Certified Kruskal's Tree Theorem

CHRISTIAN STERNAGEL
University of Innsbruck, Austria

This article presents the first formalization of Kurskal's tree theorem in a proof assistant. The Isabelle/HOL development is along the lines of Nash-Williams' original minimal bad sequence argument for proving the tree theorem. Along the way, proofs of Dickson's lemma and Higman's lemma, as well as some technical details of the formalization are discussed.

1. INTRODUCTION

Termination is a key ingredient for total correctness of programs and thus key to program verification. Instead of focusing on a specific programming language, termination is typically considered in a more abstract setting. In this respect, one of the most studied models of computation is term rewriting, as confirmed by the many automatic tools that are available nowadays (e.g., AProVE [GSKT06], C*i*ME [CCF+11], Matchbox [Wal04], MU-TERM [AGLNM11], $\mathsf{T_TT_2}$ [KSZM09], and VMTL [SG09]; to name a few). A central task in this area is to synthesize well-founded relations. Often this is done incrementally, e.g., a given well-founded relation is extended to a bigger structure, like sets, multisets, lists, etc. Since this is not always easy, there is interest in stronger conditions than well-foundedness that preserve well-foundedness when extending a given order to bigger structures in more cases. To illustrate the issue, consider the following example.

Example 1.1. Given a quasi-order $\leq$ and two sets A and B, write $A \leq^+ B$ whenever for every $a \in A$ there is some $b \in B$ such that $a \leq b$. In other words, B majorizes A element-wise. One might ask whether the strict part of $\leq^+$, i.e., $<^+ \, = \, \leq^+ \setminus \geq^+$, is well-founded whenever the strict part of $\leq$ is. The following counterexample shows that this is not the case. Take $\geq_{\mathsf{d}}$ to denote the divisibility order on natural numbers, i.e, $m \geq_{\mathsf{d}} n$ whenever there is a natural number k such that $k \cdot n = m$. Note that the strict part of $\geq_{\mathsf{d}}$ is well-founded but allows for infinite antichains, e.g., the sequence $p_1, p_2, p_3, \ldots$ of all prime numbers in increasing order. Now let P_i denote the set of all prime numbers starting from the first i-th, i.e., $P_i = \{p_k\}_{k \geq i}$. Then we obtain the strictly decreasing sequence

$$P_1 >^+_{\mathsf{d}} P_2 >^+_{\mathsf{d}} P_3 >^+_{\mathsf{d}} \cdots$$

showing that $>_{\mathsf{d}}$ is not well-founded.

This research was supported by the Austrian Science Fund (FWF) project J3202.

It turns out that by preventing infinite antichains, one can obtain well-foundedness of (the strict part of) $\leq^+$, i.e., when the given quasi-order $\leq$ does not allow for infinite antichains *and* its strict part is well-founded, then so is the strict part of $\leq^+$. An order satisfying these two conditions (or several equivalent ones) is called a *well-quasi-order* (wqo for short).

A famous result of wqo theory is Kruskal's tree theorem [Kru60] (sometimes called *the* tree theorem or Kruskal's theorem in the following).

Kruskal's Tree Theorem. *Whenever a set A is well-quasi-ordered by a relation $\preceq$, then the set of finite trees over A is well-quasi-ordered by homeomorphic embedding w.r.t. $\preceq$.*

Its usefulness for termination proving was first shown by Dershowitz [Der79, Der82], who employed *simplification orders* – a class of reduction orders for which well-foundedness follows from Kruskal's theorem.

Nash-Williams gave a short and elegant proof of the tree theorem [NW63], where he first established what is now known as the *minimal bad sequence argument*: first assume the existence of a minimal "bad" infinite sequence of elements, then construct an even smaller "bad" infinite sequence, thus contradicting minimality and proving well-quasi-orderedness (since the definition of wqo requires all infinite sequences of elements to be "good").

Besides the minimal bad sequence argument, Nash-Williams' work [NW63] contains proofs of Dickson's lemma [Dic13] (*if A and B are well-quasi-ordered, then so is the Cartesian product $A \times B$*) and a variant of Higman's lemma [Hig52] (*if A is well-quasi-ordered, 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 along the lines of Nash-Williams' original proofs in the proof assistant Isabelle [NPW02].[1] 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 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 two thousand lines of Isabelle/HOL theories) proofs. In this article, a high-level overview of the formalization is given. The full development is part of the *Archive of Formal Proofs* [Ste12b].

Contributions. This article is a reworked version of an earlier account by the author [Ste13]. 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 [Der82, MZ97] was formalized – on top of the presented work – as part of IsaFoR,[2] where it is applied to show well-foundedness of the Knuth-Bendix order [ST13].

Moreover, the author believes that besides their high trustworthiness, formalizations of existing mathematical results are also of archival and educational value.

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

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

Especially since 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 [Wen02] is a huge improvement in that respect). Thus, the author hopes that this high-level overview makes the presented formalization more accessible.

Comparison to Previous Work. In my previous work [Ste13] the focus was on following Nash-Williams' original argumentation as close as possible. With hindsight this turned out to pose unnecessary complications in some proofs. However, it is always easier to say which of two variants of a proof is better suited for mechanization after formalizing both. By slightly deviating from the original proofs and starting from a crucial fact about *homogeneous subsequences* (e.g., presented by Marc Bezem [Ter03, Appendix 5]) I was able to significantly simplify three parts of the development compared to my previous work: the construction of minimal bad sequences, the proof of Higman's lemma, and the proof of the tree theorem.

A more detailed comparison to my previous work can be found at the end of every section whose corresponding formalization changed significantly.

Overview. The remainder is structured as follows. In Section 2, necessary preliminaries are covered. Then, in Section 3, a crucial fact about almost-full relations is discussed, which will be useful for many of the later proofs. The next four sections present a formalization of Dickson's lemma, in Section 4; a general construction of 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. Some example instances of finite tree data types are discussed in Section 8. Finally, the paper concludes in Section 9, where also applications are sketched, and future as well as related work is discussed.

2. PRELIMINARIES

Throughout this article, 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. [HKNS13]: *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.

