A Note on Kruskal's Theorem*

Gyesik Lee • Hyeon-Suk Na**

【Abstract】It is demonstrated that there is a simple, canonical way to show the independency of the Friedman-style miniaturization of Kruskal's theorem with respect to $(\Pi^1_2 - BI)_0$. This is done by a non-trivial combination of some well-known, non-trivial previous works concerning directly or indirectly the (proof-theoretic) strength of Kruskal's theorem.

【Key Words】Kruskal's theorem, Friedman-style miniaturization, Unprovability, $(\Pi^1_2 - BI)_0$
1. Introduction

Kruskal's theorem (Kruskal 1960), based on a conjecture by Vazsonyi, states that the set of finite trees over a well-quasi-ordered set of labels is itself well-quasi-ordered with respect to tree homeomorphic embedding:

\[
\text{For every infinite sequence } T_0, T_1, \ldots \text{ of finite rooted trees there exist natural numbers } i, j \text{ such that } i < j \text{ and } T_i \text{ embeds into } T_j.
\]

The original proof by Kruskal was a slight extension of that of Higman’s lemma (Higman 1952). In 1963, Nash-Williams (1963) gave a short, elegant, powerful, but non-constructive proof of Kruskal’s theorem. Later, Veldman (2004) showed that the arguments given by Higman and Kruskal are essentially constructive and acceptable from an intuitionistic point of view.

Kruskal's theorem plays a fundamental role in many areas. In computer science, it has been used to prove the well-foundedness of certain orderings or the termination of many term rewriting systems. In mathematical logic, its meaning was made obvious when Friedman (Simpson 1985) showed that there is a surjective, order-preserving function from the set of all finite trees to \( \Gamma_0 \), the Feferman-Schütte ordinal, also known as the proof-theoretic strength of the system \( ATR_0 \), the system of arithmetical transfinite recursion. The real proof-theoretic strength of Kruskal's theorem was established in 1993 by Rathjen and Weiermann (1993) who showed that \( ACA_0 \) plus Kruskal's theorem is proof-theoretically as
strong as \((\Pi_2^1-\text{BI})_0\) which is proof-theoretically much stronger than \(\text{ATR}_0\). The system \((\Pi_2^1-\text{BI})_0\) denotes a subsystem of the second order Peano arithmetic \(Z_2\) and will be formally introduced in Section 5.

Another celebrated result is the finite form of Kruskal's theorem, introduced by Friedman (Simpson 1985). The finite form is also called Friedman-style miniaturization:

For any \(k\) there exists a constant \(n\) so large that, for any finite sequence \(T_0, \ldots, T_n\) of finite rooted trees with \(\|T_i\| \leq k+i\) \((i \leq n)\), there are indices \(i, j\) such that \(i < j \leq n\) and \(T_i\) embeds into \(T_j\).

(Here \(\|T\|\) denotes the number of nodes in \(T\).) This finite form is a \(\Pi_2^0\) sentence, hence a first-order sentence. Friedman showed that it is still not provable in \(\text{ATR}_0\). With the Paris-Harrington theorem (Paris and Harrington 1977), this result is sometimes considered as one of two spectacular results highlighting the mathematical relevance of the Gödel incompleteness theorems, see (Kolata 1982). Furthermore, Weiermann (2003) showed that there is a kind of threshold of PA-provability of the parameterized version of the Friedman-style finite form of Kruskal's theorem, cf. Theorem 10.

However, while the real strength of Kruskal's theorem corresponds to that of \((\Pi_2^1-\text{BI})_0\) which is far stronger than the first-order Peano arithmetic \(\text{PA}\), the arithmetical comprehension \(\text{ACA}_0\), and the arithmetical transfinite recursion \(\text{ATR}_0\), it is
unknown yet whether the Friedman-style miniaturization of Kruskal's theorem is provable in \( (\Pi_2^{1-BI})_0 \) or not. In this paper we show that it is the case, i.e., it is as strong as \( (\Pi_2^{1-BI})_0 \).

