A direct proof of the equivalence between Brouwer’s fan theorem and König’s lemma with a uniqueness hypothesis

Helmut Schwichtenberg

Mathematisches Institut, Universität München

Frauenchiemsee, 19. Juni 2006
Goal

(1) A direct proof of the equivalence of
   - the weak (that is, binary) form of König’s lemma with a uniqueness condition (WKL!), and
   - Brouwer’s fan theorem (Fan).

(2) Extract computational content from formalizations of these proofs.
[Bridges and Richman 1987], chapter 6:

\[ \text{Fan} \iff \text{each positive valued uniformly continuous function defined on } [0, 1] \text{ has a positive infimum.} \]

Berger and Ishihara [MLQ 2005] have shown a number of equivalents to Fan, including WKL!

\[ \text{WKL!} \implies \text{Fan is proved explicitly.} \]

\[ \text{Fan} \implies \text{WKL!} \text{ is proved less directly; the emphasis is to provide equivalents to Fan, and to do the proofs economically by giving a circle of implications.} \]
Equivalents to Fan

▶ A unique version of Cantor’s intersection theorem, CIT!: Each decreasing sequence of inhabited, closed, and located subsets of a compact metric space with at most one common point has an inhabited intersection.

▶ A unique version of the minimum principle, MIN!: Each uniformly continuous function from a compact metric space to $\mathbb{R}$ with at most one minimum point has a minimum point.

▶ A unique version of the weak König’s lemma, WKL!: Every infinite tree with at most one path has a path.

▶ A unique fixed point theorem, FIX!: Each uniformly continuous function from a compact metric space $X$ into itself with at most one fixed point and approximate fixed point has a fixed point.

▶ A positivity property, POS: Each positive valued uniformly continuous function defined on a compact metric space has a positive infimum.
Equivalents to Fan (continued)

Proofs in [Berger and Ishihara 2005]:

- **Fan ⇒ POS**: Uses Theorem 1.4 in chapter 5 of [Bridges and Richman 1987]
- **POS ⇒ CIT!**: Uses Theorem 4.9 in chapter 4 of [Bishop and Bridges, 1987]
- **CIT! ⇒ MIN!**: Again uses Theorem 4.9 in chapter 4 of [Bishop and Bridges, 1987]
- **MIN! ⇒ FIX! and FIX! ⇒ WKL!** are easy.
- **WKL! ⇒ Fan** is proved by a direct construction.
Basic definitions

Let $\mathbf{N}$ be the type of natural numbers, $\mathbf{B}$ the type of booleans $\mathsf{tt}$, $\mathsf{ff}$ and $\mathbf{L}(\mathbf{B})$ the type of lists of booleans. It is convenient to write lists in reverse order, that is, add elements at the end. We fix the types of some variables and state their intended meaning:

- $a$, $b$, $c$ of type $\mathbf{L}(\mathbf{B})$ for nodes,
- $r$, $s$, $t$ of type $\mathbf{L}(\mathbf{B}) \to \mathbf{B}$ for decidable sets of nodes,
- $as$, $bs$, $cs$ of type $\mathbf{N} \to \mathbf{L}(\mathbf{B})$ for sequences of nodes,
- $f$, $g$, $h$ of type $\mathbf{N} \to \mathbf{B}$ for paths,
- $n$, $m$, $k$, $i$, $j$ of type $\mathbf{N}$ for natural numbers,
- $p$, $q$ of type $\mathbf{B}$ for booleans,
- $ns$, $ms$, $ks$ of type $\mathbf{N} \to \mathbf{N}$ for sequences of natural numbers.
Basic definitions (continued)

Let $|a|$ be the length of $a$. Let $\bar{a}(n)$ denote the initial segment of $a$ of length $n$, if $n \leq |a|$, and $a$ otherwise. Similarly let $\bar{f}(n)$ denote the initial segment of $f$ of length $n$, that is, the list $:f(0) :: f(1) \cdots :: f(n-1)$. Let $(a)_n$ denote the $n$-th element of $a$, if $n < |a|$, and \texttt{tt} otherwise. Clearly

$$|a| = n + 1 \rightarrow \bar{a}(n) :: (a)_n = a,$$

$$n \leq m \leq |a| \rightarrow \bar{a}(m)(n) = \bar{a}(n).$$

We will also need to deal with lists of pairs of booleans, using variables

- $bc$ of type $\mathbf{L}(\mathbf{B} \times \mathbf{B})$ for pair nodes,
- $ss$ of type $\mathbf{L}(\mathbf{B} \times \mathbf{B}) \rightarrow \mathbf{B}$ for decidable sets of pair nodes,
- $gh$ of type $\mathbf{N} \rightarrow \mathbf{B} \times \mathbf{B}$ for paths, w.r.t. pair nodes,
- $pq$ of type $\mathbf{B} \times \mathbf{B}$ for pairs of booleans.
Basic definitions (continued)