The following constants from Isabelle/HOL's library are freely used in the remainder: $\circ::(\alpha \Rightarrow \beta) \Rightarrow (\gamma \Rightarrow \alpha) \Rightarrow \gamma \Rightarrow \beta$, where $f \circ g$ denotes the functional composition of the two functions f and g, i.e., $f \circ g \overset{\mathsf{def}}{=} \lambda x.\ f\ (g\ x)$, 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*, i.e., a function from the natural numbers to the natural numbers); $\mathit{fst}::\alpha \times \beta \Rightarrow \alpha$ and $\mathit{snd}::\alpha \times \beta \Rightarrow \beta$ extract the first and second component of a pair, respectively; $\mathit{set}::\alpha\ \mathit{list} \Rightarrow \alpha\ \mathit{set}$, where $\mathit{set}\ \mathit{xs}$ is the set of elements occurring in the list xs; $[]::\alpha\ \mathit{list}$, the empty list; $\cdot::\alpha \Rightarrow \alpha\ \mathit{list} \Rightarrow \alpha\ \mathit{list}$, where $x \cdot \mathit{xs}$ denotes adding the element x in front of the list xs; and $@::\alpha\ \mathit{list} \Rightarrow \alpha\ \mathit{list} \Rightarrow \alpha\ \mathit{list}$, where $\mathit{xs}\ @\ \mathit{ys}$ denotes the concatenation of the two lists xs and ys. Note that since $\cdot$ and @ are both right-associative and have the same priority, $\mathit{xs}\ @\ y \cdot \mathit{ys}$ is the same as $\mathit{xs}\ @\ (y \cdot \mathit{ys})$ 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 $\mathit{refl}_A(\preceq)$, if and only if $\forall\, x{\in}A.\ x \preceq x$; and *transitive on* A, written $\mathit{trans}_A(\preceq)$, if and only if $\forall\, x{\in}A.\ \forall\, y{\in}A.\ \forall\, z{\in}A.\ x \preceq y \wedge y \preceq z \longrightarrow x \preceq z$.

An infinite sequence over elements of type α is represented by a function f of type $\mathit{nat} \Rightarrow \alpha$. The set of all infinite sequences over elements from a set A is denoted by A^{ω}. A binary relation $\preceq$ is *transitive on a sequence* f, written $\mathit{trans}_f(\preceq)$, if and only if $\forall\, i\ j.\ i < j \longrightarrow f\ i \preceq f\ j$. Note that $<::\mathit{nat} \Rightarrow \mathit{nat} \Rightarrow \mathit{bool}$ is transitive on an index-mapping φ if and only if φ is a strictly monotone mapping from natural numbers to natural numbers. Thus, for every f and strictly monotone φ, f_{φ} is a subsequence of f whose elements are in the same relative order.

A sequence f is *good* w.r.t. a relation $\preceq$, written $\mathit{good}_{\preceq}(f)$, if and only if there are indices $i < j$ such that $f\ i \preceq f\ j$. A sequence that is not good, is called *bad*.

The author follows Veldman [Vel04] and Vytiniotis et al. 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 $\mathit{af}_A(\preceq)$, if and only if all infinite sequences over elements of A are good, i.e., $\forall\, f{\in}A^{\omega}.\ \mathit{good}_{\preceq}(f)$. Note that every almost-full relation is necessarily reflexive: just take an infinite sequence f that repeats an arbitrary element $a \in A$ ad infinitum, then reflexivity trivially follows from the definitions of almost-full and good, i.e., there are $i < j$ such that $f\ i \preceq f\ j$ and thus $a \preceq a$.

Let $\preceq$ be almost-full on A. If in addition $\preceq$ is transitive on A, then $\preceq$ is a *wqo on* A (or A is well-quasi-ordered by $\preceq$), written $\mathit{wqo}_A(\preceq)$. In the literature, several equivalent definitions for wqos are used. One of them, also mentioned in the introduction, is that a wqo is a quasi-order that does not allow for infinite antichains and whose strict part is well-founded (see theory *Well-Quasi-Orders* for other definitions and equivalence proofs). Here, an *infinite antichain* f is an infinite sequence such that every two elements at disjoint positions are incomparable, i.e., $\forall\, i\ j.\ i < j \longrightarrow f\ i \not\preceq f\ j \wedge f\ j \not\preceq f\ i$.

3. HOMOGENEOUS SEQUENCES

While the definition of almost-full relations just requires that in every infinite sequence there are two elements such that the former is smaller than or equal to the latter, it can be shown that every infinite sequence contains a subsequence on which $\preceq$ is transitive. (In the literature, such sequences are called *homogeneous* [Ter03].) In some cases, this result allows us to obtain transitivity for free (and hence prove several results already for almost-full relations rather than wqos).

Before formally stating the above result, let us have a look at the following variant of Ramsey's theorem (see Isabelle/HOL's library, file `~~/src/HOL/Library/Ramsey.thy`) which is used in its proof.

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

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.

LEMMA 3.1. *Every infinite sequence f over elements of a set A that is almost-full w.r.t. $\preceq$ contains a homogeneous subsequence. That is, there is a strictly monotone index-mapping φ::nat $\Rightarrow$ nat such that f_φ is transitive w.r.t. $\preceq$. In Isabelle:* $[\![\mathit{af}_A(\preceq);\ f \in A^\omega]\!] \Longrightarrow \exists\,\varphi.\ \forall\, i\ j.\ i < j \longrightarrow \varphi\ i < \varphi\ j \wedge f_\varphi\ i \preceq f_\varphi\ j$.

PROOF. Let $\preceq$ be almost-full on A and $f \in A^\omega$. Then partition the set of two-element subsets of the natural numbers into the set $X = \{\{i,\ j\} \mid i < j \wedge f\ i \preceq f\ j\}$ and its complement $Y = -\ X$ and colorize two-element sets $\{i,\ j\}$ of natural numbers by *0* (*white*) and *1* (*black*) according to the following function:

$$h\ \{i,\ j\} = \begin{cases} \mathit{0} & \text{if } \{i,\ j\} \in X, \\ \mathit{1} & \text{otherwise.} \end{cases}$$

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 and a color c, such that for all $i \neq j$ in I the corresponding color $h\ \{i,\ j\}$ is c, are obtained. Since I is well-ordered, there is a function φ::*nat* $\Rightarrow$ *nat* that enumerates its elements in increasing order, i.e., $\varphi\ i < \varphi\ j$ for all $i < j$. Moreover, $h\ \{\varphi\ i,\ \varphi\ j\} = c$ for all $i < j$. Consider the following two cases (for arbitrary but fixed $i < j$):

— **case** (c is *white*). Then, $h\ \{\varphi\ i,\ \varphi\ j\} = \mathit{0}$ and thus $\{\varphi\ i,\ \varphi\ j\} \in X$ which implies $f_\varphi\ i \preceq f_\varphi\ j$.

