The 5 Colour Theorem in Isabelle/Isar

Gertrud Bauer and Tobias Nipkow

Technische Universität München
Institut für Informatik, Arcisstrasse 21, 80290 München, Germany
http://www4.in.tum.de/~bauerg/
http://www.in.tum.de/~nipkow/

Abstract. Based on an inductive definition of triangulations, a theory of undirected planar graphs is developed in Isabelle/HOL. The proof of the 5 colour theorem is discussed in some detail, emphasizing the readability of the computer assisted proofs.

1 Introduction

It is well known that traditional mathematics is in principle reducible to logic. There are two main motivations for carrying out computer-based formalizations of mathematics in practice: to demonstrate the actual feasibility (in a particular domain), and to develop the formal underpinnings for some applications. Our formalization of graph theory is driven by both motivations.

First of all we would like to explore how feasible computer proofs are in an area that is (over)loaded with graphic intuition and does not have a strong algebraic theory, namely the realm of planar graphs. A first experiment in that direction was already reported by Yamamoto *et al.* [18]. Their main result was Euler's formula. This is just one of many stepping stones towards our main result, the 5 colour theorem (5CT). At the same time we try to lay the foundations for a project one or two orders of magnitude more ambitious: a computer-assisted proof of the 4 colour theorem (4CT). We come back to this point in the conclusion. Finally we have an orthogonal aim, namely of demonstrating the advantage of Wenzel's extension of Isabelle, called Isar [14], namely readable proofs. Hence some of the formal proofs are included, together with informal comments. It is not essential that the reader understands every last detail of the formal proofs. Isar is as generic as Isabelle but our work is based on the logic HOL.

There is surprisingly little work on formalizing graph theory in the literature. Apart from the article by Yamamoto *et al.* on planar graphs [18], from which we inherit the inductive approach, we are only aware of three other publications [17, 6, 19], none of which deal with planarity.

Before we embark on the technical details, let us briefly recall the history and main proof idea for the 4 and 5 colour theorem. The 4CT was first conjectured in 1853 by Francis Guthrie as a map colouring problem. The first incorrect proof attempts were given 1879 by Kempe and 1880 by Tait. Kempe already used an argument today known as Kempe chains. The incorrectness of Kempe's proof was pointed out by Heawood in 1890, but he could weaken Kempe's argument to the 5CT. In 1969 Heesch [9] introduced the methods of reducibility and discharging which were used in the first proof by Appel and Haken in 1976 [1, 2, 3]. The proof was simplified and improved 1995 by Robertson, Sanders, Seymour and Thomas [11, 12]. Both proofs rely heavily on large case analyses performed by (unverified) computer programs, which is contrary to the tradition of mathematical proofs.

The proof of the 5CT is by induction on the size of the graph g (although many textbooks [15, 8] prefer an indirect argument). Let g be non-empty. It can be shown that any non-empty planar graph has a vertex of degree ≤ 5. Let v be such a vertex in g and let g' be g without v. By induction hypothesis g' is 5-colourable because g' is smaller than g. Now we distinguish two cases. If v has degree less than 5, there are fewer neighbours than colours, and thus there is at least one colour left for v. Thus g is also 5-colorable. If v has degree 5, it is more complicated to construct a 5-colouring of g' from one of g. This core of the proof is explained in the body of the paper. In principle, the proof of the 4CT is similar, but immensely more complicated in its details.

We have intentionally not made an effort to find the slickest proof of the 5CT but worked with a standard one (except for using induction rather than a minimal counterexample). This is because we intended the proof to be a benchmark for our formalization of graph theory.

1.1 Notation

We briefly list the most important non-standard notations in Isabelle/Isar.

The notation $[\![P_1; \ldots; P_n]\!] \Longrightarrow P$ is short for the iterated implication $P_1 \Longrightarrow \ldots \Longrightarrow P_n \Longrightarrow P$. The symbol $\bigwedge$ denotes Isabelle's universal quantifier from the meta-logic. Set comprehension is written $\{x.P\}$ instead of $\{x \mid P\}$. Function *card* maps a finite set to its cardinality, a natural number. The notation c ‘ A is used for the image of a set A under a function c.

The keyword **constdefs** starts the declaration and definition of new constants; "$\equiv$"is definitional equality. Propositions in definitions, lemmas, and proofs can be preceded by a name, written "*name*: *proposition*"; We use the technique of suppressing subproofs, denoted by the symbol "$\langle$*proof*$\rangle$", to illustrate the structure of a proof. The subproofs may be trivial subproofs, by simplification or predicate calculus or involve some irrelevant Isabelle specific steps. If a proposition can be proved directly, its proof starts with the keyword **by** followed by some builtin proof method like *simp*, *arith*, *rule*, *blast* or *auto* [10]; The name *?thesis* in an Isar proof refers to the proposition we are proving at that moment.

1.2 Overview

In §2 we introduce graphs and their basic operations. In §3 we give an inductive definition of near triangulations and define planarity using triangulations. In §4 we discuss two fundamental topological properies of planar graphs and their representations in our formalization. In §5 we introduce colourings and Kempe chains and present the Isar proof of the 5CT.

2 Formalization of graphs

2.1 Definition of graphs

In this section we define the type of graphs and introduce some basic graph operations (insertion and deletion of edges and deletion of vertices) and some classes of graphs.

A (finite) graph g consists of a finite set of vertices $\mathcal{V}\ g$ and a set of edges $\mathcal{E}\ g$, where each edge is a two-element subset of $\mathcal{V}\ g$. In the field of planar graphs or graph colouring problems, isolated vertices do not matter much, since we can always assign them any colour. Hence we consider only vertices which are connected to another vertex, and leave out an explicit representation of $\mathcal{V}\ g$. This leads to an edge point of view of graphs, which keeps our formalisation as simple as possible. We do not restrict the definition of graphs to simple graphs but most of the graphs we actually work with are simple by construction.

We define a new type α *graph* as an isomorphic copy of the set of finite sets of two-element sets with the morphisms *edges* and *graph-of*:

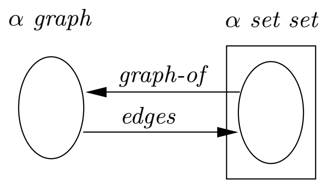

Fig. 1. Definition of α *graph*

typedef α *graph* $= \{g{::}\alpha\ \mathit{set\ set}.\ \mathit{finite}\ g \wedge (\forall\, e \in g.\ \exists\, x\ y.\ e = \{x,\ y\})\}$
  morphisms *edges graph-of*

The representing set is not empty as it contains, for example, the empty set.