To switch from \( L(B \times B) \) to \( L(B) \) and back we use Zip and Unzip:

\[
\text{Zip}(bc :: pq) := \text{Zip}(bc) :: \text{Lft}(pq) :: \text{Rht}(pq), \quad \text{Zip}(\text{Nil}) := \text{Nil},
\]

\[
\text{Unzip}(n + 1, a :: p :: q) := \text{Unzip}(n, a) :: (p, q),
\]

\[
\text{Unzip}(n + 1, :p) := \text{Unzip}(n + 1, \text{Nil}) := \text{Unzip}(0, a) := \text{Nil}.
\]

When in a context containing \( gh \) we use \( g \) or \( h \), we mean \( \text{Lft} \circ gh \) or \( \text{Rht} \circ gh \). Using this notation, for \( N \to B \times B \) and \( N \to B \) we similarly define \( Fzip \) and \( \text{Funzip} \), by

\[
\text{Fzip}(gh, 2i) := g(i), \quad \text{Fzip}(gh, 2i + 1) := h(i),
\]

\[
\text{Funzip}(f, i) := (f(2i), f(2i + 1)).
\]

Clearly \( \text{Fzip}(\text{Funzip}(f)) = f \) and \( \text{Funzip}(\text{Fzip}(gh)) = gh \), and

\[
\text{Unzip}(|bc|, \text{Zip}(bc)) = bc,
\]

\[
|\text{Zip}(bc)| = 2|bc|,
\]

\[
\text{Zip}((\text{Funzip}(f)(m))) = \bar{f}(2m).
\]
Call \( f \) a \textbf{path in} \( t \) if all its initial segments \( \overline{f}(n) \) are in \( t \).

Call \( t \) \textbf{infinite} if for every \( n \) there is a node of length \( n \) in \( t \).

Call \( t \) a \textbf{tree} if it is downwards closed: \( \forall a \forall n \leq |a| \cdot a \in t \rightarrow \overline{a}(n) \in t \).

Call \( s \) a \textbf{bar} if each path hits \( s \), that is, \( \forall_f \exists_m \overline{f}(m) \in s \).

Call \( s \) a \textbf{uniform bar} if, for some \( k \), each path hits \( s \) before \( k \), that is, \( \exists_k \forall_f \exists_m \leq_k \overline{f}(m) \in s \). We say that \( t \) has \textbf{at most one path} if:

\[
\text{EffUniq}_t: \text{for any } g, h \text{ and } n \text{ with } \overline{g}(n) \neq \overline{h}(n), \text{ there is an } m \text{ such that it is impossible that both } \overline{g}(m) \text{ and } \overline{h}(m) \text{ are in } t.
\]

We can now formulate the two statements:

\textbf{Fan}: Every bar is uniform.

\textbf{WKL!}: Every infinite tree with at most one path has a path.
Let $s$ be given and assume $\text{Bar}(s) \colon \forall f \exists m \bar{f}(m) \in s$. We need to construct a uniform bound, that is, some $k$ such that each path hits $s$ before $k$, that is, $\forall f \exists m \leq k \bar{f}(m) \in s$.

Let $r := \{ a \mid \exists n \leq |a| \bar{a}(n) \in s \}$ be the upwards closure of $s$.

Call $n$ big if every node of length $n$ is in $r$. It suffices to construct a big $k$.

We extend the complement of $r$ to an infinite tree $t$ satisfying $\text{EffUniq}_t$, so that WKL! can be applied. Idea: if the complement of $r$ is finite, extend the leftmost of its longest nodes by $t$'s.
More precisely, we define the extension $t$ as follows. A node $b$ belongs to $t$ if it is not in $r$. If it is, check whether its length $|b|$ is big. If not, $b$ is not in $t$. If it is big, let $k$ be such that $k + 1$ is big but $k$ is not.

\[
\begin{align*}
k+1: & \quad + + + + \ldots + + \\
k: & \quad + \ldots + a
\end{align*}
\]

Let $a$ be the unique node such that on its length $k$ to the left of $a$ there are only nodes in $r$, but $a$ itself is not in $r$. Then $b$ is in $t$ iff it is the extension of $a$ by \tt's to the length of $b$. So

\[
t := \{ \ b \mid b \in r \rightarrow \text{Big}(|b|) \land b = a :: \tt :: \cdots :: \tt \} \]
WKL! implies Fan (continued)

We show that $t$ is infinite. So let $n$ be given. If $n$ is big, let $a$ be as above. Then $a :: tt \cdot \cdot \cdot :: tt$ of length $n$ is in $t$. If $n$ is not big, an arbitrary node $b$ of length $n$ that is not in $r$ is in $t$.