— **case** (c is *black*). Then, $h\ \{\varphi\ i,\ \varphi\ j\} = \mathit{1}$, and thus $\{\varphi\ i,\ \varphi\ j\} \in Y$ which implies $f_\varphi\ i \not\preceq f_\varphi\ j$ and thus yields the bad sequence f_φ, contradicting the fact that $\preceq$ is almost-full on A. □

Comparison to Previous Work. Also in my previous work Ramsey's theorem was employed. However, only to obtain a proof of Dickson's lemma without transitivity and not for the more general result about homogeneous subsequences of this section.

4. DICKSON'S LEMMA

In essence, the presented formalization is about preservation of well-quasi-orderedness 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:

Definition 4.1. Given two orders $\preceq_1$ and $\preceq_2$, the *pointwise order* on pairs is defined by $(a_1,\ a_2) \preceq_1{\times}{\preceq_2}\ (b_1,\ b_2) \overset{\text{def}}{=} a_1 \preceq_1 b_1 \wedge a_2 \preceq_2 b_2$.

Using Lemma 3.1, Dickson's lemma for almost-full relations is shown.

Lemma 4.2. *The pointwise combination $\preceq_1{\times}{\preceq_2}$ of two almost-full relations $\preceq_1$ and $\preceq_2$ on sets A_1 and A_2, is almost-full on the Cartesian product $A_1 \times A_2$. In Isabelle: $[\![\mathit{af}_{A_1}(\preceq_1);\ \mathit{af}_{A_2}(\preceq_2)]\!] \Longrightarrow \mathit{af}_{A_1 \times A_2}(\preceq_1{\times}{\preceq_2})$.*

Proof. Assume $\mathit{af}_{A_1}(\preceq_1)$ and $\mathit{af}_{A_2}(\preceq_2)$. Moreover, to derive a contradiction, assume $\neg\ \mathit{af}_{A_1 \times A_2}(\preceq_1{\times}{\preceq_2})$. Then there is a sequence f on $A_1 \times A_2$ which is bad. Note that $\mathit{fst} \circ f \in {A_1}^{\omega}$ and $\mathit{snd} \circ f \in {A_2}^{\omega}$. With Lemma 3.1 we obtain a strictly monotone index-mapping φ such that $\mathit{fst}\ (f_\varphi\ i) \preceq_1 \mathit{fst}\ (f_\varphi\ j)$ for all $i < j$. Then $\mathit{snd} \circ f \circ \varphi \in {A_2}^{\omega}$ and thus $\mathit{snd} \circ f \circ \varphi$ is good since A_2 is almost-full by assumption. Thus, we obtain indices $i < j$ such that $\mathit{snd}\ (f_\varphi\ i) \preceq_2 \mathit{snd}\ (f_\varphi\ j)$. In total, we have $f_\varphi\ i \preceq_1{\times}{\preceq_2}\ f_\varphi\ j$ which together with $\varphi\ i < \varphi\ j$ contradicts the badness of *f*. □

Lemma 4.2 trivially extends to wqos.

Dickson's Lemma. *The pointwise combination of two wqos is again a wqo. In Isabelle: $[\![\mathit{wqo}_{A_1}(\preceq_1);\ \mathit{wqo}_{A_2}(\preceq_2)]\!] \Longrightarrow \mathit{wqo}_{A_1 \times A_2}(\preceq_1{\times}{\preceq_2})$.*

Proof. Assuming transitivity of $\preceq_1$ on A_1 and $\preceq_2$ on A_2, it is trivial to show transitivity of $\preceq_1{\times}{\preceq_2}$ on $A_1 \times A_2$. With Lemma 4.2, this concludes the proof. □

Comparison to Previous Work. The new proof of Lemma 4.2 for almost-full relations is based on homogeneous subsequences. As before, the effect is that transitivity on some infinite sequence is obtained without requiring transitivity of the whole relation.

5. MINIMAL BAD SEQUENCES

Since the minimal bad sequence argument is needed for Higman's lemma as well as Kruskal's 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 (early versions, that could be simplified drastically since, were presented at the *Isabelle Users Workshop* in 2012 [Ste12a] and at the *3rd International Conference on Certified Programs and Proofs* [Ste13]). The locale fixes the following constant:

—A set A whose elements are equipped with a size-function $|\cdot|{::}\alpha \Rightarrow \mathit{nat}$.

(For Isabelle initiates: here $|\cdot|$ refers to the library type class *size*, which is automatically instantiated for all data types). Since $|\cdot|$ is a well-founded measure, it makes sense to talk about *minimal* elements. It turns out that these ingredients are enough to construct – under the assumption that there is a bad sequence – a minimal bad sequence. Informally, a bad infinite sequence is a *minimal* bad sequence, when replacing any element by a smaller one, turns it into a good sequence. To make this more formal, a partial order on bad infinite sequences is introduced.

Definition 5.1. Infinite sequences over A are partially ordered by the following relation. An infinite sequence f is considered less than another infinite sequence g, written $f \lhd^\omega g$, whenever there is a position i such that the two sequences are equal for all earlier elements and $|f\ i| < |g\ i|$, i.e., $\exists\, i.\ |f\ i| < |g\ i| \wedge (\forall\, j{<}i.\ g\ j = f\ j)$. The reflexive closure of $\lhd^\omega$ on A is denoted by $\unlhd^\omega$.

In other words, infinite sequences are compared lexicographically w.r.t. the size of their elements. First note that this order is not well-founded in general.

Example 5.2. Take the set of strings over the alphabet $\{a_1, a_2, a_3, \ldots\}$, ordered by $w \preceq v$ if and only if the set of letters in w is a subset of the set of letters in v. Moreover, let size of w be its length. Now, consider the infinite descending sequence of sequences

$$\begin{array}{rccccc}
A_1 = & a_1a_1 & a_2 & a_3 & a_4 & \cdots \\
A_2 = & a_1 & a_2a_2 & a_3 & a_4 & \cdots \\
A_3 = & a_1 & a_2 & a_3a_3 & a_4 & \cdots \\
A_4 = & a_1 & a_2 & a_3 & a_4a_4 & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

that is, $A_i = a_1, a_2, a_3, \ldots, a_ia_i, \ldots$. Obviously all the A_i are bad infinite sequences. Furthermore, $A_1, A_2, A_3, \ldots$ is an infinite decreasing sequence that shows that $\lhd^\omega$ is not well-founded.

The example shows that we cannot directly obtain a minimal bad sequence by means of $\unlhd^\omega$. Thus, in the following we will construct a minimal bad sequence by choosing smallest possible elements from left to right, which is possible since $|\cdot|$ is well-founded. To this end, we need some auxiliary constructions, e.g., to filter the set of bad sequences such that only those remain that are equal to a given sequence up to a certain point.

