Benjamin Gorry & Bill J. Ellis
July 16, 2003

# Scottish Theorem Provers at St Andrews

## 1 Introduction

On Thursday July the $10^{\text{th}}$ we attended the Scottish Theorem Provers (STP) seminar at St Andrews.

## 2 Andrew Rowley: WalkQSAT - using stochastic local search to solve quantified Boolean formulae

Quantified Boolean formulae is first order predicate logic where the only qualification is over the set of Booleans, *i.e.* $\{True, False\}$. The goal is to prove that the formulae is satisfiable by finding a set of instantiations to variables $\{Var = \{True \text{ or } False\}, \ldots\}$ that make the formula true. QBF can be used to model hardware and finding satisfiability can be used to determine the correctness of this hardware.

QBF satisfiability is decidable using an algorithm of complexity NP-C. Thus the problem is not finding if a QBF is satisfiable, rather finding that it is satisfiable in reasonable time.

The problem of satisfiability can be though of as a game between $\exists$ and $\forall$ players setting variables to $True$ and $False$ in turns until all of the variables have a value, with appropriate considerations for quantification[1]. The result is an observation that, by focusing on the winning strategy, certain moves appear more promising. This can be encoded within a small algorithm and has been implemented as WalkQSAT. WalkQSAT is a competitive incomplete QBF solver which sometimes returns unknown.

WalkQSAT starts from a random position and does not guarantee termination. WalkQSAT works best when there are lots of solutions to the problem. However it performs well compared to the classic GSAT and shows signs of promise against the leading system QuBE-BJ. Summary of the associated Q/A session:

**Unknown:** Did you compare space as well as time?

**Andrew Rowley:** In this case space and time is directly proportional, so one can be defined in terms of the other.

**Alan Bundy:** Are there applications where the incomplete solver is useful?

**Andrew Rowley** If it comes back with unknown a useful application may be games. If the result is unknown it may be the case that the game doesn't have a move to win in that way. Another possible application area is hardware verification - false results may show that a particular circuit definitely doesn't work.

**Alan Bundy:** It seems quite well suited to parallel processing, setting off $n$ different algorithms.

**Andrew Rowley:** That sounds like a good idea.

**Alan Bundy:** Are there heuristics for choosing the variable order?

**Andrew Rowley:** There is a certain amount of heuristics.

*Notes in this series are for $\epsilon$-baked ideas, for $1 \geq \epsilon \geq 0$. Only exceptionally should they be cited or distributed outwith the NuSPADE project (EPSRC GR/R24081).

[1] See: http://www-hons.dcs.st-and.ac.uk/ProjectMuseum/SHProjects/projects/ajp

## 3 James McKinna: McCarthy-Painter induction in EPIGRAM

This talk explored a new system and notation called EPIGRAM which aims to allow for the universal presentation of recursive objects, such as functions, specifications and proofs.

It was observed that it is sometimes better to prove larger, more complicated, properties rather than several smaller properties to pursue proofs of implementations. It was further noted that functions built around more straight forward proofs tend to be less efficient while functions built around more complex proofs tend to be more efficient – *i.e.* it is harder to prove efficient functions[2].

McCarthy-Painter induction was coined as the name for a class of recursion induction. Something called "productive induction" was introduced, noting that its details have yet to be fully defined.

## 4 Tom Kelsy: using symmetry breaking in model checking for hardware verification

Tom gave an overview of the areas he hoped to look at. He originally mentioned Computation Tree Logic and then went on to mention SPIN (which uses Propositional Linear Temporal Logic). He was asked whether he had considered the techniques currently used in model checking to reduce the size of the state space and he said he planned to look into it. A model checker which uses a derivation of CTL is SMV (Symbolic Model Verifier). SMV used Bryant's OBDDs (Ordered Binary Decision Diagrams) to allow the search-graph to be reconstructed to allow it to be searched in a simpler fashion. This reduction in the state space uses symmetry techniques to a certain extent. Tom mentioned a tool called ECLIPSE that he had started to try the techniques out on, but he didn't go into any further detail. This seemed like the beginning of a piece of work which had not been applied to any of the the current model checkers and it seemed like it could turn out to be an interesting piece of work.

## 5 Advert: British Logic Colloquium:

A number of experts will converge on St Andrews for the British Logic Colloquium between the $3^{\text{rd}}$ and $6^{\text{th}}$ September 2003. Students can (probably) attend with greatly reduced conference fees. The deadline for submission is the 26th of July.

## 6 Next time...

The next Scottish Theorem Provers meeting will take place at the University of Strathclyde, sometime in December.

[2]However, it was noted that the example used in the presentation did not conform to this observation.