October 2009

Theorem Proving in the Propositional Algebra

Geoff Phillips

Introduction

This paper deals with "Propositional Logic" as described in (Fitting (1990)). The objects of Propositional Logic are so-called "well-formed formulas" (wffs) and the Classical Propositional Calculus (see Mendelson (1997)) is an axiomatic method for deciding whether one "well-formed formula" (wff) is a consequence of others. There is a variety of well established methods for determining the truth of theorems, in particular using the axioms and rules of inference to create proofs. "Propositional Algebra" refers to the Classical Positive Propositional Algebra (Curry (1977)), in which true statements are precisely the tautologies as determined in the ordinary two-valued Truth Tables. The appeal of studying this subject is that it formalises the process of the logical argument used in ordinary language, at least as far as Propositional Algebra is able to do so.

The process of proving theorems in the Propositional Algebra is an intuitive one, where rules of inference are selected by observation and axioms are used where they seem to be appropriate. Proving theorems in Euclidean geometry is approached in a similar way. By studying the process of proof in the Propositional Algebra, it may be possible to cast light on the intuitive approach usually employed.

Propositional Algebra

The letters of the alphabet are taken as elemental "well-formed formulas (wffs)" and more complex wffs can be constructed using the following and brackets ():

- a unary operator $\neg$ meaning "not"
- a binary operator $\wedge$ meaning "and"
- a binary operator $\vee$ meaning "or"
- a binary operator $\underline{\vee}$ meaning "exclusive or", and
- a binary operator $\supset$ meaning "implies"

The Propositional Algebra consists of these wffs together with a finite set of "rules of inference". A certain finite set of the wffs is identified as the axioms of the system. A proof is a sequence $A_1, A_2, ...A_n$ of wffs such that, for each i, either A_i is either an axiom or a direct consequence of some of the preceding wffs by virtue of one of the rules of inference. A theorem of the Propositional Algebra is such the A_n as above, which is not one of the axioms. The theorem can be denoted as $A_1 \Rightarrow A_n$.

The Propositional Algebra regarded as a set together with the structure provided by the operators $\neg$, $\wedge$, $\vee$ is called a Boolean Algebra.

Rewrite Systems and the Propositional Algebra

Rewrite systems (also called "term rewriting systems") (Benninghofen et al (1987)) are defined to be methods of replacing subterms of a formula with other terms. In the most basic form, a rewrite system consists of a set of terms, plus relations on how to transform these terms. Term rewriting can be non-deterministic, in the sense that there is no set way to apply the rewrite rules. Given an algorithm for applying the rules, rewrite systems provide a method of automating theorem proving.

An arrow notation $A \rightarrow B$ represents simplification of the formula on the left (and is also a *logical* equivalence). The application of a single rewrite rule is represented as $A \rightarrow B$. Application of a sequence of two or more rewrite steps, such as $A \rightarrow B$, $B \rightarrow C$ is represented as $A \rightarrow^* C$. Examples of rewrite rules in the Propositional Algebra are shown below.

De Morgan's Laws
$(A \wedge B) \vee C \rightarrow (A \vee C) \wedge (B \vee C)$
$A \vee (B \wedge C) \rightarrow (A \vee B) \wedge (A \vee C)$,
Distributivity
$\neg(A \wedge B) \rightarrow \neg A \vee \neg B$
$\neg(A \vee B) \rightarrow \neg A \wedge \neg B$,
Double negative elimination: $\neg\neg A \rightarrow A$

More about Rewrite Systems

Suppose the set of terms $T = A, B, C$ and the rules are $A \rightarrow B$, $B \rightarrow A$, $A \rightarrow C$, and $B \rightarrow C$ hold. From these rules, observe that these rules can be applied to both A and B in any order to get the term C. Note that C is, in a sense, a "simplest" term in the system, since nothing can be applied to C to transform it any further. Terms which cannot be written any further are called completely reduced forms. There are rewriting systems which do not have completely reduced forms: a very simple one is the rewriting system on two terms A and B with $A \rightarrow B$, $B \rightarrow A$.

The potential existence or uniqueness of completely reduced forms can be used to classify and describe certain rewriting systems. The existence of *unique* completely reduced forms is known as confluence. Let S be a set of terms and let $A, B, C \in S$, with $A \rightarrow^* B$ and $A \rightarrow^* C$. If A is confluent, there exists a $D \in S$ with $B \rightarrow^* D$ and $C \rightarrow^* D$. If every $A \in S$ is confluent, we say that $\rightarrow$ is confluent.

Boolean Rings

A Boolean ring R is a ring (with identity) for which $x^2 = x$ for all x in R; that is, R

consists only of idempotent elements.

Boolean rings are automatically commutative and of characteristic 2 (see below for proof). A Boolean ring is essentially the same thing as a Boolean algebra, with ring multiplication corresponding to conjunction or meet, and ring addition to exclusive disjunction or symmetric difference (not disjunction).

Examples of Boolean Rings

One example of a Boolean ring is the power set of any set X, where the addition in the ring is symmetric difference, and the multiplication is intersection.

