Mathematical Theory and Modeling
ISSN 2224-5804 (Paper) ISSN 2225-0522 (Online)
Vol.3, No.13, 2013

Simplified Proof of Kruskal's Tree Theorem

D. Singh[1], Ali Mainguwa Shuaibu[2*] and Ndayawo, M.S.[2]
[1]Department of Mathematics, Ahmadu Bello University, Zaria-Nigeria. Email: mathdss@yahoo.com.
[2]Department of Mathematics, Statistics and Computer science, Kaduna Polytechnic, P.M.B. 2021, Kaduna, Nigeria.
Email: shuaibuali16@gmail.com ([*]Corresponding Author).

Abstract

There are different versions of proof of Kruskal's tree theorem. In this paper, we provide a simplified version of proof of Kruskal's tree theorem. The proof is essentially due to Nash-williams. Though, our proof is similar to the Kruskal's original proof formulated in terms of well-quasi-orders by Gallier. In our case, we use well-partial-orders and follow the simplified proof of Kruskal's theorem of Gallier. Kruskal's tree theorem is the main ingredient to prove well-foundedness of simplification orders for first-order rewriting. It implies that if an order satisfies some simplification property, well-foundedness is obtained for free. This theorem plays a crucial role in computer science, specially, termination of term rewriting systems.

Keywords: Kruskal's Theorem, Simplification order, Term rewriting, well-foundedness

1. Introduction

A well-known method for proving termination is the *recursive path ordering (rpo)*. The fundamental idea of such path ordering is that a well-founded ordering on terms is defined, starting from a given order called *precedence* on the operation symbols recursively. If every reduction (rewrite) step in a *term rewriting system (TRS)* corresponds to a decrease according to this ordering, one can conclude that the system is *terminating*. If every reduction step is *closed* under contexts and substitutions then the decrease only has to be checked for the *rewrite rules* instead of all the reduction steps (Dershowitz, 1982). The bottleneck of this kind of method is how to prove that such an order defined recursively on terms is indeed a well-founded order. Proving irreflexivity and transitivity often turns out to be feasible, using some induction and case analysis. However, when presenting an arbitrary recursive definition of such an order, well-foundedness is very hard to prove directly (Middeldorp and Zantema, 1997). Fortunately, the *Kruskal's tree theorem* (Kruskal, 1960) implies that if the order satisfies some simplification property, well-foundedness is obtained for free. An order satisfying this property is called a *simplification order*. This notion of simplification consists of two ingredients: (i) a term decreases by removing parts of it, and (ii) a term decreases by replacing an operation symbol with a smaller one, according to the precedence used.

It is amazing that in the term rewriting literature the notion of simplification order is motivated by the applicability of Kruskal's tree theorem using the first ingredient only (see Gallier, 1991; Middeldorp and Zantema, 1997, for details). The problem with the generalization of simplfication to the higher order case is the fact that there is no suitable extension of Kruskal's theorem for higher order terms. However, Middeldorp and Zantema (1997) propose a definition of simplification order that matches exactly the requirements of Kruskal's theorem, since that is the basic

motivation for the notion of simplification order. According to this new definition all simplification orders are well-founded, both over finite and infinite signatures. Therefore, the usual definition of simplification order is only helpful for proving termination of systems over finite signatures. It is straightforward from the definition that every *rpo* over a well-founded precedence can be extended to a simplification order, and hence is well-founded (Dershowitz, 1987).

Essentially, we provide a simplified proof version of Kruskal's tree theorem which is similar to the proof due to Gallier (Gallier, 1991), using well-partial-order.

