Automatic Theorem Proving and Discovery

by Marek Rychlik, Professor, Department of Mathematics (rychlik@u.arizona.edu)

A Special Topics Course Proposal — Fall 2005
Course Website: http://alamos.math.arizona.edu/atp

An Overview

Automatic Theorem Proving is a field devoted to creating automatic systems capable of proving and discovering mathematical theorems via computation. Just as the computer today is able to beat the best of humans at chess, in the not so distant future the computer will be better at proving and discovering mathematical theorems. This course is devoted to both the theory of design of such systems as well as a review of today's systems for automatic theorem proving.

When in 1996 one such system proved a new mathematical theorem, the news appeared on the pages of New York Times. The story is available on the Internet:

http://www.nytimes.com/library/cyber/week/1210math.html

The Textbook and Material Covered

We will likely use the following textbook:

Melvin Fitting: *First-Order Logic and Automated Theorem Proving*, 1996, 2nd ed, Springer-Verlag, ISBN:0387945938

The course will begin with a mathematically rigorous exposition of propositional first-order logic. This is the framework independent of any particular proof mechanization technique. Subsequently, we will study well-known proof procedures: tableau, resolution, natural deduction, Gentzen sequents and axiom systems.

We will see how the subject ties in with deep mathematical issues of completeness of deduction systems. Some theorems and topics covered in the class will include: a Model Existence Theorem, Models and Interpretations, Compactness and Interpolation, Beth Definability Theorem. The subject matter will be illustrated with demonstrations of theorem provers written in the *Prolog* programming language and other software systems (Otter, ACL2, NqThm and programs I have written).

Prerequisites

A course in one or more of the following subjects: Foundations of Mathematics, Real Analysis, Discrete Mathematics, Theory of Computation. Or good general mathematical background and a dose of enthusiasm! The following are a plus: working knowledge of a programming language, experience with a CAS like Mathematica, Maxima (or MACSYMA) or Maple, general experience in the use of computers.

An Example of a Proof Written by a Computer

Prof. Edward Nelson described the following mathematical problem and his experience in using

an automated system in proving it (http://www.math.princeton.edu/~nelson/ar.html):

> Huntington and many others use $+$ (infix) for $\cup$ (union) in Boolean algebra. This is a bad notation ($+$ should be reserved for symmetric difference, when regarding a Boolean algebra as a commutative algebra –- in the usual mathematical sense –- with unit over the field of two elements), but it has the advantage of being on the typewriter keyboard. He uses ' (postfix) for complement. In his 1933 paper (p. 280 "the fourth set"), Huntington gives the following axioms for Boolean algebra:
>
> 1. (Commutativity) $a+b=b+a$
> 2. (Associativity) $(a+b)+c=a+(b+c)$
> 3. (Huntington's axiom H) $(a'+b')'+(a'+b)'=a$
>
> together with idempotency $a+a=a$. Huntington shows that these axioms are indeed axioms for Boolean algebra and states falsely that they are irredundant ("independent"). He gives an incorrect model purporting to satisfy the other axioms but not idempotency. In the correction he proves idempotency from the other axioms. This evidently caused him much trouble, for he thanks Mr. B. Notcutt for an essential step in the proof. I submitted the problem to McCune's automated deduction system Otter, and it proved idempotency from the other axioms in 53 seconds on tea (SUN-3/50M-4). The proof was sent to the ILF (Integration of Logical Functions) mail server in Berlin, and a few minutes later I got back an automatically generated humanly readable proof.

At the end of this document you have an example of a computer-generated, humanly readable proof obtained by Edward Nelson by submitting the problem by e-mail to one of the software systems. An excerpt of the proof that Prof. Nelson obtained from the computer follows:

Idempotency*

Nelson

February 16, 1997

Axiom 0.1 (Commutativity) $\forall(x_1,x_2)\ x_2\cup x_1=x_1\cup x_2$.

Axiom 0.2 (Associativity) $\forall(x_1,x_2,x_3)\ (x_1\cup x_2)\cup x_3=x_1\cup x_2\cup x_3$.

Axiom 0.3 (Huntington's axiom) $\forall(x_1,x_2)\ x_1\cup\overline{x_2}\cup\overline{\overline{x_1}\cup\overline{x_2}}=x_2$.

Theorem 0.1 $a\cup a=a$.

