (4.2) Monotonicity of } \vee \rangle \\
 & \Box\, p \vee \Diamond\, q.
\end{array}
$$

Previously proved theorem (42) Eventuality is $p\ \mathcal{U}\ q \Rightarrow \Diamond\, q$. The application of (4.2) is with the following textual substitution:

$$
\begin{array}{ll}
 & ((p \Rightarrow q) \Rightarrow (p \vee r \Rightarrow q \vee r))[p, q, r := p\ \mathcal{U}\ q, \Diamond\, q, \Box\, p] \\
= & \quad \langle \text{Textual substitution} \rangle \\
 & (p\ \mathcal{U}\ q \Rightarrow \Diamond\, q) \Rightarrow (p\ \mathcal{U}\ q \vee \Box\, p \Rightarrow \Diamond\, q \vee \Box\, p).
\end{array}
$$

In other words, because $p\ \mathcal{U}\ q$ implies $\Diamond\, q$, $p\ \mathcal{U}\ q \vee \Box\, p$ implies $\Diamond\, q \vee \Box\, p$.

2.1.4 Predicate Calculus. The predicate calculus of the calculational system has a consistent quantification notation that applies to Abelian monoids in both mathematics and logic. Denoting a general Abelian monoid as the infix operator $\star$, the form of a quantification is

$$(\star\ \mathit{dummies} \mid \mathit{range} : \mathit{body}).$$

All quantifications have explicit scope for the dummy variable denoted by the outer parentheses. Within the parentheses the quantification consists of three parts:

- the infix operator $\star$ and dummy variable(s),
- the range, which is a Boolean expression, and
- the body, which is an expression that is type compatible with the operator $\star$.

A vertical bar separates the operator and dummy variable from the range, and a colon separates the range from the body. An abbreviation is to omit the range when it is *true*. For example, $(\forall i \mid : P)$ is an abbreviation for $(\forall i \mid \mathit{true} : P)$.

For example, the standard mathematical notation for writing the sum of the squares of the first n positive integers is

$$\sum_{i=1}^{n} i^2,$$

where $\star$ is Abelian monoid +, and Σ is the quantified symbol for addition. The calculational notation for the same expression is

$$(\Sigma i \mid 1 \leq i \leq n : i^2).$$

Similarly, the standard logic notation for writing that there exists a number between 10 and 20 inclusive that divides n is

$$\exists i(10 \leq i \leq 20 \wedge divides(i, n)),$$

where $\star$ is Abelian monoid $\vee$, $\exists$ is the quantified symbol for disjunction, and divides is a predicate that is true when i divides n. The calculational notation for the same expression is

$$(\exists i \mid 10 \leq i \leq 20 : \text{divides}(i, n)).$$

Predicate calculus in the calculational system of LADM begins with nine general axioms that apply to all Abelian monoids. For example, here are the first two axioms.

For symmetric and associative binary operator $\star$ with identity u.

(8.13) **Axiom, Empty range:** $(\star x \mid false : P) = u$,

(8.14) **Axiom, One-point rule:** Provided $\neg occurs(\text{`}x\text{'}, \text{`}E\text{'})$,
$(\star x \mid x = E : P) = P[x := E]$.

It has two axioms for universal quantification.

(9.2) **Axiom, Trading:** $(\forall x \mid R : P) \equiv (\forall x \mid : R \Rightarrow P)$,

(9.5) **Axiom, Distributivity of $\vee$ over $\forall$:** Provided $\neg occurs(\text{`}x\text{'}, \text{`}P\text{'})$,
$P \vee (\forall x \mid R : Q) \equiv (\forall x \mid R : P \vee Q)$.

And it has one axiom for existential quantification.

(9.17) **Axiom, Generalized De Morgan:** $(\exists x \mid R : P) \equiv \neg(\forall x \mid R : \neg P)$.

2.2 Linear Temporal Logic

The operators of propositional calculus, $\neg$, $=$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftarrow$, and $\equiv$ are static. That is, they apply at a single point in time. Each operator has a truth table that dictates how to evaluate the truth value of an expression. A state is an assignment of a truth value to each variable in the expression. A given Boolean expression may be false in all states, true in some states, and false in others, or true in all states, in which case the expression is known as a theorem or validity or tautology.

The operators of temporal logic, $\bigcirc$, $\Diamond$, $\Box$, $\mathcal{U}$, and $\mathcal{W}$ are dynamic. That is, they do not apply at a single point in time, but apply over an infinite sequence of states. Each state corresponds to a discrete point in time that represents one point in the execution of a program, possibly having several threads running concurrently but whose instruction executions have been serialized. As one instruction in the program is executed, the state changes, and hence the truth value of an expression may change as well.

2.2.1 Models and Anchored Sequences. A program consists of, among other things, a set of variables and constants. Using state expressions, with operations provided by the programming language, the program changes the values of the variables as it executes. When the value of a variable changes, a property associated with that variable might also change. Properties are described by state formulas (assertions). V is the set of variables that is combined with the operations of the programming language to form state expressions and with the Boolean operations of logic to describe properties.

A model σ over V is an infinite sequence of the form

$$\sigma : s_0, s_1, s_2, \ldots,$$

where s_0 is the initial state of a computation and each state $s_i, 0 \leq i$ is the state at time i [21].

For example, suppose x is an integer variable whose value varies at each step of the computation. Then, x and the property $x \geq 10$ might evolve as follows:

σ	s_0	s_1	s_2	s_3	s_4	...
x	8	9	10	11	12	...
$x \geq 10$	F	F	T	T	T	...

The bottom row shows the evaluation of the state formula for each state in the sequence.

An anchored sequence is a pair (σ, j) where j is a natural number (the anchor) that specifies a state in model σ [24]. The anchor point j partitions the states s_i of σ into the past $0 \leq i < j$, present $i = j$, and future $i > j$. The notation

$$(\sigma, j) \models p$$

means that the property p holds at position j in a sequence σ. In this example,

$$(\sigma, 3) \models x \geq 10.$$

The symbol $\models$ means "satisfies," so the above expression is read as "State 3 of sequence σ satisfies $x \geq 10$." Or, using "holds," the same expression is read as, "$x \geq 10$ holds in state 3 of sequence σ."

In the above example, evaluation of the property $x \geq 10$ in the anchored sequence (σ, j) depends only on the value of variable x at the anchor point j. In general, the truth of a temporal assertion at j may depend on future states as well. For example, an informal English assertion is, "p is now, and always will be from this point on, true." The temporal notation for this assertion is $\Box p$. If you assume that x in the above sequence keeps increasing by one, then $\Box p$ holds in state 3 of sequence σ. However, the truth of this assertion depends not only on the fact that p holds at s_3 but that p also holds at $s_4, s_5, \ldots$. A more precise formulation is that p holds at s_3 and that $\Box p$ also holds at each subsequent state. See Schneider [24] for a formal treatment, which depends on the formulation of prefix and suffix anchored sequences.

There is a distinction between the constant *true* and the truth value of an expression T in a given state. The constant *true* is an expression that evaluates to T in every state. Similarly, there is a distinction between the constant *false* and the truth value of an expression F in a given state. The constant *false* is an expression that evaluates to F in every state.

σ	s_0	s_1	s_2	s_3	s_4	...
true	T	T	T	T	T	...
false	F	F	F	F	F	...

The propositional logic system of LADM [13] describes a case analysis metatheorem as follows: If $E[z := \mathit{true}]$ and $E[z := \mathit{false}]$ are theorems, then so is $E[z := p]$. This metatheorem does *not* hold in LTL, because the two cases, $z := \mathit{true}$ and $z := \mathit{false}$, account for only two out of an infinite number of possible sequences of T's and F's in σ.

2.2.2 The Temporal Operators. This section uses the anchored sequence (σ, j) and $\models$ to formalize the interpretation of each temporal operator. See the online version for a more extensive discussion.

The *next* Operator $\circ$. The semantics of the unary prefix operator $\circ$ are

$$(\sigma, j) \models \circ p \quad \text{iff} \quad (\sigma, j+1) \models p.$$

That is, $\circ p$ holds at position j iff p holds at position $j+1$.

For example, the following sequence $\circ\, 10 \le x < 13$ holds at state s_1, because $10 \le x < 13$ holds at state s_2.

σ	s_0	s_1	s_2	s_3	s_4	s_5	s_6	…
x	8	9	10	11	12	13	14	…
$10 \le x < 13$	F	F	T	T	T	F	F	…
$\circ\, 10 \le x < 13$	F	T	T	T	F	F	F	…

In other words,

$$(\sigma, 1) \models \circ\, 10 \le x < 13 \quad \text{because} \quad (\sigma, 2) \models 10 \le x < 13.$$

Furthermore, $\circ\, 10 \le x < 13$ does not hold at state s_4 even though $10 \le x < 13$ does hold in that state, because $10 \le x < 13$ does not hold in state s_5.

This definition of $\circ$ assumes an infinite sequence of states. Emerson [10] shows variations of the *next* operator that would apply to a finite sequence of states suitable for modeling a program that terminates.

The until *Operator* $\mathcal{U}$. The semantics of the binary infix operator $\mathcal{U}$ are

$$(\sigma, j) \models p\ \mathcal{U}\ q \quad \text{iff} \quad (\exists k \mid k \ge j : (\sigma, k) \models q \wedge (\forall i \mid j \le i < k : (\sigma, i) \models p)).$$

If $p\ \mathcal{U}\ q$ holds at state s_j, then p holds at state s_j and continues to hold at every state after s_j until q holds at some future state. $p\ \mathcal{U}\ q$ guarantees that q will eventually hold at some future state and that p will continue to hold until then. After the state in which q holds for the first time, there are no restrictions on either p or q.

For example, suppose x and y evolve in the computation as follows:

σ	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	…
x	−1	0	1	2	3	4	5	6	7	8	…
y	9	8	7	6	5	4	3	2	1	0	…
$0 < x < y$	F	F	T	T	T	F	F	F	F	F	…
$2 \le y < 5$	F	F	F	F	F	T	T	T	F	F	…
$(0 < x < y)\ \mathcal{U}\ (2 \le y < 5)$	F	F	T	T	T	T	T	T	F	F	…

The bottom row shows the evaluation of the expression $p\ \mathcal{U}\ q$ where $p \equiv 0 < x < y$ and $q \equiv 2 \le y < 5$. In states s_0 and s_1, $p\ \mathcal{U}\ q$ is false, because both p and q are false. Starting at state s_2, $p\ \mathcal{U}\ q$ is true, because in that state p is true and will remain true until q eventually becomes true in state s_5.

The *until* operator $\mathcal{U}$ is not associative as shown by the following sequence:

σ	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7	...
p	F	F	T	T	T	T	F	F	...
q	F	T	F	T	F	F	F	F	...
r	F	F	F	T	T	F	T	F	...
$p \mathcal{U} q$	F	T	T	T	F	F	F	F	...
$q \mathcal{U} r$	F	F	F	T	T	F	T	F	...
$p \mathcal{U} (q \mathcal{U} r)$	F	F	T	T	T	T	T	F	...
$(p \mathcal{U} q) \mathcal{U} r$	F	T	T	T	T	F	T	F	...

State s_1 in the last two rows of the above table shows that $(p \mathcal{U} q) \mathcal{U} r$ does not imply $p \mathcal{U} (q \mathcal{U} r)$, and state s_5 shows that $p \mathcal{U} (q \mathcal{U} r)$ does not imply $(p \mathcal{U} q) \mathcal{U} r$.

The Eventually *Operator* $\Diamond$. The semantics of the unary prefix operator $\Diamond$ are

$$(\sigma, j) \models \Diamond p \quad \text{iff} \quad (\exists k \mid k \geq j : (\sigma, k) \models p).$$

So, $\Diamond p$ holds in state s_j if p holds in state s_j or in any other state s_k where $k \geq j$; that is, if p holds in the current state or in any other future state.

For example, suppose x evolves in the computation as follows:

σ	s_0	s_1	s_2	s_3	s_4	s_5	s_6	...
x	1	2	3	4	5	6	7	...
$3 \leq x < 6$	F	F	T	T	T	F	F	...
$\Diamond (3 \leq x < 6)$	T	T	T	T	T	F	F	...

The bottom row shows the evaluation of the expression $\Diamond p$ where $p \equiv 3 \leq x < 6$. In states s_0 and s_1, $\Diamond p$ is true, because there is a state, either now or in the future, in which p will hold.

If $\Diamond p$ is ever false in any state s_i in a sequence σ, then it must be false in all subsequent states s_j, $j \geq i$. If $\Diamond p$ is ever true in any state s_i in a sequence σ, then it must be true in all preceding states s_j, $j \leq i$. For example, suppose p and q evolve in the computation as follows:

σ	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	...
p	F	F	T	F	F	T	F	F	F	F	...
q	F	F	T	T	F	F	T	T	F	F	...
$\Diamond p$	T	T	T	T	T	T	F	F	F	F	...
$\Diamond q$	T	T	T	T	T	T	T	T	T	T	...

The bottom two rows show the evaluation of the expressions $\Diamond p$ and $\Diamond q$ assuming that p remains false indefinitely and q continues to switch between true and false indefinitely.

The Always *Operator* $\Box$. The semantics of the unary prefix operator $\Box$ are

$$(\sigma, j) \models \Box p \quad \text{iff} \quad (\forall k \mid k \geq j : (\sigma, k) \models p).$$

So, $\Box p$ holds in state s_j if p holds in state s_j and in all other states s_k where $k \geq j$; that is, if p holds in the current state and in all other future states.

For example, suppose x evolves in the computation as follows:

σ	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7	...
x	1	2	3	4	5	6	7	8	...
$x < 4 \vee x \geq 6$	T	T	T	F	F	T	T	T	...
$\Box\,(x < 4 \vee x \geq 6)$	F	F	F	F	F	T	T	T	...

The bottom row shows the evaluation of the expression $\Box\, p$ where $p \equiv x < 4 \vee x \geq 6$. In states s_3 and s_4, $\Box\, p$ is false, because p does not hold in those states. In states s_0, s_1, and s_2, p is true. However, $\Box\, p$ is false in those states, because p does not hold in all future states. In states s_5, s_6, s_7, and subsequent states, $\Box\, p$ is true, because p holds in in those states and in all future states as well.

If $\Box\, p$ is ever true in any state s_i in a sequence σ, then it must be true in all subsequent states s_j, $j \geq i$. If $\Box\, p$ is ever false in any state s_i in a sequence σ, then it must be false in all preceding states s_j, $j \leq i$.

For example, suppose p and q evolve in the computation as follows:

σ	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	...
p	T	T	F	T	T	F	T	T	T	T	...
q	T	T	F	F	T	T	F	F	T	T	...
$\Box\, p$	F	F	F	F	F	F	T	T	T	T	...
$\Box\, q$	F	F	F	F	F	F	F	F	F	F	...

The bottom two rows show the evaluation of the expressions $\Box\, p$ and $\Box\, q$ assuming that p remains true indefinitely and q continues to switch between true and false indefinitely.