Definition 5.3. Two infinite sequences are *equal up to* position i, when they are equal for all previous positions. For a set of infinite sequences S over elements of A, let S_i^f denote all those elements of S that are equal to f up to position i. Moreover, let $S[i]$ denote the "i-th column" of the sequences in S, i.e., the set $\{f\ i \mid f \in S\}$. Finally, for a subset B of A, let min_B denote a minimal element of B w.r.t. its size (which exists, whenever B is not empty; note however that in general it is not uniquely determined, thus the use of Hilbert's choice operator below).

In the formalization min_B is defined by

$$\mathit{min}_B = (\mathit{SOME}\ x.\ x \in B \wedge (\forall\, y{\in}A.\ |y| < |x| \longrightarrow y \notin B))$$

where *SOME* $x.\ Q\ x$ is Hilbert's epsilon operator, i.e., it yields a witness x such that $Q\ x$, whenever $\exists\, x.\ Q\ x$, and some arbitrary value of the appropriate type, otherwise. The above definitions are employed to construct an infinite sequence from a given set of infinite sequences as follows:

Definition 5.4. Given the set $\mathcal{B}$ of all bad infinite sequences over elements of A, define a new infinite sequence ℓ (intended to be a lower bound of $\mathcal{B}$ w.r.t. $\trianglelefteq^\omega$) as follows:

$$\ell\ i = min_{\mathcal{B}_i^\ell[i]}$$

That is, $\ell\ 0$ is a minimal element among the first elements of sequences in $\mathcal{B}$ (since $S_0^f = S$ for all sets S and sequences f); and to obtain the i+1-th element, first restrict $\mathcal{B}$ to those sequences that are equal to ℓ up to position i+1, and of the resulting set of sequences take a minimal element among their i+1-th elements. The well-definedness of the above definition is guaranteed by the fact that to obtain the i+1-th element, we only have to consult all the previous elements of ℓ.

The elements of ℓ satisfy the following properties:

$$h \in \mathcal{B} \Longrightarrow \ell\ i \in \mathcal{B}_i^\ell[i] \tag{1}$$

$$[\![h \in \mathcal{B};\ y \in A;\ |y| < |\ell\ i|]\!] \Longrightarrow y \notin \mathcal{B}_i^\ell[i] \tag{2}$$

That is, under the assumption that there is a bad sequence h, the i-th element of ℓ is in the i-th column of the sequences of $\mathcal{B}$ that are equal to ℓ up to position i, and is minimal amongst its elements.

Of course it has to be shown that ℓ is indeed a bad infinite sequence.

Lemma 5.5. *If there is at least one bad infinite sequence, then ℓ is bad. In Isabelle: $h \in \mathcal{B} \Longrightarrow \ell \in \mathcal{B}$.*

Proof. To derive a contradiction, assume that ℓ is good. Then there are indices $i < j$ such that $\ell\ i \preceq \ell\ j$. Moreover, from (1) we obtain $\ell\ j \in \mathcal{B}_j^\ell[j]$, which means that there is some bad infinite sequence g in $\mathcal{B}_j^\ell$ such that $g\ k = \ell\ k$ for all $k \leq j$, and thus $g\ i \preceq g\ j$. This, in turn, means that g is good and therefore contradicts the previously derived $g \in \mathcal{B}_j^\ell$. □

The second crucial property of ℓ is that it is a lower bound of the set $\mathcal{B}$. That is, every infinite sequence that is strictly smaller than ℓ is not bad.

Lemma 5.6. *If there is at least one bad infinite sequence, then every infinite sequence that is strictly smaller than ℓ w.r.t. $\lhd^\omega$ is good. In Isabelle: $h \in \mathcal{B} \Longrightarrow \forall\, g.\ g \lhd^\omega \ell \longrightarrow g \notin \mathcal{B}$.*

At this point it can be shown that if a relation is not almost-full, then there is a minimal bad sequence.

Theorem 5.7. *Let $\preceq$ be a relation that is not almost-full on A. Then there is a minimal bad sequence, i.e., a bad sequence such that all sequences that are strictly smaller w.r.t. $\lhd^\omega$ are good. In Isabelle: $\neg\ af_A(\preceq) \Longrightarrow \exists\, m{\in}\mathcal{B}.\ \forall\, g.\ g \lhd^\omega m \longrightarrow good_\preceq(g)$.*

Proof. Assume that $\preceq$ is not almost-full. Then there is some sequence $h \in \mathcal{B}$. Together with Lemma 5.5 and Lemma 5.6, we obtain that ℓ is a minimal bad sequence. □

Comparison to Previous Work. Instead of basing the *mbs* locale on some arbitrary well-founded and transitive relation (as in [Ste13]), minimality is now fixed to refer to the size of elements. While this is only a specific instance of the previous construction, it suffices for all the later proofs.

Moreover, the construction of a minimal bad sequence could be significantly simplified by step-wise narrowing down the set of all bad sequences using the notions of *equal up to*, *filtering* sets of infinite sequences w.r.t. a given infinite sequence, *column* of a set of infinite sequences, and *minimal element* of a set (only the first of which was present in my previous work).

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*. 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 size of a list is measured by its length (i.e., number of elements). Homeomorphic embedding on lists, for a given base order $\preceq$, is defined inductively by the rules

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

(In this article the notation $\preceq^*$ is used consistently to denote list-embedding w.r.t. the base order $\preceq$ and is not to be confused with the reflexive and transitive closure of a relation.) Intuitively, it might be easier to think about homeomorphic embedding on lists as follows: a list xs is embedded in a list ys if and only if 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, $xs =^* ys$ if and only if the list xs can be obtained from the list ys by dropping elements.

The *mbs* locale can be instantiated by taking A^* for its parameter A and the length of lists as their size. Thus,

$$\neg\ af_{A^*}(\preceq^*) \Longrightarrow \exists\, m{\in}\mathcal{B}.\ \forall\, g.\ g \trianglelefteq^{\omega}\ m \longrightarrow good_{\preceq^*}(g)$$

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

Lemma 6.1. *Homeomorphic embedding w.r.t. an almost-full relation $\preceq$ on a set A, is almost-full on the set of finite lists over A. In Isabelle: $af_A(\preceq) \Longrightarrow af_{A^*}(\preceq^*)$.*

Proof. Assume $af_A(\preceq)$ but $\neg\ af_{A^*}(\preceq^*)$, for the sake of a contradiction. Then there is a 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., $m\ i = h\ i \cdot t\ i$).