We show that $t$ is a tree. So let $b \in t$, $n \leq |b|$; we must show $\bar{b}(n) \in t$. So assume $\bar{b}(n) \in r$. Then also $b \in r$, because $r$ is upwards closed. Hence $|b|$ is big and $b = a :: tt \cdot \cdot \cdot :: tt$. By definition of $t$, any initial segment of $b$ is in $t$.

We show that $t$ satisfies $\text{EffUniq}_t$. Consider $g$, $h$, $n$ such that $\bar{g}(n) \neq \bar{h}(n)$. Since every path hits $s$, there is an $m \geq n$ such that $\bar{g}(m)$, $\bar{h}(m)$ both are in its upwards closure $r$. Assume for contradiction that both are in $t$. Then by construction of $t$ both are of the form $a :: tt \cdot \cdot \cdot :: tt$ and of the same length, hence equal, and therefore also $\bar{g}(n) = \bar{h}(n)$. This is the desired contradiction.

Now WKL! gives a path $f$ in $t$. It must hit the bar $s$, hence $r$, and at this length we have the desired big $k$. 
Fan implies WKL!

Given an infinite tree $t$ satisfying $\text{EffUniq}_t$, we construct a path in $t$.

We derive from Fan a related auxiliary proposition PFan, referring to pair nodes. Using PFan, from $\text{EffUniq}_t$ we can prove

$\text{FanBound}_t$: For every $n$ there is a $k \geq n$ such that for all $b, c$ of length $k$ and in $t$ we have $\vec{b}(n) = \vec{c}(n)$,

From $\text{FanBound}_t$ we then easily construct a path in $t$. 
Fan implies PFan

From Fan we want to prove

PFan: \( \forall n \forall ss \cdot (\forall bc \forall n \leq |bc| \cdot \overline{bc}(n) \in ss \rightarrow bc \in ss) \rightarrow \\
(\forall gh \cdot \tilde{g}(n) \neq \tilde{h}(n) \rightarrow \exists m \overline{gh}(m) \in ss) \rightarrow \\
\exists k \forall gh \cdot \tilde{g}(n) \neq \tilde{h}(n) \rightarrow \overline{gh}(k) \in ss. \)
Given $n$, $ss$. Assume $\text{Upclosed}_{ss}: \forall bc\forall n \leq |bc|. \overline{bc}(n) \in ss \rightarrow bc \in ss$ and $\text{Bar}_{ss}: \forall gh. \bar{g}(n) \neq \bar{h}(n) \rightarrow \exists m \, gh(m) \in ss$. To construct: $k$.

We use Fan for

$$s_n := \{ a | \forall i < n. (a)_{2i} \neq (a)_{2i+1} \rightarrow \text{Unzip}(\lceil |a|/2 \rceil, a) \in ss \}.$$ 

We need to show that every path $f$ hits $s_n$. Let $f$ be given. **Case** $f(2i) = f(2i + 1)$ for all $i < n$. Then

$$(\bar{f}(2n))_{2i} = f(2i) = f(2i + 1) = (\bar{f}(2n))_{2i+1}$$

for all $i < n$, hence $\bar{f}(2n) \in s_n$. 

Fan implies PFan (continued)
Fan implies PFan (continued)

**Case** $f(2i) \neq f(2i + 1)$ for some $i < n$. Then Funzip($f$) is some $gh$ with $\bar{g}(n) \neq \bar{h}(n)$, for

$$(\bar{g}(n))_i = g(i) = (\text{Lft} \circ \text{Funzip}(f))(i) = f(2i),$$

$$(\bar{h}(n))_i = h(i) = (\text{Rht} \circ \text{Funzip}(f))(i) = f(2i + 1).$$

By Bar$_{ss}$ we can find an $m$ such that $bc := \text{Funzip}(f)(m) \in ss$; because of Upclosed$_{ss}$ we may assume $n \leq m$. Now with

$$a := \text{Zip}(bc) = \text{Zip}(\text{Funzip}(f)(m)) = \bar{f}(2m)$$

we have $a \in s_n$, for

$$\text{Unzip}(\lfloor |a|/2 \rfloor, a) = \text{Unzip}(\lfloor |\text{Zip}(bc)|/2 \rfloor, \text{Zip}(bc)) =$$

$$\text{Unzip}(|bc|, \text{Zip}(bc)) = bc.$$
Now by Fan we have $k$ such that $\forall f \exists m \leq k \bar{f}(m) \in s_n$. Since $s_n$ clearly is upwards closed, we may assume that $k$ is even and $2n \leq k$. We show

$$\forall gh. \bar{g}(n) \neq \bar{h}(n) \rightarrow \overline{gh(\lfloor k/2 \rfloor)} \in ss.$$ 

