EVENT: Start with the initial **nqthm** theory.

```
;;; The proof in here is based on the hint to exercise (8) on
;;; page 43 of Kunen's Set Theory book.

;; Imagine sets a and b and corresponding functions fa and fb which
;; map a to b and vice-versa, where both are one-one.
```

DEFINITION: $\mathrm{id}(x) = x$

CONSERVATIVE AXIOM: fa-and-fb-are-one-one

$((\mathrm{a}(x) \land \mathrm{a}(y) \land (x \neq y)) \rightarrow (\mathrm{fa}(x) \neq \mathrm{fa}(y)))$
$\land \quad ((\mathrm{b}(x) \land \mathrm{b}(y) \land (x \neq y)) \rightarrow (\mathrm{fb}(x) \neq \mathrm{fb}(y)))$
$\land \quad (\mathrm{a}(x) \rightarrow \mathrm{b}(\mathrm{fa}(x)))$
$\land \quad (\mathrm{b}(x) \rightarrow \mathrm{a}(\mathrm{fb}(x)))$
$\land \quad (\mathrm{truep}(\mathrm{a}(x)) \lor \mathrm{falsep}(\mathrm{a}(x)))$
$\land \quad (\mathrm{truep}(\mathrm{b}(x)) \lor \mathrm{falsep}(\mathrm{b}(x)))$

Simultaneously, we introduce the new function symbols *fa*, *fb*, *a*, and *b*.

DEFINITION:
$\text{in-fa-range}(x) \leftrightarrow \exists\, \textit{fa-1}\ (\mathrm{a}(\textit{fa-1}) \land (\mathrm{fa}(\textit{fa-1}) = x))$

```
;; The following 3 events were generated automatically to help with
;; the proof-checker's application of the macro command SK*.
```

EVENT: Disable in-fa-range.

THEOREM: in-fa-range-suff
$(\mathrm{a}(\textit{fa-1}) \land (\mathrm{fa}(\textit{fa-1}) = x)) \rightarrow \text{in-fa-range}(x)$

THEOREM: in-fa-range-necc
$(\neg\ (\mathrm{a}(\text{fa-1}(x)) \land (\mathrm{fa}(\text{fa-1}(x)) = x))) \rightarrow (\neg\ \text{in-fa-range}(x))$

DEFINITION:
$\text{in-fb-range}(x) \leftrightarrow \exists\, \textit{fb-1}\ (\mathrm{b}(\textit{fb-1}) \land (\mathrm{fb}(\textit{fb-1}) = x))$

```
;; The following 3 events were generated automatically to help with
;; the proof-checker's application of the macro command sk*.
```

EVENT: Disable in-fb-range.

THEOREM: in-fb-range-suff
$(\mathrm{b}(\mathit{fb\text{-}1}) \wedge (\mathrm{fb}(\mathit{fb\text{-}1}) = x)) \rightarrow \text{in-fb-range}(x)$

THEOREM: in-fb-range-necc
$(\neg\, (\mathrm{b}(\text{fb-1}(x)) \wedge (\mathrm{fb}(\text{fb-1}(x)) = x))) \rightarrow (\neg\, \text{in-fb-range}(x))$

DEFINITION:
$$
\begin{aligned}
&\text{circled}(\mathit{flg},\, x,\, n)\\
= \quad &\textbf{if } \mathit{flg} = \texttt{'a}\\
&\textbf{then if } n \simeq \texttt{0} \textbf{ then } \mathrm{a}(x)\\
&\qquad \textbf{else } \text{in-fb-range}(x) \wedge \text{circled}(\texttt{'b},\, \text{fb-1}(x),\, n - 1) \textbf{ endif}\\
&\textbf{elseif } n \simeq \texttt{0} \textbf{ then } \mathrm{b}(x)\\
&\textbf{else } \text{in-fa-range}(x) \wedge \text{circled}(\texttt{'a},\, \text{fa-1}(x),\, n - 1) \textbf{ endif}
\end{aligned}
$$

DEFINITION:
$$
\begin{aligned}
&\text{a-core}(x)\\
\leftrightarrow \quad &(\mathrm{a}(x)\\
&\quad \wedge \quad \forall\, \mathit{a\text{-}level}\, (((\mathit{a\text{-}level} \in \mathbf{N}) \wedge \text{circled}(\texttt{'a},\, x,\, \mathit{a\text{-}level}))\\
&\qquad\qquad \rightarrow \quad \text{circled}(\texttt{'a},\, x,\, 1 + \mathit{a\text{-}level})))
\end{aligned}
$$

EVENT: Disable a-core.