2. Preliminaries

A *strict partial ordering* $\succ$ on a set M is a transitive and irreflexive binary relation on M. In general, any transitive and irreflexive relation is called an *order*. An order $\succ$ is called *total*, if for any two distinct elements s, t one has $s \succ t \vee t \succ s \vee s = t$. A reflexive and transitive relation is a *quasi-order (or, preorder)*, usually denoted $\succsim$. If $\succsim$ is a quasi-order, $s \succ t \Leftrightarrow s \succsim t \wedge \neg(t \succsim s)$ is the associated strict order and $s \sim t \Leftrightarrow s \succsim t \wedge t \succsim s$ is the associated equivalence relation. We use the relation $\succ$ for partial orderings and $\succsim$ for quasi-orderings Let $\mathcal{F}$ be a set of *function symbols* and $\mathcal{V}$ a set of *variable symbols*. We denote the set of terms constructed over $\mathcal{F}$ and $\mathcal{V}$ by $\mathcal{T}(\mathcal{F}, \mathcal{V})$. A binary relation R on terms is *closed under contexts* if $s\ R\ t$ implies $C[s]\ R\ C[t]$ for all contexts C, and a binary relation R on terms is *closed under substitutions* if $s\ R\ t$ implies $s\sigma\ R\ t\sigma$ for all substitutions σ. A *rewrite rule* is a pair of terms (l, r) usually written as $l \longrightarrow r$ satisfying the following conditions: (i) $l \notin \mathcal{V}$. i.e., l is a non-variable term (ii) $\mathcal{V}ar(r) \subseteq \mathcal{V}ar(l)$. i.e., each variable symbol which occurs in r also occurs in l. A *TRS* $\mathcal{R}$ is a finite set of rewrite rules $l \longrightarrow r$ where, l and r are terms. Given a *TRS* $\mathcal{R}$, an order $\succ$ on $\mathcal{T}(\mathcal{F}, \mathcal{V})$ is said to be *compatible* with $\mathcal{R}$ if $s \succ t$ whenever $s \longrightarrow t$. An order $\succ$ on $\mathcal{T}(\mathcal{F}, \mathcal{V})$ is said to have the *subterm property* if $f(t_1, \ldots, t_n) \succ t_i$, for any $f \in \mathcal{F}$ and terms $t_1, \ldots, t_n \in \mathcal{T}(\mathcal{F}, \mathcal{V})$, where $n \in arity(f)$.We write $s \trianglerighteq t$ to mean s is a *subterm* of t and a subterm s of t is called *proper* if it is distinct from t, denoted $s \triangleright t$. The subterm property of a relation $\succ$ can be expressed more concisely by the inclusion $\triangleright \subseteq \succ$. The task of showing that a given transitive relation $\succ$ has the subterm property amounts to verifying $f(t_1, \ldots, t_n) \succ t_i$, for all function symbols f of arity $n \geq 1$, terms $t_1, \ldots, t_n$, and $i \in \{1, \ldots, n\}$.

Definition1

A partial ordering $\succ$ over a set *M* is said to be *well-founded* if there is no infinite sequence $x_1, x_2, x_3, \ldots$ of elements of *M* such that $x_i \succ x_{i+1}$ for all $i \geqslant 1$. Such a sequence $x_1, x_2, x_3, \ldots$ is called an infinite descending chain. Well-founded orderings are sometimes called *Noetherian* in the term rewriting literature. In fact, the adjective *Noetherian* is usually used to exclude *infinite ascending chains*.For example,

$$\ldots \succ f(f(f(a))) \succ f(f(a)) \succ a \succ f(a)$$

is a well-founded ordering.

The usual ordering $>$ on the set of natural numbers is well-founded, since no sequence of natural numbers can descend beyond 0. However, $>$ on the set of all integers is not a well-founded ordering, since, $-1 > -2 > -3 > \ldots$ is an infinite descending sequence in the set of integers and so is the case with the set of real numbers.

Definition 2.

Let $\mathcal{V}$ be a set of variables. *The homeomorphic embedding* $\trianglerighteq_{emb}$, a binary relation on $\mathcal{T}(\mathcal{F},\mathcal{V})$, is defined as follows: $s \trianglerighteq_{emb} t$ if and only if one of the followingh conditions holds:

1. $s = x = t$ for a variable $x \in \mathcal{V}$.

2. $s = f(s_1,\ldots,s_n)$ and $t = f(t_1,\ldots,t_n)$ for a function symbol $f \in \mathcal{F}^{(n)}$, and $s_1 \trianglerighteq_{emb} t_1,\ldots,s_n \trianglerighteq_{emb} t_n$.

3. $s = f(s_1,\ldots,s_n)$ for a function symbol $f \in \mathcal{F}^{(n)}$, and $s_j \trianglerighteq_{emb} t$ for some $j, 1 \le j \le n$.

For example,

$$f(f(h(a),h(x)),f(h(x),a)) \trianglerighteq_{emb} f(f(a,x),x).$$

Definition 3.

