Basic Research in Computer Science

BRICS RS-98-39 D. Fridlender: An Interpretation of the Fan Theorem in Type Theory

An Interpretation of the Fan Theorem in Type Theory

Daniel Fridlender

BRICS Report Series **RS-98-39**

ISSN 0909-0878 **December 1998**

See back inner page for a list of recent BRICS Report Series publications. Copies may be obtained by contacting:

BRICS
Department of Computer Science
University of Aarhus
Ny Munkegade, building 540
DK–8000 Aarhus C
Denmark
Telephone: +45 8942 3360
Telefax: +45 8942 3255
Internet: BRICS@brics.dk

BRICS publications are in general accessible through the World Wide Web and anonymous FTP through these URLs:

`http://www.brics.dk`
`ftp://ftp.brics.dk`
This document in subdirectory `RS/98/39/`

An Interpretation of the Fan Theorem in Type Theory*

Daniel Fridlender

BRICS**, Department of Computer Science, University of Aarhus
Ny Munkegade, Building 540, DK-8000 Aarhus C, Denmark
e-mail: daniel@brics.dk

Abstract. This article presents a formulation of the fan theorem in Martin-Löf's type theory. Starting from one of the standard versions of the fan theorem we gradually introduce reformulations leading to a final version which is easy to interpret in type theory. Finally we describe a formal proof of that final version of the fan theorem.

Keywords: type theory, fan theorem, inductive bar.

1 Introduction

In informal constructive mathematics, the fan theorem is an easy consequence of the rule of bar induction. Both are about infinite objects which makes their interpretation in Martin-Löf's type theory non trivial. Bar induction can be represented in type theory, as proposed in [Mar68] and shown also in this article. But still from this interpretation it is not clear how to formulate and prove the fan theorem formally in type theory.

This is because, whereas the usual informal language to treat bar induction and the fan theorem is the same, the formal treatment of the fan theorem in type theory is technically more involved than that of bar induction. The concept of finiteness is difficult to handle simultaneously in an elegant, completely formal and constructive way; and it seems hard to avoid dealing explicitly with *fans*, whereas *spreads* are avoided in the type-theoretic interpretation of bar induction.

* Partially developed during the author's stay at Göteborg University, Sweden.
** Basic Research in Computer Science,
Centre of the Danish National Research Foundation.

The fan theorem is very important in constructive mathematics since it makes possible to reconstruct large parts of traditional analysis. For explanations of the fan theorem and its role in constructive analysis see for instance [Dum77] and [TvD88].

The goal in this article is to present a formulation and a proof of the fan theorem in type theory. The type-theoretic version of the fan theorem presented here has been used in [Fri97] to interpret in type theory an intuitionistic proof of Higman's lemma which uses the fan theorem [Vel94]. However, in [Fri97] the type-theoretic fan theorem is only mentioned and the proof is omitted. The importance of the fan theorem justifies this more extended presentation.

Type theory here means Martin-Löf's type theory, of which there exist different formulations (for example, [Mar75], [Mar84], [NPS90] and [Tas97]). The exposition here should suit all of them. The proof of the fan theorem presented here has been written down in full detail with the assistance of the proof-editor ALF [Mag94] which is an implementation of the formulation of type theory given in [Tas97].

The rest of this article is organized as follows. Section 2 introduces some notations and definitions to be used in the whole article, and gives an informal presentation of bar induction and the fan theorem.

Section 3 shows a type-theoretic interpretation of bar induction and some of its properties.

Finally, Section 4 formulates and proves the fan theorem in type theory.

2 Bar induction and the fan theorem

2.1 Preliminaries

Notations:

$\mathcal{N}$ the set of the natural numbers. Variables: n, m, k.

$\mathcal{A}^*$ the set of the lists (finite sequences) of elements of the set $\mathcal{A}$.
Variables: $\overline{u}$, $\overline{v}$, $\overline{w}$. Even $\overline{\overline{u}}$, $\overline{\overline{v}}$, $\overline{\overline{w}}$ when $\mathcal{A}$ is a set of lists.
$<a_1, \ldots, a_n>$ is the notation for lists.
$\overline{u} * \overline{v}$ is the concatenation between lists.
$\overline{u} \bullet a$ is a notation for concatenations of the form $\overline{u} * <a>$.

The variables α, β are used to denote infinite sequences of natural numbers. An initial segment $<\alpha(0), \ldots, \alpha(n-1)>$ of α is denoted $\overline{\alpha}(n)$. Given a set $\mathcal{S}$ of finite sequences of natural numbers, if $\forall n \ \ [\overline{\alpha}(n) \in \mathcal{S}]$, then we write $\alpha \in \mathcal{S}$. We denote by $\mathcal{S}^c$ the set $\mathcal{N}^* \backslash \mathcal{S}$.

Definition 1 (tree). *A* tree *is a set $\mathcal{T}$ of finite sequences of natural numbers (intuitively, a set of finite branches) which satisfy*

$<> \in \mathcal{T}$	*$\mathcal{T}$ is inhabited*
$\forall \overline{u} \ \ [\overline{u} \in \mathcal{T} \vee \overline{u} \notin \mathcal{T}]$	*$\mathcal{T}$ is decidable*
$\forall \overline{u}, n \ \ [\overline{u} \bullet n \in \mathcal{T} \Rightarrow \overline{u} \in \mathcal{T}]$	*$\mathcal{T}$ is closed under predecessor*

Definition 2 (finitely branching). *A* finitely branching tree *is a tree $\mathcal{T}$ which satisfy*

$$\forall \overline{u} \in \mathcal{T} \ \ \exists m \ \ \forall n \ \ [\overline{u} \bullet n \in \mathcal{T} \Rightarrow n < m].$$

Definition 3 (spread, fan). *A* spread *is a tree in which every node has at least one successor, that is, a tree $\mathcal{S}$ satisfying*

$$\forall \overline{u} \in \mathcal{S} \ \ \exists n \ \ [\overline{u} \bullet n \in \mathcal{S}].$$

A finitely branching spread is called a fan.