The Wait *Operator* $\mathcal{W}$. The semantics of the binary infix operator $\mathcal{W}$ in terms of $\mathcal{U}$ and $\Box$ are

$$(\sigma, j) \models p\ \mathcal{W}\ q \quad \text{iff} \quad (\sigma, j) \models p\ \mathcal{U}\ q\ \vee\ (\sigma, j) \models \Box\, p.$$

The *wait* operator $\mathcal{W}$ is weaker than the *until* operator $\mathcal{U}$, because $p\ \mathcal{W}\ q$ does not require q to ever be true, while $p\ \mathcal{U}\ q$ does. Furthermore, theorem (174) shows that $p\ \mathcal{U}\ q \Rightarrow p\ \mathcal{W}\ q$.

For example, suppose p and q evolve in the computation as follows:

σ	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	s_{10}	...
p	F	F	T	T	F	F	F	F	T	T	T	...
q	F	F	F	F	T	T	F	F	F	F	F	...
$\Box\, p$	F	F	F	F	F	F	F	F	T	T	T	...
$p\ \mathcal{U}\ q$	F	F	T	T	T	T	F	F	F	F	F	...
$p\ \mathcal{W}\ q$	F	F	T	T	T	T	F	F	T	T	T	...

The bottom two rows show the evaluation of the expressions $p\ \mathcal{U}\ q$ and $p\ \mathcal{W}\ q$ assuming that p remains true indefinitely and q remains false indefinitely. From s_0 to s_7, $p\ \mathcal{U}\ q$ and $p\ \mathcal{W}\ q$ hold in the same states. From s_8 on, however, $p\ \mathcal{U}\ q$ does not hold, because q never holds thereafter, while $p\ \mathcal{W}\ q$ does hold, because p always holds thereafter.

2.2.3 Duality. LADM [13] defines the dual P_D of a Boolean expression P to be the expression constructed from P by interchanging occurrences of

true and *false*,
$\wedge$ and $\vee$,
$\equiv$ and $\not\equiv$,
$\Rightarrow$ and $\not\Leftarrow$, and
$\Leftarrow$ and $\not\Rightarrow$.

This definition of P_D gives rise to the following metatheorem from LADM:

(2.3) **Metatheorem Duality**
(a) P is valid iff $\neg P_D$ is valid,
(b) $P \equiv Q$ is valid iff $P_D \equiv Q_D$ is valid.

Linear temporal logic extends the definition of P_D for the temporal operators to include interchanging occurrences of

$\circ$ and $\circ$ (self dual), and
$\Box$ and $\Diamond$.

It is not the case that $\mathcal{W}$ is the dual of $\mathcal{U}$. Ben-Ari [4] defines the *release* operator $\mathcal{R}$ as

$$p \,\mathcal{R}\, q \;\equiv\; \neg(\neg p \,\mathcal{U}\, \neg q)$$

to be the dual of the binary operator $\mathcal{U}$. For simplicity, we avoid adding another operator to our system by restricting the LTL binary operators to the more common $\mathcal{U}$ and $\mathcal{W}$.

3 THE CALCULATIONAL TEMPORAL SYSTEM

This section presents an axiomatic deductive system of temporal logic and proves its theorems with the calculational logic $\mathcal{E}$ of Gries and Schneider's *A Logical Approach to Discrete Math* (LADM) [13]. Theorems cited in a proof hint take two forms. A numbered reference enclosed in parentheses *without* a period is a reference to an axiom or a previously proved theorem in this article. A numbered reference enclosed in parentheses *with* a period is a reference to an axiom or a theorem from the propositional calculus in LADM. The numbering is consistent with that text with the chapter number followed by the equation number separated by the period. Additional theorems, either not included in LADM or included but not numbered, are indicated by a three-part number with two period separators. The terms "definition" and "axiom" are synonymous.

The propositional calculus theorems from LADM are included in the Appendix section. The following exposition includes the theorems from LADM in the proof hints, except that theorems are omitted for (4.2) and (4.3) Monotonicity, as they are described in Section 2.1.

3.1 Next

The following two axioms define the *next* operator $\circ$.

(1) **Axiom, Self-dual:** $\circ \neg p \equiv \neg \circ p$,

(2) **Axiom, Distributivity of $\circ$ over $\Rightarrow$:** $\circ (p \Rightarrow q) \equiv \circ p \Rightarrow \circ q$.

Self duality states that p not holding in the next state is equivalent to *next* p not holding in the current state. Distributivity states that p implies q in the next state is equivalent to *next* p implies *next* q in the current state. From this axiom, subsequent theorems prove that the *next* operator distributes over all the propositional binary operators.

Linearity follows from self-dual.

(3) **Linearity:** $\circ p \equiv \neg \circ \neg p$

Proof:

$$
\begin{array}{ll}
 & \circ p \equiv \neg \circ \neg p \\
= & \quad \langle (3.11)\ \neg p \equiv q \equiv p \equiv \neg q \text{ with } p, q := \circ \neg p, \circ p \rangle \\
 & \neg \circ p \equiv \circ \neg p \quad -(1) \text{ Self-dual } \blacksquare
\end{array}
$$

The proof that $\circ$ distributes over $\vee$ uses the distributivity of $\circ$ over $\Rightarrow$. The proofs that it also distributes over $\wedge$ and $\equiv$ are similar.

(4) **Distributivity of $\circ$ over $\vee$:** $\circ (p \vee q) \equiv \circ p \vee \circ q$,

Proof: See online version

(5) **Distributivity of $\circ$ over $\wedge$:** $\circ (p \wedge q) \equiv \circ p \wedge \circ q$,

(6) **Distributivity of $\circ$ over $\equiv$:** $\circ (p \equiv q) \equiv \circ p \equiv \circ q$.

Now, *true* holds in the next state, and *false* does not hold in the next state. In the calculational logic of LADM, *true* is Theorem (3.4) and is equivalent to all other theorems. Theorem (7) shows that all propositional logic theorems hold at the next state and, by induction, hold in all states. The proof of (7) uses (3.28) Excluded middle. The proof of (8) uses (3.8) Definition of *false*, $false \equiv \neg true$.

(7) **Truth of $\circ$:** $\circ true \equiv true$,

Proof: See online version

(8) **Falsehood of $\circ$:** $\circ false \equiv false$.

3.2 Until

This system defines the *until* operator $\mathcal{U}$ with the following 10 axioms: The first axiom, distributivity of $\circ$ over $\mathcal{U}$, implies the distributivity of $\circ$ over $\mathcal{W}$ as Section 3.9 shows. Thus, the *next* operator distributes over all binary operators, both propositional and temporal.

(9) **Axiom, Distributivity of $\circ$ over $\mathcal{U}$:** $\circ (p \ \mathcal{U} \ q) \equiv \circ p \ \mathcal{U} \circ q$

The second axiom, expansion of $\mathcal{U}$, makes the *until* operator different from most propositional binary operators. Its right operand has an existential characteristic and its left operand has a universal characteristic. Expansion states that $p \ \mathcal{U} \ q$ is true iff q is true in the current state or p is true in the current state and $p \ \mathcal{U} \ q$ is true in the next state. Thus, q relates to the definition through disjunction, which is existential, while p relates through conjunction, which is universal. Consequently, the *until* operator is neither symmetric (i.e., commutative) nor associative.

(10) **Axiom, Expansion of $\mathcal{U}$:** $p \ \mathcal{U} \ q \equiv q \vee (p \wedge \circ (p \ \mathcal{U} \ q))$

The third axiom states that *false* is the right zero of $\mathcal{U}$ and is not noted in other LTL deductive systems.

(11) **Axiom, Right zero of $\mathcal{U}$:** $p \ \mathcal{U} \ false \equiv false$

The next four axioms describe how the *until* operator distributes over conjunction and disjunction. Because $\mathcal{U}$ is not symmetric, this system requires separate axioms for left and right distributivity.

(12) **Axiom, Left distributivity of $\mathcal{U}$ over $\vee$:** $p\ \mathcal{U}\ (q \vee r) \equiv p\ \mathcal{U}\ q \vee p\ \mathcal{U}\ r$,

(13) **Axiom, Right distributivity of $\mathcal{U}$ over $\vee$:** $p\ \mathcal{U}\ r \vee q\ \mathcal{U}\ r \Rightarrow (p \vee q)\ \mathcal{U}\ r$,

(14) **Axiom, Left distributivity of $\mathcal{U}$ over $\wedge$:** $p\ \mathcal{U}\ (q \wedge r) \Rightarrow p\ \mathcal{U}\ q \wedge p\ \mathcal{U}\ r$,

(15) **Axiom, Right distributivity of $\mathcal{U}$ over $\wedge$:** $(p \wedge q)\ \mathcal{U}\ r \equiv p\ \mathcal{U}\ r \wedge q\ \mathcal{U}\ r$.

The *until* operator is not associative. The last three axioms describe the ordering property, the right ordering property under disjunction, and the right ordering property under conjunction, of $\mathcal{U}$. These theorems do not appear in other LTL systems. Other systems do, however, list their $\mathcal{W}$ versions, which in this system are (253), (249), and (250).

(16) **Axiom, $\mathcal{U}$ implication ordering:** $p\ \mathcal{U}\ q \wedge \neg q\ \mathcal{U}\ r \Rightarrow p\ \mathcal{U}\ r$,

(17) **Axiom, Right $\mathcal{U}$ $\vee$ ordering:** $p\ \mathcal{U}\ (q\ \mathcal{U}\ r) \Rightarrow (p \vee q)\ \mathcal{U}\ r$,

(18) **Axiom, Right $\wedge$ $\mathcal{U}$ ordering:** $p\ \mathcal{U}\ (q \wedge r) \Rightarrow (p\ \mathcal{U}\ q)\ \mathcal{U}\ r$.

Theorem (19) shows how $\mathcal{U}$ distributes over $\Rightarrow$ and is not listed in other deductive systems.

(19) **Right distributivity of $\mathcal{U}$ over $\Rightarrow$:** $(p \Rightarrow q)\ \mathcal{U}\ r \Rightarrow (p\ \mathcal{U}\ r \Rightarrow q\ \mathcal{U}\ r)$.

Proof: See online version

Theorem (20) shows that *true* is a right zero of $\mathcal{U}$, which is unusual, because axiom (11) shows that *false* is also a right zero of $\mathcal{U}$. Theorem (21) shows that *false* is the left identity of $\mathcal{U}$. Proofs of both use (10) Expansion of $\mathcal{U}$. Theorems (11), (20), and (21) cover three of the possibilities of constants *true* and *false* on either side of $\mathcal{U}$. None of these three theorems seem to appear in the temporal logic literature. The fourth possibility with *true* as the left argument is the basis of the definition of the *eventually* operator $\Diamond$ in Section 3.3.

(20) **Right zero of $\mathcal{U}$:** $p\ \mathcal{U}\ \mathit{true} \equiv \mathit{true}$,

(21) **Left identity of $\mathcal{U}$:** $\mathit{false}\ \mathcal{U}\ q \equiv q$.

Theorem (22) shows that the *until* operator is idempotent. Its proof uses (10) Expansion of $\mathcal{U}$ followed by (3.43b) Absorption. Theorem (23) is the *until* version of excluded middle, which is proved from (12) Left distributivity of $\mathcal{U}$ over $\vee$. The proof of (24) is based on (17) Right $\mathcal{U}$ $\vee$ ordering with $p := \neg p$. The proof of (25) is similar. The proofs of (26) and (27) use (16) $\mathcal{U}$ implication ordering. The proofs of (28), (29), and (30) require only two steps.

(22) **Idempotency of $\mathcal{U}$:** $p\ \mathcal{U}\ p \equiv p$,

(23) **$\mathcal{U}$ excluded middle:** $p\ \mathcal{U}\ q \vee p\ \mathcal{U}\ \neg q$,

(24) $\neg p\ \mathcal{U}\ (q\ \mathcal{U}\ r) \wedge p\ \mathcal{U}\ r \Rightarrow q\ \mathcal{U}\ r$,

(25) $p\ \mathcal{U}\ (\neg q\ \mathcal{U}\ r) \wedge q\ \mathcal{U}\ r \Rightarrow p\ \mathcal{U}\ r$,

(26) $p\ \mathcal{U}\ q \wedge \neg q\ \mathcal{U}\ p \Rightarrow p$,

(27) $p \wedge \neg p\ \mathcal{U}\ q \Rightarrow q$,

(28) $p\ \mathcal{U}\ q \Rightarrow p \vee q$,

(29) **$\mathcal{U}$ Insertion:** $q \Rightarrow p\ \mathcal{U}\ q$,

(30) $p \wedge q \Rightarrow p\ \mathcal{U}\ q$.

This system has the following five absorption properties that do not seem to appear in the temporal logic literature. Most can be proved in one step.

(31) **Absorption:** $p \vee p \ \mathcal{U} \ q \equiv p \vee q$,

(32) **Absorption:** $p \ \mathcal{U} \ q \vee q \equiv p \ \mathcal{U} \ q$,

(33) **Absorption:** $p \ \mathcal{U} \ q \wedge q \equiv q$,

(34) **Absorption:** $p \ \mathcal{U} \ q \vee (p \wedge q) \equiv p \ \mathcal{U} \ q$,

(35) **Absorption:** $p \ \mathcal{U} \ q \wedge (p \vee q) \equiv p \ \mathcal{U} \ q$.

All systems have the following two absorption theorems. Manna and Pnueli [21] refer to these as idempotence properties. This article follows Schneider [24], which refers to them as absorption properties. The proof of each uses mutual implication.

(36) **Left absorption of $\mathcal{U}$:** $p \ \mathcal{U} \ (p \ \mathcal{U} \ q) \equiv p \ \mathcal{U} \ q$,

(37) **Right absorption of $\mathcal{U}$:** $(p \ \mathcal{U} \ q) \ \mathcal{U} \ q \equiv p \ \mathcal{U} \ q$.

3.3 Eventually

Eventually $\Diamond$ is a special case of $\mathcal{U}$ when the left-hand side is *true*. Equation (38) is its only defining axiom:

(38) **Definition of $\Diamond$:** $\Diamond q \equiv \mathit{true} \ \mathcal{U} \ q$.

Theorem (39) shows how the unary operator *eventually* absorbs into the binary operator *until*. Its proof uses (15) Right distributivity of $\mathcal{U}$ over $\wedge$. Theorems (40) and (41) show also that the binary operator *until* absorbs into the unary operator *eventually*. They are proved by mutual implication. Theorem (42) shows that $p \ \mathcal{U} \ q$ guarantees that q will eventually be *true*. Its proof uses (39). Theorems (43) and (44), Truth and Falsehood of $\Diamond$, do not appear in other LTL systems. Their proofs are simple.

