4/12/2006

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 and to provide a scheme for automation of the process. This subject is also discussed in (Fitting (1990)).

Aim

The purpose of this paper is to describe the following:

- a standard reduced form for each of the well-formed formulas
- an algorithm for reducing any formula to its standard form, and
- a complete set of theorems relating the standard reduced forms

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 $\veebar$ 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 $A_1 \Rightarrow A_n$.

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.

Knuth-Bendix Completion Method

The Knuth-Bendix completion method (Knuth and Bendix (1970)) is a way of transforming a set of equations (between terms) into a confluent term rewriting system. Given an assignment of a weight to each term, so that the term substitution rules change terms of higher weight into terms of lower weight, the method can be described more accurately as an algorithm. When this algorithm succeeds, it has effectively solved the word problem for the specified algebra. Because the word problem is, in general, undecidable, the algorithm will not always terminate successfully. If it fails, it will either run forever, or encounter an unorientable equation (i.e. an equation that it cannot turn into a rewrite rule).

Knuth-Bendix and the Propositional Algebra

Applying the Knuth-Bendix method to the Propositional Algebra, as defined above, leads to a variety of difficulties, in particular unorientable equations. The Knuth-Bendix method covers many different schemes for assigning weights. For example, if the symbol $\supset$ is assigned a higher weight than the symbols $\vee$ and $\neg$ then we can expect the symbol $\supset$ to be eliminated when terms can be reduced according to the algorithm. Because there are many options, it is useful to have some general criteria for what is desired in reduced forms of expressions.

There are already some standard forms for terms in the Propositional Algebra. One of these is "disjunctive normal form" (Choo and Taylor (1992)), also called "disjunctive standard expression" (Hu (1965)). This reduced form is straightforward but does not offer any intuition about methods of proof and is also not reduced, in the sense that a given "disjunctive normal form" can be reduced to a simpler algebraic expression using the method of Karnaugh maps or the Quine-McClusky algorithm (Choo and Taylor (1992)).

A better approach is to use the representation of the terms of the Propositional Algebra as the elements of a Boolean Ring, which is a Ring with an identity and such that every element is an idempotent (Johnstone (1982)). 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:

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

Reduced Forms in the Propositional Algebra

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. 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 there are no more occurrences of each variable than occur in the equivalence class representative, and there are no double negations. For the Propositional Algebra, these equivalence classes take the place of *unique* completely reduced forms.

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 lattice with implication ($\Rightarrow$) as the partial order of the lattice. Moreover, there are 2^{2^n+n-1} theorems among the reduced forms, to which all other theorems (other than equivalences) between n variable forms can be reduced.

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

$$0(False)$$

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

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

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

$$1(True)$$

The thirty-two theorems which correspond to the linkages in the lattice above reduce to twenty-five when symmetries between A and B are taken into account. The resulting twenty-five theorems listed below:

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

$$(A \wedge B) \Rightarrow A \quad (A \wedge B) \Rightarrow B \quad (A \wedge B) \Rightarrow \neg(A \underline{\vee} B)$$

$$\neg(B \supset A) \Rightarrow B \quad \neg(B \supset A) \Rightarrow \neg A \quad \neg(B \supset A) \Rightarrow (A \underline{\vee} B)$$

$$\neg(A \vee B) \Rightarrow \neg A \quad \neg(A \vee B) \Rightarrow \neg B \quad \neg(A \vee B) \Rightarrow \neg(A \underline{\vee} B)$$

$$A \Rightarrow A \vee B \quad A \Rightarrow B \supset A$$

$$\neg(A \underline{\vee} B) \Rightarrow A \supset B \quad \neg(A \underline{\vee} B) \Rightarrow B \supset A$$

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

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

$$A \underline{\vee} B \Rightarrow A \vee B \quad A \underline{\vee} B \Rightarrow \neg(A \wedge B)$$

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

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.

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.

References

[1] Benninghofen,B., Kemmerich, S., Richter, M.M., *Systems of Reductions*, Springer Lecture Notes in Computer Science 277, New York, 1987.

[2] Choo, K.G. and Taylor, D.E., *Lectures on Discrete Mathematics* 3rd Edition, University of Sydney, 1992.

[3] Curry, H.B., *Foundations of Mathematical Logic* Dover, New York, 1977.

[4] Fitting, M., *First-Order Logic and Automated Theorem Proving*, Springer-Verlag, New York, 1990.

[5] Hu, S.T., *Threshold Logic* University of California Press, Los Angeles, 1965.

[6] Johnstone, P.T., *Stone Spaces*, Cambridge Studies in Advanced Mathematics 3, Cambridge University Press, Cambridge 1982.

[7] Knuth, D.E. and Bendix, P.B., Simple Word Problems in Abstract Algebra, in *Computational Problems in Abstract Algebra*, Pergammon Press, Oxford, 1970.

[8] Lambek, J. and Scott, R.J., *Introduction to Higher Order Categorical Logic*, Cambridge Studies in Advanced Mathematics 7, Cambridge University Press, Cambridge 1986.

[9] Mendelson, Elliott. *Introduction to Mathematical Logic*, 4th Edition, Wadsworth, London, 1997.

.....