Definition 4 (bar). *Given a set $\mathcal{U} \subseteq \mathcal{N}^*$ and a spread $\mathcal{S}$, $\mathcal{U}$ is a* bar on $\mathcal{S}$ *if*

$$\forall \alpha \in \mathcal{S} \ \ \exists n \ \ [\overline{\alpha}(n) \in \mathcal{U}].$$

When $\mathcal{S} = \mathcal{N}^*$, $\mathcal{S}$ is called the *universal spread* and $\mathcal{U}$ is said to be a *bar*.

Proposition 1. *Given a spread $\mathcal{S}$ and a bar $\mathcal{U}$ on $\mathcal{S}$, then $\mathcal{V} = \mathcal{U} \cup \mathcal{S}^c$ is a bar.*

We can prove that $\mathcal{V}$ is a bar by letting α be an arbitrary infinite sequence of natural numbers and finding n such that $\overline{\alpha}(n) \in \mathcal{V}$. To this end, we determine a sequence of natural numbers β whose initial segments are the same as those of α as long as they belong to $\mathcal{S}$. As soon as an initial segment of α does not belong to $\mathcal{S}$, β deviates

from α. From that point, the initial segments of β are arbitrary segments in $\mathcal{S}$. That is,

$$\beta(i) = \begin{cases} \alpha(i) & \text{if } \overline{\alpha}(i{+}1) \in \mathcal{S} \\ k & \text{if } \overline{\alpha}(i{+}1) \notin \mathcal{S}, \text{for some } k \text{ such that } \overline{\beta}(i) \bullet k \in \mathcal{S} \end{cases}$$

As $\beta \in \mathcal{S}$, and $\mathcal{U}$ is a bar on $\mathcal{S}$, we can obtain n such that $\overline{\beta}(n) \in \mathcal{U}$. Now, either $\overline{\alpha}(n) \in \mathcal{S}$, in which case $\overline{\alpha}(n) = \overline{\beta}(n) \in \mathcal{U} \subseteq \mathcal{V}$, or $\overline{\alpha}(n) \notin \mathcal{S}$, hence $\overline{\alpha}(n) \in \mathcal{S}^c \subseteq \mathcal{V}$. Therefore, $\mathcal{V}$ is a bar.

2.2 Bar induction

Bar induction is the following rule, which is an axiom of intuitionistic logic

$$\frac{\begin{array}{ll} \forall \overline{u} \in \mathcal{X} \;\; \overline{u} \in \mathcal{Y} & \mathcal{X} \text{ is included in } \mathcal{Y} \\ \forall \overline{u} \in \mathcal{X} \;\; \forall n \;\; [\overline{u} \bullet n \in \mathcal{X}] & \mathcal{X} \text{ is monotone} \\ \forall \overline{u} \;\; \{[\forall n \;\; \overline{u} \bullet n \in \mathcal{Y}] \Rightarrow \overline{u} \in \mathcal{Y}\} & \mathcal{Y} \text{ is hereditary} \\ \forall \alpha \;\; \exists n \;\; [\overline{\alpha}(n) \in \mathcal{X}] & \mathcal{X} \text{ is a bar} \end{array}}{<> \in \mathcal{Y}} \text{ BI}$$

for $\mathcal{X}, \mathcal{Y} \subseteq \mathcal{N}^*$. For other formulations of the rule of bar induction and their justification see [Dum77].

2.3 Fan theorem

The most important consequence of the rule of bar induction is the fan theorem.

Theorem 1 (fan theorem). *Given a fan $\mathcal{F}$, and a monotone bar $\mathcal{U}$ on $\mathcal{F}$, then*

$$\exists n \;\; \forall \alpha \in \mathcal{F} \;\; [\overline{\alpha}(n) \in \mathcal{U}].$$

Intuitively, the fan theorem states that for any finitely branching tree all whose branches are finite, there is an upper bound on the length of the branches. The tree, not explicit in the statement of the theorem, is the set $\mathcal{F} \setminus \mathcal{U}$ (when $\mathcal{U}$ is decidable and $<> \notin \mathcal{U}$).

The fan theorem can also be read as stating that every finitely branching tree all whose branches are finite is itself finite, that is,

has a finite number of nodes. This is so, since for a finitely branching tree, the existence of an upper bound on the length of the branches is equivalent with it being finite.

A proof of the fan theorem can be obtained using the rule of bar induction with $\mathcal{Y} = \{\overline{u} \mid \exists n \ \ \forall \alpha \in \mathcal{F} \ \ [\alpha \text{ starts with } \overline{u} \Rightarrow \overline{\alpha}(n) \in \mathcal{U}]\}$ and $\mathcal{X} = \mathcal{U} \cup \mathcal{F}^c$. Proposition 1 guarantees that $\mathcal{X}$ is a bar. The monotonicity of $\mathcal{X}$ follows from those of $\mathcal{U}$ and $\mathcal{F}^c$. The inclusion of $\mathcal{X}$ in $\mathcal{Y}$ can be proved by letting $\overline{u} \in \mathcal{X}$ be arbitrary and choosing n as the length of $\overline{u}$. To prove that $\mathcal{Y}$ is hereditary we assume that, for an arbitrary $\overline{u}$, $\forall k \ \ \overline{u} \bullet k \in \mathcal{Y}$ holds, and prove that $\overline{u} \in \mathcal{Y}$ also holds. If $\overline{u} \notin \mathcal{F}$, then $\overline{u} \in \mathcal{Y}$ clearly holds, since no $\alpha \in \mathcal{F}$ starts with $\overline{u}$. Otherwise, as $\mathcal{F}$ is finitely branching there exists m such that for all k, $\overline{u} \bullet k \in \mathcal{F} \Rightarrow k < m$. As for each k, $\overline{u} \bullet k \in \mathcal{Y}$, it is possible to determine $n_0, \ldots n_{m-1}$ such that for each $k < m$ and $\alpha \in \mathcal{F}$ if α starts with $\overline{u} \bullet k$, then $\overline{\alpha}(n_k) \in \mathcal{U}$. To show that $\overline{u} \in \mathcal{Y}$, we choose n to be max $\{n_k \mid k < m\}$ and use the monotonicity of $\mathcal{U}$.