An infinite sequence $t_1, t_2, t_3,\ldots$ of terms $\mathcal{T}(\mathcal{F},\mathcal{V})$ is *self-embedding* if there exist $1 \le i < j$ such that $t_i \trianglelefteq_{emb} t_j$. Homeomorphic embedding $\trianglerighteq_{emb}$ could also be defined as the reduction relation $\rightarrow^*_{\mathcal{R}_{emb}}$ induced by the rewrite system

$$\mathcal{R}_{emb} := \{f(x_1,\ldots,x_n) \rightarrow x_i | n \ge 1, f \in \mathcal{F}^{(n)}, 1 \le i \le n\}.$$

Since $\mathcal{R}_{emb}$ is obviously terminating, this shows that $\rightarrow^*_{\mathcal{R}_{emb}} = \trianglerighteq_{emb}$ is a well-founded partial order. In fact, in view of Kruskal's tree theorem (proved in section 3), $\trianglerighteq_{emb}$ satisfies a stronger property called *well-partial-order (wpo)* for finite $\mathcal{F}$ and $\mathcal{V}$.

Definition 4.

A partial order $\trianglerighteq$ on a set A is a *well-partial-order (wpo)* if for every infinite sequence $a_1, a_2, a_3,\ldots$ of elements of A there exist two natural numbers i and j such that $i < j$ and $a_i \trianglelefteq a_j$. This is equivalent to saying that every partial order on A that extends $\trianglerighteq$ is well-founded. An infinite sequence $a_1, a_2, a_3,\ldots$ is called *good* (with respect to $\trianglerighteq$) if

and only if there exist $i < j$ such that $a_i \preccurlyeq a_j$. Otherwise, the sequence is called *bad*. An infinite sequence $a_1, a_2, a_3, \ldots$ is called a *chain* if $a_i \preccurlyeq a_{i+1}$ for all $i \geq 1$. Moreover, the sequence $a_1, a_2, a_3, \ldots$ is said to contain a chain if it has a subsequence that is a chain. The sequence $a_1, a_2, a_3, \ldots$ is called an *antichain* if neither $a_i \preccurlyeq a_j$ nor $a_j \preccurlyeq a_i$, for all $1 \leq i < j$. Obviously, an infinite chain $a_1 \succ a_2 \succ a_3 \succ \ldots$ cannot be good follows from definition that every *wpo* is well-founded. The converse need not be true (Baader and Nipkow, 1998).

Definition 5.

A quasi-order $\lesssim$ is called a *well-quasi-order (wqo)*, iff every infinite sequence of elements of *A* is good. Among the various characterizations of *wqos*, the following are particularly useful in the proof of Kruskal's tree theorem:

(i) every infinite sequence is good with respect to $\lesssim$ (ii) there are no infinite antichain and no infinite decreasing sequence with respect to $\lesssim$. (iii) every quasi-order extending $\lesssim$ (including $\lesssim$ itself) is well-founded.

3. Simplified Proof of Kruskal's Tree Theorem

This section is devoted to Kruskal's theorem. We state the finite version of Kruskal's theorem and refrain from proving it, since it is a special case of the general version of Krukal's tree theorem, which will be proved subsequently.

Theorem 1(Kruskal's Theorem- Finite Version): Every infinite sequence of ground terms is self-embedding.

The proof of Kruskal's tree theorem is facilitated by the following two lemmas.

Lemma 1.

Let $\succcurlyeq$ be a *wpo* on the set A. Then every infinite sequence $a_1, a_2, a_3, \ldots$ of elements of A has an infinite ascending subsequence, i.e., there exist infinitely many indices $i_1 < i_2 < i_3 < \ldots$ such that $a_{i_1} \preccurlyeq a_{i_2} \preccurlyeq a_{i_3} \preccurlyeq \ldots$

Lemma 2.

Let $\succcurlyeq_1, \ldots, \succcurlyeq_n$ be *wpo*s on the sets $A_1, \ldots, A_n$. Then the relation $\succcurlyeq$ said to be defined component-wise by $(a_1, \ldots, a_n) \succcurlyeq (a_1', \ldots, a_n')$ iff $a_1 \succcurlyeq_1 a_1' \wedge \ldots \wedge a_n \succcurlyeq_n a_n'$ is a *wpo* on $A_1 \times \ldots \times A_n$.