(39) **Absorption of $\Diamond$ into $\mathcal{U}$:** $p \ \mathcal{U} \ q \wedge \Diamond q \equiv p \ \mathcal{U} \ q$,

(40) **Absorption of $\mathcal{U}$ into $\Diamond$:** $p \ \mathcal{U} \ q \vee \Diamond q \equiv \Diamond q$,

(41) **Absorption of $\mathcal{U}$ into $\Diamond$:** $p \ \mathcal{U} \ \Diamond q \equiv \Diamond q$,

(42) **Eventuality:** $p \ \mathcal{U} \ q \Rightarrow \Diamond q$,

(43) **Truth of $\Diamond$:** $\Diamond \mathit{true} \equiv \mathit{true}$,

(44) **Falsehood of $\Diamond$:** $\Diamond \mathit{false} \equiv \mathit{false}$.

Expansion of $\Diamond$, like expansion of $\mathcal{U}$, has two disjuncts. The first describes the current state and the second contains the operation in the next state. The expansion of $\Diamond$ follows directly from the expansion of $\mathcal{U}$. The two weakening theorems (46) and (47) follow directly from expansion of $\Diamond$.

(45) **Expansion of $\Diamond$:** $\Diamond p \equiv p \vee \bigcirc \Diamond p$,

(46) **Weakening of $\Diamond$:** $p \Rightarrow \Diamond p$,

(47) **Weakening of $\Diamond$:** $\bigcirc p \Rightarrow \Diamond p$.

The two absorption theorems (48) and (49) do not seem to appear in the temporal logic literature. The following four theorems (50), (51), (52), and (53) are common to all temporal logic systems:

(48) **Absorption of $\vee$ into $\Diamond$:** $p \vee \Diamond p \equiv \Diamond p$,

(49) **Absorption of $\Diamond$ into $\wedge$:** $\Diamond p \wedge p \equiv p$,

(50) **Absorption of $\Diamond$:** $\Diamond \Diamond p \equiv \Diamond p$,

(51) **Exchange of $\bigcirc$ and $\Diamond$:** $\bigcirc \Diamond p \equiv \Diamond \bigcirc p$,

(52) **Distributivity of $\Diamond$ over $\vee$:** $\Diamond (p \vee q) \equiv \Diamond p \vee \Diamond q$,

(53) **Distributivity of $\Diamond$ over $\wedge$:** $\Diamond (p \wedge q) \Rightarrow \Diamond p \wedge \Diamond q$.

3.4 Always

This system defines the *always* operator $\Box$ in terms of the *eventually* operator $\Diamond$. $\Box p$ is true when p is true in the current state and in all future states. The defining equation (54) states that p is always true iff it is not the case that $\neg p$ is eventually true. The two induction axioms do not appear in other LTL systems, either as axioms or theorems.

(54) **Definition of $\Box$:** $\Box p \equiv \neg \Diamond \neg p$,

(55) **Axiom, $\mathcal{U}$ Induction:** $\Box (p \Rightarrow (\bigcirc p \wedge q) \vee r) \Rightarrow (p \Rightarrow \Box q \vee q \ \mathcal{U} \ r)$,

(56) **Axiom, $\mathcal{U}$ Induction:** $\Box (p \Rightarrow \bigcirc (p \vee q)) \Rightarrow (p \Rightarrow \Box p \vee p \ \mathcal{U} \ q)$.

Induction theorem (57) is common to many systems. It follows from (56) with $q := \mathit{false}$. The negation of the dual of Theorem (58) is equivalent to Theorem (57). Theorem (59) expresses $\Diamond p$ in terms of $\Box p$ and is the dual of the defining Equation (54).

(57) **$\Box$ Induction:** $\Box (p \Rightarrow \bigcirc p) \Rightarrow (p \Rightarrow \Box p)$,

(58) **$\Diamond$ Induction:** $\Box (\bigcirc p \Rightarrow p) \Rightarrow (\Diamond p \Rightarrow p)$,

(59) $\Diamond p \equiv \neg \Box \neg p$.

Whereas the *next* operator $\bigcirc$ is its own dual, the *eventually* operator $\Diamond$ and the *always* operator $\Box$ are mutually dual, as are $\Diamond \Box$ and $\Box \Diamond$. Each of the following four theorems can be proved directly without invoking (2.3) Metatheorem Duality. However, with P and Q defined as the expressions $P : \neg \Box p$ and $Q : \Diamond \neg p$, the dual expressions are $P_D : \neg \Diamond p$ and $Q_D : \Box \neg p$. Because theorem (60) is the expression $P \equiv Q$ and Theorem (61) is the expression $P_D \equiv Q_D$, the validity of (61) can be asserted by invoking (2.3b) Metatheorem Duality with Theorem (60). Similarly, the validity of (63) can be asserted by invoking duality with Theorem (62).

(60) **Dual of $\Box$:** $\neg \Box p \equiv \Diamond \neg p$,

(61) **Dual of $\Diamond$:** $\neg \Diamond p \equiv \Box \neg p$,

(62) **Dual of $\Diamond \Box$:** $\neg \Diamond \Box p \equiv \Box \Diamond \neg p$,

(63) **Dual of $\Box \Diamond$:** $\neg \Box \Diamond p \equiv \Diamond \Box \neg p$.

Theorems (64) and (65), Truth and Falsehood of $\Box$, do not appear in other LTL systems.

(64) **Truth of $\Box$:** $\Box \mathit{true} \equiv \mathit{true}$,

(65) **Falsehood of $\Box$:** $\Box \mathit{false} \equiv \mathit{false}$.

While the expansions of $\mathcal{U}$ and $\Diamond$ have two disjuncts, the expansion of $\Box$ has two conjuncts. As usual, the first describes the current state and the second contains the operation in the next state. Theorem (66) is the dual of (45), which can be used in its direct proof.

(66) **Expansion of $\Box$:** $\Box p \equiv p \wedge \bigcirc \Box p$,

(67) **Expansion of $\Box$:** $\Box p \equiv p \wedge \bigcirc p \wedge \bigcirc \Box p$.

Theorem (68) absorption of $\wedge$ into $\Box$, is the dual of (48) the absorption of $\vee$ into $\Diamond$, while (69) absorption of $\Box$ into $\vee$ is the dual of (49) the absorption of $\Diamond$ into $\wedge$. As with (48) and (49), neither seem to appear in the temporal logic literature.

Conjunction $\wedge$ and the *always* operator $\Box$ are both universal, while disjunction $\vee$ and the *eventually* operator $\Diamond$ are both existential. When the left side of the equivalence contains both existential (or both universal) operators as in (48) and (68), the right side retains the same type of unary operator. When existential and universal operators are mixed on the left side, as in (49) and (69), the equivalence is just a statement about p at the current time.

(68) **Absorption of $\wedge$ into $\Box$:** $p \wedge \Box p \equiv \Box p$,

(69) **Absorption of $\Box$ into $\vee$:** $\Box p \vee p \equiv p$.

The absorption of $\Diamond$ into $\Box$ and of $\Box$ into $\Diamond$ do not appear in the LTL systems we survey. Their proofs are straightforward applications of the previous absorption theorems.

(70) **Absorption of $\Diamond$ into $\Box$:** $\Diamond p \wedge \Box p \equiv \Box p$,

(71) **Absorption of $\Box$ into $\Diamond$:** $\Box p \vee \Diamond p \equiv \Diamond p$.

Theorem (72) absorption of $\Box$ is the dual of (50) the absorption of $\Diamond$, and (73) the exchange of $\bigcirc$ and $\Box$ is the dual of (51) the exchange of $\bigcirc$ and $\Diamond$.

(72) **Absorption of $\Box$:** $\Box \Box p \equiv \Box p$,

(73) **Exchange of $\bigcirc$ and $\Box$:** $\bigcirc \Box p \equiv \Box \bigcirc p$.

Theorem (74) does not appear in other LTL systems. Theorem (75) states that if p holds and eventually $\neg p$ holds, there must eventually be a state where p holds in that state and it does not hold in the next state. Theorem (75) is the contrapositive of, and therefore equivalent to, (57) $\Box$ Induction.

(74) $p \Rightarrow \Box p \equiv p \Rightarrow \bigcirc \Box p$,

(75) $p \wedge \Diamond \neg p \Rightarrow \Diamond (p \wedge \bigcirc \neg p)$.

The following four strengthening theorems for $\Box$ are common and contrast with the weakening theorems (46) and (47) for $\Diamond$. Theorem (80) is listed in one other system. Theorem (81) is unique to this one.

(76) **Strengthening of $\Box$:** $\Box p \Rightarrow p$,

(77) **Strengthening of $\Box$:** $\Box p \Rightarrow \Diamond p$,

(78) **Strengthening of $\Box$:** $\Box p \Rightarrow \bigcirc p$,

(79) **Strengthening of $\Box$:** $\Box p \Rightarrow \bigcirc \Box p$,

(80) $\bigcirc$ **generalization:** $\Box p \Rightarrow \Box \bigcirc p$,

(81) $\Box p \Rightarrow \neg(q \ \mathcal{U} \ \neg p)$.

3.5 Temporal Deduction

The following deduction proof technique is a metatheorem in LADM:

(4.4) **Deduction (assume conjuncts of antecedent):**
To prove $P_1 \wedge P_2 \Rightarrow Q$, assume P_1 and P_2, and prove Q.
You cannot use textual substitution in P_1 or P_2.

Corresponding to the deduction metatheorem of the propositional calculus is the following temporal deduction metatheorem:

(82) **Temporal deduction:**

To prove $\Box P_1 \wedge \Box P_2 \Rightarrow Q$, assume P_1 and P_2, and prove Q.
You cannot use textual substitution in P_1 or P_2.

Temporal deduction is Theorem (2.1.6) of Kröger and Merz [20], who also give the justification. Note that if you assume P in a step of an LTL proof of Q, you have *not* proved that $P \Rightarrow Q$, but rather that $\Box P \Rightarrow Q$.

3.6 Always, Continued

The following two theorems, (83) and (84), do not appear in other LTL systems. However, they are required for the proof of later theorems that are included in other systems. In particular, the proofs of (85) and (86) depend on (83) Distributivity of $\wedge$ over $\mathcal{U}$. The proof of (83) illustrates temporal deduction in a calculational proof. The proof of (84) is similar.

(83) **Distributivity of $\wedge$ over $\mathcal{U}$:** $\Box p \wedge q \ \mathcal{U} \ r \Rightarrow (p \wedge q) \ \mathcal{U} \ (p \wedge r)$

Proof: The proof is by (82) Temporal deduction.

$$
\begin{array}{ll}
 & \Box p \wedge q \ \mathcal{U} \ r \Rightarrow (p \wedge q) \ \mathcal{U} \ (p \wedge r) \\
= & \quad \langle (3.65) \text{ Shunting}, \ p \wedge q \Rightarrow r \ \equiv \ p \Rightarrow (q \Rightarrow r) \rangle \\
 & \Box p \Rightarrow (q \ \mathcal{U} \ r \Rightarrow (p \wedge q) \ \mathcal{U} \ (p \wedge r)).
\end{array}
$$

And now,

$$
\begin{array}{ll}
 & q \ \mathcal{U} \ r \Rightarrow (p \wedge q) \ \mathcal{U} \ (p \wedge r) \\
= & \quad \langle \text{Assume antecedent } p \rangle \\
 & q \ \mathcal{U} \ r \Rightarrow (\mathit{true} \wedge q) \ \mathcal{U} \ (\mathit{true} \wedge r) \\
= & \quad \langle (3.39) \text{ Identity of } \wedge, \ p \wedge \mathit{true} \equiv p \rangle \\
 & q \ \mathcal{U} \ r \Rightarrow q \ \mathcal{U} \ r \quad -(3.71) \text{ Reflexivity of } \Rightarrow, \ p \Rightarrow p. \quad \blacksquare
\end{array}
$$

(84) $\mathcal{U}$ **implication:** $\Box p \wedge \Diamond q \Rightarrow p \ \mathcal{U} \ q$,

(85) **Right monotonicity of $\mathcal{U}$:** $\Box (p \Rightarrow q) \Rightarrow (r \ \mathcal{U} \ p \Rightarrow r \ \mathcal{U} \ q)$,

(86) **Left monotonicity of $\mathcal{U}$:** $\Box (p \Rightarrow q) \Rightarrow (p \ \mathcal{U} \ r \Rightarrow q \ \mathcal{U} \ r)$.

Theorem (87) states that if it is always the case that p is false, then it is not the case that p is always true, but not the converse. Suppose, for example, that p continually oscillates between true and false over time. Then, the consequent of (87) is true, but the antecedent is false. Theorem (88) shows how $\Diamond$ distributes over $\wedge$.

(87) **Distributivity of¬over $\Box$:** $\Box \neg p \Rightarrow \neg \Box p$,

(88) **Distributivity of $\Diamond$ over $\wedge$:** $\Box p \wedge \Diamond q \Rightarrow \Diamond (p \wedge q)$.

Theorems (89), (90), and (91) are the linear temporal versions of the excluded middle axiom of propositional logic, (3.28) $p \vee \neg p$. Theorems (92), (93), and (94) are the linear temporal versions of the contradiction theorem of propositional logic, (3.42) $p \wedge \neg p \equiv false$. Theorems (95), (96), (97), and (98) are variations. These theorems are obvious, and their proofs are simple, which is perhaps why they do not appear in other LTL systems.

(89) **$\Diamond$ excluded middle:** $\Diamond p \vee \Box \neg p$,

(90) **$\Box$ excluded middle:** $\Box p \vee \Diamond \neg p$,

(91) **Temporal excluded middle:** $\Diamond p \vee \Diamond \neg p$,

(92) **$\Diamond$ contradiction:** $\Diamond p \wedge \Box \neg p \equiv false$,

(93) **$\Box$ contradiction:** $\Box p \wedge \Diamond \neg p \equiv false$,

(94) **Temporal contradiction:** $\Box p \wedge \Box \neg p \equiv false$,

(95) **$\Box \Diamond$ excluded middle:** $\Box \Diamond p \vee \Diamond \Box \neg p$,

(96) **$\Diamond \Box$ excluded middle:** $\Diamond \Box p \vee \Box \Diamond \neg p$,

(97) **$\Box \Diamond$ contradiction:** $\Box \Diamond p \wedge \Diamond \Box \neg p \equiv false$,

(98) **$\Diamond \Box$ contradiction:** $\Diamond \Box p \wedge \Box \Diamond \neg p \equiv false$.

Theorem (99) shows that $\Box$, a universal operator, distributes over conjunction. Because disjunction is existential, (100) shows that $\Box$ distributes over conjunction in only one direction. Theorems (101), (102), and (103) reflect the concept of logical equivalence $\cong$ in Reference [20]. Theorems (104) and (105) show how $\Diamond$ distributes over $\Rightarrow$.