We introduce the symbol $\mathcal{E}$ for the function *edges* and define $\mathcal{V}\ g$ as the set of all vertices which have an incident edge.

constdefs $\mathit{vertices} :: \alpha\ \mathit{graph} \Rightarrow \alpha\ \mathit{set}$ ($\mathcal{V}$)
  $\mathcal{V}\ g \ \equiv\ \bigcup (\mathcal{E}\ g)$

2.2 Basic graph operations

Size We define the *size* of a graph as the (finite) number of its vertices.

$\mathit{size}\ g \ \equiv\ \mathit{card}\ (\mathcal{V}\ g)$

Empty graph, insertion and deletion of edges We introduce the following basic graph operations: the empty graph $\emptyset$, insertion $g \oplus \{x,\ y\}$ of an edge, deletion $g \ominus \{x,\ y\}$ of an edge and deletion $g \odot x$ of a vertex x, i.e. deletion of all edges which are incident with x.

constdefs *empty-graph* $::\ \alpha\ graph$ $\quad(\emptyset)$
$\emptyset\ \equiv\ graph\text{-}of\ \{\}$

ins $::\ \alpha\ graph \Rightarrow \alpha\ set \Rightarrow \alpha\ graph$ $\quad$ (**infixl** $\oplus$ 60)
$e = \{x,\ y\} \Longrightarrow g \oplus e\ \equiv\ graph\text{-}of\ (insert\ e\ (\mathcal{E}\ g))$

del $::\ \alpha\ graph \Rightarrow \alpha\ set \Rightarrow \alpha\ graph$ $\quad$ (**infixl** $\ominus$ 60)
$g \ominus e\ \equiv\ graph\text{-}of\ (\mathcal{E}\ g\ -\ \{e\})$

del-vertex $::\ \alpha\ graph \Rightarrow \alpha \Rightarrow \alpha\ graph$ $\quad$ (**infixl** $\odot$ 60)
$g \odot x\ \equiv\ graph\text{-}of\ \{e.\ e \in \mathcal{E}\ g \wedge x \notin e\}$

Subgraph A graph g is a (spanning) subgraph of h, $g \preceq h$, iff g can be extended to h by only inserting edges between existing vertices.

constdefs *subgraph* $::\ \alpha\ graph \Rightarrow \alpha\ graph \Rightarrow bool$ (**infixl** $\preceq$ 60)
$g \preceq h\ \equiv\ \mathcal{V}\,g = \mathcal{V}\,h \wedge \mathcal{E}\ g \subseteq \mathcal{E}\ h$

Degree The neighbourhood $\Gamma\ g\ x$ of x is the set of incident vertices. The degree of a vertex $x \in \mathcal{V}\,g$ is the number of neighbours of x.

constdefs *neighbours* $::\ \alpha\ graph \Rightarrow \alpha \Rightarrow \alpha\ set$ $\quad(\Gamma)$
$\Gamma\ g\ x\ \equiv\ \{y.\ \{x,\ y\} \in \mathcal{E}\ g\}$

degree $::\ \alpha\ graph \Rightarrow \alpha \Rightarrow nat$
$degree\ g\ x\ \equiv\ card\ (\Gamma\ g\ x)$

2.3 Some classes of graphs

Complete graphs with n vertices are simple graphs where any two different vertices are incident. For example a triangle is a complete graph with 3 vertices.

constdefs K_3 $::\ \alpha \Rightarrow \alpha \Rightarrow \alpha \Rightarrow \alpha\ graph$ $\quad(K_3)$
$K_3\ a\ b\ c\ \equiv\ \emptyset \oplus \{a,\ b\} \oplus \{a,\ c\} \oplus \{b,\ c\}$

Cycles are simple connected graphs where any vertex has degree 2. We do not require connectivity, and thus obtain sets of cycles.

constdefs *cycles* $::\ \alpha\ graph \Rightarrow bool$
$cycles\ g\ \equiv\ simple\ g \wedge (\forall\, v \in \mathcal{V}\,g.\ degree\ g\ v = 2)$

We introduce abbreviations *cycle-ins-vertex* and *cycle-del-vertex* for insertion and deletion of vertices in cycles (see Fig. 2).

constdefs *cycle-ins-vertex* $::\ \alpha\ graph \Rightarrow \alpha \Rightarrow \alpha \Rightarrow \alpha \Rightarrow \alpha\ graph$
$cycle\text{-}ins\text{-}vertex\ g\ x\ y\ z\ \equiv\ g \ominus \{x,\ z\} \oplus \{x,\ y\} \oplus \{y,\ z\}$

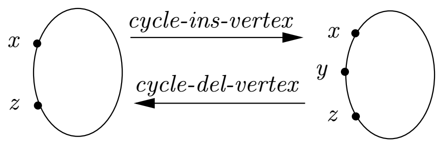

Fig. 2. Insertion and deletion of vertices in cycles

cycle-del-vertex :: α *graph* $\Rightarrow \alpha \Rightarrow \alpha \Rightarrow \alpha \Rightarrow \alpha$ *graph*
cycle-del-vertex $g\ x\ y\ z \equiv g \ominus \{x, y\} \ominus \{y, z\} \oplus \{x, z\}$

3 Triangulations and planarity

3.1 Inductive construction of near triangulations

To lay the foundations for our definition of planarity based on triangulations, we start in this section with the inductive definition of near triangulations. The idea of defining planar graphs inductively is due to Yamamoto *et al.* [18], but the formulation in terms of near triangulations is due to Wiedijk [16]. We will then derive some fundamental properties of near triangulations such as Euler's theorem and the existence of a vertex of degree at most 5.