This paper is far from being self-contained and rather gives an overview of the role of Kruskal's theorem and its variants in proof theory. The next section reminds just some preliminaries like well-partial-ordering, (maximal) order type, etc. for a better understanding of this paper. Then Friedman-style miniaturization, Kruskal's theorem, Rathjen and Weiermann's results will be just introduced without going into further detail. Finally, we show how to use them in order to reach our goal.

**Notational conventions**

Given a non-negative real number \( x \), \([x]\) is the largest natural number not bigger than \( x \). \([x]\) denotes the smallest natural number not smaller than \( x \). And \( \log \) denotes the logarithm to the base 2. Note that \([\log(n+1)]\) is the length of the binary representation of the natural number \( n \). For convenience, we set \( \log 0 := 0 \). Given two functions \( f, g : \mathbb{N} \to \mathbb{R}^+ \), \( f(n) \sim g(n) \) denotes \( \lim_{n \to \infty} \frac{f(n)}{g(n)} = 1 \), that is, \( f(n) \) and \( g(n) \) become eventually the same as \( n \) grows.

2. Well-partial-orderings

A *partial ordering* is a pair \( (X, \leq) \), where \( X \) is a set and \( \leq \) is a transitive, reflexive and antisymmetric binary relation on \( X \). If
For any partial ordering \((X, \leq)\) and any \(x, y \in X\), we write \(x < y\) for \(x \leq y\) and \(y \not\leq x\). A linear ordering is a partial ordering \((X, \leq)\) such that any two elements are \(\leq\)-comparable.

A well-partial-ordering (wpo) is a partial ordering \((X, \leq)\) such that there is no infinite bad sequence: A sequence \(\langle x_i \rangle_{i \in \omega}\) is called bad if \(x_i \not\leq x_j\) for all \(i < j\). \((X, \leq)\) is called a well-ordering if \((X, \leq)\) is a linear wpo.

The following condition is necessary and sufficient for a partial ordering \((X, \leq)\) to be a wpo:

\[
\text{Every extension of } \leq \text{ to a linear ordering on } X \text{ is a well-ordering.}
\]

The order type of a well-ordering \((X, <)\), \(o_{\text{typ}}(<)\), is the least ordinal for which there is an order-preserving function \(f : X \to \alpha\):

\[
o_{\text{typ}}(<) := \min \{ \alpha : \text{there is an order-preserving function } f : X \to \alpha \}.
\]

Given two partial ordering \((X, \leq_X)\) and \((Y, \leq_Y)\), the function \(f : X \to Y\) is called order-preserving when \(x \leq_X y\) implies \(f(x) \leq_Y f(y)\). Given a wpo \((X, \leq)\), its maximal order type is defined by \(o(X, \leq) := \sup \{ o_{\text{typ}}(<^+) : <^+ \text{ is a well-ordering on } X \text{ extending } \leq \}\). We simply write \(o(X)\) for \(o(X, \leq)\) if it causes no confusion.

**Theorem 1** (de Jongh and Parikh 1977)

If \((X, <)\) is a wpo, then there is a well-ordering \(<^+\) on \(X\) extending \(\leq\) such that \(o(X) = o_{\text{typ}}(<^+)\).
We refer the reader to Schmidt (1979) for more extensive study concerning maximal order type.

3. Friedman-style miniaturization

Let $T$ be a subsystem of the second order Peano arithmetic $Z_2$ and $\langle B, \leq \rangle$ a primitive recursive ordinal notation system\(^1\) of $T$ with a norm function $\| \cdot \|_B : B \to \mathbb{N}$, i.e., for any $n \in \mathbb{N}$, the set $\{ \beta \in B : \| \beta \|_B \leq n \}$ is finite. An ordinal notation system of the system $T$ can be thought of as the least ordinal whose well-orderedness cannot be proved in $T$.

Assume that this norm function is provably recursive in PA and that there is a uniform, elementary bound on $\text{card}(\{ \beta \in B : \| \beta \|_B \leq n \})$ for every $n \in \mathbb{N}$.