We now present a general version of the Kruskal's tree theorem. The proof, essentially is due to Nash-Williams (Nash-Williams, 1963) and has the same structure as the the proof of Higman's Lemma (Higman, 1952). Our proof is very similar to the proof of Gallier (Gallier, 1991) formulated in terms of *wpos* but in a simplified form.

Theorem 2 (Kruskal's Tree Theorem-General Version):

Let $\mathcal{F}$ be a finite signature and $\mathcal{V}$ a finite set of variables. Then the homeomorphic embedding $\succcurlyeq_{emb}$ on $\mathcal{T}(\mathcal{F},\mathcal{V})$ is a *wpo*.

Proof.

We have to show that there are no bad sequences of terms in $\mathcal{T}(\mathcal{F},\mathcal{V})$. Let us assume the contrary that there exists a bad sequence (with respect to $\succcurlyeq_{emb}$) in $\mathcal{T}(\mathcal{F},\mathcal{V})$. We construct a *minimal bad sequence* by induction as follows:

We define t_n to be a smallest term, with respect to size such that there exists a bad sequence starting with $t_1, \ldots, t_n\ (n \geq 0)$. If $n = 0$, this obviously means that there exists a bad sequence. Let $t_{n+1} \in \mathcal{T}(\mathcal{F},\mathcal{V})$ be a minimal term (with respect to size) among all terms that occur at position $n+1$ of a bad sequence in $\mathcal{T}(\mathcal{F},\mathcal{V})$ that starts with $t_1, \ldots, t_n$. By induction hypothesis, there exists at least one such bad sequence. Obviously, the definition of t_{n+1} implies that there exists a bad sequence starting with $t_1, \ldots, t_{n+1}$.

In the limit, this defines an infinite bad sequence $t_1, t_2, t_3, \ldots$. The following analysis constitutes the proof,

(i) For $i \geq 1$, we define $S_i = \emptyset$, if t_i is a variable. Otherwise, if $t_i = f_i(s_1^{(i)}, \ldots, s_{n_i}^{(i)})$ for a function symbol $f_i \in \mathcal{F}^{(n_i)}$ and terms $s_1^{(i)}, \ldots, s_n^{(i)}$, we define $S_i = \{s_1^{(i)}, \ldots, s_n^{(i)}\}$. We claim that $\succcurlyeq_{emb}$ is a *wpo* on $S = \bigcup_{i\geq 1} S_i$. Assume that $s_1, s_2, s_3, \ldots$ is a bad sequence in S, and let k be such that $s_1 \in S_k$. Since $\succcurlyeq_{emb}$ is reflexive, the sequence can only be bad if all s_i are distinct. Thus, since $U = \bigcup_{i=1}^{k-1} S_i$ is finite, there exists an $l \geq 1$ such that $s_i \in S - U$ for all $i \geq l$. Since the size of $s_1 \in S_k$ is smaller than the size of t_k, minimality of the sequence $t_1, t_2, t_3, \ldots$ implies that the sequence

$$t_1, \ldots t_{k-1}, s_1, s_l, s_{l+1}, \ldots$$

is good. Thus, the sequences $t_1, t_2, t_3, \ldots$ and $s_1, s_2, s_3, \ldots$ are bad, which can only be possible if there exist indices $i \in \{1, \ldots, k-1\}$ and $j \in \{1, l, l+1, \ldots\}$ such that $t_i \preccurlyeq_{emb} s_j$. If $j = 1$, then $s_j = s_1$ is a subterm of t_k, and thus $t_i \preccurlyeq_{emb} s_j = s_1$ yields $t_i \preccurlyeq_{emb} t_k$. Because $i < k$, this implies that $t_1, t_2, t_3, \ldots$ is good, which is a contradiction. Otherwise, let m be such that $s_j \in S_m$. Since $j \geq 1$, we know that $s_j \notin U$, which yields $i < k \leq m$. However, $s_j \in S_m$ means that s_j is a subterm of t_m, and therefore, $t_i \preccurlyeq_{emb} s_j$ implies $t_i \preccurlyeq_{emb} t_m$. Sake of $i < m$, this again contradicts the fact that $t_1, t_2, t_3, \ldots$ was constructed as a bad sequence.