Clearly, $h \in A^\omega$ and thus, by Lemma 3.1, there is a strictly monotone index-mapping such that h_φ is a $\preceq$-homogeneous sequence. Moreover, t_φ is bad, since otherwise m would be good.

Let n abbreviate $\varphi\ 0$ and c be the combination of the infinite sequences m and t, defined by $c\ i \overset{\mathsf{def}}{=} \textsf{\textit{if}}\ i < n\ \textsf{\textit{then}}\ m\ i\ \textsf{\textit{else}}\ t\ (\varphi\ (i - n))$ (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 the 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 $m\ i \preceq^*\ t\ (\varphi\ j')$ (from $c\ i \preceq^*\ c\ j$). Moreover, $m\ i \preceq^*\ m\ (\varphi\ j')$ (by the second clause of the inductive definition of embedding). 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. □

This result can be easily extended to wqos.

Higman's Lemma. *Whenever a set A is well-quasi-ordered by a relation $\preceq$, then the set of finite lists over A is well-quasi-ordered by homeomorphic embedding w.r.t. $\preceq^*$. In Isabelle: $wqo_A(\preceq) \Longrightarrow wqo_{A^*}(\preceq^*)$.*

Proof. For transitivity of $\preceq^*$ (under the assumption that $\preceq$ is transitive), refer to lemma *list-emb-trans* in theory *Sublist*. Together with Lemma 6.1, this yields Higman's lemma. □

Comparison to Previous Work. By employing Lemma 3.1, the slightly tedious reasoning about the non-existence of an infinite bad sequence "of special shape" (which is also to be found in Nash-Williams' original proof) could be completely avoided. This change made it possible to shorten the previous 166-line proof to more reasonable 66 lines.

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

$$\textbf{datatype}\ \alpha\ t = \mathit{Tree}\ \alpha\ (\alpha\ t\ \mathit{list})$$
$$\textbf{datatype}\ \alpha\ t' = E \mid N\ \alpha\ (\alpha\ t'\ \mathit{list})$$

or the type of first-order terms

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

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 [ST13]). 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 *kruskal-tree* that fixes the following constants (see theory *Kruskal* for details):

—A set $\mathcal{F}$::(β × *nat*) *set* representing the signature over which trees are built.

—A function *mk*::$\beta \Rightarrow \alpha$ *list* $\Rightarrow \alpha$ that is used to construct a finite tree from a given node and a given list of finite trees.

—A function *root*::$\alpha \Rightarrow \beta$ × *nat* that extracts the root node together with its arity from a given tree.

—A function *args*::$\alpha \Rightarrow \alpha$ *list* that extracts the list of arguments (direct subtrees) from a given tree.

—As well as the set $\mathcal{T}(\mathcal{F})$::α *set* of well-formed trees w.r.t. the signature $\mathcal{F}$.

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

$$[\![t \in \mathcal{T}(\mathcal{F});\ s \in \mathit{set}\ (\mathit{args}\ t)]\!] \Longrightarrow |s| < |t| \tag{F1}$$

$$(f,\ |ts|) \in \mathcal{F} \Longrightarrow \mathit{root}\ (\mathit{mk}\ f\ ts) = (f,\ |ts|) \tag{F2}$$

$$(f,\ |ts|) \in \mathcal{F} \Longrightarrow \mathit{args}\ (\mathit{mk}\ f\ ts) = ts \tag{F3}$$

$$t \in \mathcal{T}(\mathcal{F}) \Longrightarrow \mathit{mk}\ (\mathit{fst}\ (\mathit{root}\ t))\ (\mathit{args}\ t) = t \tag{F4}$$

$$t \in \mathcal{T}(\mathcal{F}) \Longrightarrow \mathit{root}\ t \in \mathcal{F} \tag{F5}$$

$$t \in \mathcal{T}(\mathcal{F}) \Longrightarrow |\mathit{args}\ t| = \mathit{snd}\ (\mathit{root}\ t) \tag{F6}$$

$$[\![t \in \mathcal{T}(\mathcal{F});\ s \in \mathit{set}\ (\mathit{args}\ t)]\!] \Longrightarrow s \in \mathcal{T}(\mathcal{F}) \tag{F7}$$

That is, the size of a direct subtree of a well-formed tree is strictly smaller than the size of the tree itself (F1); *mk* is injective when applied to a number of arguments corresponding to the arity of a node (i.e., $[\![(f,\ |ss|) \in \mathcal{F};\ (g,\ |ts|) \in \mathcal{F}]\!] \Longrightarrow (\mathit{mk}\ f\ ss = \mathit{mk}\ g\ ts) = (f = g \wedge ss = ts)$; (F2) and (F3)); and *mk*, *root*, and *args* interact "as expected" on well-formed trees ((F4), (F5), (F6), and (F7))

Homeomorphic embedding on (well-formed) finite trees is defined inductively by the two rules:

$$\frac{(f,\ m) \in \mathcal{F} \qquad |ts| = m \qquad \mathit{set}\ ts \subseteq \mathcal{T}(\mathcal{F}) \qquad t \in \mathit{set}\ ts \qquad s \preceq_{\mathsf{emb}} t}{s \preceq_{\mathsf{emb}} \mathit{mk}\ f\ ts}$$

$$\frac{\begin{array}{c}(f,\ m) \in \mathcal{F} \qquad (g,\ n) \in \mathcal{F} \qquad |ss| = m \qquad |ts| = n \\ \mathit{set}\ ss \subseteq \mathcal{T}(\mathcal{F}) \qquad \mathit{set}\ ts \subseteq \mathcal{T}(\mathcal{F}) \qquad (f,\ m) \preceq (g,\ n) \qquad ss \preceq_{\mathsf{emb}}{}^{*}\ ts\end{array}}{\mathit{mk}\ f\ ss \preceq_{\mathsf{emb}} \mathit{mk}\ g\ ts}$$

The first rule subsumes what is often called the *subterm property* (i.e., a proper subtree of a well-formed tree is also in the embedding relation). The second rule states that the nodes of a tree may be replaced by smaller ones w.r.t. $\preceq$ and their arguments by smaller ones w.r.t. list-embedding where the underlying order is $\preceq_{\mathsf{emb}}$.