Triangulations are plane graphs where any face is a triangle. Near triangulations are plane graphs where any face except the outer face is a triangle. We define near triangulations g with boundary h and inner faces f in an inductive way (see Fig. 3): any triangle $K_3\ a\ b\ c$ of three distinct vertices is a near triangulation. Near triangulations are extended by adding triangles on the outside in two different ways: in the first case we introduce a new vertex b by inserting two edges joining b with a and c, where a and c are incident on h. In the other case we insert a new edge joining a and c, where a and c are both incident with b on h. The boundary of the new near triangulation is constructed from the original

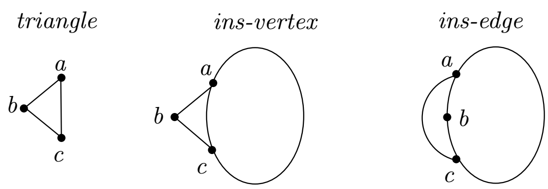

Fig. 3. Inductive definition of near triangulations

one by inserting or deleting the vertex b on h. The set of inner faces f is extended in both cases by the new triangle $K_3\ a\ b\ c$.

consts *near-triangulations* :: (α *graph* $\times$ α *graph* $\times$ α *graph set*) *set*
inductive *near-triangulations*
intros
triangle:
$distinct\ [a,\ b,\ c] \Longrightarrow (K_3\ a\ b\ c,\ K_3\ a\ b\ c,\ \{K_3\ a\ b\ c\}) \in near\text{-}triangulations$

ins-vertex:
$[\![\ distinct\ [a,\ b,\ c];\ \{a,\ c\} \in \mathcal{E}\ h;\ b \notin \mathcal{V}\ g;$
$(g,\ h,\ f) \in near\text{-}triangulations\ ]\!] \Longrightarrow$
$(g \oplus \{a,\ b\} \oplus \{b,\ c\},\ cycle\text{-}ins\text{-}vertex\ h\ a\ b\ c,\ f \cup \{K_3\ a\ b\ c\}) \in near\text{-}triangulations$

ins-edge:
$[\![\ distinct\ [a,\ b,\ c];\ \{a,\ b\} \in \mathcal{E}\ h;\ \{b,\ c\} \in \mathcal{E}\ h;\ \{a,\ c\} \notin \mathcal{E}\ g;$
$(g,\ h,\ f) \in near\text{-}triangulations\ ]\!] \Longrightarrow$
$(g \oplus \{a,\ c\},\ cycle\text{-}del\text{-}vertex\ h\ a\ b\ c,\ f \cup \{K_3\ a\ b\ c\}) \in near\text{-}triangulations$

A near triangulation is a graph g which can be constructed in this way. A triangulation is a special near triangulation where the boundary consist of 3 vertices. Of course there may be many different ways of constructing a near triangulation. A boundary $\mathcal{H}\ g$ is some boundary in one possible construction of g, $\mathcal{F}\ g$ is some set of inner faces in one possible construction of g. Note that both the inner faces and the boundary (which can be counsidered as the outer face) are not unique, since some planar graphs can be drawn in different ways.

Note that *SOME* is Hilbert's ε-operator, the choice construct in HOL.

constdefs *near-triangulation* :: α *graph* $\Rightarrow$ *bool*
$near\text{-}triangulation\ g\ \equiv\ \exists\, h\, f.\ (g,\ h,\ f) \in near\text{-}triangulations$

triangulation :: α *graph* $\Rightarrow$ *bool*
$triangulation\ g\ \equiv\ \exists\, h\, f.\ (g,\ h,\ f) \in near\text{-}triangulations \wedge card\ (\mathcal{V}\ h) = 3$

boundary :: α *graph* $\Rightarrow$ α *graph* ($\mathcal{H}$)
$\mathcal{H}\ g\ \equiv\ SOME\ h.\ \exists f.\ (g,\ h,\ f) \in near\text{-}triangulations$

faces :: α *graph* $\Rightarrow$ α *graph set* ($\mathcal{F}$)
$\mathcal{F}\ g\ \equiv\ SOME\ f.\ \exists h.\ (g,\ h,\ f) \in near\text{-}triangulations$

3.2 Fundamental properties of near triangulations

Our next goal is to prove that any planar graph has at least one vertex of degree ≤ 5. Since our definition of planarity is based on near triangulations, we will see that it suffices to show that any near triangulation contains a vertex of degree ≤ 5. To this end we will first establish a series of equations about the number of edges, vertices and faces in near triangulations. Finally we will show that any near triangulation contains a vertex of degree ≤ 5.

The first equation relates the number of inner faces and the number of edges. Any face is adjoined by 3 edges, any edge belongs to 2 faces except the edges on the boundary which belong only to one face. The proof is by induction over the construction of near triangulations.

lemma *nt-edges-faces*:
$(g,\ h,\ f) \in \mathit{near\text{-}triangulations} \Longrightarrow 2 * \mathit{card}\ (\mathcal{E}\ g) = 3 * \mathit{card}\ f + \mathit{card}\ (\mathcal{V}\ h)$ ⟨*proof*⟩

Euler's theorem for near triangulations is also proved by induction. Note that $\mathcal{F}\ g$ contains only the inner faces of g, so the statement contains a 1 instead of the customary 2. We present the top-level structure of the proof, relating the considered quantities in the extended and original near triangulation. Note that we introduce an abbreviation *?P* for the statement we want to prove.

theorem *Euler*:
  $\mathit{near\text{-}triangulation}\ g \Longrightarrow 1 + \mathit{card}\ (\mathcal{E}\ g) = \mathit{card}\ (\mathcal{V}\ g) + \mathit{card}\ (\mathcal{F}\ g)$
proof −
  assume *near-triangulation g*
  then show $1 + \mathit{card}\ (\mathcal{E}\ g) = \mathit{card}\ (\mathcal{V}\ g) + \mathit{card}\ (\mathcal{F}\ g)$ (**is** $?P\ g\ (\mathcal{F}\ g)$)
  proof (*induct rule*: *nt-f-induct*)
    case (*triangle a b c*)
    show $?P\ (K_3\ a\ b\ c)\ \{K_3\ a\ b\ c\}$ ⟨*proof*⟩
  next
    case (*ins-vertex a b c f g h*)
    have $\mathit{card}\ (\mathcal{E}\ (g \oplus \{a,\ b\} \oplus \{b,\ c\})) = \mathit{card}\ (\mathcal{E}\ g) + 2$ ⟨*proof*⟩
    moreover have $\mathit{card}\ (\mathcal{V}\ (g \oplus \{a,\ b\} \oplus \{b,\ c\})) = 1 + \mathit{card}\ (\mathcal{V}\ g)$ ⟨*proof*⟩
    moreover have $\mathit{card}\ (f \cup \{K_3\ a\ b\ c\}) = \mathit{card}\ f + 1$ ⟨*proof*⟩
    moreover assume *?P g f*
    ultimately show $?P\ (g \oplus \{a,\ b\} \oplus \{b,\ c\})\ (f \cup \{K_3\ a\ b\ c\})$ **by** *simp*
  next
    case (*ins-edge a b c f g h*)
    have $\mathit{card}\ (\mathcal{E}\ (g \oplus \{a,\ c\})) = 1 + \mathit{card}\ (\mathcal{E}\ g)$ ⟨*proof*⟩
    moreover have $\mathit{card}\ (\mathcal{V}\ (g \oplus \{a,\ c\})) = \mathit{card}\ (\mathcal{V}\ g)$ ⟨*proof*⟩
    moreover have $\mathit{card}\ (f \cup \{K_3\ a\ b\ c\}) = 1 + \mathit{card}\ f$ ⟨*proof*⟩
    moreover assume *?P g f*
    ultimately show $?P\ (g \oplus \{a,\ c\})\ (f \cup \{K_3\ a\ b\ c\})$ **by** *simp*
  qed
qed