(ii) Let us consider the minimal bad sequence $t_1, t_2, t_3, \ldots$ constructed above. Since $\mathcal{F} \cup \mathcal{V}$ is finite, there are infinitely many indices $i_1 < i_2 < i_3 < \ldots$ such that the root symbols of the terms $t_{i_1}, t_{i_2}, t_{i_3}, \ldots$ coincide. If this symbol is a variable or a constant, then we have $t_{i_1} = t_{i_2}$, which implies $t_{i_1} \preccurlyeq_{emb} t_{i_2}$. This contradicts the fact that $t_1, t_2, t_3, \ldots$ is bad. Thus, let the root symbol of $t_{i_1}, t_{i_2}, t_{i_3}, \ldots$ be a function symbol $f \in \mathcal{F}^{(n)}$ for $n > 0$, i.e., $t_{i_j} = f(s_1^{(i_j)}, \ldots, s_n^{(i_j)})$. Because of (i) and lemma 2, the sequence

$(s_1^{(i_1)},\ldots,s_n^{(i_1)})$, $(s_1^{(i_2)},\ldots,s_n^{(i_2)}),\ldots$ is good with respect to the component-wise order on $S\times\ldots\times S$, which yields indices $v<\lambda$ such that $s_1^{(i_v)} \preccurlyeq_{emb} s_1^{(i_\lambda)} \wedge \ldots \wedge s_n^{(i_v)} \preccurlyeq_{emb} s_n^{(i_\lambda)}$, and hence $t_{i_v} \preccurlyeq_{emb} t_{i_\lambda}$. Accordingly, since $v<\lambda$ implies $i_v < i_\lambda$, this contradicts the fact that $t_1, t_2, t_3, \ldots$ is bad.
We have shown that our original assumption that there exists a bad sequence in $\mathcal{T}(\mathcal{F},\mathcal{V})$, and in turn, the existence of a minimal bad sequence $t_1, t_2, t_3, \ldots$, leads to a contradiction

Lemma 3

Let $\succ$ be a simplification ordering on a set of terms $\mathcal{T}(\mathcal{F},\mathcal{V})$, and $s,t\in\mathcal{T}(\mathcal{F},\mathcal{V})$. Then $s \succcurlyeq_{emb} t$ implies $s \succcurlyeq t$.

Proof

Assume that $s \succcurlyeq_{emb} t$. We consider the three cases in the definition of $\succcurlyeq_{emb}$, and prove $s \succcurlyeq t$ by induction on $|s|$. (i) If $s=x=t$ then $s \succcurlyeq t$, because $\succcurlyeq$ is reflexive. (ii) Assume that $s=f(s_1,\ldots,s_n)$ and $t=f(t_1,\ldots,t_n)$ for a function symbol $f\in\mathcal{F}^{(n)}$ and $s_1 \succcurlyeq_{emb} t_1, \ldots, s_n \succcurlyeq_{emb} t_n$. By induction, we obtain $s_1 \succcurlyeq t_1,\ldots,s_n \succcurlyeq t_n$. Since $\succ$ is a rewrite order, where $f(s_1,\ldots,s_n) \succcurlyeq f(t_1,\ldots,t_n)$. (iii) Assume that $s=f(s_1,\ldots,s_n)$ for a function symbol $f\in\mathcal{F}^{(n)}$ and $s_j \succcurlyeq_{emb} t$ for some $j, 1\le j\le n$. By induction, we obtain $s_j \succcurlyeq t$. In addition, the subterm property of $\succ$ yields $s \succ s_j$, and thus $s \succ t$.

Lemma 4

Let $\mathcal{R}$ be a TRS over a finite signature $\mathcal{F}$. Then every simplification order is a reduction order.

Proof.