Let $\text{WO}(B)$ denote that $\langle B, \leq \rangle$ is well-ordered. For each $\beta \in B$, $\text{WO}(\beta)$ is the assertion that $B$ is well-ordered up to $\beta$, i.e., $B$ contains no infinite descending sequence beginning with $\beta$. Note that $\text{WO}(B)$ is a $\Pi^1_1$ sentence and not provable in $T$.

Interestingly, Friedman translated this $\Pi^1_1$ sentence into a $\Pi^0_2$ sentence which still remains $T$-unprovable. It is a variation of the following assertion $\text{PRWO}(B)$ that $B$ is primitive recursively well-ordered: $B$ contains no infinite decreasing primitive recursive sequence. Similarly, we define $\text{PRWO}(\beta)$ for each $\beta \in B$. Note

\(^1\) Smith (1985) used a more general concept, i.e., reasonable ordinal notation systems. Here we just need to know that all the well-known notation systems in proof theory are reasonable.
that they are all $\Pi_2^0$ sentences.

**Definition 2** (Friedman (Simpson 1985), Smith 1985)

Let $\langle \beta_i \rangle_{i<\omega}$ an infinite sequence of elements from $B$.

1. $\langle \beta_i \rangle_{i<\omega}$ is called slow if there is a natural number $k$ such that $\| \beta_i \|_B \leq k+i$ for all $i \in \mathbb{N}$.

2. SWO($B, \leq, id$) denotes that $B$ is slowly well-ordered, i.e., $B$ contains no infinitely descending slow sequence.

By König's Lemma (König 1927), SWO($B, \leq, id$) is equivalent to the following $\Pi_2^0$ sentence, where $f = id$.

For any $k$ there exists an $n$ such that for any finite sequence $\beta_0, ..., \beta_n$ from $B$ satisfying the condition that $\| \beta_i \|_B \leq k+f(i)$ for any $i \leq n$ there are indices $\ell, m$ such that $\ell < m \leq n$ and $\beta_\ell \leq \beta_m$.

This assertion is denoted by SWO($B, \leq, f$). Now let $(Q, \leq)$ be a primitive recursive well-partial-ordering based on a norm function $\| \cdot \|_Q : Q \to \mathbb{N}$. Assume its maximal order type is the proof-theoretic ordinal of $T$. The slowly-well-partial-orderedness of $Q$, SWP($Q, \leq, f$), is defined as follows:

For any $k$ there exists an $n$ such that for any finite sequence $\gamma_0, ..., \gamma_n$ from $Q$ satisfying the condition that $\| \gamma_i \|_Q \leq k+f(i)$ for any $i \leq n$ there are indices $\ell, m$ such that $\ell < m \leq n$ and $\gamma_\ell \leq \gamma_m$.

---

2) We use the refined version of Smith (1985) instead of the original definition of Friedman.
Note that $\text{SWO}(B, \leq, f)$ and $\text{SWP}(Q, \leq, f)$ are true for any function $f : \mathbb{N} \to \mathbb{N}$. It is just because of the well-foundedness. However, they are strong enough not to be $T$-provable as it is demonstrated by Friedman and Smith.

**Theorem 3** (Friedman (Simpson 1985), Smith 1985)

In $ACA_0$, the following are equivalent:
1. $\text{SWO}(B, \leq, id)$
2. $\text{SWP}(Q, \leq, id)$
3. 1-consistency of $T$
4. $\Pi^0_2$-soundness of the formal system $ACA_0 + \{WO(\beta) : \beta \in B\}$

The 1-consistency of a theory $T$ is the assertion: if $\varphi$ is a $\Sigma^0_1$ sentence provable from $T$, then $\varphi$ is true.

**Corollary 4** (Friedman (Simpson 1985), Smith 1985)

$\text{SWO}(B, \leq, id)$ and $\text{SWP}(Q, \leq, id)$ are $T$-independent.