2.4 Other formulations of the fan theorem

So far, we have used the terminology which is standard in the literature. It is possible to give alternative presentations of the fan theorem, some of which, are actually not formulated in terms of fans but in terms of arbitrary finitely branching trees.

In this section, we explore other formulations of the fan theorem with the purpose of obtaining one which is easier to represent in type theory. We shall see that there is no need to introduce notions like fan or tree in type theory, since the fan theorem can be reformulated without explicit use of those notions.

Some of the formulations that we will introduce are in terms of a special kind of tree, which we call *independent-choice trees*.

Definition 5 (independent-choice). *An* independent-choice tree *is a tree $\mathcal{I}$ such that for all $\overline{u}, \overline{v} \in \mathcal{I}$ of equal length,*

$$\forall n \ \ [\overline{u} \bullet n \in \mathcal{I} \Leftrightarrow \overline{v} \bullet n \in \mathcal{I}].$$

There is a one-to-one correspondence between independent-choice fans and infinite sequences of nonempty finite subsets of $\mathcal{N}$. An independent-choice fan $\mathcal{I}$ is determined by a sequence $\mathcal{I}_0, \mathcal{I}_1, \ldots$ of

nonempty finite subsets of $\mathcal{N}$. The branches of $\mathcal{I}$ of length n are obtained by choosing one element from each of the sets $\mathcal{I}_0, \mathcal{I}_1, \ldots, \mathcal{I}_{n-1}$ in that order. Every choice is independent of the other choices done to determine the branch. Similarly, there is a one-to-one correspondence between independent-choice finitely branching trees and (not necessarily infinite) sequences of nonempty finite subsets of $\mathcal{N}$.

We list a few statements equivalent to the one of the fan theorem.

Theorem 2 (alternatives to fan theorem). *The fan theorem is equivalent to the validity of*

$$\forall \text{ monotone bar } \mathcal{U} \quad \exists n \quad \forall \alpha \in \mathcal{T} \quad [\overline{\alpha}(n) \in \mathcal{U}]$$

in any of the following cases:

1. *for all fan $\mathcal{T}$,*
2. *for all finitely branching tree $\mathcal{T}$,*
3. *for all independent-choice fan $\mathcal{T}$,*
4. *for all independent-choice finitely branching tree $\mathcal{T}$.*

The only difference between the fan theorem and item 1 is that in the latter $\mathcal{U}$ runs over bars on the universal spread, rather than over bars on the fan. With this modification, the fan theorem can be formulated for finitely branching trees as well (item 2). On the other hand, it is enough to restrict attention to independent-choice fans or trees (items 3 and 4).

To prove Theorem 2 notice that the domain on which $\mathcal{T}$ ranges in item 2 includes the one on which it ranges in item 1, and so item 2 $\Rightarrow$ item 1. Analogously, item 2 $\Rightarrow$ item 4, item 1 $\Rightarrow$ item 3, and item 4 $\Rightarrow$ item 3. Similarly, the domain on which $\mathcal{U}$ ranges in the fan theorem includes the one on which it ranges in Theorem 2, so Theorem 1 $\Rightarrow$ item 1.

To finish the proof of Theorem 2 it is enough to prove that item 3 $\Rightarrow$ item 2 and item 1 $\Rightarrow$ Theorem 1. For the former, let $\mathcal{T}$ be an arbitrary finitely branching tree and $\mathcal{U}$ an arbitrary monotone bar. Let $\mathcal{I}$ be the least independent-choice fan containing $\mathcal{T}$. Determine n such that $\forall \alpha \in \mathcal{I} \quad [\overline{\alpha}(n) \in \mathcal{U}]$. As $\alpha \in \mathcal{T} \Rightarrow \alpha \in \mathcal{I}$, we obtain $\forall \alpha \in \mathcal{T} \quad [\overline{\alpha}(n) \in \mathcal{U}]$.

Finally, to prove that item 1 $\Rightarrow$ Theorem 1, let $\mathcal{F}$ be an arbitrary fan and $\mathcal{U}$ an arbitrary bar on $\mathcal{F}$. Define $\mathcal{V} = \mathcal{U} \cup \mathcal{F}^c$. By Proposition 1, $\mathcal{V}$ is a bar. Then, by item 1 there is an n such that for all $\alpha \in \mathcal{F}$, $\overline{\alpha}(n) \in \mathcal{V}$. As $\overline{\alpha}(n) \in \mathcal{F}$, $\overline{\alpha}(n) \in \mathcal{U}$.

Theorem 3 (more alternatives to fan theorem). *The fan theorem is equivalent to the validity of*

$$\forall \text{ monotone bar } \mathcal{U} \ \ \exists n \ \ \forall \overline{u} \in \mathcal{T} \ \ [\mathit{length}(\overline{u}) = n \ \Rightarrow \ \overline{u} \in \mathcal{U}]$$

in any of the following cases:

5. *for all fan $\mathcal{T}$,*
6. *for all finitely branching tree $\mathcal{T}$,*
7. *for all independent-choice fan $\mathcal{T}$,*
8. *for all independent-choice finitely branching tree $\mathcal{T}$.*

Just as in the proof of Theorem 2, it is easy to obtain that item 6 $\Rightarrow$ item 5, item 6 $\Rightarrow$ item 8, item 5 $\Rightarrow$ item 7, and that item 8 $\Rightarrow$ item 7. Item 6 follows from item 7 in the same way as item 2 followed from item 3 in Theorem 2.

Finally, the equivalence between item 5 and item 1 of Theorem 2 is also easy, since given a fan $\mathcal{T}$, all $\overline{u} \in \mathcal{T}$ of length n is equal to $\overline{\alpha}(n)$, for some $\alpha \in \mathcal{T}$.