(99) **Distributivity of $\Box$ over $\wedge$:** $\Box (p \wedge q) \equiv \Box p \wedge \Box q$,

(100) **Distributivity of $\Box$ over $\vee$:** $\Box p \vee \Box q \Rightarrow \Box (p \vee q)$,

(101) **Logical equivalence law of $\circ$:** $\Box (p \equiv q) \Rightarrow (\circ p \equiv \circ q)$,

(102) **Logical equivalence law of $\Diamond$:** $\Box (p \equiv q) \Rightarrow (\Diamond p \equiv \Diamond q)$,

(103) **Logical equivalence law of $\Box$:** $\Box (p \equiv q) \Rightarrow (\Box p \equiv \Box q)$,

(104) **Distributivity of $\Diamond$ over $\Rightarrow$:** $\Diamond (p \Rightarrow q) \equiv (\Box p \Rightarrow \Diamond q)$,

(105) **Distributivity of $\Diamond$ over $\Rightarrow$:** $(\Diamond p \Rightarrow \Diamond q) \Rightarrow \Diamond (p \Rightarrow q)$.

The next three frame laws (106), (107), and (108) state that if $\Box p$ holds, then p may be "added" by conjunction under each temporal operator [20]. For completeness, we show that they may be

added under disjunction, implication, and equivalence as well. Theorems (148) to (150) extend the frame laws to $\mathcal{U}$ and theorems (210) to (212) extend them to $\mathcal{W}$.

(106) $\wedge$ **frame law of** $\circ$**:** $\quad \Box p \Rightarrow (\circ q \Rightarrow \circ (p \wedge q))$

Proof:

$$
\begin{array}{ll}
 & \Box p \Rightarrow (\circ q \Rightarrow \circ (p \wedge q)) \\
= & \quad \langle (3.65)\ \text{Shunting}, p \wedge q \Rightarrow r \ \equiv \ p \Rightarrow (q \Rightarrow r) \rangle \\
 & \Box p \wedge \circ q \Rightarrow \circ (p \wedge q)
\end{array}
$$

And now,

$$
\begin{array}{ll}
 & \Box p \wedge \circ q \\
\Rightarrow & \quad \langle (78)\ \text{Strengthening of}\ \Box\ \text{and (4.3) Monotonicity of}\ \wedge \rangle \\
 & \circ p \wedge \circ q \\
= & \quad \langle (5)\ \text{Distributivity of}\ \circ\ \text{over}\ \wedge \rangle \\
 & \circ (p \wedge q) \quad \blacksquare
\end{array}
$$

(107) $\wedge$ **frame law of** $\Diamond$**:** $\quad \Box p \Rightarrow (\Diamond q \Rightarrow \Diamond (p \wedge q))$,

(108) $\wedge$ **frame law of** $\Box$**:** $\quad \Box p \Rightarrow (\Box q \Rightarrow \Box (p \wedge q))$,

(109) $\vee$ **frame law of** $\circ$**:** $\quad \Box p \Rightarrow (\circ q \Rightarrow \circ (p \vee q))$,

(110) $\vee$ **frame law of** $\Diamond$**:** $\quad \Box p \Rightarrow (\Diamond q \Rightarrow \Diamond (p \vee q))$,

(111) $\vee$ **frame law of** $\Box$**:** $\quad \Box p \Rightarrow (\Box q \Rightarrow \Box (p \vee q))$,

(112) $\Rightarrow$ **frame law of** $\circ$**:** $\quad \Box p \Rightarrow (\circ q \Rightarrow \circ (p \Rightarrow q))$,

(113) $\Rightarrow$ **frame law of** $\Diamond$**:** $\quad \Box p \Rightarrow (\Diamond q \Rightarrow \Diamond (p \Rightarrow q))$,

(114) $\Rightarrow$ **frame law of** $\Box$**:** $\quad \Box p \Rightarrow (\Box q \Rightarrow \Box (p \Rightarrow q))$,

(115) $\equiv$ **frame law of** $\circ$**:** $\quad \Box p \Rightarrow (\circ q \Rightarrow \circ (p \equiv q))$,

(116) $\equiv$ **frame law of** $\Diamond$**:** $\quad \Box p \Rightarrow (\Diamond q \Rightarrow \Diamond (p \equiv q))$,

(117) $\equiv$ **frame law of** $\Box$**:** $\quad \Box p \Rightarrow (\Box q \Rightarrow \Box (p \equiv q))$.

Theorems (118), (119), and (120) show that all unary temporal operators are monotonic. Theorem (120) can also be considered distributivity of $\Box$ over $\Rightarrow$. Proofs of the consequence rules (121), (122), and (123) use the monotonicity theorems as shown in the proof of (121). Proofs of the catenation rules (124), (125), and (126) are similar.

(118) **Monotonicity of** $\circ$**:** $\quad \Box (p \Rightarrow q) \Rightarrow (\circ p \Rightarrow \circ q)$,

(119) **Monotonicity of** $\Diamond$**:** $\quad \Box (p \Rightarrow q) \Rightarrow (\Diamond p \Rightarrow \Diamond q)$,

(120) **Monotonicity of** $\Box$**:** $\quad \Box (p \Rightarrow q) \Rightarrow (\Box p \Rightarrow \Box q)$,

(121) **Consequence rule of** $\circ$**:** $\quad \Box ((p \Rightarrow q) \wedge (q \Rightarrow \circ r) \wedge (r \Rightarrow s)) \Rightarrow (p \Rightarrow \circ s)$

Proof:

$$
\begin{array}{ll}
 & \Box\,((p \Rightarrow q) \wedge (q \Rightarrow \bigcirc r) \wedge (r \Rightarrow s)) \\
= & \quad \langle (99)\ \text{Distributivity of } \Box \text{ over } \wedge \rangle \\
 & \Box\,(p \Rightarrow q) \wedge \Box\,(q \Rightarrow \bigcirc r) \wedge \Box\,(r \Rightarrow s) \\
\Rightarrow & \quad \langle (76)\ \text{Strengthening of } \Box \text{ and (4.3) Monotonicity of } \wedge, \text{ twice} \rangle \\
 & (p \Rightarrow q) \wedge (q \Rightarrow \bigcirc r) \wedge \Box\,(r \Rightarrow s) \\
\Rightarrow & \quad \langle (3.82a)\ \text{Transitivity and (4.3) Monotonicity of } \wedge \rangle \\
 & (p \Rightarrow \bigcirc r) \wedge \Box\,(r \Rightarrow s) \\
\Rightarrow & \quad \langle (118)\ \text{Monotonicity of } \bigcirc \text{ and (4.3) Monotonicity of } \wedge \rangle \\
 & (p \Rightarrow \bigcirc r) \wedge (\bigcirc r \Rightarrow \bigcirc s) \\
\Rightarrow & \quad \langle (3.82a)\ \text{Transitivity} \rangle \\
 & p \Rightarrow \bigcirc s \quad \blacksquare
\end{array}
$$

(122) **Consequence rule of $\Diamond$:** $\Box\,((p \Rightarrow q) \wedge (q \Rightarrow \Diamond r) \wedge (r \Rightarrow s)) \Rightarrow (p \Rightarrow \Diamond s)$,

(123) **Consequence rule of $\Box$:** $\Box\,((p \Rightarrow q) \wedge (q \Rightarrow \Box r) \wedge (r \Rightarrow s)) \Rightarrow (p \Rightarrow \Box s)$,

(124) **Catenation rule of $\Diamond$:** $\Box\,((p \Rightarrow \Diamond q) \wedge (q \Rightarrow \Diamond r)) \Rightarrow (p \Rightarrow \Diamond r)$,

(125) **Catenation rule of $\Box$:** $\Box\,((p \Rightarrow \Box q) \wedge (q \Rightarrow \Box r)) \Rightarrow (p \Rightarrow \Box r)$,

(126) **Catenation rule of $\mathcal{U}$:** $\Box\,((p \Rightarrow q\ \mathcal{U}\ r) \wedge (r \Rightarrow q\ \mathcal{U}\ s)) \Rightarrow (p \Rightarrow q\ \mathcal{U}\ s)$.

Most of the remaining theorems in this section are included in a single source in our survey.

(127) **$\mathcal{U}$ strengthening rule:** $\Box\,((p \Rightarrow r) \wedge (q \Rightarrow s)) \Rightarrow (p\ \mathcal{U}\ q \Rightarrow r\ \mathcal{U}\ s)$,

(128) **Induction rule $\Diamond$:** $\Box\,(p \vee \bigcirc q \Rightarrow q) \Rightarrow (\Diamond p \Rightarrow q)$,

(129) **Induction rule $\Box$:** $\Box\,(p \Rightarrow \bigcirc p \wedge q) \Rightarrow (p \Rightarrow \Box q)$,

(130) **Induction rule $\mathcal{U}$:** $\Box\,(p \Rightarrow \neg q \wedge \bigcirc p) \Rightarrow (p \Rightarrow \neg(r\ \mathcal{U}\ q))$,

(131) **$\Diamond$ Confluence:** $\Box\,((p \Rightarrow \Diamond\,(q \vee r)) \wedge (q \Rightarrow \Diamond\, t) \wedge (r \Rightarrow \Diamond\, t)) \Rightarrow (p \Rightarrow \Diamond\, t)$,

(132) **Temporal generalization law:** $\Box\,(\Box p \Rightarrow q) \Rightarrow (\Box p \Rightarrow \Box q)$,

(133) **Temporal particularization law:** $\Box\,(p \Rightarrow \Diamond q) \Rightarrow (\Diamond p \Rightarrow \Diamond q)$,

(134) $\Box\,(p \Rightarrow \bigcirc q) \Rightarrow (p \Rightarrow \Diamond q)$,

(135) $\Box\,(p \Rightarrow \bigcirc \neg p) \Rightarrow (p \Rightarrow \neg\Box p)$.

Because the implication relation is reflexive, antisymmetric, and transitive, it defines a partially ordered set on linear temporal logic expressions. Figure 3 is a collection of seven Hasse diagrams showing some implication relations. Each number in parentheses is a linear temporal logic theorem. A number that labels an edge in a Hasse diagram is an implication theorem, and a number that labels a box is an equivalence theorem. For example, edge (87) represents the theorem that $\Box \neg p$ implies $\neg\Box p$, and box (61) represents the theorem that $\neg\Diamond p$ is equivalent to $\Box \neg p$.

The collection of theorems in this article omit some implication theorems that are trivially derived by mutual transitivity. For example, one such theorem is that $\Box \neg p$ implies $\Diamond \neg p$, which follows from the theorems that $\Box \neg p$ implies $\neg\Box p$ and that $\neg\Box p$ is equivalent to $\Diamond \neg p$. The edge labeled by (87) thus represents four implication theorems, one for each combination of the two

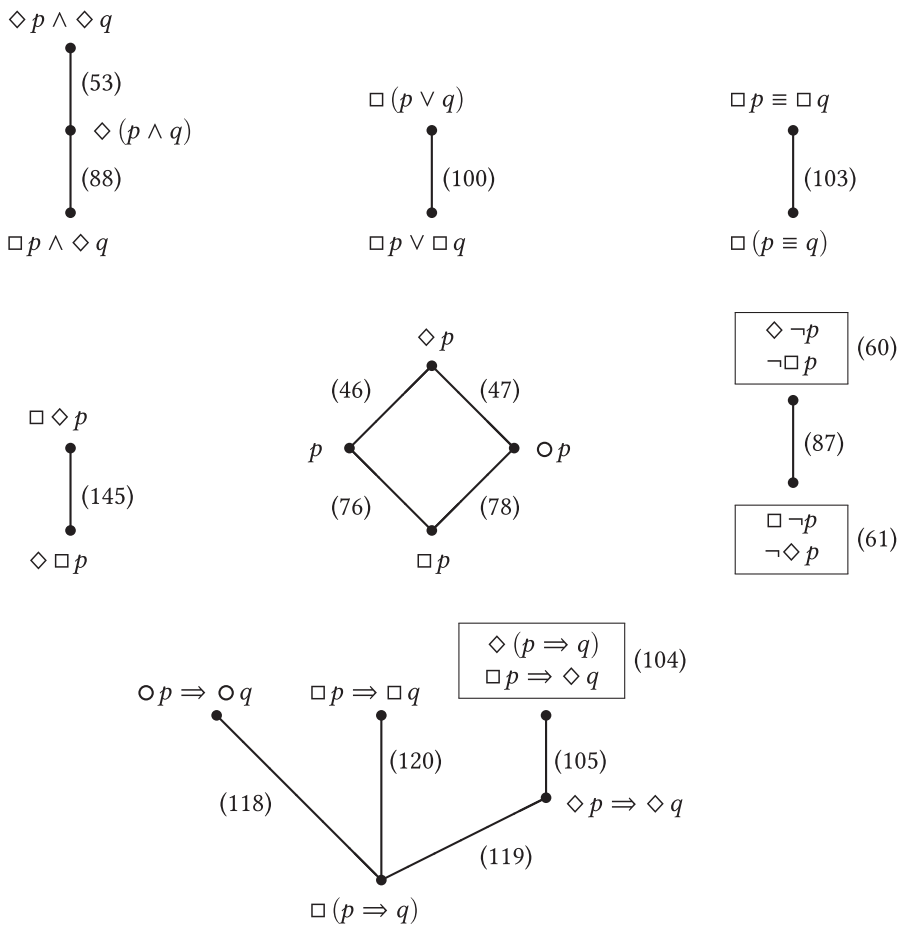

Fig. 3. Seven Hasse diagrams showing some implication relations of linear temporal logic.

antecedents $\Box \neg p$ and $\neg \Diamond p$ and the two consequents $\Diamond \neg p$ and $\neg \Box p$. Likewise, the edge labeled by (105) represents two implication theorems.

3.7 Proof Metatheorems

In the calculational system $\mathcal{E}$, Gries and Schneider (LADM) prove the metatheorem (9.16), which states that P is a theorem iff $(\forall x \mid : P)$ is a theorem [13]. Theorems in $\mathcal{E}$ are thus said to be "implicitly universally quantified." A similar concept applies to temporal logic theorems in $\mathcal{E}$ except that the implicit application is in the temporal dimension. The following metatheorem shows that theorems "implicitly always hold." Case 1 in the proof below is known as the temporal generalization rule [24], and Case 2 is known as the specialization rule [21].

(136) **Metatheorem:** P is a theorem iff $\Box P$ is a theorem.

Proof: The proof is by (4.7) Mutual implication. The proof of each case is by (4.4) Deduction.

Case 1. If P is a theorem, then $\Box P$ is a theorem.

Suppose P is a theorem. Because all theorems are equivalent to each other, and (3.4) *true* is a theorem, P is equivalent to *true*. Then, $\Box P$ can be proved to be a theorem as follows:

$\Box P$
$=$ ⟨P is a theorem⟩
$\Box\, true$
$=$ ⟨(64) Truth of $\Box$⟩
$true$

Case 2. If $\Box P$ is a theorem, then P is a theorem.