So let $gh$ with $\bar{g}(n) \neq \bar{h}(n)$ be given. Let $f := Fzip(gh)$. By assumption $a := \bar{f}(k) \in s_n$. Now

$$a = :g(0) :: h(0) :: \cdots :: g(\lfloor k/2 \rfloor - 1) :: h(\lfloor k/2 \rfloor - 1).$$

Because of $\bar{g}(n) \neq \bar{h}(n)$ and $n \leq \lfloor k/2 \rfloor$ we have $\exists i < n(a)_{2i} \neq (a)_{2i+1}$. Hence

$$\overline{gh(\lfloor k/2 \rfloor)} = \text{Unzip}(\lfloor k/2 \rfloor, a) = \text{Unzip}(\lceil |a|/2 \rceil, a) \in ss.$$
A bound for the fan

We shall prove

\[ \text{FanBound}_t: \text{ For every } n \text{ there is a } k \geq n \text{ such that for all } b, c \text{ of length } k \text{ and in } t \text{ we have } \bar{b}(n) = \bar{c}(n). \]

The proof uses PFan – which we just proved from Fan – and also EffUniq\_t, to obtain one of its hypotheses. We fix \( n \) and apply PFan to

\[ ss_t := \{bc \mid b \in t \rightarrow c \in t \rightarrow F \}. \]

\( \forall bc \forall n \leq |bc|. \bar{bc}(n) \in ss_t \rightarrow bc \in ss_t \) holds because \( t \) is a tree.

\[ \forall gh. \bar{g}(n) \neq \bar{h}(n) \rightarrow \exists m \bar{gh}(m) \in ss_t \]

follows from EffUniq\_t: it provides an \( m \) such that it is impossible that both \( \bar{g}(m) \) and \( \bar{h}(m) \) are in \( t \). Hence \( \bar{gh}(m) \in ss_t \).
Now PFan yields a $k$ such that $\forall_{gh.} \bar{g}(n) \neq \bar{h}(n) \rightarrow \bar{gh}(k) \in ss_t$. We may assume $k \geq n$. To prove FanBound$_t$, let $b, c$ of length $k$ and in $t$ be given; we have to show $\bar{b}(n) = \bar{c}(n)$. Let $gh$ be the extension of $bc$ by (pairs of) $tt$’s. Assume for contradiction $\bar{b}(n) \neq \bar{c}(n)$, hence $\bar{g}(n) \neq \bar{h}(n)$. Therefore $\bar{gh}(k) \in ss_t$, that is $\bar{b}(k)$ and $\bar{c}(k)$ cannot both be in $t$. This is the desired contradiction.
Construction of the path

Let $k_0$ be the function provided by FanBound$_t$, and let $k_s$ be the canonical monotone upper bound of $k_0$. Write $k_n$ for $k_s(n)$, $a_n$ for $as(n)$, $b_n$ for $bs(n)$ etc.

Because $t$ is infinite, we have $a_n$ of length $n$ in $t$. Define $b_n \in t$ by

$$b_n := a_{k_n}(n).$$

We claim that the $b_n$’s extend each other and hence make up a path, i.e., with $f(n) := (b_{n+1})_n$ we have $\bar{f}(n) = b_n \in t$. It suffices to prove

$$b_n = \overline{b_{n+1}}(n),$$

(1)

for then we obtain $\bar{f}(n) = b_n$ by induction, as follows.
Construction of the path (continued)

We show \( \bar{f}(n) = b_n \) by induction: The base case is obvious, and in the step case we have

\[
\bar{f}(n+1) = \bar{f}(n) :: f(n) = b_n :: (b_{n+1})_n = \overline{b_{n+1}}(n) :: (b_{n+1})_n = b_{n+1}.
\]

For (1) we apply \( \text{FanBound}_t \) to the two nodes \( a_{k_n} \) and \( \overline{a_{k_{n+1}}}(k_n) \), which are both of length \( k_n \) and in \( t \). Hence

\[
b_n = \overline{a_{k_n}}(n) = \overline{a_{k_{n+1}}(k_n)}(n) = a_{k_{n+1}}(n) = \overline{a_{k_{n+1}}(n+1)}(n) = \overline{b_{n+1}}(n).
\]
Realizability

One can extract from a (constructive) proof of a formula with computational content a term that “realizes” the formula. Why?

