Certified Kruskal's Tree Theorem

Christian Sternagel*

JAIST, Japan
c-sterna@jaist.ac.jp

Abstract. This paper gives the first formalization of Kruskal's tree theorem in a proof assistant. More concretely, an Isabelle/HOL development of Nash-Williams' minimal bad sequence argument for proving the tree theorem is presented. Along the way, the proofs of Dickson's lemma and Higman's lemma are discussed.

Keywords: Well-Quasi-Orders, Dickson's Lemma, Minimal Bad Sequences, Higman's Lemma, Kruskal's Tree Theorem

1 Introduction

Kruskal's tree theorem [1] (sometimes called *the* tree theorem in the following) is a famous result in combinatorics, more precisely well-quasi-order (wqo) theory.

Kruskal's Tree Theorem. *When a set A is wqo'd (by a relation $\preceq$), then so is the set of finite trees over A (by homeomorphic embedding w.r.t. $\preceq$).*

Nash-Williams gave a short and elegant proof of the tree theorem [2], where he first established what is now known as the *minimal bad sequence argument*: assume the existence of a minimal "bad" infinite sequence of elements, construct an even smaller "bad" infinite sequence, thus contradicting minimality and proving wqo'dness (since the definition of wqo requires all infinite sequences of elements to be "good").

Besides the minimal bad sequence argument, Nash-Williams' work [2] contains proofs of Dickson's lemma [3] (*if A and B are wqo'd, then so is the Cartesian product $A \times B$*) and a variant of Higman's lemma [4] (*if A is wqo'd, then so is the set of finite subsets of A*), where the latter also incorporates an instance of the minimal bad sequence argument.

The work at hand constitutes a formalization of Nash-Williams' original proofs in the proof assistant Isabelle [5].[1] As indicated also by others, his argumentation is short (in fact, Nash-Williams' paper consists of only two and a half pages in total) and elegant (which was also the main reason for basing the formalization on his work). However, formalizations using proof assistants typically

* Supported by the Austrian Science Fund (FWF): J3202.

[1] Available from http://isabelle.in.tum.de (try Isabelle/jEdit for browsing).

require us to be more rigorous than with pen and paper. Thus, the formalization is more detailed in places, which results in somewhat longer (about three and a half thousand lines of Isabelle/HOL theories) and slightly less elegant proofs. Fortunately the most detailed part could be localized (pun intended), thus not derogating the elegance of the remaining proofs.

The author wants to stress that everything presented in the following, is formalized using the proof assistant Isabelle. In this paper, a high-level overview of this formalization is given. The full development is part of the *Archive of Formal Proofs* [6].

Contributions. To the best of the author's knowledge, the presented work constitutes the first unrestricted formalization of Higman's lemma in Isabelle/HOL as well as the first formalization of Kruskal's tree theorem ever. Both are important combinatorial results with applications in rewriting theory. For example, the theory of simplification orders [7] was formalized as part of IsaFoR,[2] where it is applied to show well-foundedness of the Knuth-Bendix-Order [8].

Moreover, the author believes that besides their high trustworthiness (which is of course very important), formalizations of existing mathematical results are also of archival and educational value. The reason is that a formalization contains *all* non-trivial steps of a proof. No doubt, more often than not, those steps were already conducted in the minds of the original proof authors. However, when the original author writes down a proof in condensed form for publishing, some of the steps may get lost. If, much later, another person tries to understand the proof, there may be some mental gaps (or in the worst case even errors).

Finally, formalizations are often hard to read for non-experts (but note that the Isar language for Isabelle [9] is a huge improvement in that respect). Thus, the author hopes that this high-level overview makes the presented formalization more accessible.

Differences to Nash-Williams' Work. The formalization presented here differs from the original presentation of Nash-Williams in several details: As stated above, Nash-Williams proved a variant of Higman's lemma [2, Lemma 2]. Also his version of the tree theorem [2, Theorem 1] does not mention homeomorphic embedding. In the following, every reference to Higman's lemma, means "*If A is wqo'd, then A^* is wqo'd by homeomorphic embedding on lists*," and every reference to the tree theorem, means "*If A is wqo'd, then the set of finite trees over A is wqo'd by homeomorphic embedding on trees.*" The structure of the proofs, stays the same.

Overview. The remainder is structured as follows. In Section 2, necessary preliminaries are covered. Then, in Section 3, the structure of Nash-Williams' original proofs is reviewed. The next four sections present a formalization of Dickson's lemma (featuring a proof of a variant of Dickson's lemma for almost-full relations, i.e., not relying on transitivity), in Section 4; a general construction of

[2] http://cl-informatik.uibk.ac.at/software/ceta/

minimal bad sequences, in Section 5; a formalization of Higman's lemma, in Section 6; and ultimately, a formalization of Kruskal's tree theorem, in Section 7. Finally, the paper concludes in Section 8, where also applications are sketched, and future as well as related work is discussed.

2 Preliminaries

Throughout this exposition, standard mathematical notation is used as far as possible. However, additionally some Isabelle specific notation is employed, since Isabelle's document preparation facilities were used for typesetting all lemmas and theorems (in the words of Haftmann et al. [10]: *no typos, no omissions, no sweat*; alas, this does not extend to the regular text). Thus, some explanation might be in order.

Isabelle/HOL is a higher-order logic based on the simply-typed lambda calculus. Thus, every term has a type, where Greek letters α, β, γ, ... are used for *type variables*; and *type constructors* like *nat* for natural numbers, $\alpha \Rightarrow \beta$ for the function space, $\alpha \times \beta$ for ordered pairs, α *set* for sets, and α *list* for finite lists. *Type constraints* are written $t{::}\tau$ and denote that term t is of type τ. As usual for lambda calculi, function application is denoted by juxtaposition, i.e., $f\,x$ denotes the application of function f to the argument x. The type $\alpha \Rightarrow \alpha \Rightarrow$ *bool* is used to encode binary relations. (An alternative would have been to use $(\alpha \times \alpha)$ *set*. However, the two representations are mostly equivalent and the former is used for many binary relations of Isabelle/HOL's library.)

Further, the following constants from Isabelle/HOL's library are freely used: $\circ{::}(\alpha \Rightarrow \beta) \Rightarrow (\gamma \Rightarrow \alpha) \Rightarrow \gamma \Rightarrow \beta$, where $f \circ g$ denotes the functional composition of the two functions f and g, i.e., $f \circ g \stackrel{\text{def}}{=} \lambda x.\ f\ (g\ x)$, and sometimes f_φ is used instead of $f \circ \varphi$ for brevity (especially when f denotes an infinite sequence and φ is an index-mapping); $fst{::}\alpha \times \beta \Rightarrow \alpha$ and $snd{::}\alpha \times \beta \Rightarrow \beta$ extract the first and second component of a pair, respectively; $set{::}\alpha\ list \Rightarrow \alpha\ set$, where *set xs* is the set of elements occurring in the list *xs*; $[]{::}\alpha\ list$, the empty list; $\cdot{::}\alpha \Rightarrow \alpha\ list \Rightarrow \alpha\ list$, where $x{\cdot}xs$ denotes "consing" the element x in front of the list *xs*; and $@{::}\alpha\ list \Rightarrow \alpha\ list \Rightarrow \alpha\ list$, where *xs* @ *ys* denotes the concatenation of the two lists *xs* and *ys*. Note that since $\cdot$ and @ are both right-associative and have the same priority, *xs* @ $y{\cdot}ys$ is the same as *xs* @ $(y{\cdot}ys)$ and denotes a list that is constructed by inserting the element y between those of *xs* and *ys*.