Suppose $\Box P$ is a theorem. Then, $\Box P$ is equivalent to *true*. P can be proved to be a theorem by (4.7.1) Truth implication as follows:

P
$\Leftarrow$ ⟨(76) Strengthening of $\Box$⟩
$\Box P$
$=$ ⟨$\Box P$ is a theorem⟩
$true$ ∎

Proofs of the following three metatheorems are similar:

(137) **Metatheorem $\bigcirc$:** If $P \Rightarrow Q$ is a theorem, then $\bigcirc P \Rightarrow \bigcirc Q$ is a theorem.

(138) **Metatheorem $\Diamond$:** If $P \Rightarrow Q$ is a theorem, then $\Diamond P \Rightarrow \Diamond Q$ is a theorem.

(139) **Metatheorem $\Box$:** If $P \Rightarrow Q$ is a theorem, then $\Box P \Rightarrow \Box Q$ is a theorem.

The proof of (142) in Section 3.8 illustrates the use of (136) Metatheorem. The proof of (166) illustrates the use of (138) Metatheorem $\Diamond$ and (139) Metatheorem $\Box$.

3.8 Always, Continued

Theorems (140) and (141) do not seem to appear in the LTL literature. However, they play a key role here in the proofs of several later theorems that do exist in the literature. The proof of (140) is based on (129) Induction rule $\Box$ with $p, q := p\ \mathcal{U}\ \Box q, p\ \mathcal{U}\ q$. It establishes the truth of the antecedent with the help of two lemmas, each of which is proved with metatheorem (136). The strengthening and ordering theorems are also unique to this system.

(140) $\mathcal{U}$ **$\Box$ implication:** $p\ \mathcal{U}\ \Box q \Rightarrow \Box (p\ \mathcal{U}\ q)$,

(141) **Absorption of $\mathcal{U}$ into $\Box$:** $p\ \mathcal{U}\ \Box p \equiv \Box p$,

(142) **Right $\wedge$ $\mathcal{U}$ strengthening:** $p\ \mathcal{U}\ (q \wedge r) \Rightarrow p\ \mathcal{U}\ (q\ \mathcal{U}\ r)$.

Proof: The proof is by (4.7.1) Truth implication.

$true$
$=$ ⟨(136) Metatheorem and (30)⟩
$\Box (q \wedge r \Rightarrow q\ \mathcal{U}\ r)$
$\Rightarrow$ ⟨(85) Right monotonicity of $\mathcal{U}$ with $p, q, r := q \wedge r, q\ \mathcal{U}\ r, p$⟩
$p\ \mathcal{U}\ (q \wedge r) \Rightarrow p\ \mathcal{U}\ (q\ \mathcal{U}\ r)$ ∎

(143) **Left $\wedge$ $\mathcal{U}$ strengthening:** $(p \wedge q)\ \mathcal{U}\ r \Rightarrow (p\ \mathcal{U}\ q)\ \mathcal{U}\ r$,

(144) **Left $\wedge$ $\mathcal{U}$ ordering:** $(p \wedge q)\ \mathcal{U}\ r \Rightarrow p\ \mathcal{U}\ (q\ \mathcal{U}\ r)$.

The $\Diamond\,\Box$ implication theorem states that $\Diamond\,\Box\,p$ ensures that p will always eventually hold, but not the converse. Suppose, for example, that p continually oscillates between true and false over time. Then, the consequent of (145) is true, but the antecedent is false. Its proof uses (140). Theorem (146) is a second version of (95) $\Box\,\Diamond$ excluded middle, and is perhaps less intuitive. Its proof uses (145).

(145) **$\Diamond\,\Box$ implication:** $\Diamond\,\Box\,p \Rightarrow \Box\,\Diamond\,p$,

(146) **$\Box\,\Diamond$ excluded middle:** $\Box\,\Diamond\,p \vee \Box\,\Diamond\,\neg p$,

(147) **$\Diamond\,\Box$ contradiction:** $\Diamond\,\Box\,p \wedge \Diamond\,\Box\,\neg p \equiv \mathit{false}$,

(148) **$\mathcal{U}$ frame law of $\bigcirc$:** $\Box\,p \Rightarrow (\bigcirc\,q \Rightarrow \bigcirc\,(p\ \mathcal{U}\ q))$,

(149) **$\mathcal{U}$ frame law of $\Diamond$:** $\Box\,p \Rightarrow (\Diamond\,q \Rightarrow \Diamond\,(p\ \mathcal{U}\ q))$,

(150) **$\mathcal{U}$ frame law of $\Box$:** $\Box\,p \Rightarrow (\Box\,q \Rightarrow \Box\,(p\ \mathcal{U}\ q))$.

The absorption theorems (151) and (152), together with absorption theorems (50) and (72), allow any arbitrary string of $\Diamond$ and $\Box$ operators of any arbitrary length to be collapsed into one of four expressions: $\Diamond\,p$, $\Box\,p$, $\Box\,\Diamond\,p$, or $\Diamond\,\Box\,p$. These theorems are common to all systems. The remaining absorption theorems (153) to (156) are simple extensions mentioned in a single source in our survey.

(151) **Absorption of $\Diamond$ into $\Box\,\Diamond$:** $\Diamond\,\Box\,\Diamond\,p \equiv \Box\,\Diamond\,p$,

(152) **Absorption of $\Box$ into $\Diamond\,\Box$:** $\Box\,\Diamond\,\Box\,p \equiv \Diamond\,\Box\,p$,

(153) **Absorption of $\Box\,\Diamond$:** $\Box\,\Diamond\,\Box\,\Diamond\,p \equiv \Box\,\Diamond\,p$,

(154) **Absorption of $\Diamond\,\Box$:** $\Diamond\,\Box\,\Diamond\,\Box\,p \equiv \Diamond\,\Box\,p$,

(155) **Absorption of $\bigcirc$ into $\Box\,\Diamond$:** $\bigcirc\,\Box\,\Diamond\,p \equiv \Box\,\Diamond\,p$,

(156) **Absorption of $\bigcirc$ into $\Diamond\,\Box$:** $\bigcirc\,\Diamond\,\Box\,p \equiv \Diamond\,\Box\,p$.

The proof of monotonicity theorem (157) uses (139) Metatheorem $\Box$ and (119) Monotonicity of $\Diamond$. The proof of monotonicity theorem (158) does the same with (120) Monotonicity of $\Box$.

(157) **Monotonicity of $\Box\,\Diamond$:** $\Box\,(p \Rightarrow q) \Rightarrow (\Box\,\Diamond\,p \Rightarrow \Box\,\Diamond\,q)$,

(158) **Monotonicity of $\Diamond\,\Box$:** $\Box\,(p \Rightarrow q) \Rightarrow (\Diamond\,\Box\,p \Rightarrow \Diamond\,\Box\,q)$.

The next group of four distributivity theorems show how $\Box\,\Diamond$ and $\Diamond\,\Box$ distribute over conjunction and disjunction. Theorem (159) shows that $\Box\,\Diamond$ distributes over conjunction only in one direction. Similarly, Theorem (160) shows that $\Diamond\,\Box$ distributes over disjunction only in one direction. However, Theorems (161) and (162) show that $\Box\,\Diamond$ distributes over disjunction and $\Diamond\,\Box$ distributes over conjunction in both directions.

(159) **Distributivity of $\Box\,\Diamond$ over $\wedge$:** $\Box\,\Diamond\,(p \wedge q) \Rightarrow \Box\,\Diamond\,p \wedge \Box\,\Diamond\,q$,

(160) **Distributivity of $\Diamond\,\Box$ over $\vee$:** $\Diamond\,\Box\,p \vee \Diamond\,\Box\,q \Rightarrow \Diamond\,\Box\,(p \vee q)$,

(161) **Distributivity of $\Box\Diamond$ over $\vee$:** $\Box\Diamond(p \vee q) \equiv \Box\Diamond p \vee \Box\Diamond q$,

(162) **Distributivity of $\Diamond\Box$ over $\wedge$:** $\Diamond\Box(p \wedge q) \equiv \Diamond\Box p \wedge \Diamond\Box q$.

Theorem (163) is Problem 4.2 in Manna and Pnueli [21]. Theorems (164) and (165) are Exercise 14.6 and 14.7, respectively, in Ben-Ari [4].

(163) **Eventual latching:** $\Diamond\Box(p \Rightarrow \Box q) \equiv \Diamond\Box\neg p \vee \Diamond\Box q$,

(164) $\Box(\Box\Diamond p \Rightarrow \Diamond q) \equiv \Diamond\Box\neg p \vee \Box\Diamond q$,

(165) $\Box((p \vee \Box q) \wedge (\Box p \vee q)) \equiv \Box p \vee \Box q$.

The metatheorems and absorption laws imply the following intuitive theorem: If p will eventually be always true, and it is always the case that q will be eventually true, then it is always the case that $p \wedge q$ will eventually be true.

(166) $\Diamond\Box p \wedge \Box\Diamond q \Rightarrow \Box\Diamond(p \wedge q)$

Proof:

$$
\begin{array}{ll}
 & \mathit{true} \\
= & \langle (88)\ \text{Distributivity of}\ \Diamond\ \text{over}\ \wedge\ \text{and (139) Metatheorem}\ \Box\ \rangle \\
 & \Box(\Box p \wedge \Diamond q) \Rightarrow \Box\Diamond(p \wedge q) \\
= & \langle (99)\ \text{Distributivity of}\ \Box\ \text{over}\ \wedge \rangle \\
 & \Box\Box p \wedge \Box\Diamond q \Rightarrow \Box\Diamond(p \wedge q) \\
= & \langle (72)\ \text{Absorption of}\ \Box\ \rangle \\
 & \Box p \wedge \Box\Diamond q \Rightarrow \Box\Diamond(p \wedge q) \\
= & \langle (3.65)\ \text{Shunting},\ p \wedge q \Rightarrow r \ \equiv\ p \Rightarrow (q \Rightarrow r) \rangle \\
 & \Box p \Rightarrow (\Box\Diamond q \Rightarrow \Box\Diamond(p \wedge q)) \\
= & \langle (138)\ \text{Metatheorem}\ \Diamond\ \text{with the above theorem} \rangle \\
 & \Diamond\Box p \Rightarrow \Diamond(\Box\Diamond q \Rightarrow \Box\Diamond(p \wedge q)) \\
= & \langle (104)\ \text{Distributivity of}\ \Diamond\ \text{over}\ \Rightarrow \rangle \\
 & \Diamond\Box p \Rightarrow (\Box\Box\Diamond q \Rightarrow \Diamond\Box\Diamond(p \wedge q)) \\
= & \langle (72)\ \text{Absorption of}\ \Box\ \text{and (151) Absorption of}\ \Diamond\ \text{into}\ \Box\ \rangle \\
 & \Diamond\Box p \Rightarrow (\Box\Diamond q \Rightarrow \Box\Diamond(p \wedge q)) \\
= & \langle (3.65)\ \text{Shunting},\ p \wedge q \Rightarrow r \ \equiv\ p \Rightarrow (q \Rightarrow r) \rangle \\
 & \Diamond\Box p \wedge \Box\Diamond q \Rightarrow \Box\Diamond(p \wedge q) \quad \blacksquare
\end{array}
$$

(167) $\Box((\Box p \Rightarrow \Diamond q) \wedge (q \Rightarrow \bigcirc r)) \Rightarrow (\Box p \Rightarrow \bigcirc\Box\Diamond r)$,

(168) **Progress proof rule:** $\Diamond\Box p \wedge \Box(\Box p \Rightarrow \Diamond q) \Rightarrow \Diamond q$.

3.9 Wait

$p\ \mathcal{U}\ q$ requires p to be true until q, which is guaranteed to eventually be true. $p\ \mathcal{W}\ q$ has no such guarantee. That is, if q is eventually true, then p is true until that time. But, if q is not eventually true, then p must be true always. Accordingly, Kröger and Merz [20] refer to $\mathcal{W}$ as the *weak* version of $\mathcal{U}$. Equations (169) and (170) are the only defining axioms for the *wait* operator.

(169) **Definition of $\mathcal{W}$:** $p\ \mathcal{W}\ q \equiv \Box p \vee p\ \mathcal{U}\ q$,

(170) **Axiom, Distributivity of $\neg$ over $\mathcal{W}$:** $\neg(p\ \mathcal{W}\ q) \equiv \neg q\ \mathcal{U}\ (\neg p \wedge \neg q)$.

The defining equation gives $\mathcal{W}$ in terms of $\mathcal{U}$. The following theorem gives $\mathcal{U}$ in terms of $\mathcal{W}$:

(171) **$\mathcal{U}$ in terms of $\mathcal{W}$:** $p\ \mathcal{U}\ q \equiv p\ \mathcal{W}\ q \wedge \Diamond q$,

(172) $p\ \mathcal{W}\ q \equiv \Box(p \wedge \neg q) \vee p\ \mathcal{U}\ q$.

The proof of (173) Distributivity of $\neg$ over $\mathcal{U}$ uses (170) Axiom, Distributivity of $\neg$ over $\mathcal{W}$. Apparently, the reverse is not possible. That is, if (173) is taken as the axiom instead of (170), we were not able to prove (170) as a theorem.

(173) **Distributivity of $\neg$ over $\mathcal{U}$:** $\neg(p\ \mathcal{U}\ q) \equiv \neg q\ \mathcal{W}\ (\neg p \wedge \neg q)$.

Theorem (174) $\mathcal{U}$ implication shows that $p\ \mathcal{U}\ q$ is stronger than $p\ \mathcal{W}\ q$. Theorem (175) Distributivity of $\wedge$ over $\mathcal{W}$ corresponds to, and is derived from, (83) Distributivity of $\wedge$ over $\mathcal{U}$. Theorem (176) $\mathcal{W}\ \Diamond$ equivalence comes from Manna and Pnueli [21] where it is used as the normal form for simple obligation formulas.

(174) **$\mathcal{U}$ implication:** $p\ \mathcal{U}\ q \Rightarrow p\ \mathcal{W}\ q$,

(175) **Distributivity of $\wedge$ over $\mathcal{W}$:** $\Box p \wedge q\ \mathcal{W}\ r \Rightarrow (p \wedge q)\ \mathcal{W}\ (p \wedge r)$,

(176) **$\mathcal{W}\ \Diamond$ equivalence:** $p\ \mathcal{W}\ \Diamond q \equiv \Box p \vee \Diamond q$.

Theorem (177) $\mathcal{W}\ \Box$ implication corresponds to (140) $\mathcal{U}\ \Box$ implication. Theorem (178) Absorption of $\mathcal{W}$ into $\Box$ corresponds to (141) Absorption of $\mathcal{U}$ into $\Box$. Theorem (179) Perpetuity for the *wait* operator corresponds to (42) Eventuality for the *until* operator. The *always* operator, which is universal, is in the antecedent of the implication in Perpetuity, while the *eventually* operator, which is existential, is in the consequent of the implication in Eventuality.