- It can be important to know for sure (and to be able to machine check) that in a proof nothing has been overlooked.
- The same applies to the algorithm implicit in the proof: even if the latter is correct, errors may occur in the implemention of the algorithm.
- Finally, even if the algorithm is correctly implemented, for sensitive applications customers may (and do) require a formal proof that the code implementing the algorithm is correct.

The realizability method takes care of all these points.
Given \( wklu0 \), \( r1 \) and a realizer \( inf2 \) for its infinity. Apply \( inf2 \) to the result of applying \( wklu0 \) to (1) the extension of the complement of the upwards closure \( Up \ r1 \) of \( r1 \), (2) a witness for its infinity and (3) a witness for the effective uniqueness of its paths. For (2), we are given \( n4 \). If \( n4 \) is big, take the left extension (by \( tt \)'s) of the uppermost leftmost node in the tree. If \( n4 \) is not big, take the first node of length \( n4 \) in the tree. For (3), we are given \( f4 \) and \( f5 \). Take the function mapping \( n \) to the max of itself and what the witness for infinity gives at \( f4 \) and \( f5 \).
Fan ⇒ PFan: Given fan0 realizing Fan, n1, ss2 and pbar3 mapping a pair path differing at n to a bar. Apply fan0 to (1) the set of all a4 such that for all n5<n1, if the elements of a4 at 2*n5 and 2*n5+1 are distinct, then the result of unzipping a4 at half of its length is in ss2, and (2) a witness that every path f4 hits this set, and add n1. For (2), distinguish cases whether for some n5<n1, f4 at 2*n5 equals f4 at 2*n5+1. If so, take 2*n1. If not, let n be the result of applying pbar3 to the unzipped form of f4, and take 2*n+2*n1.
We are given a functional $\text{pfan0}$ realizing $\text{PFan}$, a tree $r_1$, a realizer $\text{uniq2}$ of the effective uniqueness property and a number $n_3$. Take the max of $n_3$ and the result of applying $\text{pfan0}$ to this number, the set of all pair nodes whose left and right parts cannot both be in $r_1$, and the functional mapping a pair path to the result of applying $\text{uniq2}$ to it and this number.
We are given a tree $r_0$, a sequence $\text{ns1}$ of numbers provided by FanBound, a sequence $\text{as2}$ of nodes witnessing the infinity of $r_0$, and an argument $n_3$ for the path to be constructed. Take the $n_3$-th element of the sequence $\text{as2}$ applied to $\text{ns1}(n_3+1)$. 

\[ [r_0, \text{ns1}, \text{as2}, n_3] \text{as2}(\text{ns1}(\text{Succ } n_3))\_n_3 \]
Putting the parts together

\[\text{[fan0,r1,as2,uniq3]}\]
\[\text{cPath r1(Mon(cACNat(cFanBound(cFanImpPFan fan0)r1 uniq3)))}\]
\[\text{(cACLlistBoole as2)}\]

cACNat and cACLlistBoole can be ignored, for they are realisers of choice axioms and hence identities.

We can unfold the contents of the auxiliary propositions, by “animating” them. The result is
cACListBoole as2
(Mon (cACNat
  ([n6]n6 max
   (fan0
    ([a7]AllBNat n6
     ([n8]
      (a7__(n8+n8)=a7__Succ(n8+n8)impb False)impb
      r1(([pq9]left pq9)map Half Lh a7 unzip a7)impb
      r1(([pq9]right pq9)map Half Lh a7 unzip a7)impb
      False))
     ([f7][if (AllBNat n6([n8]f7(n8+n8)=f7(Succ(n8+n8))))
       (n6+n6)
       (uniq3([n8]f7(n8+n8))([n8]f7(Succ(n8+n8)))n6+n6+
        uniq3([n8]f7(n8+n8))([n8]f7(Succ(n8+n8)))n6+
        n6])+n6)))
   (Succ n4))___n4)
Conclusion

We have seen a direct proof of $\text{Fan} \Leftrightarrow \text{WKL}!$.

From the formalized proofs of $\text{WKL}! \Rightarrow \text{Fan}$ and $\text{Fan} \Rightarrow \text{WKL}!$ we have extracted terms expressing their computational content.

When supplied with concrete arguments, these terms can be evaluated (i.e., normalized) to yield the uniform bound or (respectively) the nodes of the path.