When stating formulas, sometimes Isabelle specific notation is used. Then, $\bigwedge$ denotes universal quantification and $\Longrightarrow$ (right-associative) implication. Moreover, nested implication, like $A \Longrightarrow B \Longrightarrow C$, is abbreviated to $[\![A;\ B]\!] \Longrightarrow C$.

Let $\preceq$ be a binary relation and A a set. The relation $\preceq$ is *reflexive on* A, written $refl_A(\preceq)$, iff $\forall\, x{\in}A.\ x \preceq x$; and *transitive on* A, written $trans_A(\preceq)$, iff $\forall\, x{\in}A.\ \forall\, y{\in}A.\ \forall\, z{\in}A.\ x \preceq y \wedge y \preceq z \longrightarrow x \preceq z$.

Infinite sequences over elements of type α are represented by functions of type $nat \Rightarrow \alpha$. A binary relation $\preceq$ is *transitive on a sequence* f, written $trans_f(\preceq)$, iff $\forall\, i\ j.\ i < j \longrightarrow f\,i \preceq f\,j$. A sequence f is *good w.r.t.* $\preceq$, written $good_\preceq(f)$, iff $\exists\, i\ j.\ i < j \wedge f\,i \preceq f\,j$. If a sequence is not good, it is called *bad*.

The author follows Veldman [11] and Vytiniotis et al. [12] in basing wqos on *almost-full* relations (which are basically wqos without transitivity). The main reason for doing so, is that all the properties of interest also hold for almost-full relations and are easily extended to wqos.

The relation $\preceq$ is *almost-full on* A, written $af_A(\preceq)$, iff all infinite sequences over elements of A are good, i.e., $af_A(\preceq) \stackrel{\text{def}}{=} \forall f.\ (\forall i.\ f\,i \in A) \longrightarrow good_{\preceq}(f)$. Note that every almost-full relation is necessarily reflexive (see, e.g., [13, Lemma 1]).

Let $\preceq$ be almost-full on A. If in addition $\preceq$ is transitive on A, then $\preceq$ is a *wqo on* A (equivalently, A is wqo'd by $\preceq$), written $wqo_A(\preceq)$.

3 Nash-Williams' Proof

Before a detailed account of the formalization is given (in the sections to come), let us review Nash-Williams' original proofs. The purpose of this section is to familiarize the reader with the overall structure of those proofs, highlight differences to the approach of this paper, and indicate places where the formalization requires additional work – marked by (D1)–(D3). Since the full proofs are not reproduced, a copy of Nash-Williams' paper [2] might be useful for reference.

Nash-Williams starts by giving a proof of Dickson's lemma: *If A and B are wqo'd, then so is $A \times B$* [2, Lemma 1]. Assume there are two infinite sequences a (over elements of A) and b (over elements of B) that are both known to be good. Then, witnesses i and j such that $i < j$ and $(a\ i,\ b\ i) \preceq (a\ j,\ b\ j)$ have to be constructed. First, construct a subsequence a_φ of a, such that $a_\varphi\ i \preceq_1 a_\varphi\ (i{+}1)$ for all i. Then, since b is good, indices $i < j$ with $b_\varphi\ i \preceq_2 b_\varphi\ j$ are obtained. At this point, in order to obtain $a_\varphi\ i \preceq_1 a_\varphi\ j$ and thus $(a_\varphi\ i,\ b_\varphi\ i) \preceq (a_\varphi\ j,\ b_\varphi\ j)$, transitivity of $\preceq_1$ is essential (refer to theory *Dickson-with-Transitivity* for a formalization of Nash-Williams' original proof, where *TRANS* marks the step in which transitivity is applied). In contrast, the presented formalization proves Dickson's lemma for almost-full relations based on an existing formalization of Ramsey's theorem, thus avoiding the transitivity requirement on $\preceq_1$.

Next comes a proof of Higman's lemma: *If A is wqo'd, then A^* is wqo'd by homeomorphic embedding on lists* [2, Lemma 2]. Assume that the statement is false. Then construct a bad sequence in which every element is as small as possible, i.e., a bad sequence such that replacing any given element by a smaller one, the resulting sequence would be good. The construction is described roughly as follows (where A° is used to denote the set of "objects" built over elements of A; which might refer to the set of finite subsets, the set of finite lists, the set of finite trees, ... in a concrete case):

> *Select an $x_1 \in A^\circ$ such that x_1 is the first term of a bad sequence of members of A° and $|x_1|$ is as small as possible. Then select an x_2 such that x_1, x_2 (in that order) are the first two terms of a bad sequence of members of A° and $|x_2|$ is as small as possible [...]. Assuming the axiom of choice, this process yields a bad sequence [...]*

In the formalization, this construction is realized by a recursive definition (assuming the existence of an appropriate choice-function). But the definition alone

is not enough. It has to be shown that

the definition is well-defined and results in a minimal bad sequence (D1)

where well-definedness relies on the existence of the mentioned choice-function. This is the first place where the formalization requires drastically more details than the original proof. Moreover, it constitutes the most technical part of the formalization.

For now, assume that there is a minimal bad sequence m (which is a sequence of finite lists). Let h be the sequence of heads of m and t the sequence of corresponding tails. It is then shown that

there is no φ *such that* t_φ *is bad and* $\varphi\ 0 \leq \varphi\ i$ *for all* i, (S1)

since otherwise m would not be minimal. Furthermore, let $T = \{t\ i \mid i \geq 0\}$. Then it is stated, without proof, that

a bad sequence over T *indicates a sequence of shape* (S1). (D2)

In the formalization the corresponding proof is mandatory. From the above it follows that T is wqo'd, since there are no bad sequences. Let $H = \{h\ i \mid i \geq 0\}$, which is wqo'd since A is. Then, by Dickson's lemma, $H \times T$ is wqo'd. Hence, there are i and j such that $i < j$ and $(h\ i,\ t\ i) \preceq (h\ j,\ t\ j)$, which implies $m\ i \preceq m\ j$ and thus contradicts the badness of m.