The following result is easily achieved by combining the previous ones.

lemma *edges-vertices*: $\mathit{near\text{-}triangulation}\ g \Longrightarrow$
  $\mathit{card}\ (\mathcal{E}\ g) = 3 * \mathit{card}\ (\mathcal{V}\ g) - 3 - \mathit{card}\ (\mathcal{V}\ (\mathcal{H}\ g))$ ⟨*proof*⟩

The sum of the degrees of all vertices counts the number of neighbours over all vertices, so every edge is counted twice. The proof is again by induction.

theorem *degree-sum*: $\mathit{near\text{-}triangulation}\ g \Longrightarrow$
  $(\sum v \in \mathcal{V}\ g.\ \mathit{degree}\ g\ v) = 2 * \mathit{card}\ (\mathcal{E}\ g)$ ⟨*proof*⟩

Now we prove our claim by contradiction. We can complete the proof with a short calculation combining the two preceding equations.

theorem *degree5*: $\mathit{near\text{-}triangulation}\ g \Longrightarrow \exists\, v \in \mathcal{V}\ g.\ \mathit{degree}\ g\ v \le 5$
proof −
  assume (∗): *near-triangulation g* **then have** (∗∗): $3 \le \mathit{card}\ (\mathcal{V}\ g)$ **by** (*rule card3*)
  show *?thesis*

proof (*rule classical*)
assume $\neg\ (\exists\, v \in \mathcal{V}\, g.\ \mathit{degree}\ g\ v \leq 5)$
then have $\bigwedge v.\ v \in \mathcal{V}\, g \Longrightarrow\ 6 \leq \mathit{degree}\ g\ v$ **by** *auto*
then have $6 * \mathit{card}\ (\mathcal{V}\, g) \leq (\sum v \in \mathcal{V}\, g.\ \mathit{degree}\ g\ v)$ **by** *simp*
also have $\ldots = 2 * \mathit{card}\ (\mathcal{E}\, g)$ **by** (*rule degree-sum*)
also from $(**)$ **and** $(*)$ **have** $\ldots < 6 * \mathit{card}\ (\mathcal{V}\, g)$
by (*simp add*: *edges-vertices*) *arith*
finally show *?thesis* **by** *arith*
qed
qed

3.3 Planar graphs

In text books, planar graphs are usually defined as those graphs which have an embedding in the two-dimensional Euclidean plane with no crossing edges. However, this approach requires a significant amount of topology. We start from the well-known and easy observation that planar graphs with at least 3 vertices are exactly those which can be extended to a triangulation by adding only edges. We do not consider graphs with less than 3 vertices, since a graph with at most n vertices can always be n-coloured. This leads to the following definition.

constdefs $\mathit{planar} :: \alpha\ \mathit{graph} \Rightarrow \mathit{bool}$
$\mathit{planar}\ g\ \equiv\ \exists\, g'.\ \mathit{triangulation}\ g' \wedge g \preceq g'$

Obviously triangulations are planar. But we also need to know that any near triangulation g is planar. Of course this is also true, we only have to insert edges until there are only 3 vertices on the boundary h of g. We can prove this by induction on the number of vertices in h.

lemma *near-triangulation-planar*: *near-triangulation* $g \Longrightarrow$ *planar* g $\langle \mathit{proof} \rangle$

We have glossed over one issue so far: is the usual topological definition of triangulation the same as our inductive one? And thus, is our notion of planarity the same as the topological one? It is clear that all of our inductively generated near triangulations are near triangulations in the topological sense, and hence that any planar graph in our sense is also planar in the topological sense. In the other direction let g be a planar graph in the topological sense such that g has at least 3 vertices. Then $g \preceq g'$ for some 2-connected planar graph g'. By Proposition 4 of [18] g' can be generated by the inductive definition in [18], where arbitrary polygons rather than just triangles are added in each step. Now there is a triangulation g'' in our sense such that $g' \preceq g''$ — just add edges to the polygons to subdivide them into triangles. Thus *planar* g because $g \preceq g''$. This finishes the informal proof that our inductive and the usual topological notion of planarity coincide.

4 Topological properties of near triangulations

4.1 Crossing paths on near triangulations

This section is dedicated to an obvious topological property of near triangulations shown in Fig. 4 on the left, where the circle is the boundary: any two paths between v_0 and v_2 and between v_1 and v_3 must intersect, i.e. have a vertex in common. In fact, this is true for all planar graphs. We give an inductive proof for near triangulations: given two paths in the graph extended by a new triangle, this induces two sub-paths in the old graph, which must intersect by induction hypothesis. The cases where the two paths lie completely within the old graph are trivial by induction hypothesis. Then there are numerous symmetric and degenerate cases where one of the two paths include (some of) the newly added edges. In Fig. 4 on the right you see the two main cases, one for inserting a vertex and one for inserting an edge. In both cases the sub-paths between v_0 and a and between v_1 and v_3 lie within the old graph and therefore intersect. In the first case one can also replace the sub-path abc by ac to obtain a path within the old graph, thus cutting down on the number of case distinctions, which is what we did in the formal proof.