(177) **$\mathcal{W}\ \Box$ implication:** $p\ \mathcal{W}\ \Box q \Rightarrow \Box(p\ \mathcal{W}\ q)$,

(178) **Absorption of $\mathcal{W}$ into $\Box$:** $p\ \mathcal{W}\ \Box p \equiv \Box p$,

(179) **Perpetuity:** $\Box p \Rightarrow p\ \mathcal{W}\ q$,

(180) **Distributivity of $\circ$ over $\mathcal{W}$:** $\circ(p\ \mathcal{W}\ q) \equiv \circ p\ \mathcal{W} \circ q$.

Expansion of the *wait* operator (181) corresponds to expansion of the *until* operator (10). Excluded middle for the *wait* operator (182) corresponds to excluded middle for the *until* operator (23). Left zero of the *wait* operator (183) corresponds to right zero of the *until* operator (11).

(181) **Expansion of $\mathcal{W}$:** $p\ \mathcal{W}\ q \equiv q \vee (p \wedge \circ(p\ \mathcal{W}\ q))$,

(182) **$\mathcal{W}$ excluded middle:** $p\ \mathcal{W}\ q \vee p\ \mathcal{W}\ \neg q$,

(183) **Left zero of $\mathcal{W}$:** $\mathit{true}\ \mathcal{W}\ q \equiv \mathit{true}$.

The next four distributive theorems for the *wait* operator correspond to, and are proved from, the distributive axioms for the *until* operator (12), (13), (14), and (15). The proof of (187) Right distributivity of $\mathcal{W}$ over $\wedge$ is an example of one benefit of $\mathcal{E}$, with its emphasis on equality, over $\mathcal{H}$, with its emphasis on implication and modus ponens. Before we formulated the calculational 8-step proof of (187), we had an earlier proof based on mutual implication that required 20 steps.

(184) **Left distributivity of $\mathcal{W}$ over $\vee$:** $p\ \mathcal{W}\ (q \vee r) \equiv p\ \mathcal{W}\ q \vee p\ \mathcal{W}\ r$,

(185) **Right distributivity of $\mathcal{W}$ over $\vee$:** $p\ \mathcal{W}\ r \vee q\ \mathcal{W}\ r \Rightarrow (p \vee q)\ \mathcal{W}\ r$,

(186) **Left distributivity of $\mathcal{W}$ over $\wedge$:** $p\ \mathcal{W}\ (q \wedge r) \Rightarrow p\ \mathcal{W}\ q \wedge p\ \mathcal{W}\ r$,

(187) **Right distributivity of $\mathcal{W}$ over $\wedge$:** $(p \wedge q)\ \mathcal{W}\ r \equiv p\ \mathcal{W}\ r \wedge q\ \mathcal{W}\ r$.

Proof:

$$
\begin{array}{ll}
 & p\ \mathcal{W}\ r \wedge q\ \mathcal{W}\ r \\
= & \langle (3.12)\ \text{Double negation}, \neg\neg p \equiv p \rangle \\
 & \neg\neg(p\ \mathcal{W}\ r \wedge q\ \mathcal{W}\ r) \\
= & \langle (3.47a)\ \text{De Morgan}, \neg(p \wedge q) \equiv \neg p \vee \neg q \rangle \\
 & \neg(\neg(p\ \mathcal{W}\ r) \vee \neg(q\ \mathcal{W}\ r)) \\
= & \langle (170)\ \text{Distributivity of}\ \neg\ \text{over}\ \mathcal{W}\ ,\ \text{twice} \rangle \\
 & \neg(\neg r\ \mathcal{U}\ (\neg p \wedge \neg r) \vee \neg r\ \mathcal{U}\ (\neg q \wedge \neg r)) \\
= & \langle (12)\ \text{Left Distributivity of}\ \mathcal{U}\ \text{over}\ \vee \rangle \\
 & \neg(\neg r\ \mathcal{U}\ ((\neg p \wedge \neg r) \vee (\neg q \wedge \neg r))) \\
= & \langle (3.46)\ \text{Distributivity of}\ \wedge\ \text{over}\ \vee,\ p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r) \rangle \\
 & \neg(\neg r\ \mathcal{U}\ (\neg r \wedge (\neg p \vee \neg q))) \\
= & \langle (3.47a)\ \text{De Morgan}, \neg(p \wedge q) \equiv \neg p \vee \neg q \rangle \\
 & \neg(\neg r\ \mathcal{U}\ (\neg r \wedge \neg(p \wedge q))) \\
= & \langle (170)\ \text{Distributivity of}\ \neg\ \text{over}\ \mathcal{W}\ \text{with}\ p, q := p \wedge q, r \rangle \\
 & \neg\neg((p \wedge q)\ \mathcal{W}\ r) \\
= & \langle (3.12)\ \text{Double negation}, \neg\neg p \equiv p \rangle \\
 & (p \wedge q)\ \mathcal{W}\ r \quad \blacksquare
\end{array}
$$

Theorem (188) for $\mathcal{W}$ is identical to (19) for $\mathcal{U}$. Both $\mathcal{W}$ and $\mathcal{U}$ obey the disjunction and conjunction rules—(189), (190), (195), and (196)—which give rise, in turn, to expanded distributivity theorems of $\neg$ over $\mathcal{W}$ and $\mathcal{U}$, (197) to (202). The conjunction and disjunction rules do not appear in other LTL systems.

(188) **Right distributivity of $\mathcal{W}$ over $\Rightarrow$:** $(p \Rightarrow q)\ \mathcal{W}\ r \Rightarrow (p\ \mathcal{W}\ r \Rightarrow q\ \mathcal{W}\ r)$,

(189) **Disjunction rule of $\mathcal{W}$:** $p\ \mathcal{W}\ q \equiv (p \vee q)\ \mathcal{W}\ q$,

(190) **Disjunction rule of $\mathcal{U}$:** $p\ \mathcal{U}\ q \equiv (p \vee q)\ \mathcal{U}\ q$,

(191) **Rule of $\mathcal{W}$:** $\neg q\ \mathcal{W}\ q$,

(192) **Rule of $\mathcal{U}$:** $\neg q\ \mathcal{U}\ q\ \equiv\ \Diamond q$,

(193) $(p \Rightarrow q)\ \mathcal{W}\ p$,

(194) $\Diamond p \Rightarrow (p \Rightarrow q)\ \mathcal{U}\ p$,

(195) **Conjunction rule of $\mathcal{W}$:** $p\ \mathcal{W}\ q \equiv (p \wedge \neg q)\ \mathcal{W}\ q$,

(196) **Conjunction rule of $\mathcal{U}$:** $p\ \mathcal{U}\ q \equiv (p \wedge \neg q)\ \mathcal{U}\ q$,

(197) **Distributivity of $\neg$ over $\mathcal{W}$:** $\neg(p\ \mathcal{W}\ q) \equiv (p \wedge \neg q)\ \mathcal{U}\ (\neg p \wedge \neg q)$,

(198) **Distributivity of $\neg$ over $\mathcal{U}$:** $\neg(p\ \mathcal{U}\ q) \equiv (p \wedge \neg q)\ \mathcal{W}\ (\neg p \wedge \neg q)$,

(199) **Dual of $\mathcal{U}$:** $\neg(\neg p\ \mathcal{U}\ \neg q) \equiv q\ \mathcal{W}\ (p \wedge q)$,

(200) **Dual of $\mathcal{U}$:** $\neg(\neg p\ \mathcal{U}\ \neg q) \equiv (\neg p \wedge q)\ \mathcal{W}\ (p \wedge q)$,

(201) **Dual of $\mathcal{W}$:** $\neg(\neg p\ \mathcal{W}\ \neg q) \equiv q\ \mathcal{U}\ (p \wedge q)$,

(202) **Dual of $\mathcal{W}$:** $\neg(\neg p\ \mathcal{W}\ \neg q) \equiv (\neg p \wedge q)\ \mathcal{U}\ (p \wedge q)$.

Theorem (203) shows that the *wait* operator, like the *until* operator, is idempotent. Theorem (204) shows that *true* is the right zero of *wait*, as it is for *until*. Theorem (205) shows that *false* is the left identity of *wait*, as it is for *until*. Theorem (206) for the *wait* operator corresponds to Theorem (28) for the *until* operator and shows that $p\ \mathcal{W}\ q$ is stronger than $p \vee q$. Theorem (207) shows that $\Box(p \vee q)$ is stronger than $p\ \mathcal{W}\ q$. Theorem (209), insertion for the *wait* operator, corresponds to (29), insertion for the *until* operator.

(203) **Idempotency of $\mathcal{W}$:** $p\ \mathcal{W}\ p \equiv p$,

(204) **Right zero of $\mathcal{W}$:** $p\ \mathcal{W}\ \mathit{true} \equiv \mathit{true}$,

(205) **Left identity of $\mathcal{W}$:** $\mathit{false}\ \mathcal{W}\ q \equiv q$,

(206) $p\ \mathcal{W}\ q \Rightarrow p \vee q$,

(207) $\Box(p \vee q) \Rightarrow p\ \mathcal{W}\ q$,

(208) $\Box(\neg q \Rightarrow p) \Rightarrow p\ \mathcal{W}\ q$,

(209) **$\mathcal{W}$ insertion:** $q \Rightarrow p\ \mathcal{W}\ q$.

The next three theorems (210), (211), and (212) complete the set of frame laws that included the theorems from (106) to (117) for binary propositional operators, and the $\mathcal{U}$ frame laws from theorems (148), (149), and (150).

(210) **$\mathcal{W}$ frame law of $\bigcirc$:** $\Box p \Rightarrow (\bigcirc q \Rightarrow \bigcirc(p\ \mathcal{W}\ q))$,

(211) **$\mathcal{W}$ frame law of $\Diamond$:** $\Box p \Rightarrow (\Diamond q \Rightarrow \Diamond(p\ \mathcal{W}\ q))$,

(212) **$\mathcal{W}$ frame law of $\Box$:** $\Box p \Rightarrow (\Box q \Rightarrow \Box(p\ \mathcal{W}\ q))$.

Here are four induction theorems for $\mathcal{W}$, the last two of which are unique to this system.

(213) **$\mathcal{W}$ induction:** $\Box(p \Rightarrow (\bigcirc p \wedge q) \vee r) \Rightarrow (p \Rightarrow q\ \mathcal{W}\ r)$,

(214) **$\mathcal{W}$ induction:** $\Box(p \Rightarrow \bigcirc(p \vee q)) \Rightarrow (p \Rightarrow p\ \mathcal{W}\ q)$,

(215) **$\mathcal{W}$ induction:** $\Box(p \Rightarrow \bigcirc p) \Rightarrow (p \Rightarrow p\ \mathcal{W}\ q)$,

(216) **$\mathcal{W}$ induction:** $\Box(p \Rightarrow q \wedge \bigcirc p) \Rightarrow (p \Rightarrow p\ \mathcal{W}\ q)$.

The next five absorption theorems correspond to the five absorption theorems for *until*, (31), (32), (33), (35), and (34), respectively. None appear in other LTL systems.

(217) **Absorption:** $p \vee p\ \mathcal{W}\ q \equiv p \vee q$,

(218) **Absorption:** $p\ \mathcal{W}\ q \vee q \equiv p\ \mathcal{W}\ q$,

(219) **Absorption:** $p\ \mathcal{W}\ q \wedge q \equiv q$,

(11) Right zero of $\mathcal{U}$: $p\ \mathcal{U}\ false \equiv false$	(183) Left zero of $\mathcal{W}$: $true\ \mathcal{W}\ q \equiv true$
(20) Right zero of $\mathcal{U}$: $p\ \mathcal{U}\ true \equiv true$	(204) Right zero of $\mathcal{W}$: $p\ \mathcal{W}\ true \equiv true$
(21) Left identity of $\mathcal{U}$: $false\ \mathcal{U}\ q \equiv q$	(205) Left identity of $\mathcal{W}$: $false\ \mathcal{W}\ q \equiv q$
(38) $true\ \mathcal{U}\ q \equiv \Diamond q$	(224) $\Box$ to $\mathcal{W}$ law: $p\ \mathcal{W}\ false \equiv \Box p$

Fig. 4. The eight possibilities of *true* and *false* on the left-hand side and right-hand side of $\mathcal{U}$ and $\mathcal{W}$.

(220) **Absorption:** $p\ \mathcal{W}\ q \wedge (p \vee q) \equiv p\ \mathcal{W}\ q$,

(221) **Absorption:** $p\ \mathcal{W}\ q \vee (p \wedge q) \equiv p\ \mathcal{W}\ q$.

The left and right absorption theorems for $\mathcal{W}$, (222) and (223), correspond to, and are proved from, the left and right absorption theorems for $\mathcal{U}$, (36) and (37). Theorem (224) corresponds to the definition of the $\Diamond$ operator (38). Figure 4 summarizes the eight possibilities of *true* and *false* on the left-hand side and right-hand side of $\mathcal{U}$ and $\mathcal{W}$.

(222) **Left absorption of $\mathcal{W}$:** $p\ \mathcal{W}\ (p\ \mathcal{W}\ q) \equiv p\ \mathcal{W}\ q$,

(223) **Right absorption of $\mathcal{W}$:** $(p\ \mathcal{W}\ q)\ \mathcal{W}\ q \equiv p\ \mathcal{W}\ q$,

(224) **$\Box$ to $\mathcal{W}$ law:** $\Box p \equiv p\ \mathcal{W}\ false$,

(225) **$\Diamond$ to $\mathcal{W}$ law:** $\Diamond p \equiv \neg(\neg p\ \mathcal{W}\ false)$.

Theorem (226) for $\mathcal{W}$ corresponds to (84) $\mathcal{U}$ implication. It is also known as an entailment law for the *wait* operator [24]. The following four absorption theorems combine an *until* operation with a *wait* operation. Theorem (231) corresponds to (141) Absorption of $\mathcal{U}$ into $\Box$. Theorem (232) corresponds to (40) Absorption of $\mathcal{U}$ into $\Diamond$. Theorem (233) corresponds to (39) Absorption of $\Diamond$ into $\mathcal{U}$.

(226) **$\mathcal{W}$ implication:** $p\ \mathcal{W}\ q \Rightarrow \Box p \vee \Diamond q$,

(227) **Absorption:** $p\ \mathcal{W}\ (p\ \mathcal{U}\ q) \equiv p\ \mathcal{W}\ q$,

(228) **Absorption:** $(p\ \mathcal{U}\ q)\ \mathcal{W}\ q \equiv p\ \mathcal{U}\ q$,

(229) **Absorption:** $p\ \mathcal{U}\ (p\ \mathcal{W}\ q) \equiv p\ \mathcal{W}\ q$,

(230) **Absorption:** $(p\ \mathcal{W}\ q)\ \mathcal{U}\ q \equiv p\ \mathcal{U}\ q$,

(231) **Absorption of $\mathcal{W}$ into $\Diamond$:** $\Diamond q\ \mathcal{W}\ q \equiv \Diamond q$,

(232) **Absorption of $\mathcal{W}$ into $\Box$:** $\Box p \wedge p\ \mathcal{W}\ q \equiv \Box p$,

(233) **Absorption of $\Box$ into $\mathcal{W}$:** $\Box p \vee p\ \mathcal{W}\ q \equiv p\ \mathcal{W}\ q$.