Finally, for the tree theorem the proof structure is very similar to the previous one (only using finite trees instead of finite lists and homeomorphic embedding on trees instead of homeomorphic embedding on lists). Assume that the statement is false. Again a minimal bad sequence m has to be constructed. Instead of heads and tails of lists, now roots and direct subtrees (which are also called successors) of trees are considered. Let r and s denote the sequences of roots and successors of m and $S\ i$ be the set of successors of the i-th tree, i.e., $S\ i = \{x \mid x \in \mathit{set}\ (s\ i)\}$ (note that s is a sequence of finite lists). Then it is shown that

there is no bad sequence t, *such that* $t\ i \in S_\varphi\ i$ *and* $\varphi\ 0 \leq \varphi\ i$ *for all* i, (S2)

since otherwise m would not be minimal. Let $S' = \{t \mid \exists\, i.\ t \in \mathit{set}\ (s\ i)\}$. Then it is stated, without proof, that

a bad sequence over S' *indicates a sequence of shape* (S2). (D3)

Again the formalization needs to provide the corresponding proof.

4 Dickson's Lemma

In essence, the formalization is about preservation of wqo'dness by certain type constructors (Dickson's lemma for pairs, Higman's lemma for lists, and the tree

theorem for trees). For each of these constructors, a way to extend the orders on the base types to an order on the newly constructed type is required. For Dickson's lemma the following is used: Given two orders $\preceq_1$ and $\preceq_2$, the pointwise order on pairs is defined by $(a_1,\ a_2) \preceq (b_1,\ b_2) \stackrel{\text{def}}{=} a_1 \preceq_1 b_1 \wedge a_2 \preceq_2 b_2$.

Before proving Dickson's lemma (i.e., that the pointwise combination of orders preserves wqo'dness when forming Cartesian products), let us have a look at how Ramsey's theorem allows us to disregard transitivity (and hence prove a similar lemma already for almost-full relations rather than wqos; see theory *Almost-Full-Relations* for the formal proof development).

The following variant of Ramsey's theorem (which is part of Isabelle/HOL's library; `~~/src/HOL/Library/Ramsey.thy`) is used:

$$[\![\mathit{infinite}\ Z;\ \forall i{\in}Z.\ \forall j{\in}Z.\ i \neq j \longrightarrow h\ \{i,\ j\} < n]\!]$$
$$\Longrightarrow \exists I\ c.\ I \subseteq Z \wedge \mathit{infinite}\ I \wedge c < n \wedge (\forall i{\in}I.\ \forall j{\in}I.\ i \neq j \longrightarrow h\ \{i,\ j\} = c)$$

In words: Let Z be an infinite set and let h be a function that, given a two-element subset of Z, returns a natural number smaller than n. Then there is an infinite subset I of Z and a natural number c smaller than n such that h encodes all two-element subsets of I by c. More abstractly, assume there is an infinite graph with nodes from Z such that every edge has exactly one of n colors. Then there is an infinite subgraph with nodes from I and all edges of color c.

Using Ramsey's theorem, the auxiliary fact that whenever the union of two binary relations is transitive on an infinite sequence, then there is an infinite subsequence on which either the first or the second relation is transitive, is shown.

Lemma 1. $\mathit{trans}_f(\preceq_1 \cup \preceq_2) \Longrightarrow \exists \varphi.\ \mathit{trans}_\varphi(<) \wedge (\mathit{trans}_{f_\varphi}(\preceq_1) \vee \mathit{trans}_{f_\varphi}(\preceq_2))$

Here φ is a strictly monotone (since $<$ is transitive on it) mapping from natural numbers to natural numbers. Hence, f_φ is a subsequence of f whose elements are in the same relative order.

Proof (of Lemma 1). Assume $\mathit{trans}_f(\preceq_1 \cup \preceq_2)$, which means that

$$\text{for all } i < j, \text{ either } f\ i \preceq_1 f\ j \text{ or } f\ i \preceq_2 f\ j. \qquad (\star)$$

Then colorize the set of two-element subsets $\{i,\ j\}$ of the natural numbers using h, defined by, if $i < j$ and $f\ i \preceq_1 f\ j$, then $h\ \{i,\ j\}$ is *0* (*white*), otherwise *1* (*black*). Now Ramsey's theorem can be applied (since the set of natural numbers is infinite and there are exactly two colors). Thus, an infinite set I of natural numbers and a color c such that for all $i \neq j$ in I, the corresponding color $h\ \{i,\ j\}$ is c, is obtained. Since I is well-ordered, there is a function $\varphi{::}\mathit{nat} \Rightarrow \mathit{nat}$ that enumerates its elements in increasing order, i.e., $\mathit{trans}_\varphi(<)$. Consider the two cases (for arbitrary but fixed $i < j$):

- **case** (c is *white*). Since φ is strictly monotone, also $\varphi\ i < \varphi\ j$. Therefore, $h\ \{\varphi\ i,\ \varphi\ j\} = 0$, and thus $f_\varphi\ i \preceq_1 f_\varphi\ j$.
- **case** (c is *black*). Again, $\varphi\ i < \varphi\ j$. Thus $h\ \{\varphi\ i,\ \varphi\ j\} = 1$, which together with ($\star$) implies $f_\varphi\ i \preceq_2 f_\varphi\ j$. □

Using this auxiliary fact, Dickson's lemma for almost-full relations is shown.

Lemma 2. $[\![af_{A_1}(\preceq_1);\ af_{A_2}(\preceq_2)]\!] \Longrightarrow af_{A_1\times A_2}(\preceq)$

Proof. Assume $af_{A_1}(\preceq_1)$ and $af_{A_2}(\preceq_2)$. Moreover, to derive a contradiction, assume $\neg\ af_{A_1\times A_2}(\preceq)$. Then there is some sequence f on $A_1 \times A_2$ which is bad. Let $x \lhd y$ and $x \blacktriangleleft y$ denote $fst\ x \not\preceq_1 fst\ y$ and $snd\ x \not\preceq_2 snd\ y$, respectively. Since f is bad, also $\forall\, i\ j.\ i < j \longrightarrow f\ i \lhd f\ j \vee f\ i \blacktriangleleft f\ j$, i.e., $trans_f(\lhd \cup \blacktriangleleft)$. Then, by Lemma 1, a strictly monotone mapping φ such that $trans_{f_\varphi}(\lhd)$ or $trans_{f_\varphi}(\blacktriangleleft)$ is obtained. In the first case $fst \circ f_\varphi$ is bad and in the second $snd \circ f_\varphi$ is bad, both contradicting the assumptions. □

The previous lemma trivially extends to wqos.

Dickson's Lemma. $[\![wqo_{A_1}(\preceq_1);\ wqo_{A_2}(\preceq_2)]\!] \Longrightarrow wqo_{A_1\times A_2}(\preceq)$

Proof. Assuming transitivity of $\preceq_1$ on A_1 and $\preceq_2$ on A_2, it is trivial to show transitivity of $\preceq$ on $A_1 \times A_2$. With Lemma 2, this yields Dickson's lemma. □

5 Minimal Bad Sequences

Since the minimal bad sequence argument is needed for Higman's lemma as well as the tree theorem, a general construction that is applicable to both cases is provided (see theory *Minimal-Bad-Sequences* for the formal proof development). To this end, Isabelle/HOL's locale mechanism is employed which allows us to define new constants and prove facts using an "interface" of hypothetical constants and assumptions. As long as the assumptions can be discharged, the new constants and proven facts can be instantiated to arbitrary special cases.