Theorem 4 (one more alternative to fan theorem). *For all monotone bar $\mathcal{U}$ and all infinite sequence $\mathcal{I}_0, \mathcal{I}_1, \ldots$ of finite subsets of $\mathcal{N}$,*

$$\exists n \ \ [\mathcal{I}_0 \times \ldots \times \mathcal{I}_{n-1} \ \subseteq \ \mathcal{U}],$$

where $\mathcal{I}_0 \times \ldots \times \mathcal{I}_{n-1} = \{<a_0, \ldots, a_{n-1}> \ \mid \ \forall i \ \ a_i \in \mathcal{I}_i\}$.

Theorem 4 is equivalent to the fan theorem.

Let $\mathcal{T}$ be the set $\bigcup\{\mathcal{I}_0 \times \ldots \times \mathcal{I}_{i-1} \mid \ i \in \mathcal{N}\}$. Clearly, $\mathcal{T}$ is a finitely branching tree. By item 6 of Theorem 3, there is a natural number n such that all the sequences in $\mathcal{T}$ of length n belong to $\mathcal{U}$. Those sequences are exactly the elements in the set $\mathcal{I}_0 \times \ldots \times \mathcal{I}_{n-1}$.

Conversely, to prove that item 8 of Theorem 3 follows from Theorem 4, let $\mathcal{T}$ be an arbitrary independent-choice finitely branching tree. Let $\mathcal{I}_i$ be the set $\{k \in \mathcal{N} \mid \ \exists \overline{u} \ \ [\mathrm{length}(\overline{u}) = i \ \wedge \ \overline{u} \bullet k \in \mathcal{T}]\}$. Given $\overline{u} \in \mathcal{T}$ of length n, we have $\overline{u} \in \mathcal{I}_0 \times \ldots \times \mathcal{I}_{n-1} \subseteq \mathcal{U}$.

The advantage of the formulation of the fan theorem as in Theorem 4 is that it avoids the notions of fan and finitely branching tree. Also, if we extend the definition of *bar* to sets of finite sequences of finite subsets of natural numbers, rather than only sets of finite sequences of natural numbers, then we may write the fan theorem in the following way. Let $\overline{\mathcal{I}}$ range over finite sequences of finite subsets of $\mathcal{N}$, and $\bigotimes$ denote the operation to obtain the Cartesian product of such a finite sequence, that is, $\bigotimes <\mathcal{I}_0, \ldots, \mathcal{I}_{n-1}> = \mathcal{I}_0 \times \ldots \times \mathcal{I}_{n-1}$.

Theorem 5 (fan theorem, final reformulation). *Given a monotone set $\mathcal{U}$ of finite sequences of natural numbers, if $\mathcal{U}$ is a bar, then so is $\{\overline{\mathcal{I}} \mid \bigotimes \overline{\mathcal{I}} \subseteq \mathcal{U}\}$.*

This is the formulation which is represented in type theory by Theorem 6.

3 Inductive bars

Following the Curry-Howard isomorphism ([CF58] and [How80]) every proposition is represented in type theory by the set of its proofs. Predicates, subsets and families of sets are identified with each other, in the sense that every predicate over the elements of a set $\mathcal{A}$, every subset of $\mathcal{A}$, and every family of sets indexed by the elements of $\mathcal{A}$, is represented by a function which when applied to an element of $\mathcal{A}$ returns a set.

Given a predicate $\mathcal{U}$ over a set $\mathcal{A}$ and a list $\overline{u}$ in $\mathcal{A}^*$, we let $\bigwedge_{\overline{u}} \mathcal{U}$ or

$$\bigwedge_{\overline{u}} \mathcal{U}$$

mean that all the elements in the list $\overline{u}$ satisfy $\mathcal{U}$. In type theory, it can be defined inductively with the following introduction rules.

$$\frac{}{\bigwedge_{<>} \mathcal{U}} \qquad \frac{\bigwedge_{\overline{u}} \mathcal{U} \quad \mathcal{U}(a)}{\bigwedge_{\overline{u} \bullet a} \mathcal{U}}$$

Notice that $\bigwedge_{\overline{u} * \overline{v}} \mathcal{U}$ is equivalent to $\bigwedge_{\overline{u}} \mathcal{U} \ \wedge \ \bigwedge_{\overline{v}} \mathcal{U}$. Associated to the definition of $\bigwedge_{\overline{u}} \mathcal{U}$ we have the following principle of induction, for every predicate $\mathcal{X}$ over $\mathcal{A}^*$.

$$\frac{\bigwedge_{\overline{u}} \mathcal{U} \quad \mathcal{X}(<>) \quad \forall \overline{v} \ \ [\mathcal{X}(\overline{v}) \wedge \mathcal{U}(a) \Rightarrow \mathcal{X}(\overline{v} \bullet a)]}{\mathcal{X}(\overline{u})}$$

When using this principle we refer to it as *induction on "the" proof that* $\bigwedge_{\overline{u}}\mathcal{U}$, where "the" proof is the proof of $\bigwedge_{\overline{u}}\mathcal{U}$ available at that moment.

In type theory, we formulate the definition of bar for predicates over lists of elements of an arbitrary set, rather than only for predicates over lists of natural numbers. The following definition is a variation on an idea taken from [Mar68].

