```
; A Simple Nqthm Proof About Coin Tossing

; Matt Kaufmann
; Internal Note 317
; Computational Logic, Inc.
; June 17, 1995

; This file contains what amounts to a proof of the following neat fact.
; Suppose 0 <= p <= q (where p and q are natural numbers, q non-zero) and you
; toss a fair coin, starting with p "credits", adding a credit each time you
; toss a head and subtracting a credit each time you toss a tail.  Then the
; probability that you first reach q credits before first reaching 0 credits is
; p/q.  A hand proof is included below.  The idea (explained a bit further in
; that hand proof) is to take the following three properties of a function f(p)
; which is defined to be q times the probability of a "win" for a given p,

#|
A. f(0) = 0
B. f(q) = q
C. f(p) = (1/2)f(p-1) + (1/2)f(p+1)  if p is neither 0 nor q.
```

```
|#

; and then prove f(p) = p from these properties.  This Nqthm proof starts by
; introducing these axioms in a convenient form with an Nqthm constrain event,
; concluding with the theorem guaranteeing f(p) = p.

; This file has been successfully processed by Nqthm-1992 in about 4 seconds on
; a Sparc 20.

; Bring in a library of facts about natural numbers.
```

EVENT: Start with the library `"naturals"` using the compiled version.

```
; Introduce the axioms about a function with the appropriate properties.
```

CONSERVATIVE AXIOM: fn-intro

$$\begin{aligned}
&(\text{fn}(0) = 0)\\
\wedge\quad &(\text{fn}(\text{Q}) = \text{Q})\\
\wedge\quad &(\text{Q} \in \mathbf{N})\\
\wedge\quad &(0 \neq \text{Q})\\
\wedge\quad &(\text{fn}(x) \in \mathbf{N})\\
\wedge\quad &(((0 < p) \wedge (p < \text{Q}))\\
&\quad \rightarrow \quad ((2 * \text{fn}(p)) = (\text{fn}(p - 1) + \text{fn}(1 + p))))
\end{aligned}$$

Simultaneously, we introduce the new function symbols *q* and *fn*.

```
; The following function expresses our plan for the proof by induction.
```

DEFINITION:

my-induction (p)

$= \quad$ **if** $(p \simeq 0) \vee (p = 1)$ **then t**

else my-induction $(p - 1) \wedge$ my-induction $((p - 1) - 1)$ **endif**

```
; Other inductive hypothesis

; The following lemma captures the heart of the argument.  It was actually
; generated by the theorem prover in the course of attempting to prove the
; lemma "main" below at one point during the proof effort, using Pc-Nqthm.
```

THEOREM: main-inductive-case

$$\begin{aligned}
&((p \neq 0)\\
&\ \wedge\quad (p \in \mathbf{N})\\
&\ \wedge\quad (p \neq 1)
\end{aligned}$$

$\wedge \quad (\text{fn}\,((p-1)-1) = (\text{fn}\,(1) * ((p-1)-1)))$
$\wedge \quad (\text{fn}\,(p-1) = (\text{fn}\,(1) * (p-1)))$
$\wedge \quad (\text{Q} \not< p))$
$\rightarrow \quad ((\text{fn}\,(p) = (\text{fn}\,(1) * p)) = \mathbf{t})$

```
; And finally, p*f(1)=f(p).
```

THEOREM: main
$((p \in \mathbf{N}) \wedge (0 \leq p) \wedge (p \leq \text{Q})) \rightarrow ((p * \text{fn}\,(1)) = \text{fn}\,(p))$

```
; And of course, f(1)=1.
```

THEOREM: helper
$\text{fn}\,(1) = 1$

THEOREM: final-theorem
$((p \in \mathbf{N}) \wedge (0 \leq p) \wedge (p \leq \text{Q})) \rightarrow (\text{fn}\,(p) = p)$

```
#| Hand proof:

Theorem:  Suppose 0 <= p <= q and you toss a fair coin, starting with p
"credits", adding a credit each time you toss a head and subtracting a credit
each time you toss a tail.  Then the probability that you first reach q credits
before first reaching 0 credits is p/q.

Proof.  Fix q for the remainder of the proof.  Now for any p with 0<=p<=q let
us write f(p) to denote q times the given probability for p and q.  So, our
goal is to prove that f(p)=p, since if q times the probability is p, then the
probability is p/q.  (This works better on paper.)

The following properties of f(p) are clear (but see below for an explanation of
C):

A. f(0) = 0
B. f(q) = q
C. f(p) = (1/2)f(p-1) + (1/2)f(p+1)  if p is neither 0 nor q.

To explain C just a bit:  The probability of getting to q credits first, from
p, is split into 2 cases:  you could flip tails (with probability 1/2) and then
have to get to q from p-1, or you could flip heads (also with probability 1/2)
and then have to get to q from p.  So the probability of "winning" from p is
1/2 times the probability of "winning" from p-1, plus 1/2 times the probability
of "winning" from p+1.  Then equation C is just the result of multiplying both
sides of the preceding sentence by q.
```

The theorem following easily from the following claim (see below):

Claim: For all p with 0<=p<=q,

f(p) = p*f(1)

For, if we believe this Claim, then we can substitute q for p to get

f(q) = q*f(1)

which implies, by Property B, that q=q*f(1) and hence (dividing both sides by q) f(1) = 1. But when you substitute f(1)=1 into the Claim, then the Claim reduces to f(p) = p, which is the goal we set for ourselves in the very first paragraph of the proof above.

To prove the Claim, let us suppose that it fails for some p and then derive a contradiction. (We are really using a form of strong induction.) In that case, fix the smallest such "bad" p. Now, p is not 0, by Property A, because the Claim is true for 0:

f(0) = 0*f(1), regardless of the value of f(1), because f(0) = 0 by Property A.

So p>0. In fact, p is not 1 either, because clearly the Claim holds for p=1, as we see by substituting 1 for p into the Claim:

f(1) = 1*f(1).

Therefore p is at least 2, and we may substitute p-1 for p in Property C:

f(p-1) = (1/2)f((p-1)-1) + (1/2)f((p-1)+1)

i.e.

2*f(p-1) = f(p-2) + f(p)

Now p-1 and p-2 are less than p, and p is suppose to be the least "bad" p. That is, we know that the Claim holds for p-1 and p-2, so we may use it to substitute into the equation above:

2*(p-1)*f(1) = (p-2)*f(1) + f(p)

which simplifies by algebra to

```
2p*f(1) - 2*f(1) = p*f(1) - 2*f(1) + f(p)

and then to

p*f(1) = f(p)

This contradicts our choice of p as a counterexample to the Claim!
|#
```

Index