Below, the locale *mbs* which captures the construction of a minimal bad sequence over elements from a given set is described (an early version, that could be simplified drastically since, was presented at the *Isabelle Users Workshop* in 2012 [13]). The locale fixes the following constants:

- The set of elements A, and
- a binary relation $\lhd$ that is used to compare the structural size of elements.

Furthermore, it has the assumptions:

$$wf_A(\lhd) \tag{M1}$$
$$[\![x \lhd y;\ y \lhd z]\!] \Longrightarrow x \lhd z \tag{M2}$$

That is, the structural comparison is well-founded on A (M1) (thus, it makes sense to talk about *minimal* elements) and transitive (M2). It turns out that these ingredients are enough to construct – under the assumption that there is a bad sequence – a minimal bad sequence. Informally, an infinite bad sequence is a *minimal* bad sequence, when replacing any element by a smaller one, turns it into a good sequence.

Definition 1 (Minimality). More formally, let an infinite sequence f be *minimal at position* n, written $min^n_{\preceq}(f)$, iff

$$\forall\, g.\ (\forall\, i.\ g\ i \in A) \wedge (\forall\, i{<}n.\ g\ i = f\ i) \wedge g\ n \lhd f\ n \longrightarrow good_{\preceq}(g)$$

A sequence is *minimal* if it is minimal at every position.

In words, the definition of $min^n_{\preceq}(f)$ is: for every sequence g whose initial part up to (but not including) position n coincides with f and where the n-th element of g is strictly smaller than the n-th element of f; g is good. This definition facilitates the construction of a minimal bad sequence from a given bad sequence by iterating over its positions: elements before the current position stay fixed and at the current position an element that is as small as possible is inserted.

As indicated above, a given sequence is modified iteratively. To this end the following auxiliary lemma is employed (which shows that from a sequence that is minimal at position n, a sequence that is also minimal at the next position $n{+}1$, can be obtained):

Lemma 3. $[\![\forall\, i.\ f\ i \in A;\ bad_{\preceq}(f);\ min^n_{\preceq}(f)]\!]$
$\Longrightarrow \exists\, g.\ (\forall\, i{\leq}n.\ g\ i = f\ i) \wedge$
$g\ (n{+}1) \trianglelefteq f\ (n{+}1) \wedge (\forall\, i.\ g\ i \in A) \wedge bad_{\preceq}(g) \wedge min^{n+1}_{\preceq}(g)$

Proof. Since $\lhd$ is well-founded on A, the induction schema

$$[\![x \in A;\ \bigwedge x.\ [\![x \in A;\ \bigwedge y.\ [\![y \in A;\ y \lhd x]\!] \Longrightarrow P\ y]\!] \Longrightarrow P\ x]\!] \Longrightarrow P\ x$$

is valid. Assume $\forall\, i.\ f\ i \in A$, $bad_{\preceq}(f)$, and $min^n_{\preceq}(f)$. Let $\exists\, g.\ \mathfrak{C}\ g\ f\ (f\ (n{+}1))$ abbreviate the conclusion of Lemma 3 (parametrized over the sequences g and f and the element on which induction will be applied). In order for the later induction to go through, a slightly stronger statement than Lemma 3 is shown. To this end, let $\mathfrak{I}\ x$ abbreviate

$$\forall f.\ x = f\ (n{+}1) \wedge (\forall\, i.\ f\ i \in A) \wedge bad_{\preceq}(f) \wedge min^n_{\preceq}(f) \longrightarrow (\exists\, g.\ \mathfrak{C}\ g\ f\ x)$$

(i.e., generalize over f and let x – on which well-founded induction will be applied – equal the $n{+}1$-th element of f).

For an arbitrary but fixed x, let $x = f\ (n{+}1)$. Hence, from the assumption $\forall\, i.\ f\ i \in A$ it follows that $x \in A$. Now the above induction schema is used to prove (discharging its first assumption by $x \in A$): $\bigwedge x.\ x = f\ (n{+}1) \Longrightarrow \mathfrak{I}\ x$.

Thus, $x \in A$ for some arbitrary but fixed x, and $\bigwedge y.\ [\![y \in A;\ y \lhd x]\!] \Longrightarrow \mathfrak{I}\ y$ is the induction hypothesis (IH). Then show $\mathfrak{I}\ x$.

To this end, assume $x = f\ (n{+}1)$, $\forall\, i.\ f\ i \in A$, $min^n_{\preceq}(f)$, and $bad_{\preceq}(f)$ for some arbitrary but fixed f. Now either $min^{n+1}_{\preceq}(f)$, concluding the proof, or there is a sequence h such that

$$h\ (n{+}1) \lhd f\ (n{+}1) \tag{1}$$
$$\forall\, i{<}n{+}1.\ h\ i = f\ i \tag{2}$$
$$\forall\, i.\ h\ i \in A \tag{3}$$
$$bad_{\preceq}(h) \tag{4}$$

employing Definition 1. From (1), (3), and the IH, obtain $\mathfrak{I}\ (h\ (n{+}1))$. Moreover, from (2) and $min^n_{\preceq}(f)$ it follows that $min^n_{\preceq}(h)$, which together with (4) yields a sequence m that satisfies $\mathfrak{C}\ m\ h\ (h\ (n{+}1))$. Additionally, from (1) and transitivity of $\trianglelefteq$ it follows that $m\ (n{+}1) \trianglelefteq x$. Combining the previous facts, we obtain $\exists\, m.\ \mathfrak{C}\ m\ f\ x$, thus finishing the prove of $\bigwedge x.\ x = f\ (n{+}1) \Longrightarrow \mathfrak{I}\ x$. Choosing $x = f\ (n{+}1)$ (i.e., discharging the first assumption by reflexivity) and using the initial assumptions yields $\exists\, g.\ \mathfrak{C}\ g\ f\ (f\ (n{+}1))$. □

For a step-wise construction of a minimal bad sequence it remains to be shown that from an arbitrary bad sequence, one that is minimal at position *0* can be obtained. This is taken care of by the next lemma.

Lemma 4. $[\![\forall\, i.\ f\, i \in A;\ bad_{\preceq}(f)]\!] \Longrightarrow \exists\, g.\ (\forall\, i.\ g\ i \in A) \wedge min^0_{\preceq}(g) \wedge bad_{\preceq}(g)$

Proof. Similar structure to the proof of Lemma 3 (but much simpler). □

At this point it can be shown that if a relation is not almost-full, then there is a minimal bad sequence, thereby taking care of (D1).