The next two pairs of theorems correspond. The *wait* versions are in the temporal logic literature. The *until* versions are unique to this system. The monotonicity theorems and the strengthening and catenation rules are common. The implication rules (242) to (245) are unique to this system.

(234) $p\ \mathcal{W}\ q \wedge \Box \neg q \Rightarrow \Box p$,

(235) $\Box p \Rightarrow p\ \mathcal{U}\ q \vee \Box \neg q$,

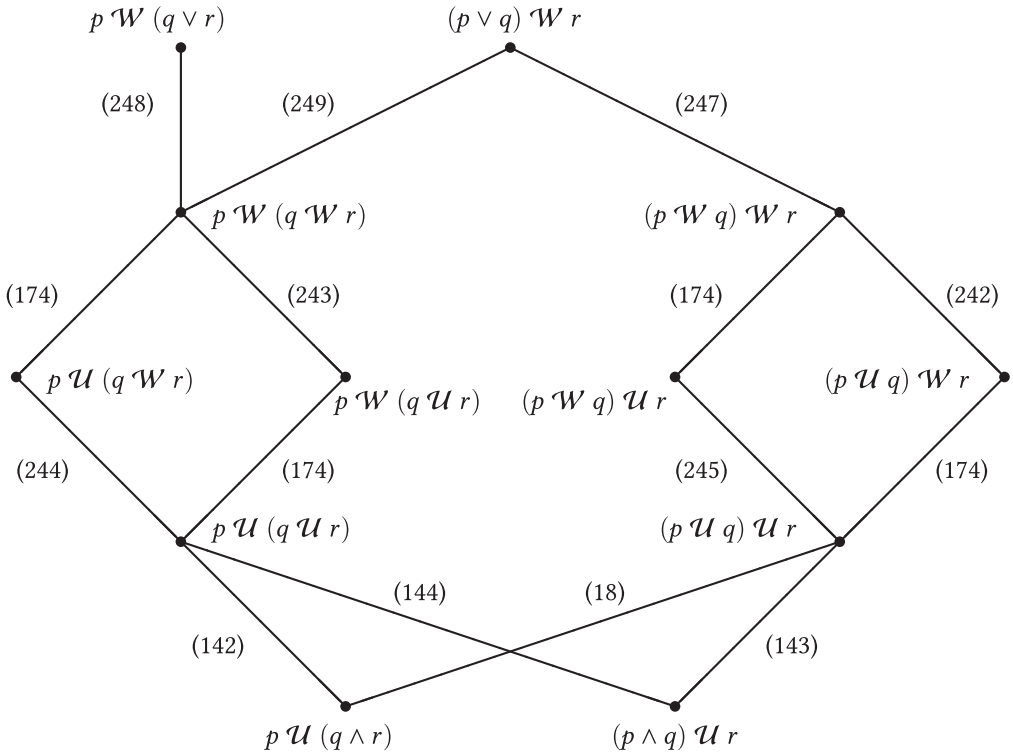

Fig. 5. A Hasse diagram showing some implication relations of linear temporal logic.

(236) $\neg\Box p \wedge p \mathcal{W} q \Rightarrow \Diamond q$,

(237) $\Diamond q \Rightarrow \neg\Box p \vee p \mathcal{U} q$,

(238) **Left monotonicity of $\mathcal{W}$:** $\Box(p \Rightarrow q) \Rightarrow (p \mathcal{W} r \Rightarrow q \mathcal{W} r)$,

(239) **Right monotonicity of $\mathcal{W}$:** $\Box(p \Rightarrow q) \Rightarrow (r \mathcal{W} p \Rightarrow r \mathcal{W} q)$,

(240) **$\mathcal{W}$ strengthening rule:** $\Box((p \Rightarrow r) \wedge (q \Rightarrow s)) \Rightarrow (p \mathcal{W} q \Rightarrow r \mathcal{W} s)$,

(241) **$\mathcal{W}$ catenation rule:** $\Box((p \Rightarrow q \mathcal{W} r) \wedge (r \Rightarrow q \mathcal{W} s)) \Rightarrow (p \Rightarrow q \mathcal{W} s)$,

(242) **Left $\mathcal{U}$ $\mathcal{W}$ implication:** $(p \mathcal{U} q) \mathcal{W} r \Rightarrow (p \mathcal{W} q) \mathcal{W} r$,

(243) **Right $\mathcal{W}$ $\mathcal{U}$ implication:** $p \mathcal{W} (q \mathcal{U} r) \Rightarrow p \mathcal{W} (q \mathcal{W} r)$,

(244) **Right $\mathcal{U}$ $\mathcal{U}$ implication:** $p \mathcal{U} (q \mathcal{U} r) \Rightarrow p \mathcal{U} (q \mathcal{W} r)$,

(245) **Left $\mathcal{U}$ $\mathcal{U}$ implication:** $(p \mathcal{U} q) \mathcal{U} r \Rightarrow (p \mathcal{W} q) \mathcal{U} r$.

Of the three strengthening rules, only (247) appears in the LTL literature. All of the following ordering rules are in the literature except for (251) $\mathcal{U}$ ordering. Figure 5 is a Hasse diagram showing some implication relations of these theorems.

(246) **Left $\mathcal{U}$ $\vee$ strengthening:** $(p \mathcal{U} q) \mathcal{U} r \Rightarrow (p \vee q) \mathcal{U} r$,

(247) **Left $\mathcal{W}$ $\vee$ strengthening:** $(p \mathcal{W} q) \mathcal{W} r \Rightarrow (p \vee q) \mathcal{W} r$,

(248) **Right $\mathcal{W}$ $\vee$ strengthening:** $p\ \mathcal{W}\ (q\ \mathcal{W}\ r) \Rightarrow p\ \mathcal{W}\ (q \vee r)$,

(249) **Right $\mathcal{W}$ $\vee$ ordering:** $p\ \mathcal{W}\ (q\ \mathcal{W}\ r) \Rightarrow (p \vee q)\ \mathcal{W}\ r$,

(250) **Right $\wedge$ $\mathcal{W}$ ordering:** $p\ \mathcal{W}\ (q \wedge r) \Rightarrow (p\ \mathcal{W}\ q)\ \mathcal{W}\ r$,

(251) **$\mathcal{U}$ ordering:** $\neg p\ \mathcal{U}\ q \vee \neg q\ \mathcal{U}\ p \equiv \Diamond (p \vee q)$,

(252) **$\mathcal{W}$ ordering:** $\neg p\ \mathcal{W}\ q \vee \neg q\ \mathcal{W}\ p$,

(253) **$\mathcal{W}$ implication ordering:** $p\ \mathcal{W}\ q \wedge \neg q\ \mathcal{W}\ r \Rightarrow p\ \mathcal{W}\ r$,

(254) **Lemmon formula:** $\Box (\Box p \Rightarrow q) \vee \Box (\Box q \Rightarrow p)$.

Proof: The proof is by (4.7.1) Truth implication.

$$
\begin{array}{ll}
 & \Box (\Box p \Rightarrow q) \vee \Box (\Box q \Rightarrow p) \\
= & \quad \langle (3.59)\ \text{Implication}\ p \Rightarrow q\ \equiv\ \neg p \vee q, \text{twice} \rangle \\
 & \Box (\neg \Box p \vee q) \vee \Box (\neg \Box q \vee p) \\
\Leftarrow & \quad \langle (206)\ \text{twice}, (120)\ \text{Monotonicity of}\ \Box, \text{and}\ (4.2)\ \text{Monotonicity of}\ \vee \rangle \\
 & \Box (\neg \Box p\ \mathcal{W}\ q) \vee \Box (\neg \Box q\ \mathcal{W}\ p) \\
\Leftarrow & \quad \langle (177)\ \mathcal{W}\ \Box\ \text{implication and}\ (4.2)\ \text{Monotonicity of}\ \vee \rangle \\
 & \neg \Box p\ \mathcal{W}\ \Box q \vee \neg \Box q\ \mathcal{W}\ \Box p \\
= & \quad \langle (252)\ \mathcal{W}\ \text{ordering with}\ p, q := \Box p, \Box q \rangle \\
 & \mathit{true}\ \blacksquare
\end{array}
$$

The 10 axioms that define the behavior of the *until* operator are (9), (10), (11), (12), (13), (14), (15), (16), (17), and (18). The corresponding theorems for the *wait* operator are (180), (181), (224), (184), (185), (186), (187), (253), (249), and (250). Of these 10 theorems, 9 are identical, with the substitution of $\mathcal{W}$ for $\mathcal{U}$, to the corresponding axioms that define the *until* operator. In addition, (170), the axiom that describes the distributivity of $\neg$ over $\mathcal{W}$, is identical to (173) with the interchange of $\mathcal{W}$ and $\mathcal{U}$. The one theorem that distinguishes $\mathcal{W}$ from the defining axioms of $\mathcal{U}$ is

(11) **Axiom, Right zero of $\mathcal{U}$:** $p\ \mathcal{U}\ \mathit{false} \equiv \mathit{false}$

for the *until* operator versus

(224) **$\Box$ to $\mathcal{W}$ law:** $\Box p \equiv p\ \mathcal{W}\ \mathit{false}$

for the *wait* operator.

4 COMPARISON WITH PREVIOUS WORK

Linear temporal logic is just one of many different modal logic systems. This section shows how linear temporal logic fits in general systems of modal logic, how calculational logic applies to modal logic, and compares this system with other LTL axiomatizations.

4.1 Modal Logic Systems

In the terminology of modal logic, each state of an anchored sequence is called a *world*. In LTL, each world represents the state of a computation at each discrete point in time, and so one world is related to another world as one point in time is related to another point in time, i.e., as occurring before or after it. In general, worlds need not have such an interpretation. Rather, a specific modal logic system is defined by a nonempty set of worlds W and a relation ρ over W. A frame is the ordered pair $\langle W, \rho \rangle$, and different modal systems are specified by different frames.

The most general modal system, known as K, extends propositional calculus by adding the unary operator $\Box$ together with the axiom $\Box(p \Rightarrow q) \Rightarrow (\Box p \Rightarrow \Box q)$, which is our theorem (120) Monotonicity of $\Box$. The Hilbert style inference rules of Uniform Substitution and modus ponens are extended by adding the rule of Necessitation: If P is a theorem, then so is $\Box P$, which is Case 1 of our (136) Metatheorem. The operator $\Diamond p$ is defined to be an abbreviation for $\neg\Box\neg p$ as in (59). With these extensions, there is no restriction on relation ρ in the frame $\langle W, \rho\rangle$ that defines K.

A stronger modal system, known as T, extends K by adding the axiom $\Box p \Rightarrow p$, sometimes called the Axiom of Necessity, which is our theorem (76). Every theorem in K is also a theorem in T, but not every theorem in T is a theorem in K. It has been shown that theorems in T are valid on every frame $\langle W, \rho\rangle$ in which ρ is reflexive, i.e., in which for all $w \in W$, $w\rho w$ [18].

A stronger yet modal system, known as S4, extends T by adding the single extra axiom $\Box p \Rightarrow \Box\Box p$, which is part of our theorem (72) Absorption of $\Box$, $\Box\Box p \equiv \Box p$ by virtue of mutual implication. Theorems in S4 are valid on every frame $\langle W, \rho\rangle$ in which ρ is both reflexive and transitive, i.e., in which for all $w, x, y \in W$, $w\rho x \wedge x\rho y \Rightarrow w\rho y$.

Linear temporal systems model time as discrete points on the number line. Each world is on a time line and is either contemporaneous with, or earlier than, itself and all worlds that come after it. This "earlier than" relation is defined formally as a connected relation, in which for all $w, x, y \in W$, $w\rho x \wedge w\rho y \Rightarrow x\rho y \vee y\rho x$. In other words, if w is contemporaneous with or earlier than x, and w is contemporaneous with or earlier than y, then either x is contemporaneous with or earlier than y, or y is contemporaneous with or earlier than x. The temporal modal system, known as S4.3 [8], extends S4 by the axiom $\Box(\Box p \Rightarrow q) \vee \Box(\Box q \Rightarrow p)$, which is our theorem (254) Lemmon formula. Theorems in S4.3 are valid on every frame $\langle W, \rho\rangle$ in which ρ is reflexive, transitive, and connected [18].

The Lemmon formula imposes linearity of the time line. The Dummett formula

$$\Box(\Box(p \Rightarrow \Box p) \Rightarrow \Box p) \Rightarrow (\Diamond\Box p \Rightarrow \Box p)$$

imposes discreteness of the time line [9, 22]. The modal system S4.3 with the addition of the Dummett formula is known as S4.3*Dum*. Our LTL system contains S4.3, because it includes as theorems the axioms of S4.3. The LTL systems we survey are close to S4.3*Dum* but do not contain the Dummett formula as an axiom. Instead, discreteness of the time line is implicit in the definition of the *next* operator $\bigcirc$. The binary operators *until* $\mathcal{U}$ and *wait* $\mathcal{W}$ are absent in classical modal logic systems.

4.2 Calculational Modal Logic Systems

Gries and Schneider [15, 16] describe the benefits of the calculational system for propositional logic and its application to discrete math. Gries and Schneider [14] and Tourlakis [25] demonstrate the soundness and completeness of such systems. The calculational method is the subject of a special issue in Reference [1].

Gries and Schneider [17] extend calculational logic to the Carnapian modal system known as C. Theorems in C are valid on every frame $\langle W, \rho\rangle$ in which ρ is the universal accessibility relation, i.e., each state is related to all states. Because C is not a linear temporal logic, the operator $\Box$ has a different interpretation from that in LTL. Denoting the Carnapian operator as $\Box_c$ the interpretation of $\Box_c P$, where P is a propositional logic expression, is "P is true in all states," or, equivalently, "P is valid." Gries and Schneider point out that this logic "… can be used for proving theorems that could otherwise be handled only at the meta-level, and most likely informally." As an example, (2.3b) Metatheorem Duality, $P \equiv Q$ is valid iff $P_D \equiv Q_D$ is valid, can be written as $\Box_c(P \equiv Q) \equiv \Box_c(P_D \equiv Q_D)$. In such a system, metatheorems become formulas in the logic and are thus directly available for use in calculational reasoning.

Schneider's graduate text *On Concurrent Programming* [24] extends the calculational logic system to linear temporal logic. It claims, and we concur, that "... proofs in Temporal Logic are often easier to read and to construct when an equational format is available." As justification for the extension, it gives a temporal logic analogue of (I1) Leibniz, TL Substitution of Equals. For proof steps that assert $p \Rightarrow q$, it gives two additional temporal logic rules: TL Monotonicity Rule and TL Antimonotonicity Rule. These rules are the basis for the justification of temporal logic calculational proofs.