To instantiate the *mbs* locale, take $\mathcal{T}(\mathcal{F})$ for its parameter A. Thus,

$$\neg\ \mathit{af}_{\mathcal{T}(\mathcal{F})}(\preceq_{\mathsf{emb}}) \Longrightarrow \exists\, m{\in}\mathcal{B}.\ \forall\, g.\ g \lhd^{\omega}\ m \longrightarrow \mathit{good}_{\preceq_{\mathsf{emb}}}(g)$$

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

THEOREM 7.1. *Homeomorphic embedding w.r.t. an almost-full relation $\preceq$ on a set $\mathcal{F}$, is almost-full on the set of finite trees over $\mathcal{F}$. In Isabelle:* $\mathit{af}_{\mathcal{F}}(\preceq) \Longrightarrow \mathit{af}_{\mathcal{T}(\mathcal{F})}(\preceq_{\mathsf{emb}})$

Proof. Assume that $\preceq$ is almost-full on $\mathcal{F}$ but, for the sake of a contradiction, $\preceq_{\mathsf{emb}}$ is not almost-full on $\mathcal{T}(\mathcal{F})$. Then, by Theorem 5.7, there is a minimal bad sequence m such that any smaller sequence w.r.t. $\lhd^{\omega}$ is good. Moreover, there are sequences r and a of roots and arguments of m (i.e., $m\ i = mk\ (\mathit{fst}\ (r\ i))\ (a\ i)$). Let A denote the set of all trees occurring in a (i.e., the set of arguments of all $m\ i$).

Then it is shown that $\preceq_{\mathsf{emb}}$ is almost-full on A. To this end, suppose the contrary. Thus, there is a sequence $s \in A^{\omega}$ which is bad. Let n be the least index such that there is some element $s\ k$ that is an argument of $m\ n$ (i.e., $s\ k \in \mathit{set}\ (a\ n)$ for some k). Let c be the combination of m and s, defined by

$$c\ i \overset{\mathsf{def}}{=} \textsf{\textit{if}}\ i < n\ \textsf{\textit{then}}\ m\ i\ \textsf{\textit{else}}\ s\ (k + (i - n))$$

Clearly, $c\ i = m\ i$ for all $i < n$ and $c\ i = s\ (k + (i - n))$, otherwise. Then c is bad, since otherwise a contradiction is obtained as follows: Assume c is good. Then, there are $i < j$ such that $c\ i \preceq_{\mathsf{emb}} c\ j$. Now analyze the following cases:

— **case** $(j < n)$. Then $m\ i \preceq_{\mathsf{emb}} m\ j$, contradicting the badness of m.

— **case** $(n \leq i)$. Let $i' = k + (i - n)$ and $j' = k + (j - n)$. Then $i' < j'$ and $s\ i' \preceq_{\mathsf{emb}} s\ j'$, contradicting the badness of s.

— **case** $(i < n$ and $n \leq j)$. Let $j' = k + (j - n)$. Then $m\ i \preceq_{\mathsf{emb}} s\ j'$. Thus, there is some index $l \geq n$ such that $s\ j' \in \mathit{set}\ (a\ l)$, which in turn implies $m\ i \preceq_{\mathsf{emb}} m\ l$. Together with $i < l$, this contradicts the badness of m.

Thus term c is bad. Since also $c \lhd^{\omega} m$ (since $c\ n$ is and argument of $m\ n$), we obtain the desired $\mathit{af}_A(\preceq_{\mathsf{emb}})$.

Now by, Lemma 6.1 and Lemma 3.1, we obtain a strictly monotone index-mapping φ such that $\varphi\ i < \varphi\ j$ and $a_{\varphi}\ i \preceq_{\mathsf{emb}}{}^{*}\ a_{\varphi}\ j$ for all $i < j$. Moreover, $r_{\varphi}\ i \in \mathcal{F}$ for all i and thus there are indices $i < j$ such that $r_{\varphi}\ i \preceq r_{\varphi}\ j$. Together, this implies $m_{\varphi}\ i \preceq_{\mathsf{emb}} m_{\varphi}\ j$, contradicting the badness of m. □

Kruskal's Tree Theorem. *Whenever a set $\mathcal{F}$ is well-quasi-ordered by a relation $\preceq$, then the set of finite trees over $\mathcal{F}$ is well-quasi-ordered by homeomorphic embedding w.r.t. $\preceq_{\mathsf{emb}}$. In Isabelle: $\mathit{wqo}_{\mathcal{F}}(\preceq) \Longrightarrow \mathit{wqo}_{\mathcal{T}(\mathcal{F})}(\preceq_{\mathsf{emb}})$.*

Proof. By induction on the definition of embedding, it can be shown that $\preceq_{\mathsf{emb}}$ is transitive whenever the base order $\preceq$ is. Together with Theorem 7.1 this yields the tree theorem. □

Notes. As in my previous work [Ste13], the definition of homeomorphic embedding on trees could have ignored arities of nodes and in turn well-formedness of trees. This would constitute a slightly simpler definition and still allow us to obtain the tree theorem. Moreover, as in my previous work, closure under context and transitivity could have been built-in. However, note that every extension of an almost-full relation is again an almost-full relation (an easy consequence of the definition of almost-full). Thus it seems desirable to have an embedding relation that is as small as possible. Since the proof of the tree theorem goes through with the current version, I went with it. But considering arities does not only make embedding potentially smaller, it is also necessary for some applications as shown in the next section.

Comparison to Previous Work. Again, by employing Lemma 3.1, the very tedious reasoning about the non-existence of an infinite bad sequence "of special shape" (which is also to be found in Nash-Williams' original proof) could be avoided completely. Thereby shortening the original 188-line proof to 90 lines and, more importantly, making the argument much simpler.

8. EXAMPLES

In this section we consider concrete instances of the *kruskal-tree* locale for the following data types:

- Rose trees: **datatype** $\alpha\ tree = Node\ \alpha\ (\alpha\ tree\ list)$
- First-order terms: **datatype** $(\alpha,\ \beta)\ term = Var\ \beta \mid Fun\ \alpha\ ((\alpha,\ \beta)\ term\ list)$
- "Arithmetic" expressions involving addition of variables and constants: **datatype** $\alpha\ exp = V\ \alpha \mid C\ nat \mid Plus\ (\alpha\ exp)\ (\alpha\ exp)$

For rose trees consider the selector functions $node\ (Node\ f\ ts) = (f,\ |ts|)$ and $succs\ (Node\ f\ ts) = ts$, as well as the inductive set of trees over a given set of nodes A:

$$\frac{f \in A \qquad \forall\, t{\in}set\ ts.\ t \in trees\ A}{Node\ f\ ts \in trees\ A}$$

The *kruskal-tree* locale is easily instantiated by

interpretation $kruskal\text{-}tree\ (A \times \mathsf{UNIV})\ Node\ node\ succs\ (trees\ A)$

and we obtain the following variant of the tree theorem

$$wqo_{A\times\mathsf{UNIV}}(\preceq) \Longrightarrow wqo_{trees\ A}(\preceq_{\mathsf{emb}}).$$

However, arities are actually not interesting (since nodes in a rose tree may have arbitrarily many successors) thus it might be desirable to start from a base order $\preceq$ on A (instead of $A \times \mathsf{UNIV}$). This is easily possible by noting that the full relation ($x \preceq y$ for all x and y) is a wqo on any set and invoking Dickson's lemma.