Theorem 1. $\neg\ af_A(\preceq) \Longrightarrow \exists\, m.\ bad_{\preceq}(m) \wedge (\forall\, n.\ min^n_{\preceq}(m)) \wedge (\forall\, i.\ m\ i \in A)$

Proof. Assume $\neg\ af_A(\preceq)$. Then there is a bad sequence f, i.e., $\forall\, i.\ f\, i \in A$ and $bad_{\preceq}(f)$. From Lemma 4 a bad sequence g that is minimal at its first position is obtained. Then, with Lemma 3, together with the axiom of choice,[3] a choice function ν such that

$$
\begin{array}{l}
\forall\, f\ n.\\
\quad (\forall\, i.\ f\ i \in A) \wedge min^n_{\preceq}(f) \wedge bad_{\preceq}(f) \longrightarrow\\
\quad (\forall\, i.\ \nu\ f\ n\ i \in A) \wedge\\
\quad (\forall\, i{\leq}n.\ \nu\ f\ n\ i = f\ i) \wedge\\
\quad \nu\ f\ n\ (n{+}1) \trianglelefteq f\ (n{+}1) \wedge bad_{\preceq}(\nu\ f\ n) \wedge min^{n+1}_{\preceq}(\nu\ f\ n)
\end{array}
$$

is obtained. That is, $\nu\ f\ n$ provides a witness to Lemma 3, provided that f and n satisfy its assumptions.

Then define an auxiliary sequence (of sequences) m' by $m'\ 0 = g$ and $m'\ (n{+}1) = \nu\ (m'\ n)\ n$. The desired minimal bad sequence m, is defined to be $\lambda i.\ m'\ i\ i$ (i.e., the "diagonal" of the auxiliary sequence m'). Of course, it has to be *proven* that m actually is a minimal bad sequence. To this end, the following statements are simultaneously shown by induction on n (i.e., they are true for any n):

$$
\begin{array}{ll}
\forall\, i.\ m'\ n\ i \in A & \forall\, i{\leq}n.\ min^i_{\preceq}(m'\ n)\\
\forall\, i{\leq}n.\ m\ i = m'\ n\ i & bad_{\preceq}(m'\ n)
\end{array}
$$

From this $bad_{\preceq}(m)$ can be shown as follows: Assume that m is not bad, then there are indices i and j, such that $m\ i \preceq m\ j$; but then also $m'\ j\ i \preceq m'\ j\ j$, contradicting $bad_{\preceq}(m'\ j)$. Moreover, from $\forall\, n\ i.\ i \leq n \longrightarrow min^i_{\preceq}(m'\ n)$ it is easy to show that $\forall\, n.\ min^n_{\preceq}(m)$. Ultimately, from $\forall\, n\ i.\ m'\ n\ i \in A$, it follows that $\forall\, i.\ m\ i \in A$, concluding the proof. □

[3] In Isabelle/HOL: $\forall\, x.\ \exists\, y.\ Q\ x\ y \Longrightarrow \exists f.\ \forall\, x.\ Q\ x\ (f\ x)$.

6 Higman's Lemma

Before Higman's lemma for almost-full relations is stated formally, a construction that extends a given order on elements to an order on lists is required: *homeomorphic embedding*. Furthermore, a kind of structural comparison between lists as well as the set of lists built over a given set of elements is needed. The set of lists over elements from a set A, written A^*, is defined inductively:

$$\frac{}{[] \in A^*} \qquad \frac{x \in A \qquad xs \in A^*}{x{\cdot}xs \in A^*}$$

The list xs is a *proper suffix* of the list ys iff $\exists\, us.\ ys = us \mathbin{@} xs \wedge us \neq []$ (written $xs < ys$). Homeomorphic embedding on lists, for a given base order $\preceq$, is defined inductively by the rules

$$\frac{}{[] \preceq^* ys} \qquad \frac{xs \preceq^* ys}{xs \preceq^* y{\cdot}ys} \qquad \frac{x \preceq^= y \qquad xs \preceq^* ys}{x{\cdot}xs \preceq^* y{\cdot}ys}$$

where $R^=$ denotes the reflexive closure of R. Note that this definition makes $\preceq^*$ reflexive for arbitrary $\preceq$. For reflexive (and thus also for almost-full) $\preceq$, the assumption $x \preceq^= y$ can be replaced by $x \preceq y$. Intuitively, it might be easier to think about homeomorphic embedding on lists as follows: a list xs is embedded in a list ys iff xs can be obtained from ys by dropping elements and replacing elements with arbitrary smaller ones (w.r.t. the base order). An important special case of embedding is $=^*$, which is called the *sublist relation*. Then, $xs =^* ys$ iff the list xs can be obtained from the list ys by dropping elements.

Using the definitions above, the *mbs* locale can be instantiated as follows (for some arbitrary relation $\preceq$): use A^* for A and $<$ for $\lhd$. The assumptions of the *mbs* locale are discharged by the following facts:

$$wf_{A^*}(<) \qquad\qquad [\![xs < ys;\ ys < zs]\!] \Longrightarrow xs < zs$$

Thus,

$$\neg\ af_{A^*}(\preceq^*) \Longrightarrow \exists\, m.\ bad_{\preceq^*}(m) \wedge (\forall\, n.\ min^n_{\preceq^*}(m)) \wedge (\forall\, i.\ m\ i \in A^*)$$

which allows us to prove Higman's lemma for almost-full relations.

Lemma 5. $af_A(\preceq) \Longrightarrow af_{A^*}(\preceq^*)$

Proof. Assume $af_A(\preceq)$ but $\neg\ af_{A^*}(\preceq^*)$, for the sake of a contradiction. Then there is a bad sequence f. This, in turn, implies the existence of a minimal bad sequence m. All lists in m are non-empty (since otherwise m would be good). Hence, there are sequences h and t of heads and tails of m (i.e., $m\ i = h\ i{\cdot}t\ i$).

First, it is shown that there is no index-mapping φ such that $\varphi\ 0 \leq \varphi\ i$ for all i and the sequence t_φ is bad. Assume, to the contrary, that such a φ exists. Let n abbreviate $\varphi\ 0$ and c be the combination of m with t, defined by $c\ i \stackrel{\text{def}}{=} \mathit{if}\ i < n\ \mathit{then}\ m\ i\ \mathit{else}\ t\ (\varphi\ (i - n))$ (i.e., c is the same as t_φ, but prepended by the first n elements of m). Then c is bad, since otherwise a contradiction is obtained as follows: Assume c is good. Then there are $i < j$ such that $c\ i \preceq^* c\ j$. Now, analyze the following cases:

– **case** ($j < n$). Then $m\ i \preceq^* m\ j$, contradicting badness of m.
– **case** ($n \leq i$). Let $i' = i - n$ and $j' = j - n$. Then $i' < j'$ and $t_\varphi\ i' \preceq^* t_\varphi\ j'$, contradicting badness of t_φ.
– **case** ($i < n$ and $n \leq j$). Let $j' = j - n$. Then $t\ (\varphi\ j') \leq m\ (\varphi\ j')$ (since the tail of a non-empty list is obviously also a suffix) and $m\ i \preceq^* t\ (\varphi\ j')$ (from $c\ i \preceq^* c\ j$). Moreover, $m\ i \preceq^* m\ (\varphi\ j')$ (since the suffix relation is a special case of embedding and embedding is transitive). Together with $i < \varphi\ j'$, this contradicts the badness of m.