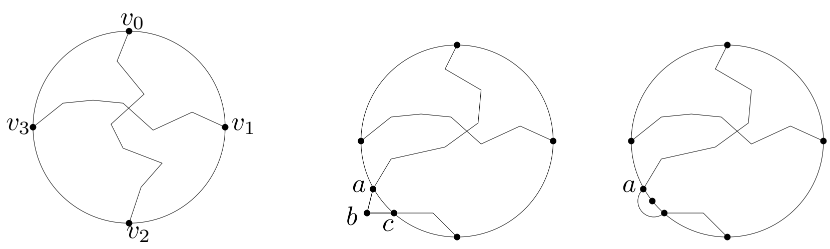

Fig. 4. Crossing paths

Although it took us a moment to find the pictorial proof, the shock came when the formal proof grew to 2000 lines. We will not discuss any details but merely the concepts involved.

A path could either be a graph or a list of vertices. We opted for lists because of their familiarity and large library. This may have been a mistake because lists are better suited for directed paths and may require additional case distinctions in proofs in an undirected setting. Given a graph g, $(x,p,y) \in paths\ g$ means that p is a list of distinct vertices leading from x to y. The definition is inductive:

consts $paths :: \alpha\ graph \Rightarrow (\alpha \times \alpha\ list \times \alpha) set$
inductive $paths\ g$
intros
basis: $(x,\ [x],\ x) \in paths\ g$
step: $[\![\ (y,\ p,\ z) \in paths\ g;\ \{x,\ y\} \in \mathcal{E}\ g;\ x \notin set\ p\ ]\!] \Longrightarrow (x,\ x\#p,\ z) \in paths\ g$

Function *set* converts a list into a set and the infix # separates the head from the tail of a list.

From a path p it is easy to recover a set of edges *pedges* p. Keyword **recdef** starts a recursive function definition and *measure size* is the hint for the automatic termination prover:

consts *pedges* :: α *list* $\Rightarrow$ α *set set*
recdef *measure length*
pedges $(x\#y\#zs) = \{\{x,\ y\}\} \cup$ *pedges* $(y\#zs)$
pedges $xs = \{\}$

Now we come to the key assumption of our main lemma shown in Fig. 4: the vertices v_0, v_1, v_2 and v_3 must appear in the right order on the boundary. We express this with the predicate *ortho* $h\ x\ y\ u\ v$ where h is the boundary, x must be opposite y and u opposite v:

constdefs *ortho* :: α *graph* $\Rightarrow \alpha \Rightarrow \alpha \Rightarrow \alpha \Rightarrow \alpha \Rightarrow$ *bool*
ortho $h\ x\ y\ u\ v \equiv x \neq y \wedge u \neq v \wedge$
$(\exists\, p\ q.\ (x,\ p,\ y) \in \mathit{paths}\ h \wedge (y,\ q,\ x) \in \mathit{paths}\ h \wedge u \in \mathit{set}\ p \wedge v \in \mathit{set}\ q \wedge$
$\mathcal{E}\ h = \mathit{pedges}\ p \cup \mathit{pedges}\ q \wedge \mathit{set}\ p \cap \mathit{set}\ q \subseteq \{x,\ y\})$

This definition is attractive because it follows very easily that x can be swapped with y and u with v. But there are many alternatives to this definition, and in retrospect we wonder if we made the right choice. As it turns out, almost half the size of this theory, i.e. 1000 lines, is concerned with proofs about *ortho*. There is certainly room for more automation. All of theses proofs involve first-order logic only, no induction.

The main theorem can now be expressed very easily:

theorem *crossing-paths*: $[\![\ (g,\ h,\ f) \in \mathit{near\text{-}triangulations};\ \mathit{ortho}\ h\ v_0\ v_2\ v_1\ v_3;$
$(v_0,\ p,\ v_2) \in \mathit{paths}\ g;\ (v_1,\ q,\ v_3) \in \mathit{paths}\ g\ ]\!] \Longrightarrow \mathit{set}\ p \cap \mathit{set}\ q \neq \{\}$ $\langle$*proof*$\rangle$

We also need to know that we can find 4 orthogonal vertices in a large enough graph:

lemma *cycles-ortho-ex*: $[\![\ \mathit{cycles}\ h;\ 4 \leq \mathit{card}\ (\mathcal{V}\ h)\ ]\!] \Longrightarrow$
$\exists\, v_0\ v_1\ v_2\ v_3.\ \mathit{ortho}\ h\ v_0\ v_2\ v_1\ v_3 \wedge \mathit{distinct}\ [v_0,\ v_1,\ v_2,\ v_3]$ $\langle$*proof*$\rangle$

4.2 Inversions of triangulations

For the proof of the 5CT we need the following topological property, which is illustrated in Fig. 5: if we delete a vertex v in a triangulation g, we obtain (in two steps) a near triangulation with boundary h where the vertices of h are exactly the neighbours v_0, v_1, v_2, v_3, v_4 of v.

theorem *del-vertex-near-triangulation*: $[\![\ \mathit{triangulation}\ g;\ 4 \leq \mathit{card}\ (\mathcal{V}\ g)\ ]\!] \Longrightarrow$
$\exists\, h\ f.(g \odot v,\ h,\ f) \in \mathit{near\text{-}triangulations} \wedge \mathcal{V}\ h = \Gamma\ g\ v$

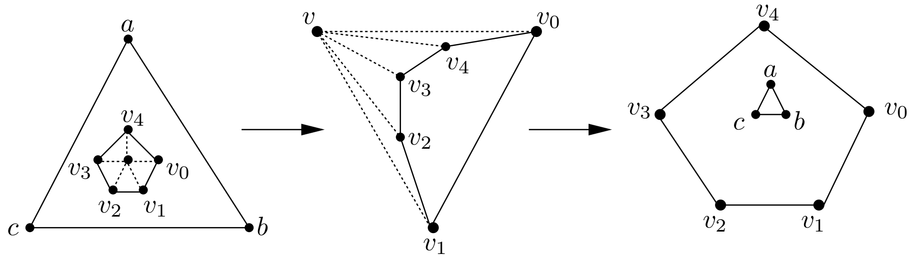

Fig. 5. Deletion of a vertex in a triangulation

This property is based on another fundamental but non-trivial property of triangulations (see Fig. 6). Given a triangulation g, we can consider any face of g as the boundary of g, i.e. we may invert the given inductive construction of g such that the boundary is one of the inner faces.