For first-order terms consider the selector functions $root\ (Fun\ f\ ts) = (f,\ |ts|)$ and $args\ (Fun\ f\ ts) = ts$, as well as the inductively defined set of ground terms over a signature $\mathcal{F}$:

$$\frac{(f,\ n) \in F \qquad |ts| = n \qquad \forall\, s{\in}set\ ts.\ s \in \mathcal{T}(F)}{Fun\ f\ ts \in \mathcal{T}(F)}$$

Again, the *kruskal-tree* locale is easily instantiated by

interpretation $kruskal\text{-}tree\ \mathcal{F}\ Fun\ root\ args\ \mathcal{T}(\mathcal{F})$

and we obtain the following variant of the tree theorem

$$wqo_{\mathcal{F}}(\preceq) \Longrightarrow wqo_{\mathcal{T}(\mathcal{F})}(\preceq_{\mathsf{emb}}).$$

For arithmetic expressions consider the constructor function

$$mk\ (v\ x)\ [] = V\ x$$
$$mk\ (c\ n)\ [] = C\ n$$
$$mk\ p\ [a,\ b] = Plus\ a\ b$$

the root selector function

$$
\begin{aligned}
&\mathit{rt}\ (V\ x) = (v\ x,\ \mathit{0})\\
&\mathit{rt}\ (C\ n) = (c\ n,\ \mathit{0})\\
&\mathit{rt}\ (\mathit{Plus}\ a\ b) = (p,\ \mathit{2})
\end{aligned}
$$

and the argument selector function

$$
\begin{aligned}
&\mathit{ags}\ (V\ x) = []\\
&\mathit{ags}\ (C\ n) = []\\
&\mathit{ags}\ (\mathit{Plus}\ a\ b) = [a,\ b]
\end{aligned}
$$

where

datatype α *symb* $= v\ \alpha \mid c\ \mathit{nat} \mid p.$

Moreover, consider the inductively defined set of arithmetic expressions:

$$
\frac{}{V\ x \in \mathit{exps}} \qquad \frac{}{C\ n \in \mathit{exps}} \qquad \frac{a \in \mathit{exps} \qquad b \in \mathit{exps}}{\mathit{Plus}\ a\ b \in \mathit{exps}}
$$

For the signature $\Sigma \overset{\mathsf{def}}{=} \{(v\ x,\ 0) \mid x \geq 0\} \cup \{(c\ n,\ 0) \mid n \geq 0\} \cup \{(p,\ \mathit{2})\}$ (which ensures that constructors are applied to the correct number of arguments), the *kruskal-tree* locale can be instantiated by

interpretation *kruskal-tree* Σ *mk rt ags exps*

and we obtain the following variant of the tree theorem

$$\mathit{wqo}_{\Sigma}(\preceq) \Longrightarrow \mathit{wqo}_{\mathit{exps}}(\preceq_{\mathsf{emb}}).$$

9. 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. The formalized proofs are reasonably simple and the tree theorem is presented in a general version that is applicable to several instances.

Parts of the presented formalization were used by Wu et al. [WZU11] to formalize a proof of: *For every language A, the languages of sub- and superstrings of A are regular.* (Details are given in the corresponding journal article [WU14].)

Moreover, the presented formalization of the tree theorem is employed for a proof that the Knuth-Bendix order is a simplification order [ST13].

There are formalizations of Higman's lemma in Isabelle/HOL by Berghofer [Ber04] and using other proof assistants by Murthy [Mur90], Fridlender [Fri98], Herbelin [Her94], Seisenberger [Sei03], and Martín-Mateos et al. [MMRRAH11].

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 [Vel04]. 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.

The tree theorem is a special case of the graph minor theorem, which was proved by Robertson and Seymour in a series of twenty papers [RS83, RS04]. The size of this (pen and paper) proof alone makes a formalization interesting. However, an extension of the current proof would constitute significant extra effort and it is unclear whether the minimal bad sequence argument could be applied at all. Thus, we leave it as future work.

References

[AGLNM11] Beatriz Alarcón, Raúl Gutiérrez, Salvador Lucas, and Rafael Navarro-Marset. Proving termination properties with MU-TERM. In Michael Johnson and Dusko Pavlovic, editors, *Proceedings of the 13th International Conference on Algebraic Methodology And Software Technology*, volume 6486 of *Lecture Notes in Computer Science*, pages 201–208. Springer Berlin Heidelberg, 2011. doi:10.1007/978-3-642-17796-5_12.

[Ber04] Stefan Berghofer. A constructive proof of Higman's lemma in Isabelle. In Stefano Berardi, Mario Coppo, and Ferruccio Damiani, editors, *Proceedings of the 3rd International Workshop on Types for Proofs and Programs*, volume 3085 of *Lecture Notes in Computer Science*, pages 66–82. Springer Berlin Heidelberg, 2004. doi:10.1007/978-3-540-24849-1_5.

[CCF$^+$11] Évelyne Contejean, Pierre Courtieu, Julien Forest, Olivier Pons, and Xavier Urbain. Automated certified proofs with C*i*ME3. In Manfred Schmidt-Schauß, editor, *Proceedings of the 22nd International Conference on Rewriting Techniques and Applications*, volume 10 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 21–30. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2011. doi:10.4230/LIPIcs.RTA.2011.21.

[Der79] Nachum Dershowitz. A note on simplification orderings. *Information Processing Letters*, 9(5):212–215, 1979. doi:10.1016/0020-0190(79)90071-1.

[Der82] Nachum Dershowitz. Orderings for term-rewriting systems. *Theoretical Computer Science*, 17(3):279–301, 1982. doi:10.1016/0304-3975(82)90026-3.

[Dic13] Leonard Eugene Dickson. Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors. *American Journal of Mathematics*, 35(4):413–422, 1913. doi:10.2307/2370405.

[Fri98] Daniel Fridlender. Higman's lemma in type theory. In Eduardo Giménez and Christine Paulin-Mohring, editors, *Proceedings of the 1st International Workshop on Types for Proofs and Programs*, volume 1512 of *Lecture Notes in Computer Science*, pages 112–133. Springer Berlin Heidelberg, 1998. doi:10.1007/BFb0097789.