Thus, c is bad. Furthermore, $\forall\, i{<}n.\ c\ i = m\ i$ and $c\ n < m\ n$, and thus c is good (since m is minimal): A contradiction, concluding the proof of

$$\nexists\, \varphi.\ (\forall\, i.\ \varphi\ 0 \leq \varphi\ i) \wedge \mathit{bad}_{\preceq^*}(t_\varphi). \tag{$\star$}$$

Let H and T denote the sets of heads and tails of the lists in m, respectively, i.e., $H = \{h\ i \mid i \geq 0\}$ and $T = \{t\ i \mid i \geq 0\}$. Obviously $\preceq$ is almost-full on H, since $H \subseteq A$ and $\preceq$ is almost-full on A. Moreover, since every bad sequence over T would admit a subsequence of the shape in ($\star$), the relation $\preceq^*$ is almost-full on T. With Lemma 2, it is shown that the pointwise combination of $\preceq$ and $\preceq^*$ is almost-full on $H \times T$. Thus, there are $i < j$ with $h\ i \preceq^{=} h\ j$ and $t\ i \preceq^* t\ j$. By definition of $\preceq^*$, this implies $m\ i \preceq^* m\ j$, contradicting the badness of m. □

But wait a moment, "*since every bad sequence over* $T \ldots$" above, is exactly (D2), for which a proof has to be provided.

Lemma 6. $[\![\mathit{refl}_{\{t\ i \mid i \geq 0\}}(\preceq);\ \forall\, i.\ f\ i \in \{t\ i \mid i \geq 0\};\ \mathit{bad}_{\preceq}(f)]\!]$
$\Longrightarrow \exists\, \varphi.\ (\forall\, i.\ \varphi\ 0 \leq \varphi\ i) \wedge \mathit{bad}_{\preceq}(t_\varphi)$

Proof. Assume that $\preceq$ is reflexive (on $\{t\ i \mid i \geq 0\}$), and f is a bad sequence (over $\{t\ i \mid i \geq 0\}$). First note that for every i, there exists a j such that $f\ i = t\ j$. By the axiom of choice, an index-mapping φ' with $f\ i = t_{\varphi'}\ i$ for all i is obtained. Since f is bad, also $t_{\varphi'}$ is bad. Next it is shown that

$$\text{for every } i \text{ there is a } j > i \text{ such that } \varphi'\ 0 \leq \varphi'\ j. \tag{$\star$}$$

Assume otherwise, then there is some i such that for all $j > i$ the index-mapping satisfies $\varphi\ j < \varphi'\ 0$. Thus, the image of φ' under $\{j \mid i < j\}$ is finite, whereas $\{j \mid i < j\}$ itself is infinite. By the pigeonhole principle, a $k > i$ is obtained such that there are infinitely many $j > i$ with $\varphi'\ j = \varphi'\ k$. But then, there is some $l > k$ for which $\varphi'\ l = \varphi'\ k$. Since $\preceq$ is reflexive and $k < l$, this implies that $t_{\varphi'}$ is good; a contradiction. Using ($\star$) and the axiom of choice, an index-mapping ψ' such that $i < \psi'\ i$ and $\varphi'\ 0 \leq \varphi'\ (\psi'\ i)$ for all i, is obtained. Now, let ψ abbreviate $\lambda i.\ \psi'^{i}\ 0$ (the i-fold application of ψ' to 0) and φ abbreviate $\varphi' \circ \psi$. Then, ψ is strictly monotone and $\varphi\ 0 \leq \varphi\ i$ for all i. Moreover, since $t_{\varphi'}$ is bad and ψ is monotone, also t_φ is bad. This concludes the proof. □

Higman's Lemma. $\mathit{wqo}_A(\preceq) \Longrightarrow \mathit{wqo}_{A^*}(\preceq^*)$

Proof. For transitivity of $\preceq^*$ (under the assumption that $\preceq$ is transitive), refer to lemma *list-hembeq-trans* in theory *Sublist*. Together with Lemma 5, this yields Higman's lemma. □

7 The Tree Theorem

The tree theorem is for finite trees, what Higman's lemma is for finite lists. However, whereas for finite lists, their representation inside Isabelle/HOL is quite unambiguous and the existing data type is generally applicable; this is not so much the case for finite trees. Consider the following two data types

datatype $\alpha\ t = \mathit{Node}\ \alpha\ (\alpha\ t\ \mathit{list})$
datatype $\alpha\ t' = \mathit{Empty} \mid \mathit{Node}\ \alpha\ (\alpha\ t'\ \mathit{list})$

or the type of first-order terms

datatype $(\alpha, \beta)\ \mathit{term} = \mathit{Var}\ \beta \mid \mathit{Fun}\ \alpha\ ((\alpha, \beta)\ \mathit{term}\ \mathit{list})$

also a kind of finite tree (and more importantly, one of the types to which the tree theorem is applied, in order to formalize the fact that the Knuth-Bendix order is a simplification order [8]). Restricting the tree theorem to a specific data type would strongly restrict its applicability. Therefore, again Isabelle/HOL's locale mechanism is employed. This time, for a locale *finite-tree* that fixes the following constants (see theory *Finite-Tree* for details):

- A function $\mathit{mk}::\beta \Rightarrow \alpha\ \mathit{list} \Rightarrow \alpha$ that is used to construct a finite tree from a given node and a given list of finite trees.
- A function $\mathit{root}::\alpha \Rightarrow \beta$ that extracts the root node from a given tree.
- As well as a function $\mathit{succs}::\alpha \Rightarrow \alpha\ \mathit{list}$ that extracts the list of direct subtrees (successors) from a given tree.

These constants are required to satisfy the following assumptions (thereby turning *mk* into kind of a data type constructor with extractors *root* and *succs*):

$$\mathit{root}\ (\mathit{mk}\ f\ ts) = f \tag{F1}$$
$$\mathit{succs}\ (\mathit{mk}\ f\ ts) = ts \tag{F2}$$
$$(\mathit{mk}\ f\ ss = \mathit{mk}\ g\ ts) = (f = g \wedge ss = ts) \tag{F3}$$

As opposed to a real data type, the above assumptions do not guarantee that *all* finite trees are built from a finite number of applications of *mk*. Thus, the set of finite trees over nodes from A, written $\mathcal{T}(A)$, is defined inductively by:

$$\frac{f \in A \qquad \forall\, t{\in}\mathit{set}\ ts.\ t \in \mathcal{T}(A)}{\mathit{mk}\ f\ ts \in \mathcal{T}(A)}$$

The notion of structural decrease, as needed to instantiate the *mbs* locale, is provided by the *subtree* relation:

$$\frac{t \in \mathit{set}\ ts}{t \lhd \mathit{mk}\ f\ ts} \qquad \frac{s \lhd t \qquad t \in \mathit{set}\ ts}{s \lhd \mathit{mk}\ f\ ts}$$

Where a tree s is a proper subtree of another tree t, if it is either a direct subtree of t itself or a proper subtree of one of the direct subtrees of t.