Definition 6 (inductive bars). *Given a set* $\mathcal{A}$ *and a predicate* $\mathcal{U}$ *over* $\mathcal{A}^*$, $\mathcal{U}$ *is an inductive bar if* $\mathcal{U} \mid <>$ *(to be read* $\mathcal{U}$ bars the empty sequence*), where this is inductively defined with the following introduction rules.*

$$\frac{\mathcal{U}(\overline{u})}{\mathcal{U} \mid \overline{u}} \qquad \frac{\mathcal{U} \mid \overline{u}}{\mathcal{U} \mid \overline{u} \bullet a} \qquad \frac{\forall a \in \mathcal{A}\ \ [\mathcal{U} \mid \overline{u} \bullet a]}{\mathcal{U} \mid \overline{u}}$$

Notice that if $\mathcal{U}(\overline{u}) \Rightarrow \mathcal{V}(\overline{u})$ for every $\overline{u} \in \mathcal{A}^*$, then also $\mathcal{U} \mid \overline{u} \Rightarrow \mathcal{V} \mid \overline{u}$ for every $\overline{u} \in \mathcal{A}^*$. Associated to the definition of $\mathcal{U} \mid \overline{u}$ we have the following principle of induction, for every predicate $\mathcal{Y}$ over $\mathcal{A}^*$.

$$\frac{\begin{array}{l}\mathcal{U} \mid \overline{u} \\ \forall \overline{v} \in \mathcal{A}^*\ \ [\mathcal{U}(\overline{v}) \Rightarrow \mathcal{Y}(\overline{v})] \\ \forall \overline{v} \in \mathcal{A}^*\ \ \forall a \in \mathcal{A}\ \ [\mathcal{Y}(\overline{v}) \Rightarrow \mathcal{Y}(\overline{v} \bullet a)] \\ \forall \overline{v} \in \mathcal{A}^*\ \ \{[\forall a \in \mathcal{A}\ \ \mathcal{Y}(\overline{v} \bullet a)] \Rightarrow \mathcal{Y}(\overline{v})\}\end{array}}{\mathcal{Y}(\overline{u})}$$

When using this principle we refer to it as *induction on "the" proof that* $\mathcal{U} \mid \overline{u}$, where "the" proof is the proof of it available at that moment.

With this principle of induction it is possible to prove in type theory that the rule BI —with inductive bars instead of bars, and arbitrary sets instead of natural numbers— is derivable. For that proof it is convenient to define the following reverse-append function, which is denoted $\leftarrowtail$.

$$\begin{array}{lcl}\overline{u} \leftarrowtail <> & = & \overline{u} \\ \overline{u} \leftarrowtail (\overline{v} \bullet a) & = & (\overline{u} \bullet a) \leftarrowtail \overline{v}\end{array}$$

An interpretation in type theory of the rule BI is:

$$\frac{\begin{array}{ll}\forall \overline{u} \in \mathcal{A}^* \;\; [\mathcal{X}(\overline{u}) \Rightarrow \mathcal{Y}(\overline{u})] & \mathcal{X} \text{ is included in } \mathcal{Y} \\ \forall \overline{u} \in \mathcal{A}^* \;\; \forall a \in \mathcal{A} \;\; [\mathcal{X}(\overline{u}) \Rightarrow \mathcal{X}(\overline{u} \bullet a)] & \mathcal{X} \text{ is monotone} \\ \forall \overline{u} \in \mathcal{A}^* \;\; \{[\forall a \in \mathcal{A} \;\; \mathcal{Y}(\overline{u} \bullet a)] \Rightarrow \mathcal{Y}(\overline{u})\} & \mathcal{Y} \text{ is hereditary} \\ \mathcal{X} \mid \overline{u} & \mathcal{X} \text{ bars } \overline{u}\end{array}}{\mathcal{Y}(\overline{u})}\ \mathrm{BI_{TT}}$$

This rule can be derived by showing $\forall \overline{v} \in \mathcal{A}^* \;\; \mathcal{Y}(\overline{u} \hookleftarrow \overline{v})$ by induction on the proof that $\mathcal{X} \mid \overline{u}$.

In a type-theoretic context, by *bar induction* we refer to the rule $\mathrm{BI_{TT}}$. When applying bar induction we will refer by *monotonicity condition* (of $\mathcal{X}$), *hereditary condition* (of $\mathcal{Y}$), and *inclusion condition* (that is, $\mathcal{X} \subseteq \mathcal{Y}$) to the instances corresponding to the premises of the rule.

Proposition 2. *Given a set $\mathcal{A}$, a monotone predicate $\mathcal{U}$ over $\mathcal{A}^*$ and a list $\overline{u}$ of elements of $\mathcal{A}$, then*

$$\mathcal{U} \mid \overline{u} \iff \mathcal{V}_{\overline{u}} \mid <>,$$

where $\mathcal{V}_{\overline{u}} = \lambda \overline{v}\, \mathcal{U}(\overline{u} * \overline{v})$.

The $\Leftarrow$ part is easy, and is left to the reader. Hint: use bar induction with $\mathcal{X} = \mathcal{V}_{\overline{u}}$ and $\mathcal{Y} = \lambda \overline{v}\, [\mathcal{U} \mid \overline{u} * \overline{v}]$; or, for another proof which does not use monotonicity of $\mathcal{U}$, by induction on the proof that $\mathcal{V}_{\overline{u}} \mid <>$.

We sketch a proof of the $\Rightarrow$ part, which is by bar induction with $\mathcal{X} = \mathcal{U}$ and $\mathcal{Y} = \lambda \overline{u}\, [\mathcal{V}_{\overline{u}} \mid <>]$. The monotonicity condition is hypothesis of the proposition and the inclusion condition is trivial. It remains to prove the hereditary condition. Assume that for all $a \in \mathcal{A}$, $\mathcal{V}_{\overline{u} \bullet a} \mid <>$. We have to show $\mathcal{V}_{\overline{u}} \mid <>$. In order to do so, we prove that for all $a \in \mathcal{A}$, $\mathcal{V}_{\overline{u}} \mid <a>$. Now, this follows from $\mathcal{V}_{\overline{u} \bullet a} \mid <>$ by bar induction with $\mathcal{X} = \mathcal{V}_{\overline{u} \bullet a}$ and $\mathcal{Y} = \lambda \overline{v}\, [\mathcal{V}_{\overline{u}} \mid <a> * \overline{v}]$.