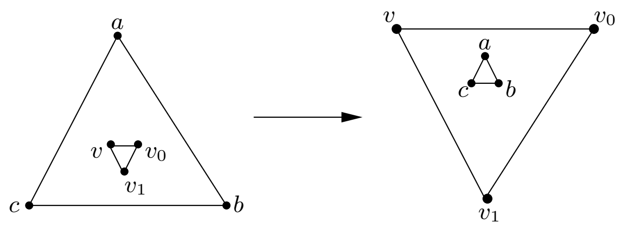

Fig. 6. Inversion of a triangulation

Now we can complete the proof of our previous claim. First we invert the triangulation such that one of the faces adjoining v is the outer one (first step in Fig. 5). Now we cut off all edges to neighbours of v and obtain a near triangulation where the vertices on h are exactly the neighbours of v. This is the only theorem we have not formally proved so far, but it is a topological property and does not concern colouring. It also is a special case of the following topological property, which may be seen as a formulation of the Jordan Curve Theorem: if we delete the inner faces of a near triangulation from a triangulation we again obtain a near triangulation.

5 The five colour theorem

5.1 Colourings and Kempe chains

A n-colouring of a graph g is a function from $\mathcal{V}\ g$ to $\{k.\ k < n\}$ such that any incident vertices have different colours. A graph g is n-colourable if there is an n-colouring of g.

constdefs *colouring* :: $nat \Rightarrow \alpha\ graph \Rightarrow (\alpha \Rightarrow nat) \Rightarrow bool$
$colouring\ n\ g\ c\ \equiv$
$(\forall v.\ v \in \mathcal{V}\ g \longrightarrow c\ v < n) \wedge (\forall v\ w.\ \{v, w\} \in \mathcal{E}\ g \longrightarrow c\ v \neq c\ w)$

constdefs *colourable* :: $nat \Rightarrow \alpha\ graph \Rightarrow bool$
$colourable\ n\ g\ \equiv\ \exists c.\ colouring\ n\ g\ c$

A Kempe chain of colours i and j is the subset of all vertices of g which are connected with v by a path of vertices of colours i and j.

We are able to prove the following major result: we can obtain a new n-colouring c' from a n-colouring c by transposing the colours of all vertices in a Kempe chain.

constdefs *kempe* :: $\alpha\ graph \Rightarrow (\alpha \Rightarrow nat) \Rightarrow \alpha \Rightarrow nat \Rightarrow nat \Rightarrow \alpha\ set$ $(\mathcal{K})$
$\mathcal{K}\ g\ c\ v\ i\ j\ \equiv\ \{w.\ \exists p.\ (v, p, w) \in paths\ g \wedge c`(set\ p) \subseteq \{i, j\}\}$

constdefs *swap-colours* :: $\alpha\ set \Rightarrow nat \Rightarrow nat \Rightarrow (\alpha \Rightarrow nat) \Rightarrow (\alpha \Rightarrow nat)$
$swap\text{-}colours\ K\ i\ j\ c\ v\ \equiv$
$if\ v \in K\ then\ if\ c\ v = i\ then\ j\ else\ if\ c\ v = j\ then\ i\ else\ c\ v\ else\ c\ v$

lemma *swap-colours-kempe*: $[\![\ v \in \mathcal{V}\ g;\ i < n;\ j < n;\ colouring\ n\ g\ c\ ]\!] \Longrightarrow$
$colouring\ n\ g\ (swap\text{-}colours\ (\mathcal{K}\ g\ c\ v\ i\ j)\ i\ j\ c)$ $\langle proof \rangle$

5.2 Reductions

A important proof principle in the proof of the 5CT is reduction of the problem of colouring g to the problem of colouring a smaller graph. For the proof of the 5CT we only need two different reductions. One for the case that g has a vertex v of degree less than 4 and one for the case that g has a vertex v of degree 5. Both reductions are based on the following property: if a colouring c on $g \odot v$ uses less than 5 colours for the neighbours $\Gamma\ g\ v$ of v, then c can be extended to a colouring on g. We only have to assign to v one of the colours which are not used in $\Gamma\ g\ v$.

lemma *free-colour-reduction*:
$[\![\ card\ (c\ `\ \Gamma\ g\ v) < 5;\ colouring\ 5\ (g \odot v)\ c;\ triangulation\ g\ ]\!] \Longrightarrow$
$colourable\ 5\ g$ $\langle proof \rangle$

The reduction for the case that v has degree less than 5 is quite obvious: there are only 4 neighbours so they cannot use more than 4 colours.

lemma *degree4-reduction*:
$[\![\ colourable\ 5\ (g \odot v);\ degree\ g\ v < 5;\ triangulation\ g\ ]\!] \Longrightarrow colourable\ 5\ g$ $\langle proof \rangle$

The reduction for the cases that v has degree 5 is a bit more complicated [8, 7]: we construct a colouring of g from a colouring of $g \odot v$ where g is a triangulation and *degree* g v = 5. We assume $g \odot v$ is colourable, so we can choose an (arbitrary) colouring c of $g \odot v$. In the case that c uses less than 5 colours in the neighbourhood Γ g v of v, we obviously can extend c on g.

lemma *degree5-reduction*:
  $[\![$ *colourable* 5 $(g \odot v)$; *degree* g $v = 5$; *triangulation* g $]\!] \Longrightarrow$ *colourable* 5 g
proof −
  assume $(*)$: *triangulation* g **and** *degree* g $v = 5$
  assume *colourable* 5 $(g \odot v)$ **then obtain** c **where** *colouring* 5 $(g \odot v)$ c **..**

  have *card* $(c$ ' Γ g $v) \leq 5$ $\langle$*proof*$\rangle$ **then show** *colourable* 5 g
  proof *cases*
    assume *card* $(c$ ' Γ g $v) < 5$ **show** *colourable* 5 g **by** (*rule free-colour-reduction*)
  next

In the case that c uses all 5 colours on the neighbours Γ g v of v, we consider the near triangulation $g \odot v$ with boundary h on Γ g v. We can find four distinct orthogonal vertices v_0 v_1 v_2 v_3 on h.