THEOREM: a-core-necc-base
$((n \simeq \texttt{0}) \wedge \text{a-core}(x)) \rightarrow \text{circled}(\texttt{'a},\, x,\, n)$

THEOREM: a-core-necc-induction
$((n \not\simeq \texttt{0}) \wedge \text{a-core}(x) \wedge \text{circled}(\texttt{'a},\, x,\, n - 1)) \rightarrow \text{circled}(\texttt{'a},\, x,\, n)$

THEOREM: a-core-necc
$(\neg\, \text{circled}(\texttt{'a},\, x,\, n)) \rightarrow (\neg\, \text{a-core}(x))$

EVENT: Disable a-core-necc-base.

EVENT: Disable a-core-necc-induction.

THEOREM: a-core-suff
$$
\begin{aligned}
&(\mathrm{a}(x)\\
&\ \wedge \quad (((\text{a-level}(x) \in \mathbf{N}) \wedge \text{circled}(\texttt{'a},\, x,\, \text{a-level}(x)))\\
&\qquad \rightarrow \quad \text{circled}(\texttt{'a},\, x,\, 1 + \text{a-level}(x))))\\
&\rightarrow \quad \text{a-core}(x)
\end{aligned}
$$

DEFINITION:
$$
\begin{aligned}
&\text{b-core}(x)\\
\leftrightarrow \quad &(\mathrm{b}(x)\\
&\quad \wedge \quad \forall\, \mathit{b\text{-}level}\, (((\mathit{b\text{-}level} \in \mathbf{N}) \wedge \text{circled}(\texttt{'b},\, x,\, \mathit{b\text{-}level}))\\
&\qquad\qquad \rightarrow \quad \text{circled}(\texttt{'b},\, x,\, 1 + \mathit{b\text{-}level})))
\end{aligned}
$$

EVENT: Disable b-core.

THEOREM: b-core-necc-base
$((n \simeq \texttt{0}) \land \text{b-core}\,(x)) \rightarrow \text{circled}\,(\texttt{'b},\ x,\ n)$

THEOREM: b-core-necc-induction
$((n \not\simeq \texttt{0}) \land \text{b-core}\,(x) \land \text{circled}\,(\texttt{'b},\ x,\ n-1)) \rightarrow \text{circled}\,(\texttt{'b},\ x,\ n)$

THEOREM: b-core-necc
$(\neg\ \text{circled}\,(\texttt{'b},\ x,\ n)) \rightarrow (\neg\ \text{b-core}\,(x))$

EVENT: Disable b-core-necc-base.

EVENT: Disable b-core-necc-induction.

THEOREM: b-core-suff

$$\begin{array}{ll}
\multicolumn{2}{l}{(\text{b}\,(x)} \\
\ \land & (((\text{b-level}\,(x) \in \mathbf{N}) \land \text{circled}\,(\texttt{'b},\ x,\ \text{b-level}\,(x))) \\
 & \quad \rightarrow \quad \text{circled}\,(\texttt{'b},\ x,\ 1 + \text{b-level}\,(x)))) \\
\rightarrow & \text{b-core}\,(x)
\end{array}$$

DEFINITION:
parity (n)
$=$ **if** $n \simeq \texttt{0}$ **then t**
else $\neg$ parity $(n-1)$ **endif**

DEFINITION:
j (x)
$=$ **if** a-core $(x) \lor$ parity (a-level (x)) **then** fa (x)
else fb-1 (x) **endif**

DEFINITION:
j-1 (y)
$=$ **if** b-core $(y) \lor (\neg$ parity (b-level (y))) **then** fa-1 (y)
else fb (y) **endif**

```
; Our goals:
;(prove-lemma j-1-j (rewrite)
;  (implies (a x)
;           (equal (j-1 (j x)) x)))

;(prove-lemma j-j-1 (rewrite)
;  (implies (b y)
;           (equal (j (j-1 y)) y)))
```

```
;; We'll start on the first of these.  The theorem-prover output
;; suggests the following lemma:

;(prove-lemma b-core-fa (rewrite)
;  (implies (a x)
;           (iff (b-core (fa x))
;                (a-core x))))

;; A main lemma is that (a-core x) => (b-core (fa x)) for x in a.
```

THEOREM: fa-1-inverts-fa
$\mathrm{a}\,(x) \rightarrow (\text{fa-1}\,(\mathrm{fa}\,(x)) = x)$

```
;; The following is useful for proof-checker rewriting:
```

THEOREM: in-fa-range-fa
$\mathrm{a}\,(x) \rightarrow \text{in-fa-range}\,(\mathrm{fa}\,(x))$

THEOREM: b-core-fa
$\mathrm{a}\,(x) \rightarrow (\text{b-core}\,(\mathrm{fa}\,(x)) \leftrightarrow \text{a-core}\,(x))$

```
;; On to Case 2 of j-1-j.  We find there the following contradictory hyps:

;(AND (A X)
;     (PARITY (A-LEVEL X))
;     (NOT (A-CORE X))
;     (PARITY (B-LEVEL (FA X))))

;; We want to prove:

;; B-LEVEL-FA

;(IMPLIES (AND (A X) (NOT (A-CORE X)))
;         (EQUAL (B-LEVEL (FA X))
;                (ADD1 (A-LEVEL X))))
```