Homeomorphic embedding on finite trees is also defined inductively by:

$$\frac{t \in set\ ts}{t \preceq_{\mathsf{emb}} mk\ f\ ts} \qquad \frac{s \preceq_{\mathsf{emb}} t \qquad t \preceq_{\mathsf{emb}} u}{s \preceq_{\mathsf{emb}} u}$$

$$\frac{s \preceq_{\mathsf{emb}} t}{mk\ f\ (ss_1\ @\ s{\cdot}ss_2) \preceq_{\mathsf{emb}} mk\ f\ (ss_1\ @\ t{\cdot}ss_2)} \qquad \frac{f \preceq^{=} g \qquad ss =^{*} ts}{mk\ f\ ss \preceq_{\mathsf{emb}} mk\ g\ ts}$$

The first three rules are easy: homeomorphic embedding extends the subtree relation, is transitive, and is closed under contexts. The last rule states that the nodes of a tree may be replaced by smaller ones (w.r.t. $\preceq$) and that arbitrary successors may be dropped. From this definition, the following property can be shown:

Lemma 7. $[\![f \preceq^{=} g;\ ss \preceq_{\mathsf{emb}}{}^{*}\ ts]\!] \Longrightarrow mk\ f\ ss \preceq_{\mathsf{emb}} mk\ g\ ts$

Proof. This property seems obvious, as $\preceq_{\mathsf{emb}}$ is reflexive, transitive, and closed under contexts. However, it turns out to be surprisingly tedious to formalize (or at least *the author* did not find an elegant way). To spare the reader some tedium the details (to be found in lemma *tree-hembeq-list-hembeq* of theory *Finite-Tree*) are skipped. □

To instantiate the *mbs* locale, the following facts (see [6] for proofs) are shown:

$$wf_{\mathcal{T}(A)}(\lhd) \qquad\qquad [\![s \lhd t;\ t \lhd u]\!] \Longrightarrow s \lhd u$$

Thus,

$$\neg\ af_{\mathcal{T}(A)}(\preceq_{\mathsf{emb}}) \Longrightarrow \exists\, m.\ bad_{\preceq_{\mathsf{emb}}}(m) \wedge (\forall\, n.\ min^{n}_{\preceq_{\mathsf{emb}}}(m)) \wedge (\forall\, i.\ m\ i \in \mathcal{T}(A))$$

Finally, the tree theorem for almost-full relations can be stated and proved (see theory *Kruskal* for details).

Theorem 2. $af_A(\preceq) \Longrightarrow af_{\mathcal{T}(A)}(\preceq_{\mathsf{emb}})$

Proof. Assume $af_A(\preceq)$ but $\neg\ af_{\mathcal{T}(A)}(\preceq_{\mathsf{emb}})$ for the sake of a contradiction. Then there is a bad sequence and thus a minimal bad sequence m. All trees in m are in the set $\mathcal{T}(A)$ (and thus non-empty). Hence, there are sequences r and s of roots and successor lists of the trees in m (i.e., $m\ i = mk\ (r\ i)\ (s\ i)$).

First it is shown that there is no sequence of trees t and index-mapping φ such that $t\ i \in set\ (s_\varphi\ i)$ (i.e., the sequence t selects an arbitrary successor of $m_\varphi\ i$ as its i-th element) and $\varphi\ 0 \leq \varphi\ i$ for all i, and t is bad. Assume, to the contrary, that such t and φ exist. Let n abbreviate $\varphi\ 0$ and c be the sequence defined by $c\ i \stackrel{\text{def}}{=} \mathit{if}\ i < n\ \mathit{then}\ m\ i\ \mathit{else}\ t\ (i - n)$. Then c is bad, since assuming that it was good results in a contradiction by a similar case analysis conducted in the proof of Lemma 5 above. Furthermore, $\forall\, i{<}n.\ c\ i = m\ i$ and $c\ n \lhd m\ n$,

and thus c is good (since m is minimal). This contradiction concludes the proof of

$$\nexists\, t\ \varphi.\ (\forall\, i.\ t\ i \in \mathit{set}\ (s_\varphi\ i) \wedge \varphi\ 0 \leq \varphi\ i) \wedge \mathit{bad}_{\preceq_{\mathsf{emb}}}(t). \qquad (\star)$$

Let R and S denote the sets of roots and successor lists of trees in m, respectively, i.e., $R = \{r\ i \mid i \geq 0\}$ and $S = \{s\ i \mid i \geq 0\}$). Clearly, $\preceq$ is almost-full on R (since $R \subseteq A$). Let S' abbreviate $\{t \mid \exists\, i.\ t \in \mathit{set}\ (s\ i)\}$. Every bad sequence over S' would admit a sequence of the shape in ($\star$), thus $\preceq_{\mathsf{emb}}$ is almost-full on S'. From Lemma 5, together with $S \subseteq S'^*$, it follows that ${\preceq_{\mathsf{emb}}}^*$ is almost-full on S. With Lemma 2, it follows that the pointwise combination of $\preceq$ and ${\preceq_{\mathsf{emb}}}^*$ is almost-full on $R \times S$. Thus, there are $i < j$ such that $r\ i \preceq^{=} r\ j$ and $s\ i \preceq_{\mathsf{emb}}^*\ s\ j$, which, employing Lemma 7, implies that $m\ i \preceq_{\mathsf{emb}}\ m\ j$ and thus contradicts the badness of m. □

Note that "*Every bad sequence over S' ...*" above, corresponds to (D3). The corresponding proof is required.

Lemma 8. *Let $\preceq$ be a binary relation and X be the set $\{t \mid \exists\, i.\ t \in \mathit{set}\ (s\ i)\}$ for a sequence of lists s. Then,*

$$[\![\mathit{refl}_X(\preceq);\ \forall\, i.\ f\ i \in X;\ \mathit{bad}_{\preceq}(f)]\!]$$
$$\Longrightarrow \exists\, t\ \varphi.\ (\forall\, i.\ t\ i \in \mathit{set}\ (s_\varphi\ i) \wedge \varphi\ 0 \leq \varphi\ i) \wedge \mathit{bad}_{\preceq}(t)$$

Proof. The proof is structured similarly to the proof of Lemma 6 but slightly more involved, due to the extra indirection via list elements. For details, refer to lemma *bad-of-special-shape'* in theory *Kruskal-Auxiliaries* of [6]. □

Kruskal's Tree Theorem. $\mathit{wqo}_A(\preceq) \Longrightarrow \mathit{wqo}_{\mathcal{T}(A)}(\preceq_{\mathsf{emb}})$

Proof. Theorem 2 and transitivity of $\preceq_{\mathsf{emb}}$ yield the tree theorem. □

8 Conclusions and Related Work

An Isabelle/HOL formalization of three important results from combinatorics was presented: Dickson's lemma, Higman's lemma, and Kruskal's tree theorem.

Parts of the presented formalization were used by Wu et al. [14] to formalize a proof of: *For every language A, the languages of sub- and superstrings of A are regular.* (Details are presented in a submitted journal version of [15].)