    assume *card* $(c$ ' Γ g $v) = 5$ **also have** $(**)$: *card* $(\Gamma$ g $v) = 5$ $\langle$*proof*$\rangle$
    finally have *inj-on* c $(\Gamma$ g $v)$ $\langle$*proof*$\rangle$

    have $4 \leq$ *card* $(\mathcal{V}\, g)$ $\langle$*proof*$\rangle$
    with $(*)$ **obtain** h f **where** $(g \odot v,\, h,\, f) \in$ *near-triangulations* **and**
      $\mathcal{V}\, h = \Gamma$ g v **by** (*rules dest*: *del-vertex-near-triangulation*)
    with $(**)$ **have** $4 \leq$ *card* $(\mathcal{V}\, h)$ **and** *cycles* h $\langle$*proof*$\rangle$
    then obtain v_0 v_1 v_2 v_3 **where** *ortho* h v_0 v_2 v_1 v_3 **and** *distinct* $[v_0, v_1, v_2, v_3]$
      by (*auto dest*: *cycles-ortho-ex*)

There cannot be a path in $g \odot v$ in the colours of v_0 and v_2 between v_0 and v_2 and at the same time one in the colours of v_1 and v_3 between v_1 and v_3. The reason is that the paths would intersect according to the *crossing-paths* lemma (see Fig. 7 on the left). This is a contradiction to the fact that all neighbours have different colours. Thus we can obtain $v_0{}'$ and $v_2{}'$ such that there is no path in the colours of $v_0{}'$ and $v_2{}'$ between $v_0{}'$ and $v_2{}'$.

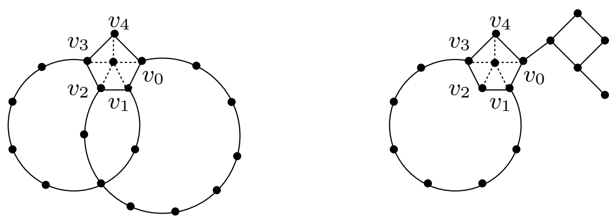

Fig. 7. Reduction for the case *degree* g v = 5

have $\neg$ (($\exists\, p.\ (v_0,\ p,\ v_2) \in \mathit{paths}\ (g \odot v) \wedge c`(\mathit{set}\ p) \subseteq \{c\ v_0,\ c\ v_2\}) \wedge$
$(\exists\, p.\ (v_1,\ p,\ v_3) \in \mathit{paths}\ (g \odot v) \wedge c`(\mathit{set}\ p) \subseteq \{c\ v_1,\ c\ v_3\}))$
proof $-$
{ **fix** p **assume** $(v_0,\ p,\ v_2) \in \mathit{paths}\ (g \odot v)$ **and** $c`(\mathit{set}\ p) \subseteq \{c\ v_0,\ c\ v_2\}$
fix q **assume** $(v_1,\ q,\ v_3) \in \mathit{paths}\ (g \odot v)$ **and** $c`(\mathit{set}\ q) \subseteq \{c\ v_1,\ c\ v_3\}$
have $\mathit{set}\ p \cap \mathit{set}\ q \neq \{\}$ **by** (*rule crossing-paths*)
then obtain s **where** $s \in \mathit{set}\ p$ **and** $s \in \mathit{set}\ q$ **by** *auto*
have $c\ s \in \{c\ v_0,\ c\ v_2\}$ **and** $c\ s \in \{c\ v_1,\ c\ v_3\}$ $\langle \mathit{proof} \rangle$
moreover have $c\ v_0 \neq c\ v_1$ **and** $c\ v_0 \neq c\ v_3$ **and**
$c\ v_1 \neq c\ v_2$ **and** $c\ v_2 \neq c\ v_3$ $\langle \mathit{proof} \rangle$
ultimately have *False* **by** *auto*
} **then show** *?thesis* **by** *auto*
qed
then obtain $v_0{}'\ v_2{}'$ **where** $v_0{}' = v_0 \wedge v_2{}' = v_2 \vee v_0{}' = v_1 \wedge v_2{}' = v_3$ **and**
$\neg\ (\exists\, p.\ p \in \mathit{paths}\ (g \odot v)\ v_0{}'\ v_2{}' \wedge c`(\mathit{set}\ p) \subseteq \{c\ v_0{}',\ c\ v_2{}'\})$ **by** *auto*

We consider the Kempe chain K of all vertices which are connected with $v_0{}'$ by a path in the colours of $v_0{}'$ and $v_2{}'$. We define a new colouring c' on $g \odot v$ by transposing the colours of $v_0{}'$ and $v_2{}'$ in K. According to our previous considerations $v_2{}'$ is separated from $v_0{}'$, so $v_2{}'$ does not lie in K. (See Fig. 7, on the right.) We can extend the colouring c' to g by assigning the colour of $v_0{}'$ to v.

def $K \equiv \mathcal{K}\ (g \odot v)\ c\ v_0{}'\ (c\ v_0{}')\ (c\ v_2{}')$
def $c' \equiv \mathit{swap\text{-}colours}\ K\ (c\ v_0{}')\ (c\ v_2{}')\ c$
obtain $\mathit{colouring}\ 5\ (g \odot v)\ c'$ $\langle \mathit{proof} \rangle$

have $v_2{}' \notin K$ $\langle \mathit{proof} \rangle$ **then have** $c'\ v_2{}' = c\ v_2{}'$ $\langle \mathit{proof} \rangle$
also have $v_0{}' \in K$ $\langle \mathit{proof} \rangle$ **then have** $c'\ v_0{}' = c\ v_2{}'$ $\langle \mathit{proof} \rangle$
finally have $c'\ v_0{}' = c'\ v_2{}'$ **.**
then have $\neg\ \mathit{inj\text{-}on}\ c'\ (\mathcal{V}\, h)$ $\langle \mathit{proof} \rangle$ **also have** $\mathcal{V}\, h = \mathit{\Gamma}\ g\ v$ **.**
finally have $\mathit{card}\ (c'\ `\ \mathit{\Gamma}\ g\ v) < 5$ $\langle \mathit{proof} \rangle$
then show $\mathit{colourable}\ 5\ g$ **by** (*rule free-colour-reduction*)
qed
qed

5.3 The proof of the five colour theorem

We prove the 5CT using the following rule for induction on *size g*.

lemma *graph-measure-induct*:
$(\bigwedge g.\ (\bigwedge h.\ \mathit{size}\ h < \mathit{size}\ g \Longrightarrow P\ h) \Longrightarrow P\ g) \Longrightarrow P\ (g{::}\alpha\ \mathit{graph})$ $\langle \mathit{proof} \rangle$