THEOREM: b-fa-equality-rewrite
$(\mathrm{a}\,(x) \wedge (\neg\, \mathrm{b}\,(y))) \rightarrow (\mathrm{fa}\,(x) \neq y)$

THEOREM: fa-range-contained-in-b
$(\neg\, \mathrm{b}\,(y)) \rightarrow (\neg\, \text{in-fa-range}\,(y))$

THEOREM: circled-implies-b
circled ('b, y, n) $\rightarrow$ b (y)

THEOREM: a-fb-equality-rewrite
(b (y) $\land$ ($\neg$ a (x))) $\rightarrow$ (fb (y) $\neq x$)

THEOREM: fb-range-contained-in-a
($\neg$ a (x)) $\rightarrow$ ($\neg$ in-fb-range (x))

THEOREM: circled-implies-a
circled ('a, y, n) $\rightarrow$ a (y)

THEOREM: circled-monotone
(circled (*flg*, x, j) $\land$ ($j \not< i$)) $\rightarrow$ circled (*flg*, x, i)

THEOREM: circled-b-fa
a (x) $\rightarrow$ (circled ('b, fa (x), n) = circled ('a, x, $n - 1$))

THEOREM: b-level-fa-hack-lemma
(b-level (fa (x)) $\in \mathbf{N}$)
$\rightarrow$ ((b-level (fa (x)) = (1 + a-level (x)))
= ($\neg$ ((b-level (fa (x)) < (1 + a-level (x)))
$\lor$ ((1 + a-level (x)) < b-level (fa (x))))))

THEOREM: b-level-fa
(a (x) $\land$ ($\neg$ a-core (x))) $\rightarrow$ (b-level (fa (x)) = (1 + a-level (x)))

```
;; On to Case 3 of j-1-j.  Our first subgoal is:

;(IMPLIES (AND (A X)
;              (NOT (A-CORE X))
;              (NOT (PARITY (A-LEVEL X)))
;              (NOT (B-CORE (FB-1 X)))
;              (PARITY (B-LEVEL (FB-1 X))))
;         (EQUAL (FB (FB-1 X)) X))

;; and this follows from the following two lemmas.
```

THEOREM: not-parity-a-level-implies-in-fb-range
(a (x) $\land$ ($\neg$ parity (a-level (x)))) $\rightarrow$ in-fb-range (x)

```
;; The next subcase of j-1-j is:

;(implies (and (a x)
;              (not (a-core x))
```

```
;               (not (parity (a-level x)))
;               (not (parity (b-level (fb-1 x)))))
;          (equal (fa-1 (fb-1 x)) x))

;; and this follows from:

;(prove-lemma b-level-fb-1 (rewrite)
;  (implies (and (a x)
;                (not (a-core x))
;                (in-fb-range x))
;           (equal (b-level (fb-1 x))
;                  (sub1 (a-level x)))))

;; I've proved nearly the analogous thing already for fa.  Let's prove that
;; one for fb and then deduce this from it.
```

THEOREM: fb-1-inverts-fb
$\mathrm{b}\,(x) \rightarrow (\text{fb-1}\,(\mathrm{fb}\,(x)) = x)$

THEOREM: in-fb-range-fb
$\mathrm{b}\,(x) \rightarrow \text{in-fb-range}\,(\mathrm{fb}\,(x))$

THEOREM: circled-a-fb
$\mathrm{b}\,(x) \rightarrow (\mathrm{circled}\,(\texttt{'a},\, \mathrm{fb}\,(x),\, n) = \mathrm{circled}\,(\texttt{'b},\, x,\, n - 1))$

THEOREM: a-level-fb-hack-lemma
$(\text{a-level}\,(\mathrm{fb}\,(x)) \in \mathbf{N})$
$\rightarrow \quad ((\text{a-level}\,(\mathrm{fb}\,(x)) = (1 + \text{b-level}\,(x)))$
$\quad = \quad (\neg\, ((\text{a-level}\,(\mathrm{fb}\,(x)) < (1 + \text{b-level}\,(x)))$
$\quad\quad \vee \quad ((1 + \text{b-level}\,(x)) < \text{a-level}\,(\mathrm{fb}\,(x))))))$

THEOREM: a-core-fb
$\mathrm{b}\,(x) \rightarrow (\text{a-core}\,(\mathrm{fb}\,(x)) \leftrightarrow \text{b-core}\,(x))$

THEOREM: a-level-fb
$(\mathrm{b}\,(x) \wedge (\neg\, \text{b-core}\,(x))) \rightarrow (\text{a-level}\,(\mathrm{fb}\,(x)) = (1 + \text{b-level}\,(x)))$