[GSKT06] Jürgen Giesl, Peter Schneider-Kamp, and René Thiemann. AProVE 1.2: Automatic termination proofs in the dependency pair framework. In Ulrich Furbach and Natarajan Shankar, editors, *Proceedings of the 3rd International Joint Conference on Automated Reasoning*, volume 4130, pages 281–286. Springer Berlin Heidelberg, 2006. doi:10.1007/11814771_24.

[Her94] Hugo Herbelin. A program from an A-translated impredicative proof of Higman's lemma, 1994. http://coq.inria.fr/pylons/contribs/view/HigmanNW/v8.3.

[Hig52] Graham Higman. Ordering by divisibility in abstract algebras. *Proceedings of the London Mathematical Society*, s3-2(1):326–336, 1952. doi:10.1112/plms/s3-2.1.326.

[HKNS13] Florian Haftmann, Gerwin Klein, Tobias Nipkow, and Norbert Schirmer. LaTeX sugar for Isabelle documents, 2013. http://isabelle.in.tum.de/website-Isabelle2013-2/dist/Isabelle2013-2/doc/sugar.pdf.

[Kru60] Joseph Bernard Kruskal. Well-quasi-ordering, the tree theorem, and Vazsonyi's conjecture. *Transactions of the American Mathematical Society*, 95(2):210–225, 1960. doi:10.2307/1993287.

[KSZM09] Martin Korp, Christian Sternagel, Harald Zankl, and Aart Middeldorp. Tyrolean Termination Tool 2. In Ralf Treinen, editor, *Proceedings of the 20th International Conference on Rewriting Techniques and Applications*, volume 5595 of *Lecture Notes in Computer Science*, pages 295–304. Springer Berlin Heidelberg, 2009. doi:10.1007/978-3-642-02348-4_21.

[MMRRAH11] Francisco Jesús Martín-Mateos, José Luis Ruiz-Reina, José Antonio Alonso, and María José Hidalgo. Proof pearl: A formal proof of Higman's lemma in ACL2. *Journal of Automated Reasoning*, 47(3):229–250, 2011. doi:10.1007/s10817-010-9178-x.

[Mur90] Chetan R. Murthy. *Extracting Constructive Content from Classical Proofs*. PhD thesis, Cornell University, 1990. http://hdl.handle.net/1813/6991.

[MZ97] Aart Middeldorp and Hans Zantema. Simple termination of rewrite systems. *Theoretical Computer Science*, 175(1):127–158, 1997. doi:10.1016/S0304-3975(96)00172-7.

[NPW02] Tobias Nipkow, Lawrence Charles Paulson, and Markus Wenzel. *Isabelle/HOL – A Proof Assistant for Higher-Order Logic*, volume 2283 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2002. doi:10.1007/3-540-45949-9.

[NW63] Crispin St. John Alvah Nash-Williams. On well-quasi-ordering finite trees. *Proceedings of the Cambridge Philosophical Society*, 59(4):833–835, 1963. doi:10.1017/S0305004100003844.

[RS83] Neil Robertson and Paul Seymour. Graph minors. i. excluding a forest. *Journal of Combinatorial Theory, Series B*, 35(1):39–61, 1983. doi:10.1016/0095-8956(83)90079-5.

[RS04] Neil Robertson and Paul Seymour. Graph minors. xx. wagner's conjecture. *Journal of Combinatorial Theory, Series B*, 92(2):325–357, 2004. doi:10.1016/j.jctb.2004.08.001.

[Sei03] Monika Seisenberger. *On the Constructive Content of Proofs*. PhD thesis, LMU Munich, 2003. http://nbn-resolving.de/urn:nbn:de:bvb:19-16190.

[SG09] Felix Schernhammer and Bernhard Gramlich. VMTL – a modular termination laboratory. In Ralf Treinen, editor, *Proceedings of the 20th International Conference on Rewriting Techniques and Applications*, volume 5595 of *Lecture Notes in Computer Science*, pages 285–294. Springer Berlin Heidelberg, 2009. doi:10.1007/978-3-642-02348-4_20.

[ST13] Christian Sternagel and René Thiemann. Formalizing Knuth-Bendix orders and Knuth-Bendix completion. In Femke van Raamsdonk, editor, *Proceedings of the 24th International Conference on Rewriting Techniques and Applications*, volume 21 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 287–302. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2013. doi:10.4230/LIPIcs.RTA.2013287.

[Ste12a] Christian Sternagel. A locale for minimal bad sequences. In *Isabelle Users Workshop*, 2012. arXiv:1208.1366.

[Ste12b] Christian Sternagel. Well-Quasi-Orders. In Gerwin Klein, Tobias Nipkow, and Lawrence Charles Paulson, editors, *Archive of Formal Proofs*. April 2012. http://afp.sf.net/devel-entries/Well_Quasi_Orders.shtml.

[Ste13] Christian Sternagel. Certified Kruskal's tree theorem. In Georges Gonthier and Michael Norrish, editors, *Proceedings of the 3rd International Conference on Certified Programs and Proofs*, volume 8307 of *Lecture Notes in Computer Science*, pages 178–193. Springer Berlin Heidelberg, 2013. doi:10.1007/978-3-319-03545-1_12.

[Ter03] Terese. *Term Rewriting Systems*, volume 55 of *Cambridge Tracts Theoret. Comput. Sci.* Cambridge Univ. Press, 2003.

[Vel04] Wim Veldman. An intuitionistic proof of Kruskal's theorem. *Archive for Mathematical Logic*, 43(2):215–264, 2004. doi:10.1007/s00153-003-0207-x.

[Wal04] Johannes Waldmann. Matchbox: A tool for match-bounded string rewriting. In Vincent van Oostrom, editor, *Proceedings of the 15th International Conference on Rewriting Techniques and Applications*, volume 3091 of *Lecture Notes in Computer Science*, pages 85–94. Springer Berlin Heidelberg, 2004. doi:10.1007/978-3-540-25979-4_6.

[Wen02] Markus Wenzel. *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.

[WU14] Chunhan Wu and Xingyuan Zhang Christian Urban. A formalisation of the Myhill-Nerode theorem based on regular expressions. *Journal of Automated Reasoning*, pages 1–30, 2014. doi:10.1007/s10817-013-9297-2.

[WZU11] Chunhan Wu, Xingyuan Zhang, and Christian Urban. The Myhill-Nerode theorem based on regular expressions. In Gerwin Klein, Tobias Nipkow, and Lawrence Charles Paulson, editors, *Archive of Formal Proofs*. August 2011. http://afp.sf.net/entries/Myhill-Nerode.shtml.