By definition of simplification orders, it remains to be shown that every simplification order is well-founded. Assume that $\succ$ is a simplification order on $\mathcal{T}(\mathcal{F},\mathcal{V})$, and $t_1 \succ t_2 \succ t_3 \succ \ldots$ is an infinite chain in $\mathcal{T}(\mathcal{F},\mathcal{V})$. We first show by contradiction that $\mathcal{V}ar(s_1)\supseteq\mathcal{V}ar(s_2)\supseteq\mathcal{V}ar(s_3)\ldots$ holds. Assume that there exists a variable $x\in\mathcal{V}ar(t_{i+1})-\mathcal{V}ar(t_i)$. Define a substitution $\sigma=\{x\mapsto t_i\}$ such that on one hand, $t_i=\sigma(t_i)$ (since x does not occur in t_i) and $\sigma(t_i)\succ\sigma(t_{i+1})$ (since $\succ$ is a rewrite order). On the other hand, since t_i is a subterm of $\sigma(t_{i+1})$, and it follows from the subterm property that $\sigma(t_{i+1})\succcurlyeq t_i$. If we combine the two inequalities, we obtain $t_i\succ t_i$, which is a contradiction. The first part of the proof shows that, for the finite set $X=\mathcal{V}ar(t_i)$, all terms in the sequence $t_1,t_2,t_3,\ldots$ belong to $\mathcal{T}(\mathcal{F},\mathcal{V})$. Since $\mathcal{F}$ and $\mathcal{V}$ are finite, Kruskal's theorem implies that this sequence is good. i.e., there exist $i<j$ such that $t_i \preccurlyeq_{emb} t_j$. Now, Lemma 3 yields $t_i \preccurlyeq t_j$, which is a contradiction since we know that $t_i\succ t_{i+1}\succ\ldots\succ t_j$.

Remark A *wqo* is a preorder that contains a *pwo*. This definition is equivalent to all other definitions of *wqo* found in the literature. Kruskal's tree theorem is usually presented in terms of *wqos* (Middeldorp and Zantema, 1997).

However, the *wqo* version of Kruskal's tree theorem is not more powerful than the *pwo* version; bearing in mind that the strict part of a *wqo* is not necessarily a *pwo.*

A direct consequence of Kruskal's theorem (Kruskal, 1960) is that any simplification order over a finite signature is well-founded as shown in the following theorem.

Theorem 3.

Simplification orders are well-founded on terms over finite signature $\mathcal{F}$.

Proof follows by Kruskal's tree theorem and Lemma 4 above.

4. Conclusion

The need for a more elementary proof of Kruskal's tree theorem is especially felt due to the fact that this theorem figures prominently in computer science. Nash-Williams (1963), Dershowitz (1979) and Gallier (1991) present different versions of the proof of Kruskal's tree theorem. In this paper, we present a simplified form of Kruskal's tree theorem in a way that is inspired by Nash-Williams' proof of the theorem (1963); as it appears in Gallier (1991). Our proof is very similar to the proof of Gallier formulated in terms of *wpos* but in a simplified form. In addition, our proof and that of Dershowitz (1979) is simpler than the other previous versions.

5. Direction for Further Research

The simplified proof of Kruskal's theorem we have presented is still less constructive. This is because the proof has two nested arguments by contradiction. Indeed, it is a research problem to find a more constructive version of the proof. Furthermore, Kruskal's theorem is a simple example of a combinatorial statement that cannot be proved by Peano Arithmatic.

We are hoping that this exposition will help in making this beautiful but seemingly arcane tool and technique for proving well-foundedness known to more researchers in logic and theoretical computer science.

References

Baader, F. and Nipkow, T. (1998). *Term Rewriting and All That*, Cambridge University Press.

Dershowitz, N. (1979). A Note on Simplification Orderings, *Information Processing Letters*, 9(5), 212-215.

Dershowitz, N. (1982). Ordering for Term Rewriting Systems, *Theoretical Computer Science*, 17 (3), 279-301.

Dershowitz, N. (1987), Termination of Rewriting, *Journal of Symbolic Computation*, 3 (1 and 2), 69-115.

Gallier, J. H. (1991). What's so special about Kruskal's theorem and the ordinal Γ_0, Γ. A survey of some results in proof theory, *Annals of Pure and Applied Logic* 53, 204-320.

Higman, G. (1952). Ordering by Divisibility in Abstract Algebras, *Proceeding, the London Philosophical Society*, 3, 326-336.

Kruskal's, J.B. (1960). Well-quasi ordering, the tree theorem, and Vazsonyi's Conjecture, *Transactions, AMS*, 95, 210-225.

Middeldorp, A. and Zantema, H. (1997). Simple Termination of Rewrite Systems, *Theoretical Computer Science*, 175, 127-158.

Nash-Williams, C. S. J. A. (1963). On Well-quasi Ordering Finite Trees. *Proceeding, Cambridge Philosophical Society*, 833-835.