We show that any planar graph is 5-colourable by induction on *size g* (compare [8, 7]). We assume that g is planar. Hence it is the spanning subgraph of a triangulation t. We know that t contains at least one vertex of degree less than 5. The size of $t \odot v$ is smaller than the size of g. Moreover, $t \odot v$ is a near triangulation and therefore planar. It follows from the induction hypothesis (*IH*) that $t \odot v$ must be 5-colourable. Now we construct a colouring of t depending on a case distinction on the degree of v by applying an appropriate reduction.

```
theorem 5CT: planar g ⟹ colourable 5 g
proof −
  assume planar g then show colourable 5 g
  proof (induct rule: graph-measure-induct)
    fix g::α graph
    assume IH: ⋀g'::α graph. size g' < size g ⟹ planar g' ⟹ colourable 5 g'
    assume planar g then obtain t where triangulation t and g ≼ t ..
    then obtain v where v ∈ 𝒱 t and d: degree t v ≤ 5 by (blast dest: degree5)

    have size (t ⊙ v) < size t .. also have size t = size g ..
    also have planar (t ⊙ v) ..
    ultimately obtain colourable 5 (t ⊙ v) by (rules dest: IH)

    from d have colourable 5 t
    proof cases
      assume degree t v < 5 show colourable 5 t by (rule degree4-reduction)
    next
      assume degree t v = 5 show colourable 5 t by (rule degree5-reduction)
    qed
    then show colourable 5 g ..
  qed
qed
```

6 Conclusion

Although we have proved what we set out to, the resulting formalization and proofs are still only a beginning. For a start, the size of the proofs for the *crossing-paths* lemma in §4.1 are too large for comfort, and the proof of theorem *del-vertex-neartriangulation* still needs to be formalized in Isabelle. It also appears that both propositions could be obtained as special cases of a discrete version of the Jordan Curve Theorem. However, in other parts, e.g. Euler's theorem and the reduction lemmas, the proofs are roughly in line with what one would expect from the informal proofs. The complete proof, without the topological properties, consists of about 20 pages basic graph theory, 15 pages of triangulations, and 7 pages for the 5CT including Kempe chains and reductions.

So what about a full formalization of one of the existing proofs of the 4CT [4, 13]? The top-level proof by Robertson *et al.* consists of two computer-validated theorems plus a lemma by Birkhoff [5]. The latter is more complicated than the 5CT, but still reasonably simple. The crucial part are the two computer-validated theorems. One would either have to verify the correctness of the algorithms, or let the algorithms produce a trace that can be turned into a proof. Although the second appears more tractable, in either case one needs a considerable amount of additional graph theory. Such an undertaking appears within reach of a dedicated group of experts in theorem proving and graph theory, and its benefits could be significant.

References

[1] K. Appel and W. Haken. Every planar map is four colourable. *Bulletin of the American mathematical Society*, 82:711–112, 1977.

[2] K. Appel and W. Haken. Every planar map is four colourable. I: Discharging. *Illinois J. math.*, 21:429–490, 1977.

[3] K. Appel and W. Haken. Every planar map is four colourable. II: Reducibility. *Illinois J. math.*, 21:491–567, 1977.

[4] K. Appel and W. Haken. *Every planar map is four colourable*, volume 98. Contemporary Mathematics, 1989.

[5] G. D. Birkhoff. The reducibility of maps. *Amer. J. Math.*, 35:114–128, 1913.

[6] C.-T. Chou. A Formal Theory of Undirected Graphs in Higher-Order Logic. In T. Melham and J. Camilleri, editors, *Higher Order Logic Theorem Proving and Its Applications*, volume 859 of *LNCS*, pages 158–176, 1994.

[7] R. Diestel. *Graph Theory*. Graduate Texts in Mathematics. Springer, 2000. Electronic Version: http://www.math.uni-hamburg.de/home/diestel/books/graph.theory/.

[8] T. Emden-Weinert, S. Hougardy, B. Kreuter, H. Prömel, and A. Steger. Einführung in Graphen und Algorithmen. http://www.informatik.hu-berlin.de/Institut/struktur/algorithmen/ga/, 1996.

[9] H. Heesch. *Untersuchungen zum Vierfarbenproblem*. Number 810/a/b in Hochschulskriptum. Bibliographisches Institut, Mannheim, 1969.

[10] T. Nipkow, L. Paulson, and M. Wenzel. *Isabelle/HOL — A Proof Assistant for Higher-Order Logic*, volume 2283 of *LNCS*. Springer, 2002. To appear.

[11] N. Robertson, D. Sanders, P. Seymour, and R. Thomas. The four colour theorem. http://www.math.gatech.edu/~thomas/FC/fourcolor.html, 1995.

[12] N. Robertson, D. Sanders, P. Seymour, and R. Thomas. A new proof of the four colour theorem. *Electron. Res. Announce. Amer. Math Soc.*, 2(1):17–25, 1996.

[13] N. Robertson, D. Sanders, P. Seymour, and R. Thomas. The four colour theorem. *J. Combin. Theory Ser. B*, 70:2–44, 1997.

[14] M. Wenzel. *Isabelle/Isar — A Versatile Environment for Human-Readable Formal Proof Documents*. PhD thesis, Institut für Informatik, Technische Universität München, 2002. http://tumb1.biblio.tu-muenchen.de/publ/diss/in/2002/wenzel.htm.

[15] D. West. *Introduction to Graph Theory*. Prentice Hall, New York, 1996.

[16] F. Wiedijk. The Four Color Theorem Project. http://www.cs.kun.nl/~freek/4ct/, 2000.

[17] W. Wong. A simple graph theory and its application in railway signalling. In M. Archer, J. Joyce, K. Levitt, and P. Windley, editors, *Proc. 1991 International Workshop on the HOL Theorem Proving System and its Applications*, pages 395–409. IEEE Computer Society Press, 1992.

[18] M. Yamamoto, S.-y. Nishizaha, M. Hagiya, and Y. Toda. Formalization of Planar Graphs. In E. Schubert, P. Windley, and J. Alves-Foss, editors, *Higher Order Logic Theorem Proving and its Applications*, volume 971 of *LNCS*, pages 369–384, 1995.

[19] M. Yamamoto, K. Takahashi, M. Hagiya, S.-y. Nishizaki, and T. Tamai. Formalization of Graph Search Algorithms and its Applications. In J. Grundy and M. Newey, editors, *Theorem Proving in Higher Order Logics*, volume 1479 of *LNCS*, pages 479–496, 1998.