Moreover, the presented formalization of the tree theorem is employed for a proof that the Knuth-Bendix order is a simplification order [8]. To this end, actually a variant of the tree theorem as presented in this paper is needed – which might be called *the term theorem*. The reason is that in the above mentioned proof it is essential to consider arities of function symbols, whereas in Section 7, a node in a tree is allowed to have an arbitrary (finite) number of successors.

It is left as future work to investigate whether the tedious induction in the proof of Theorem 1 can be replaced by an invocation of Zorn's lemma (and this

in turn, by an application of open induction [16,17], thereby hopefully giving also insight into the computational content of the minimal bad sequence argument).

There are formalizations of Higman's lemma in Isabelle/HOL by Berghofer [18] and using other proof assistants by Murthy [19], Fridlender [20], Herbelin [21], Seisenberger [22], and Martín-Mateos et al. [23].

Since Berghofer's work was also conducted using Isabelle/HOL, some comments on the relation to the presented work are in order. First note that Berghofer's formalization is constructive (based on an earlier proof by Coquand and Fridlender in an unpublished manuscript entitled *A Proof of Higman's Lemma by Structural Induction*). Furthermore, it is restricted to a two letter alphabet (and Berghofer notes that *"the extension of the proof to an arbitrary finite alphabet is not at all trivial"*). Also noteworthy is that the focus of Berghofer's work is on program extraction and the computational behavior of the resulting program. In contrast, the presented work constitutes a formalization of Higman's lemma without restricting the alphabet, i.e., the alphabet may be infinite as long as it is equipped with a wqo (which is always the case for finite alphabets).

An intuitionistic proof of Kruskal's tree theorem is presented in [11]. However, to the best of the author's knowledge the presented work constitutes the first formalization of the tree theorem in a proof assistant ever.

Acknowledgments. I thank Mizuhito Ogawa for helpful discussions on everything related to the tree theorem, as well as enabling (together with the Austrian Science Fund) my stay in Japan.

References

1. Kruskal, J.B.: Well-quasi-ordering, the tree theorem, and Vazsonyi's conjecture. Trans. Amer. Math. Soc. **95**(2) (1960) 210–225 doi:10.2307/1993287.
2. Nash-Williams, C.S.J.A.: On well-quasi-ordering finite trees. Proc. Cambridge Philos. Soc. **59**(4) (1963) 833–835 doi:10.1017/S0305004100003844.
3. Dickson, L.E.: Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors. Amer.J.Math. **35**(4) (1913) 413–422 doi:10.2307/2370405.
4. Higman, G.: Ordering by divisibility in abstract algebras. Proc. London Math. Soc. **s3-2**(1) (1952) 326–336 doi:10.1112/plms/s3-2.1.326.
5. Nipkow, T., Paulson, L.C., Wenzel, M.: Isabelle/HOL - A Proof Assistant for Higher-Order Logic. Volume 2283 of LNCS. Springer (2002) doi:10.1007/3-540-45949-9.
6. Sternagel, C.: Well-Quasi-Orders. In Klein, G., Nipkow, T., Paulson, L.C., eds.: AFP. (2012) http://afp.sf.net/devel-entries/Well_Quasi_Orders.shtml.
7. Middeldorp, A., Zantema, H.: Simple termination of rewrite systems. Theor. Comput. Sci. **175**(1) (1997) 127–158 doi:10.1016/S0304-3975(96)00172-7.
8. Sternagel, C., Thiemann, R.: Formalizing Knuth-Bendix orders and Knuth-Bendix completion. In van Raamsdonk, F., ed.: RTA'13. Volume 21 of LIPIcs., Schloss Dagstuhl (2013) 286–301 doi:10.4230/LIPIcs.RTA.2013287.
9. Wenzel, M.: Isabelle/Isar – A Versatile Environment for Human-readable Formal Proof Documents. PhD thesis, Technische Universität München (2002) http://tumb1.biblio.tu-muenchen.de/publ/diss/in/2002/wenzel.pdf.

10. Haftmann, F., Klein, G., Nipkow, T., Schirmer, N.: LaTeX sugar for Isabelle documents (2013) http://isabelle.in.tum.de/dist/Isabelle2013/doc/sugar.pdf.
11. Veldman, W.: An intuitionistic proof of Kruskal's theorem. Arch. Math. Logic **43**(2) (2004) 215–264 doi:10.1007/s00153-003-0207-x.
12. Vytiniotis, D., Coquand, T., Wahlstedt, D.: Stop when you are almost-full - adventures in constructive termination. In Beringer, L., Felty, A., eds.: ITP'12. Volume 7406 of LNCS., Springer (2012) 250–265 doi:10.1007/978-3-642-32347-8_17.
13. Sternagel, C.: A locale for minimal bad sequences. In: IUW'12. arXiv:1208.1366.
14. Wu, C., Zhang, X., Urban, C.: The Myhill-Nerode theorem based on regular expressions. In Klein, G., Nipkow, T., Paulson, L.C., eds.: AFP. (2011) http://afp.sf.net/entries/Myhill-Nerode.shtml.
15. Wu, C., Zhang, X., Urban, C.: A formalisation of the Myhill-Nerode theorem based on regular expressions (proof pearl). In van Eekelen, M., Geuvers, H., Schmaltz, J., Wiedijk, F., eds.: ITP'11. Volume 6898 of LNCS., Springer (2011) 341–356 doi:10.1007/978-3-642-22863-6_25.
16. Raoult, J.C.: Proving open properties by induction. Inform. Process. Lett. **29**(1) (1988) 19–23 doi:10.1016/0020-0190(88)90126-3.
17. Ogawa, M., Sternagel, C.: Open Induction. In Klein, G., Nipkow, T., Paulson, L.C., eds.: AFP. (2012) http://afp.sf.net/devel-entries/Open_Induction.shtml.
18. Berghofer, S.: A constructive proof of Higman's lemma in Isabelle. In Berardi, S., Coppo, M., Damiani, F., eds.: TYPES'03. Volume 3085 of LNCS., Springer (2004) 66–82 doi:10.1007/978-3-540-24849-1_5.
19. Murthy, C.R.: Extracting Constructive Content from Classical Proofs. PhD thesis, Cornell University (1990) http://hdl.handle.net/1813/6991.
20. Fridlender, D.: Higman's lemma in type theory. In Giménez, E., Paulin-Mohring, C., eds.: TYPES'96. Volume 1512 of LNCS., Springer (1996) 112–133 doi:10.1007/BFb0097789.
21. Herbelin, H.: A program from an A-translated impredicative proof of Higman's lemma (1994) http://coq.inria.fr/pylons/contribs/view/HigmanNW/v8.3.
22. Seisenberger, M.: On the Constructive Content of Proofs. PhD thesis, LMU Munich (2003) http://nbn-resolving.de/urn:nbn:de:bvb:19-16190.
23. Martín-Mateos, F.J., Ruiz-Reina, J.L., Alonso, J.A., Hidalgo, M.J.: Proof pearl: A formal proof of Higman's lemma in ACL2. J. Autom. Reason. **47**(3) (2011) 229–250 doi:10.1007/s10817-010-9178-x.