4. Kruskal's theorem and its miniaturizations

A *finite rooted tree* is a finite partial ordering $(T, \leq)$ such that, if $T$ is not empty,

- $T$ has a smallest element called the *root* of $T$.
- For each $b \in T$, the set $\{a \in T : a \leq b\}$ is totally ordered.
Let \( a \wedge b \) denote the infimum of \( a \) and \( b \) for \( a, b \in T \). Given finite rooted trees \( T_1 \) and \( T_2 \), a homeomorphic embedding of \( T_1 \) into \( T_2 \) is an one-to-one mapping \( f: T_1 \to T_2 \) such that \( f(a \wedge b) = f(a) \wedge f(b) \) for all \( a, b \in T_1 \). We write \( T_1 \sqsubseteq T_2 \) if there exists a homeomorphic embedding \( f: T_1 \to T_2 \), and in that case one says \( T_1 \) is homeomorphically embeddable into \( T_2 \).

**Theorem 5** (Kruskal's theorem (Kruskal 1960))

For any infinite sequence of finite rooted trees \( \langle T_k \rangle_{k < \omega} \), there are indices \( \ell < m \) satisfying \( T_\ell \sqsubseteq T_m \).

Note that Kruskal's theorem is a \( \Pi^1_1 \) sentence saying that \( \sqsubseteq \) is a well-partial-ordering on the set \( T \) of all finite rooted trees.

**Theorem 6** (Friedman (Simpson 1985))

Kruskal's theorem is not provable in \( ATR_0 \).

Let \( L_2 \) be the language of the second-order Peano arithmetic. Then for a binary relation \( < \) and an arbitrary formula \( F(a) \) of \( L_2 \) we define

- \( \text{Prog}(<,X) := \forall x \left[ \forall y \left( y < x \rightarrow y \in X \right) \rightarrow x \in X \right] \) (progressiveness)
- \( \text{TI}(<,X) := \text{Prog}(<,X) \rightarrow \forall x (x \in X) \) (transfinite induction)
- \( \text{WF}(<) := \forall X \left[ \text{TI}(<,X) \right] \) (well-foundedness)
The system $(\Pi^1_2 - BI)_0$ is $ACA_0$ extended with the $\Pi^1_2$ bar induction scheme, i.e., all formulas of the form

$$WF(<) \rightarrow TI(<,F)$$

where $< \in \Pi^1_0$ and $F \in \Pi^1_2$ stands for $\{x : F(x)\}$.

**Theorem 7** (Rathjen and Weiermann 1993)

1. In $ACA_0$, Kruskal's theorem and the well-foundedness of the small Veblen ordinal $\vartheta_{\Omega^2}$ are equivalent.
2. The proof-theoretic ordinal of $(\Pi^1_2 - BI)_0$ is $\vartheta_{\Omega^2}$.

Now we turn our attention to Friedman-style miniaturization of Kruskal's theorem and its parameterized version introduced by Weiermann. Let $\|T\|$ denote the number of nodes of the finite tree $T$. Assume further that the set of finite rooted trees is coded primitive recursively into a set of natural numbers in a standard way. Given $f : \mathbb{N} \rightarrow \mathbb{R}$, the **slowly-well-partially-orderedness** is a Friedman-style miniaturization of Kruskal's Theorem:

For any $k$ there exists a constant $n$ so large that, for any finite sequence $T_0, \ldots, T_n$ of finite rooted trees with $\|T_i\| \leq k + f(i)$ for all $i \leq n$ there exist indices $\ell, m$ such that $\ell < m \leq n$ and $T_\ell \sqsubseteq T_m$.

Let $SWP(\mathcal{T}, \sqsubseteq, f)$ denotes the above $\Pi^0_2$ sentence. Then it is still unprovable in $ATR_0$.

**Theorem 8** (Friedman (Simpson 1985), Smith 1985)

$SWP(\mathcal{T}, \sqsubseteq, id)$ is independent of $ATR_0$. 

Loebl and Matoušek proved a very interesting property about the finite form of Kruskal's theorem in the sense that it indicates the existence of a kind of threshold for the provability of the parameterized finite form which could depend on real numbers between 1/2 and 4.

