An Algebraic Characterization of Inductive Soundness in Proof by Consistency

Shao Zhiqing (邵志清) and Song Guoxin (宋国新)
Department of Computer Science, East China University of Science and Technology, Shanghai 200237

Received July 12, 1993; revised April 28, 1994.

Abstract

Kapur and Musser studied the theoretical basis for proof by consistency and obtained an inductive completeness result: \( p \equiv q \) if and only if \( p = q \) is true in every inductive model. However, there is a loophole in their proof for the soundness part: \( p \equiv q \) implies \( p = q \) is true in every inductive model. The aim of this paper is to give a correct characterization of inductive soundness from an algebraic view by introducing strong inductive models.

Keywords: Proof by consistency, inductive soundness, strong inductive model, congruence relation, equation.

Proof by consistency\(^1\) consists of using pure equational reasoning for proving an equation valid in the initial algebra of a finite set of equational axioms, which would generally need some kind of induction. In a proof by consistency approach proving some equation is an inductive consequence of a set of axiom equations is reduced to check whether a congruence relation on ground terms induced by these axioms remains invariant when adding the equation to be proved. The consistency check is based on applying the Knuth-Bendix completion procedure\(^2\).

Kapur and Musser\(^3\) is the first to study the general theory of proof by consistency in an algebraic framework and obtained a theorem similar to Birkhoff's Completeness Theorem: \( \langle p, q \rangle \) is in the inductive congruence relation \( \equiv \) if and only if the equation \( p = q \) is true in all inductive models. Nevertheless, there is a loophole in their proof for the inductive soundness part: \( p \equiv q \) implies \( p = q \) is true in every inductive model.

In this paper we will discuss the inductive soundness problem using universal algebra\(^4\). We try to define a concept of strong inductive models and then prove the inductive soundness theorem by properties of free algebras.

1 Background and Basic Concepts

For simplicity we will consider single-sorted equational specifications. Let \( F \) be a finite set of function symbols such that a nonnegative integer \( n \) is assigned to each member \( f \) of \( F \) and in this case \( f \) is said to be an \( n \)-ary function symbol. Let \( X \) be an infinite set of variables, disjoint from \( F \). A term is either a variable from \( X \) or consists of an \( n \)-ary function symbol \( f \) of \( F \) and a finite sequence \( t_1, \ldots, t_n \) of terms, i.e., \( f(t_1, \ldots, t_n) \). Let \( T(F, X) \) denote the set of all terms and \( T(F) \) denote all terms free of variables. When it makes no confusion we write \( T(X) \) and \( T \) for \( T(F, X) \) and \( T(F) \) respectively. Terms from \( T \) are also called ground terms.

An algebra \( A \) is an ordered pair \( (A, F_0) \), where \( A \) is a nonempty set (called the universe) and \( F_0 \) is a family of finitary operations on \( A \) such that corresponding to each \( n \)-ary function symbol...
symbol \( f \in F \) there is an \( n \)-ary operation \( f^A \in F_0 \) on \( A \). In practice we prefer to write just \( f \) for \( f^A \) when it does not create any ambiguity. An algebra \( B \) is called a subalgebra of another algebra \( A \) if \( B \subseteq A \) and for every function symbol \( f \in F \), \( f^B \) is \( f^A \) restricted to \( B \). The term algebra, written as \( T(X) \), has \( T(X) \) as its universe and for each \( n \)-ary function symbol \( f \in F \) and \( p_i \in T(X) \) \((1 \leq i \leq n)\), \( f^{T(X)}(p_1, \ldots, p_n) = f(p_1, \ldots, p_n) \).

An equation is a pair of terms \( p, q \in T(X) \), usually written \( p = q \) or \( p(x_1, \ldots, x_n) = q(x_1, \ldots, x_n) \) to indicate that all variables in \( p \) or \( q \) are from \( \{x_1, \ldots, x_n\} \). Given a set of equations \( E \), we call that an algebra \( M \) is a model of \( E \) if every equation \( p = q \) of \( E \) is true in \( M \). It is known that if \( M \) is a model of \( E \), then every subalgebra \( M' \) of \( M \) is also a model of \( E \), we may say it is a submodel of \( M \).

Define a system \( S \) as a triple \((T(X), C, E)\), where \( C \) is a set of ground terms containing at least two elements and \( E \) is a finite set of equations. The purpose of \( C \) is to designate a set of terms that cannot be equated to each other. We call \( M \) a model of \( S = (T(X), C, E) \) if \( M \) is a model of \( E \) and every pair of different ground terms \( c, d \) in \( C \) have different interpretations in \( M \).

An \( S \)-congruence relation is defined to be a congruence relation on \( T(X) \) that contains \( \equiv_E \) (i.e., the smallest congruence relation on \( T(X) \) generated by \( E \)) and respects \( C \) (i.e., it contains no congruence between distinct elements of \( C \)). An \( S \)-congruence relation \( \theta \) is maximal if there is no pair \((p, q) \not\in \theta \) of terms for which the congruence closure of \( \theta \cup \{(p, q)\} \) is an \( S \)-congruence relation. We define the inductive congruence relation, denoted by \( \equiv \), as the intersection of all maximal \( S \)-congruence relations.

Given an algebra \( M = (M, F_0) \), a function from \( X \) to \( M \) is called an assignment. The value of a term \( t(x_1, \ldots, x_n) \in T(X) \) under an assignment \( \sigma \) is defined as usual and denoted by \( t^M(\sigma) \), or simply \( t^M(\sigma(x_1), \ldots, \sigma(x_n)) \).

2 Characterizing Inductive Soundness Using Universal Algebra

**Definition 1.** Suppose \( A \) and \( B \) are two algebras. We say that a mapping from \( A \) to \( B \) is a homomorphism from \( A \) to \( B \), written \( \alpha : A \rightarrow B \), if

\[
f^A(a_1, \ldots, a_n) = f^B(\alpha a_1, \ldots, \alpha a_n)
\]

for each \( n \)-ary \( f \) in \( F \) and each sequence \( a_1, \ldots, a_n \) from \( A \). If, in addition, the mapping is one to one, then it is called an isomorphism from \( A \) to \( B \). In case \( A = B \) a homomorphism is also called an endomorphism of \( A \). A homomorphism \( \alpha : A \rightarrow B \) with \( B = \alpha(A) \) is called an epimorphism. The kernel of a homomorphism \( \alpha : A \rightarrow B \), written \( \text{Ker}(\alpha) \), is defined by

\[
\text{Ker}(\alpha) = \{(a, b) \in A \times A : \alpha(a) = \alpha(b)\}.
\]

Kapur and Musser defined an inductive model of a system \( S = (T(X), C, E) \) to be a model \( M \) of \( S \) such that no proper epimorphic image of \( M \) is a model of \( S \). They delivered a completeness result analogous to Birkhoff's Theorem, but for \( \equiv \) instead of for \( \equiv_E \), i.e., \( p \equiv q \) if and only if \( p = q \) is true in every inductive model of \( S \). The key point of their proof is to obtain the following proposition: A model of \( S \) is inductive if and only if it is isomorphic to a model induced by a maximal \( S \)-congruence relation \( \theta \), i.e., \( T(X)/\theta \). Since the inductive congruence relation \( \equiv \) is the intersection of all maximal \( S \)-congruence relations, it follows that

\[
p \equiv q \quad \text{iff for every maximal } S \text{-congruence relation } \theta, (p, q) \in \theta
\]

\[
\text{iff for every maximal } S \text{-congruence relation } \theta, T(X)/\theta \models p = q
\]

\[
\text{iff } p = q \text{ is true in every inductive model of } S.
\]