Proposition 3. *Given a set $\mathcal{A}$, two monotone predicates $\mathcal{U}, \mathcal{V}$ over $\mathcal{A}^*$ and a list $\overline{u}$ of elements of $\mathcal{A}$, then*

$$\mathcal{U} \mid \overline{u} \;\wedge\; \mathcal{V} \mid \overline{u} \;\Longrightarrow\; \mathcal{W} \mid \overline{u},$$

where $\mathcal{W} = \lambda \overline{u}\, [\mathcal{U}(\overline{u}) \wedge \mathcal{V}(\overline{u})]$.

We sketch a proof of Proposition 3 by bar induction with $\mathcal{X} = \mathcal{U}$ and $\mathcal{Y} = \lambda\overline{u}\ [\mathcal{V} \mid \overline{u} \Rightarrow \mathcal{W} \mid \overline{u}]$. The monotonicity condition is hypothesis of the proposition. The hereditary condition follows from the facts that $\lambda\overline{u}\ [\mathcal{W} \mid \overline{u}]$ is hereditary and $\lambda\overline{u}\ [\mathcal{V} \mid \overline{u}]$ is monotone. Finally, the inclusion condition can be proved by bar induction with $\mathcal{X} = \mathcal{V}$ and $\mathcal{Y} = \lambda\overline{u}\ [\mathcal{U}(\overline{u}) \Rightarrow \mathcal{W} \mid \overline{u}]$, repeating the previous reasoning, except that the new inclusion condition is trivial.

4 Fan theorem in type theory

The result we present here is a type-theoretic version of the fan theorem as formulated in Theorem 5, except that it will be expressed for an arbitrary set $\mathcal{A}$ rather than only for natural numbers. Finite subsets $\mathcal{I}_i$ of $\mathcal{A}$ will be represented by lists $\overline{u}_i$ of elements of $\mathcal{A}$. Finite sequences $\overline{\mathcal{I}}$ of such subsets, by lists $\overline{\overline{u}}$ of lists. The function $\bigotimes$ occurring in the statement of Theorem 5 will be represented by a function which when applied to a list of lists $<\overline{u}_1, \ldots, \overline{u}_{n-1}>$ computes another list representing the Cartesian product $\mathcal{I}_1 \times \ldots \times \mathcal{I}_{n-1}$.

To define $\bigotimes$ we first define the binary Cartesian product $\times^f$ parametrized with a function f. Then, the finite Cartesian product $\bigotimes_b^f$ also parametrized. Finally we instantiate it to obtain $\bigotimes$.

Given a function $f : \mathcal{A} \to \mathcal{B}$, we denote by $\overline{f} : \mathcal{A}^* \to \mathcal{B}^*$ the function which maps f on every element of its argument.

$$\begin{aligned} \overline{f}(<>) &= <> \\ \overline{f}(\overline{u} \bullet a) &= \overline{f}(\overline{u}) \bullet f(a) \end{aligned}$$

Example 1. $\overline{f}(<a_0, \ldots, a_{n-1}>) = <f(a_0), \ldots, f(a_{n-1})>$.

Now, the function $\times^f$, which given a function $f : \mathcal{A} \to \mathcal{B} \to \mathcal{C}$, and two lists $\overline{u} \in \mathcal{A}^*$ and $\overline{v} \in \mathcal{B}^*$ returns a variation of the Cartesian product of $\overline{u}$ and $\overline{v}$. Instead of returning a list in $(\mathcal{A} \times \mathcal{B})^*$, it returns a list in $\mathcal{C}^*$ by applying the function f to the components of each possible pair.

$$\begin{aligned} <> \ \times^f \ \overline{v} \ &= \ <> \\ (\overline{u} \bullet a) \ \times^f \ \overline{v} \ &= \ \overline{u} \times^f \overline{v} \ * \ \overline{f(a)}(\overline{v}) \end{aligned}$$

Example 2. $\overline{u} \ \times^f <> \ = \ <>$, for every $\overline{u}$.

Example 3.

$$<a_0, a_1> \ \times^f \ <b_0, b_1> = <f(a_0, b_0), f(a_0, b_1), f(a_1, b_0), f(a_1, b_1)>.$$

The function $\bigotimes_b^f$, given a function $f : \mathcal{B} \to \mathcal{A} \to \mathcal{B}$, a base value $b \in \mathcal{B}$, and $\overline{\overline{u}} \in \mathcal{A}^{**}$, returns a list in $\mathcal{B}^*$, each of whose values is the result of iterating the function f along one tuple, assigning b to the empty tuple. Each tuple consists of one element from the first list of $\overline{\overline{u}}$, one from the second, etc. in the style of the Cartesian product.

$$\bigotimes_b^f(<>) = <b>$$
$$\bigotimes_b^f(\overline{\overline{u}} \bullet \overline{u}) = \bigotimes_b^f(\overline{\overline{u}}) \times^f \overline{u}$$

Example 4.

$$\bigotimes_b^f(\ll a_0, a_1>, <b_0, b_1\gg)$$
$$= <f(f(b, a_0), b_0), f(f(b, a_0), b_1), f(f(b, a_1), b_0), f(f(b, a_1), b_1)>.$$

Finally, the Cartesian product is obtained by giving $\bullet$ as the function to iterate, and $<>$ as the base value.

$$\bigotimes(\overline{\overline{u}}) = \bigotimes_{<>}^{\bullet}(\overline{\overline{u}})$$

Example 5. $\bigotimes(<>) = \ll>>$.

Example 6. $\bigotimes(\overline{\overline{u}} \bullet <>) = <>$, for every $\overline{\overline{u}}$.