4.3 Survey of LTL Deductive Systems

As a check on comprehensiveness, we inventoried the linear temporal logic theorems and inference rules in Ben-Ari [4], Emerson [10], Kröger and Merz [20], Manna and Pnueli [21], and Schneider [24], and included them all in this survey. This section compares the axiomatization systems of those sources with this work.

Ben-Ari [4] takes the temporal operators $\Box$, $\bigcirc$, and $\mathcal{U}$ as basic and defines $\Diamond$ to be an abbreviation for $\neg\Box\neg$ as in (59). The $\mathcal{W}$ operator is not covered in his system for LTL.

The two stated rules of inference in the Ben-Ari deductive system correspond to (3.77) Modus ponens and the generalization part of (136) Metatheorem. The five axioms that define $\bigcirc$ and $\Box$ correspond to (120) Monotonicity of $\Box$, (2) Distributivity of $\bigcirc$ over $\Rightarrow$, (67) Expansion of $\Box$, (57) $\Box$ Induction, and (3) Linearity. The two axioms that define $\mathcal{U}$ correspond to (10) Expansion of $\mathcal{U}$ and (42) Eventuality.

Emerson [10] uses the symbol X to denote the *next* operator, F to denote *eventually*, and G to denote *always*. He also writes $\overset{\infty}{\mathrm{F}}$ to denote *always eventually* and $\overset{\infty}{\mathrm{G}}$ to denote *eventually always*. With these conventions $\Box p \equiv p \wedge \bigcirc \Box p$ is written as $\mathrm{G}\ p \equiv p \wedge \mathrm{X}\ \mathrm{G}\ p$, and $\neg\Diamond\Box p \equiv \Box\Diamond\neg p$ is written as $\neg\overset{\infty}{\mathrm{G}} p \equiv \overset{\infty}{\mathrm{F}}\ \neg p$. Emerson's notation for the *until* operator is **U**, which is sometimes written $\mathbf{U}_\exists$ to distinguish it from the *wait* operator, which is written $\mathbf{U}_\forall$. With these conventions $p\ \mathcal{U}\ q \equiv p\ \mathcal{W}\ q \wedge \Diamond q$ is written as $p\ \mathbf{U}_\exists\ q \equiv p\ \mathbf{U}_\forall\ q \wedge \mathrm{F}\ q$.

Emerson's deductive system is for Computational Tree Logic (CTL), which is a system of branching time logic. In contrast to linear time logics, which model time as an anchored sequence of states, branching time logics model time as a tree structure where at each point in time the computation may split into several possible future states. CTL extends LTL to multiple timelines (branches) through the addition of two additional quantifiers over these branches, A (for all futures) and E (for some futures). Consequently, Emerson's deductive system does not directly apply to LTL. The CTL inference rules and axioms without the additional quantifiers, however, do correspond to the LTL deductive system of our system as follows:

As with the LTL system of Ben-Ari, the two stated rules of inference correspond to (3.77) Modus ponens and the generalization part of (136) Metatheorem. The nine axioms correspond to (38) Definition of $\Diamond$, (54) Definition of $\Box$, (4) Distributivity of $\bigcirc$ over $\vee$, (3) Linearity, (10) Expansion of $\mathcal{U}$, (7) Truth of $\bigcirc$, (129) and (130) Induction rules $\Box$ and $\mathcal{U}$, and (118) Monotonicity of $\bigcirc$.

Kröger and Merz [20] use the symbol **unt** (an abbreviation for until) to denote the *until* operator $\mathcal{U}$ and the symbol **unl** (an abbreviation for unless) to denote the *wait* operator $\mathcal{W}$. They call these *non-strict* operators in contrast to variations of the operators termed *strict* operators.

Kröger and Merz first define a *propositional linear temporal logic* consisting of only the unary temporal operators $\bigcirc$ and $\Box$. They define $\Diamond p$ to be an abbreviation for $\neg\Box\neg p$ as in (59). The three inference rules correspond to (3.77) Modus ponens, (78) Strengthening of $\Box$, and (129) Induction rule $\Box$. The three axioms correspond to (1) Self-dual, (2) Distributivity of $\bigcirc$ over $\Rightarrow$, and (66) Expansion of $\Box$. They introduce the *until* operator and the *wait* operator as an extension

to the propositional linear temporal logic. The four axioms for the extension correspond to (10) Expansion of $\mathcal{U}$, (42) Eventuality, (181) Expansion of $\mathcal{W}$, and (179) Perpetuity.

Manna and Pnueli [21] use the $\rightarrow$ symbol for implication, so that $p \Rightarrow q$ of our system is written as $p \rightarrow q$ in theirs. They introduce the symbol $\Rightarrow$ to stand for always implies, so that $\Box(p \rightarrow q)$ is written as $p \Rightarrow q$ in their system. Similarly, $p \equiv q$ of our system is written as $p \leftrightarrow q$ in theirs and $\Box(p \leftrightarrow q)$ is written as $p \Leftrightarrow q$.

Manna and Pnueli define a proof system that combines the future operators $\bigcirc$, $\Diamond$, $\Box$, $\mathcal{U}$, and $\mathcal{W}$ with a set of corresponding past operators. For the future operators they take $\bigcirc$ and $\mathcal{W}$ as basic and define $\Box p$ to be an abbreviation for $p\ \mathcal{W}\ \mathit{false}$ as in (224), $\Diamond p$ to be an abbreviation for $\neg\Box\neg p$ as in (59), and $p\ \mathcal{U}\ q$ to be an abbreviation for $p\ \mathcal{W}\ q \wedge \Diamond q$ as in (171).

The four basic inference rules in the Manna and Pnueli deductive system are generalization and specialization, corresponding to (136) Metatheorem, instantiation, corresponding to inference rule Substitution (Section 2.1), and modus ponens, corresponding to (3.77). The derived rules include particularization, corresponding to (76) Strengthening of $\Box$, entailment modus ponens, corresponding to $\Box(p \Rightarrow q) \wedge \Box p \Rightarrow \Box q$, and entailment transitivity, corresponding to $\Box(p \Rightarrow q) \wedge \Box(q \Rightarrow r) \Rightarrow \Box(p \Rightarrow r)$. The last two expressions are easy to prove from (120) Monotonicity of $\Box$.

Their eight future axioms correspond to (76) Strengthening of $\Box$, (1) Self-dual, (2) Distributivity of $\bigcirc$ over $\Rightarrow$, (120) Monotonicity of $\Box$, (80) $\bigcirc$ generalization, (57) $\Box$ Induction, (181) Expansion of $\mathcal{W}$, and (179) Perpetuity.

Schneider [24] is the only treatment of LTL that is based on the calculational deductive system developed in Gries and Schneider's LADM [13]. He does not consider the *until* operator $\mathcal{U}$ (apart from an exercise for the student) but uses the symbol $\mathcal{U}$ for the *wait* operator. The expression $p\ \mathcal{W}\ q$ is written $p\ \mathcal{U}\ q$ and read "p unless q."

The rules of inference in Schneider's deductive system include TL substitution, corresponding to inference rule Substitution, TL Modus ponens, corresponding to (3.77) Modus ponens, and Temporal generalization rule, corresponding to the generalization part of (136) Metatheorem. There are also a set of derived inference rules corresponding to (123) Consequence rule of $\Box$, (125) Catenation rule of $\Box$, (122) Consequence rule of $\Diamond$, (124) Catenation rule of $\Diamond$, (121) Consequence rule of $\bigcirc$, (57) $\Box$ Induction, and (129) Induction rule $\Box$.

Schneider's deductive system consists of two axioms for $\Box$ corresponding to (76) Strengthening of $\Box$ and (120) Monotonicity of $\Box$. It defines $\Diamond$ as in theorem (59). It has five axioms for $\bigcirc$ corresponding to (1) Self-dual, (2) Distributivity of $\bigcirc$ over $\Rightarrow$, (78) Strengthening of $\Box$, (79) Strengthening of $\Box$, and (57) $\Box$ Induction. The two axioms for the *wait* operator correspond to (179) Perpetuity and (181) Expansion of $\mathcal{W}$.

A striking feature of this survey is how each author chooses to include a set of theorems that all other authors omit. Ben-Ari has 13 unique theorems, Emerson has 14, Kröger and Merz have 10, Manna and Pnueli have 18, and Schneider has 19. There are 19 theorems that are common to all five sources in the survey—namely, (1), (2), (4), (5), (45), (46), (50), (51), (52), (66), (72), (73), (76), (78), (99), (119), (120), (151), and (152).

This system includes all the theorems from the survey. It has 254 theorems, 18 of which are axioms. Of the axioms, six are theorems that do not appear in other LTL systems—namely, (11), (16), (17), (18), (55), and (56).

5 CONCLUSION

Dijkstra and Scholten [7], and Feijen [11] originally developed $\mathcal{E}$ as a logic system to prove program correctness based on a calculational style. Gries and Schneider [13] extend that system to a theory

of sets, a theory of sequences, relations and functions, a theory of integers, recurrence relations, modern algebra, and a theory of graphs. Similarly, this system extends $\mathcal{E}$ to a theory of linear temporal logic. It takes unary operator *next* $\circ$ and binary operator *until* $\mathcal{U}$ as primitives and defines *eventually* $\diamond$, *always* $\Box$, and *wait* $\mathcal{W}$ in terms of them.

The calculational deductive system $\mathcal{E}$ has several advantages over other logic systems. The primary advantage is that the calculational system has only four inference rules. Consequently, proofs of theorems are easier to understand and more intuitive to those schooled in that system. One goal of this basic introduction is to make linear temporal logic accessible at the undergraduate level.

Many users of LTL are concerned with the scalability of reasoning and automated theorem proving. In contrast, the goal of this project is to make manual proofs accessible to human users. It would be an interesting area for future research to determine if and/or how the calculational system might be applied to LTL synthesis.

In our judgment, the progress we were able to make in exploring the structure of linear temporal systems is directly attributable to our training in the calculational deductive system $\mathcal{E}$. We believe the advantages of $\mathcal{E}$ over other logic systems is so substantial that it should be the tool of choice for computer science theory. We hope that this extension of $\mathcal{E}$ to linear temporal logic will not only be of use in the temporal logic community, but will serve as an example to promote $\mathcal{E}$ in the broader computer science community.

ACKNOWLEDGMENTS

The authors would like to thank David Gries, who provided a prepublication manuscript of LADM, which we immediately adopted and have used at our institution ever since. He has been a source of constant encouragement over the years. David Gries and Fred Schneider provided valuable comments on draft manuscripts of this article. Mordechai Ben-Ari's text [3] inspired us to use LTL to teach concurrent programming principles. Fred Schneider's graduate-level text [24] inspired us to create this calculational system to be accessible at the undergraduate level. Ray McIntyre, Ravi Mohan, Michael Ortiz, and Kyle Sundman contributed to the proofs.

REFERENCES

[1] Roland Backhouse, D. Gries, W. M. Turski, and F. Dehne (Eds.). 1995. Special issue on the calculational method. *Inf. Process. Lett.* 53, 3 (1995).

[2] Christel Baier and Joost-Pieter Katoen. 2008. *Principles of Model Checking*. The MIT Press, Cambridge, MA.

[3] Mordechai Ben-Ari. 2006. *Principles of Concurrent and Distributed Programming* (2nd ed.). Addison-Wesley Pearson, Harlow, England.

[4] Mordechai Ben-Ari. 2012. *Mathematical Logic for Computer Science* (3rd ed.). Springer-Verlag, London.

[5] Edward Cohen. 1990. *Programming in the 1990's: An Introduction to the Calculation of Programs*. Springer-Verlag, New York.

[6] Edsger W. Dijkstra. 1968. Letters to the editor: Go to statement considered harmful. *Commun. ACM* 11, 3 (Mar. 1968), 147–148. DOI: https://doi.org/10.1145/362929.362947

[7] Edsger W. Dijkstra and Carel S. Scholten. 1990. *Predicate Calculus and Program Semantics*. Springer-Verlag, New York.

[8] M. A. E. Dummett and E. J. Lemmon. 1959. Modal logics between S4 and S5. *Zeitsch. Math. Logik Grund. Math.* 5 (1959), 250–64.

[9] Michael A. E. Dummett. 1978. *Truth and Other Enigmas*. Harvard University Press, Cambridge, MA.

[10] E. Allen Emerson. 1990. *Handbook of Theoretical Computer Science (Vol. B)*. The MIT Press, Cambridge, MA, Chapter: "Temporal and Modal Logic," 995–1072. Retrieved from http://dl.acm.org/citation.cfm?id=114891.114907.

[11] Wim H. H. Feijen. 1990. Exercises in formula manipulation. In *Formal Development of Programs*, E. W. Dijkstra (Ed.). Addison-Wesley, Menlo Park, NJ, 139–158.

[12] David Gries. 1999. Monotonicity in calculational proofs. In *Correct System Design, Recent Insight and Advances, (to Hans Langmaack on the Occasion of His Retirement from His Professorship at the University of Kiel)*. Springer-Verlag, Berlin, 79–85. Retrieved from http://dl.acm.org/citation.cfm?id=646005.673872.

[13] David Gries and Fred B. Schneider. 1994. *A Logical Approach to Discrete Math*. Springer-Verlag, New York.

[14] David Gries and Fred B. Schneider. 1995. Equational propositional logic. *Inform. Process. Lett.* 53, 3 (1995), 145–152.

[15] David Gries and Fred B. Schneider. 1995. A new approach to teaching discrete mathematics. *PRIMUS* 5, 2 (1995), 113–138. DOI: https://doi.org/10.1080/10511979508965779
[16] David Gries and Fred B. Schneider. 1995. Teaching math more effectively, through calculational proofs. *Amer. Math. Month.* 102, 8 (1995), 691–697. Retrieved from http://www.jstor.org/stable/2974638.
[17] David Gries and Fred B. Schneider. 1998. Adding the everywhere operator to propositional logic. *J. Logic Comput.* 8 (12 1998).
[18] G. E. Hughes and M. J. Cresswell. 1996. *A New Introduction to Modal Logic*. Routledge, New York.
[19] Anne Kaldewaij. 1990. *Programming: The Derivation of Algorithms*. Prentice-Hall International (UK) Ltd., Hertfordshire, UK.
[20] Fred Kröger and Stephan Merz. 2008. *Temporal Logic and State Systems*. Springer-Verlag, Berlin.
[21] Zohar Manna and Amir Pnueli. 1992. *The Temporal Logic of Reactive and Concurrent Systems: v. 1, Specification*. Springer-Verlag, New York.
[22] Arthur N. Prior. 1967. *Past, Present and Future*. Oxford University Press.
[23] Kenneth H. Rosen. 2007. *Discrete Mathematics and Its Applications* (6th ed.). McGraw-Hill, New York.
[24] Fred B. Schneider. 1997. *On Concurrent Programming*. Springer-Verlag, New York.
[25] George Tourlakis. 2001. On the soundness and completeness of equational predicate logics. *J. Logic Comput.* 11, 4 (2001), 623–653.

Received August 2019; revised March 2020; accepted March 2020