Proof[1]. We show directly that

$$a\cup a=a. \tag{1}$$

Because of Huntington's axiom and by associativity

$$\forall(x_1,x_2,x_3)\ \overline{x_1\cup\overline{x_2}}\cup\overline{\overline{x_1}\cup\overline{x_2}}\cup x_3=x_2\cup x_3. \tag{2}$$

We show directly that

$$\forall(x_1,x_2,x_3)\ x_2\cup x_1\cup x_3=x_1\cup x_2\cup x_3. \tag{3}$$

Let us consider arbitrary v_1,v_2,v_3. Because of commutativity and by associativity $v_1\cup v_2\cup v_3=(v_2\cup v_1)\cup v_3=v_2\cup v_1\cup v_3$. This completes the proof of (3).

Hence by Huntington's axiom

$$\forall(x_1,x_2,x_3)\ x_1\cup\overline{x_3}\cup x_2\cup\overline{\overline{x_1}\cup\overline{x_3}}=x_2\cup x_3. \tag{4}$$

Because of commutativity and by Huntington's axiom

$$\forall(x_1,x_2)\ \overline{x_2}\cup x_1\cup\overline{\overline{x_1}\cup\overline{x_2}}=x_2. \tag{5}$$

*This manuscript was generated by ILF. The development of ILF was supported by the Deutsche Forschungsgemeinschaft. For information on ILF contact gehne@mathematik.hu-berlin.de.

[1] Otter and Ilf

1

Figure 1. The first page of the proof

This completes the proof of (33).

By (19) and by (29)

$$\forall(x_1, x_2, x_3)\ x_1 \cup \overline{x_1} = \overline{x_2} \cup x_2 \cup x_3. \tag{34}$$

We show directly that

$$\forall(x_1, x_2)\ \overline{x_1 \cup \overline{x_1}} \cup x_2 = x_2 \cup x_2. \tag{35}$$

Let us consider arbitrary v_1, v_2. By (34) and by (30) $\overline{v_1 \cup \overline{v_1}} \cup \overline{\overline{v_2}} = v_2 \cup \overline{\overline{v_2}}$. Hence by (19) $\overline{v_1 \cup \overline{v_1}} \cup v_2 = v_2 \cup \overline{\overline{v_2}} = v_2 \cup v_2$. This completes the proof of (35).

We show directly that

$$\forall(x_1, x_2)\ \overline{\overline{x_1} \cup x_1} \cup \overline{x_2 \cup x_2} = \overline{x_2}. \tag{36}$$

Let us consider arbitrary v_1, v_2. By (16), (9), and by (19) $\overline{v_2} = \overline{\overline{v_1} \cup v_1} \cup \overline{\overline{v_2} \cup v_2} = \overline{\overline{v_1} \cup v_1} \cup \overline{v_2 \cup v_2}$. This completes the proof of (36).

Hence by (19)

$$\forall(x_1, x_2)\ \overline{x_1 \cup \overline{x_1}} \cup \overline{x_2 \cup x_2} = \overline{x_2}. \tag{37}$$

By (12) and by commutativity $\forall(x_1, x_2)\ x_1 \cup \overline{x_1 \cup \overline{x_2}} = \overline{x_2 \cup \overline{x_1}} \cup x_2$. Hence by commutativity

$$\forall(x_1, x_2)\ x_2 \cup \overline{x_2 \cup \overline{x_1}} = x_1 \cup \overline{x_1 \cup \overline{x_2}}. \tag{38}$$

We show directly that

$$\forall(x_1, x_2)\ x_2 \cup \overline{x_2 \cup x_1 \cup \overline{x_1}} = x_2. \tag{39}$$

Let us consider arbitrary v_1, v_2. By (35), (38), and by (37) $v_2 \cup \overline{v_2 \cup \overline{v_1 \cup \overline{v_1}}} = \overline{v_1 \cup \overline{v_1}} \cup \overline{\overline{v_2 \cup \overline{v_2}}} = \overline{\overline{v_2}}$. Hence by (19) $v_2 = v_2 \cup v_2 \cup \overline{v_1 \cup \overline{v_1}} = v_2 \cup v_2 \cup v_1 \cup \overline{v_1}$. This completes the proof of (39).

Hence by (33) $\forall(x_1, x_2)\ \overline{\overline{x_1} \cup x_1} \cup x_2 = x_2$. Hence by (31) $\forall\ x_1\ x_1 \cup x_1 = x_1$. Thus we have completed the proof of (1).

q.e.d.

5

Figure 2. The last page of the proof