Example 7.

$$\bigotimes(\ll a_0, a_1>, <b_0, b_1\gg) = \ll a_0, b_0>, <a_0, b_1>, <a_1, b_0>, <a_1, b_1\gg.$$

The set $\{\overline{\mathcal{I}} \mid \bigotimes \overline{\mathcal{I}} \subseteq \mathcal{U}\}$ in Theorem 5 can be interpreted as a predicate $\mathcal{P}$ on lists $\overline{\overline{u}}$ of lists which is true when $\bigotimes(\overline{\overline{u}})$ is "included" in $\mathcal{U}$. As $\bigotimes(\overline{\overline{u}})$ is actually not a set but a list, by it being "included" in $\mathcal{U}$ we mean that every element in the list $\bigotimes(\overline{\overline{u}})$ satisfies $\mathcal{U}$, that is, $\bigwedge_{\bigotimes(\overline{\overline{u}})} \mathcal{U}$. Thus, the predicate $\mathcal{P}$ is in fact interpreted by the function $\lambda\overline{\overline{u}}\left[\bigwedge_{\bigotimes(\overline{\overline{u}})} \mathcal{U}\right]$. Hence, in type theory Theorem 5 becomes:

Theorem 6 (fan theorem in type theory). *Given a set $\mathcal{A}$ and a monotone predicate $\mathcal{U}$ over $\mathcal{A}^*$, then if $\mathcal{U}$ is an inductive bar, so is the predicate*

$$\lambda\overline{\overline{u}}\left[\bigwedge_{\bigotimes(\overline{\overline{u}})} \mathcal{U}\right].$$

Lemma 1. *The following properties hold for every* $\overline{u}$, $\overline{v}$, $\overline{w}$, *and* $\overline{\overline{u}}$

1. $\overline{u} * \overline{v} \ \times^f \ \overline{w} = (\overline{u} \times^f \overline{w}) * (\overline{v} \times^f \overline{w})$
2. $<a> \times^f \overline{u} * \overline{v} = (<a> \times^f \overline{u}) * (<a> \times^f \overline{v})$
3. $\bigotimes(<\overline{w} \bullet a> * \overline{\overline{u}}) = \bigotimes(<\overline{w}> * \overline{\overline{u}}) * \bigotimes(\ll a \gg * \overline{\overline{u}})$
4. $\bigwedge_{\bigotimes(\overline{\overline{u}})} [\lambda \overline{u} \, \mathcal{U}(<a> * \overline{u})] \implies \bigwedge_{\bigotimes(\ll a \gg * \overline{\overline{u}})} \mathcal{U}$

Item 1 can be proved by induction on $\overline{v}$. Item 2 follows from the fact that $\overline{g}(\overline{u} * \overline{v}) = \overline{g}(\overline{u}) * \overline{g}(\overline{v})$ (letting g be $f(a)$), which can also be proved by induction on $\overline{v}$. Item 3 can be proved by induction on $\overline{\overline{u}}$, using Example 6 in the base case and item 1 in the inductive case.

Though technically laborious, item 4 is intuitively clear since all the tuples in $\bigotimes(\ll a \gg * \overline{\overline{u}})$ are of the form $<a> * \overline{u}$ with $\overline{u}$ a tuple in $\bigotimes(\overline{\overline{u}})$. We omit that proof here.

For the proof of Theorem 6, we define, for $\overline{u} \in \mathcal{A}^*$,

$$\mathcal{V}_{\overline{u}} = \lambda \overline{\overline{u}} \left[\bigwedge_{\bigotimes(\overline{\overline{u}})} (\lambda \overline{v} \, \mathcal{U}(\overline{u} * \overline{v})) \right].$$

We give a proof by bar induction with $\mathcal{X} = \mathcal{U}$ and $\mathcal{Y} = \lambda \overline{u} \, \{\mathcal{V}_{\overline{u}} \mid <>\}$.

The inclusion condition is $\mathcal{U}(\overline{u}) \Rightarrow \mathcal{V}_{\overline{u}} \mid <>$, which is easy, since when $\mathcal{U}(\overline{u})$ holds, even $\mathcal{V}_{\overline{u}}(<>)$ holds because $\bigotimes(<>) = <<>>$ by Lemma 1. The monotonicity condition is hypothesis of the theorem. The hereditary condition is $(\forall a \in \mathcal{A} \ \ [\mathcal{V}_{\overline{u} \bullet a} \mid <>]) \Rightarrow \mathcal{V}_{\overline{u}} \mid <>$. We assume

$$\forall a \in \mathcal{A} \ \ [\mathcal{V}_{\overline{u} \bullet a} \mid <>] \tag{1}$$

and given an arbitrary $\overline{v}$ we prove $\mathcal{V}_{\overline{u}} \mid \ <\overline{v}>$ by induction on $\overline{v}$.

If $\overline{v} = <>$, then $\mathcal{V}_{\overline{u}} \mid \ <<>>$ is direct since $\mathcal{V}_{\overline{u}}(<<>>)$ holds because of the facts that $\bigotimes(<<>>) = <>$ holds by Lemma 1 and that $\bigwedge_{<>}$ is trivially true regardless of the predicate.

If $\overline{v} = \overline{w} \bullet a$ for some $\overline{w} \in \mathcal{A}^*$ (such that $\mathcal{V}_{\overline{u}} \mid \ <\overline{w}>$) and $a \in \mathcal{A}$, then we know by (1) that

$$\mathcal{V}_{\overline{u} \bullet a} \mid <> \quad \text{and} \quad \mathcal{V}_{\overline{u}} \mid \ <\overline{w}>$$

and still have to prove

$$\mathcal{V}_{\overline{u}} \mid \ <\overline{w} \bullet a> .$$

By Proposition 2 it can be written like this: we know

$$\mathcal{V}_{\overline{u}\bullet a} \mid <> \quad \text{and} \quad [\lambda\overline{\overline{u}}\ \ \mathcal{V}_{\overline{u}}(<\overline{w}> *\overline{\overline{u}})] \mid <>,$$

(hence, by Proposition 3 we know also that

$$[\lambda\overline{\overline{u}}\quad [\mathcal{V}_{\overline{u}\bullet a}(\overline{\overline{u}}) \wedge \mathcal{V}_{\overline{u}}(<\overline{w}> *\overline{\overline{u}})]] \mid <> \tag{2}$$

holds) and have to prove

$$[\lambda\overline{\overline{u}}\ \ \mathcal{V}_{\overline{u}}(<\overline{w} \bullet a> *\overline{\overline{u}})] \mid <> . \tag{3}$$