**Theorem 9** (Loebl and Matoušek 1987) In PA, the following hold.

1. SWP($\mathbb{T}, \preceq, i \mapsto \frac{1}{2} \log i$) is provable.
2. SWP($\mathbb{T}, \preceq, i \mapsto 4 \log i$) is not provable.

Indeed, Weiermann could show that such a phenomenon does happen: Let $\alpha$ be the so-called *Otter's tree constant* $\alpha = 2.955765...$ satisfying

$$t(n) \sim \beta \cdot \alpha^n \cdot n^{-2/3}$$

for some real number $\beta$, where $t(n) = \text{card}(\{T: \|T\| = n\})$. See Otter (1948) for more about the tree constant.

**Theorem 10** (Weiermann 2003)

Let $c = \frac{1}{\log \alpha}$ and $r$ be a primitively recursive real number. Set $f_r(i) := r \cdot \log i$. Then $PA \vdash \text{SWP}(\mathbb{T}, \preceq, f_r)$ if and only if $r > c$. 


5. The real strength of the finite form of Kruskal's theorem

Now we show that we can strengthen previous results. That is, the unprovability and the threshold results hold still with respect to \((\Pi^1_2 - \text{BI})_0\) instead of \(\text{PA}\). We emphasize that we just need to combine all the previous works together.

**Theorem 11**

Let \(c, r\) and \(f_r\) be as above.

1. \(\text{SWP}(\mathbb{T}, \preceq_{id})\) is independent of \((\Pi^1_2 - \text{BI})_0\).

2. Further it holds that \((\Pi^1_2 - \text{BI})_0 \nvdash \text{SWP}(\mathbb{T}, \preceq_{f_r})\) if and only if \(r > c\).

**Proof.** The first claim is a direct result of Theorem 3 and Theorem 7. The second one follows from Theorem 3 and the first one because Weiermann’s proof of Theorem 10 shows in fact that, in \(\text{ACA}_0\), the provability of \(\text{SWP}(\mathbb{T}, \preceq_{f_r})\) implies that of \(\text{SWP}(\mathbb{T}, \preceq_{id})\) if \(r > c\). Let \(F_r\) be the Skolem function of \(\text{SWP}(\mathbb{T}, \preceq_{f_r})\) and \(F_{id}\) that of \(\text{SWP}(\mathbb{T}, \preceq_{id})\). Then it was shown there that \(F_r(k)\) grows eventually faster than \(F_{id}(\lfloor k/3 \rfloor)\). That is, there is some \(K\) such that for any \(k \geq K\) it holds that \(F_r(k) \geq F_{id}(\lfloor k/3 \rfloor)\).

6. Conclusion

This note on Kruskal’s theorem was done while trying to establish a canonical way to get Friedman-style independence
results concerning the proof-theoretic strength of Kruskal's theorem. This will be presented in another paper, and see Lee (2005) for more about independence results.

7. Acknowledgement

We would like to thank the anonymous referees for their helpful comments.
References


Schmidt, D.(1979), Well-Partial Orderings and Their Maximal order
Types, Habilitationsschrift, Heidelberg.


숭실대학교 컴퓨터학부(나현숙)
School of Computing, Soongsil University
hsnaa@ssu.ac.kr

한경대학교 컴퓨터웹정보공학과(이계식)
Department of Computer & Web Information Engineering, Hankyong National University
gslee@hknu.ac.kr
A Note on Kruskal's Theorem

Gyesik Lee • Hyeon-Suk Na

프리드먼에 의해 제안된 “크루스칼 정리의 소형화 정리”가 2차 페아노 공리체계의 부분 시스템인 $(\Pi^1_2-\text{BI})_0$에서 증명될 수 없음을 증명한다. 또한 위 증명이 크루스زال 정리와 관련된 기존의 연구에서 알려진 중요한 정리들을 잘 조합함으로 해서 가능함을 보인다.

주요어: 크루스칼 정리, 프리드먼 방식의 소형화, 증명 불가능성, $(\Pi^1_2-\text{BI})_0$