Given a Boolean ring R, for x and y in R we can define:

$$x \wedge y = xy$$

$$x \vee y = x + y + xy$$

$$\neg x = 1 + x$$

These operations then satisfy all of the axioms for meets, joins, and complements in a Boolean algebra. Thus every Boolean ring becomes a Boolean algebra. Similarly, every Boolean algebra becomes a Boolean ring thus:

$$xy = x \wedge y$$

$$x + y = (x \vee y) \wedge \neg(x \wedge y)$$

If a Boolean ring is translated into a Boolean algebra in this way, and then the Boolean algebra translates back to the original Boolean ring. The analogous result holds beginning with a Boolean algebra. A map between two Boolean rings is a ring homomorphism if and only if it is a homomorphism of the corresponding Boolean algebras. Hence the category of Boolean algebras is isomorphic to the category of Boolean rings.

Some Properties of Boolean Rings

Every Boolean ring R satisfies x + x = 0 for all x in R, since

$$x + x = (x + x)^2 = x^2 + 2x^2 + x^2 = x + 2x + x = x + x + x + x$$

and since R is an abelian group, we can subtract $x+x$ from both sides of this equation, which gives $x+x = 0$. A similar proof shows that every Boolean ring is commutative:

$$x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$$

and this yields $xy + yx = 0$, which means $xy = yx$ (using the first property above).

The property $x + x = 0$ shows that any Boolean ring is an associative algebra over the field F_2 with two elements, in just one way.

Reduced Forms in the Propositional Algebra

The Boolean Ring representation allows reduction to unique completely reduced forms, which can then be translated into more meaningful expressions of the Propositional Algebra. Let A and B be propositions corresponding to elements a and b of a Boolean Ring. Then the following correspondences apply:

$$\begin{aligned} \neg A: &\quad 1 + a \\ A \wedge B: &\quad ab \\ A \vee B: &\quad a + b + ab \\ A \underline{\vee} B: &\quad a + b \\ A \supset B: &\quad 1 + a + ab \end{aligned}$$

Any expression in the Boolean Ring has an obvious "completely reduced form". For two variables, the sixteen completely reduced forms made up from $1, a, b$ and ab each correspond to at least one wff with no more than one occurrence of A and B. The complete set is shown in the Table below.

Completely Reduced Forms	
$0(False)$	0
$(A \wedge B)$	ab
$\neg(B \supset A)$	$b + ab$
$\neg(A \supset B)$	$a + ab$
$\neg(A \vee B)$	$1 + a + b + ab$
A	a
$\neg(A \underline{\vee} B)$	$1 + a + b$
B	b
$\neg A$	$1 + a$
$(A \underline{\vee} B)$	$a + b$
$\neg B$	$1 + b$
$(A \vee B)$	$a + b + ab$
$(A \supset B)$	$1 + a + ab$
$(B \supset A)$	$1 + b + ab$
$\neg(A \wedge B)$	$1 + ab$
$1(True)$	1

Some of the wffs are equivalent to other equally simple ones. For example $\neg(A \supset B)$ is equivalent to $A \wedge \neg B$. So $\neg(A \supset B)$ can be taken to be the representative of an equivalence class of equally simple forms. "Equally simple" means equally few occuences and variables and operators. For the Propositional Algebra, these equivalence classes correspond to the *unique* completely reduced forms in the Boolean Ring. Moreover, each completely reduced form corresponds to a particular pattern of zeros and ones in a four row Truth Table.

In the Boolean Ring representation, the wffs of the Propositional Algebra with n variables form a confluent rewrite system with exactly 2^{2^n} reduced forms of n or less variables. These reduced forms make up a complete lattice with implication ($\Rightarrow$) as the partial order of the lattice. Moreover, all other theorems (other than equivalences) between n variable forms can be reduced to these theorems among the reduced forms.

For the case of two variables, A and B, the lattice of reduced forms is set out below.

$$0(False)$$

$$(A \wedge B) \quad \neg(B \supset A) \quad \neg(A \supset B) \quad \neg(A \vee B)$$

$$A \qquad \neg(A \underline{\vee} B) \qquad B \qquad \neg A \qquad (A \underline{\vee} B) \qquad \neg B$$

$$(A \vee B) \quad (A \supset B) \quad (B \supset A) \quad \neg(A \wedge B)$$

$$1(True)$$

Theorem Proving in the Propositional Algebra

Any wff in the Propositional Algebra can be translated into the Boolean Ring formulation. Each algebraic simplification in the Boolean Ring can be mirrored by a simplification of the wff. So given a proposed theorem of the Propositional Algebra, a proof can be constructed by reducing both the premises and the conclusion to "completely reduced forms". The complete set of theorems between completely reduced forms then provides a lookup table to test the truth of the proposed theorem. The process just described can be used to create a proof of any true theorem in the Propositional Algebra.

Example

Proving an equivalence such as $p \supset (q \supset r) \equiv (p \wedge q) \supset r$ can be done easily by reducing each side of the equivalence to its Boolean Ring formulation, as follows:

$$\begin{aligned} p \supset (q \supset r) &= 1 + p + p(1 + q + qr) \\ &= 1 + p + p + pq + pqr \\ &= 1 + pq + pqr \\ &= (p \wedge q) \supset r \end{aligned}$$

Conclusion

Each of the wffs of the Propositional Algebra can be reduced to a standard form within a small equivalence class. A proof of any theorem in the Propositional Algebra can be constructed using the methods presented using the Boolean Ring formulation.

.....