To prove that (2) $\Rightarrow$ (3), it is enough to prove that for every $\overline{\overline{u}} \in \mathcal{A}^{**}$,

$$\mathcal{V}_{\overline{u}\bullet a}(\overline{\overline{u}}) \ \wedge\ \mathcal{V}_{\overline{u}}(<\overline{w}> *\overline{\overline{u}}) \quad \Longrightarrow \quad \mathcal{V}_{\overline{u}}(<\overline{w} \bullet a> *\overline{\overline{u}})$$

holds. By the definition of $\mathcal{V}_{\overline{u}}$ and item 3 of Lemma 1, the right-hand side is equivalent to

$$\mathcal{V}_{\overline{u}}(<\overline{w}> *\overline{\overline{u}}) \quad \wedge \quad \mathcal{V}_{\overline{u}}(\ll a \gg *\overline{\overline{u}})$$

which follows from the left-hand side because, by item 4 of Lemma 1, $\mathcal{V}_{\overline{u}\bullet a}(\overline{\overline{u}})$ implies $\mathcal{V}_{\overline{u}}(\ll a \gg *\overline{\overline{u}})$.

Acknowledgements

I am grateful to Marc Bezem, Thierry Coquand, Monika Seisenberger, Jan Smith and Wim Veldman for fertile discussions about the fan theorem.

References

[CF58] H. Curry and R. Feys. *Combinatory Logic*, volume I. North-Holland, 1958.

[Dum77] M. Dummett. *Elements of Intuitionism.* Clarendon Press, Oxford, 1977.

[Fri97] D. Fridlender. Higman's Lemma in Type Theory. In *Types for proofs and programs*, Lecture Notes in Computer Science 1512, 1997.

[How80] W. Howard. The Formulae-as-Types Notion of Construction. In J. Seldin and J. Hindley, editors, *To H.B. Curry: Essays on Combinatory Logic, Lambda Calculus and Formalism*, pages 479–490. Academic Press, London, 1980.

[Mag94] L. Magnusson. *The Implementation of ALF - a Proof Editor Based on Martin-Löf's Monomorphic Type Theory with Explicit Substitution.* PhD thesis, Department of Computing Science, Chalmers University of Technology and University of Göteborg, 1994.

[Mar68] P. Martin-Löf. *Notes on Constructive Mathematics.* Almqvist & Wiksell, 1968.

[Mar75] P. Martin-Löf. An Intuitionistic Theory of Types: Predicative Part. In H. E. Rose and J. C. Shepherdson, editors, *Logic Colloquium 1973*, pages 73–118, Amsterdam, 1975. North-Holland Publishing Company.

[Mar84] P. Martin-Löf. *Intuitionistic Type Theory.* Bibliopolis, Napoli, 1984.

[NPS90] B. Nordström, K. Petersson, and J. Smith. *Programming in Martin-Löf's Type Theory. An Introduction.* Oxford University Press, 1990.

[Tas97] A. Tasistro. *Substitution, Record Types and Subtyping in Type Theory, with Applications to the Theory of Programming.* PhD thesis, Department of Computing Science at Chalmers University of Technology and University of Göteborg, 1997.

[TvD88] A. Troelstra and D. van Dalen. *Constructivism in Mathematics, An Introduction, Volume I.* North-Holland, 1988.

[Vel94] W. Veldman. Intuitionistic Proof of the General non-Decidable case of Higman's Lemma. Personal communication, 1994.

Recent BRICS Report Series Publications

RS-98-39 **Daniel Fridlender.** ***An Interpretation of the Fan Theorem in Type Theory*****. December 1998. 15 pp. To appear in** ***International Workshop on Types for Proofs and Programs 1998*****, TYPES '98 Selected Papers, LNCS, 1999.**

RS-98-38 **Daniel Fridlender and Mia Indrika.** ***An n-ary `zipWith` in Haskell*****. December 1998. 12 pp.**

RS-98-37 **Ivan B. Damgård, Joe Kilian, and Louis Salvail.** ***On the (Im)possibility of Basing Oblivious Transfer and Bit Commitment on Weakened Security Assumptions*****. December 1998. 22 pp. To appear in** ***Advances in Cryptology: International Conference on the Theory and Application of Cryptographic Techniques*****, EUROCRYPT '99 Proceedings, LNCS, 1999.**

RS-98-36 **Ronald Cramer, Ivan B. Damgård, Stefan Dziembowski, Martin Hirt, and Tal Rabin.** ***Efficient Multiparty Computations with Dishonest Minority*****. December 1998. 19 pp. To appear in** ***Advances in Cryptology: International Conference on the Theory and Application of Cryptographic Techniques*****, EUROCRYPT '99 Proceedings, LNCS, 1999.**

RS-98-35 **Olivier Danvy and Zhe Yang.** ***An Operational Investigation of the CPS Hierarchy*****. December 1998.**

RS-98-34 **Peter G. Binderup, Gudmund Skovbjerg Frandsen, Peter Bro Miltersen, and Sven Skyum.** ***The Complexity of Identifying Large Equivalence Classes*****. December 1998. 15 pp.**

RS-98-33 **Hans Hüttel, Josva Kleist, Uwe Nestmann, and Massimo Merro.** ***Migration = Cloning ; Aliasing (Preliminary Version)*****. December 1998. 40 pp. To appear in** ***6th International Workshop on the Foundations of Object-Oriented*****, FOOL6 Informal Proceedings, 1998.**

RS-98-32 **Jan Camenisch and Ivan B. Damgård.** ***Verifiable Encryption and Applications to Group Signatures and Signature Sharing*****. December 1998. 18 pp.**

RS-98-31 **Glynn Winskel.** ***A Linear Metalanguage for Concurrency*****. November 1998. 21 pp.**

RS-98-30 **Carsten Butz.** ***Finitely Presented Heyting Algebras*****. November 1998. 30 pp.**