THEOREM: b-level-fb-1
$(\mathrm{a}\,(x) \wedge (\neg\, \text{a-core}\,(x)) \wedge \text{in-fb-range}\,(x))$
$\rightarrow \quad (\text{b-level}\,(\text{fb-1}\,(x)) = (\text{a-level}\,(x) - 1))$

```
;; It remains only to prove the following subcase, and then we're done with j-1-j:

;(implies (and (a x)
```

```
;               (not (a-core x))
;               (not (parity (a-level x)))
;               (b-core (fb-1 x)))
;          (equal (fa-1 (fb-1 x)) x))

;; I've already proved a-core-fb, and this should be useful.
```

THEOREM: b-core-implies-b
$\text{b-core}\,(x) \rightarrow \text{b}\,(x)$

THEOREM: fb-fb-1
$(\text{a}\,(x) \wedge \text{in-fb-range}\,(x)) \rightarrow (\text{fb}\,(\text{fb-1}\,(x)) = x)$

THEOREM: b-core-fb-1
$(\text{a}\,(x) \wedge (\neg\ \text{a-core}\,(x)) \wedge (\neg\ \text{parity}\,(\text{a-level}\,(x))))$
$\rightarrow \quad (\neg\ \text{b-core}\,(\text{fb-1}\,(x)))$

```
;; Now finally for our first main goal:
```

THEOREM: j-1-j
$\text{a}\,(x) \rightarrow (\text{j-1}\,(\text{j}\,(x)) = x)$

```
;;;; We're ready now for the converse.  Here's the first sticking point:

;(implies (and (b-core y)
;               (a-core (fa-1 y)))
;          (equal (fa (fa-1 y)) y))

;; We need only the following two easy lemmas:
```

THEOREM: b-core-implies-in-fa-range
$\text{b-core}\,(y) \rightarrow \text{in-fa-range}\,(y)$

THEOREM: fa-fa-1
$\text{in-fa-range}\,(y) \rightarrow (\text{fa}\,(\text{fa-1}\,(y)) = y)$

```
;; Our next goal is:

;(implies (and (b-core y)
;               (not (a-core (fa-1 y)))
;               (not (parity (a-level (fa-1 y)))))
;          (equal (fb-1 (fa-1 y)) y))

;;; which is taken care of simply by:
```

THEOREM: a-core-fa-1
in-fa-range $(y) \rightarrow$ (a-core (fa-1 $(y)) \leftrightarrow$ b-core (y))

```
;; next we have to prove

;(implies (and (b y)
;              (not (parity (b-level y)))
;              (a-core (fa-1 y)))
;         (equal (fa (fa-1 y)) y))

;; which follows from fa-fa-1 together with an obvious analog of
;; NOT-PARITY-A-LEVEL-IMPLIES-IN-FB-RANGE:
```

THEOREM: not-parity-b-level-implies-in-fa-range
(b $(y) \wedge (\neg$ parity (b-level $(y)))) \rightarrow$ in-fa-range (y)

```
;; It remains only to prove:

;(implies (and (b y)
;              (not (parity (b-level y)))
;              (not (b-core y))
;              (not (parity (a-level (fa-1 y)))))
;         (equal (fb-1 (fa-1 y)) y))

;; which follows from an analogue of B-LEVEL-FB-1:
```

THEOREM: a-level-fa-1
(b $(y) \wedge (\neg$ b-core $(y)) \wedge$ in-fa-range (y))
$\rightarrow$ (a-level (fa-1 $(y)) =$ (b-level $(y) - 1$))

```
;;; and we're done!!!
```

THEOREM: j-j-1
b $(y) \rightarrow$ (j (j-1 $(y)) = y$)

```
;; To summarize:

;; From the axiom saying that fa maps a one-one into b and fb maps b one-one into a,

;(constrain fa-and-fb-are-one-one (rewrite)
;  (and (implies (and (a x) (a y) (not (equal x y)))
;                (not (equal (fa x) (fa y))))
```

```
;       (implies (and (b x) (b y) (not (equal x y)))
;                (not (equal (fb x) (fb y))))
;       (implies (a x) (b (fa x)))
;       (implies (b x) (a (fb x)))
;       (or (truep (a x)) (falsep (a x)))
;       (or (truep (b x)) (falsep (b x))))
;  ((fa id) (fb id) (a (lambda (x) t)) (b (lambda (x) t))))

;; to finish this off we simply prove the obvious lemmas needed for
;; j-iso below.  For the first, j-range,
;; we need a lemma (as seen from observing the failed proof transcript).
```

THEOREM: in-fb-range-implies-b-fb-1
in-fb-range $(y) \rightarrow$ b (fb-1 (y))

THEOREM: j-range
a $(x) \rightarrow$ b (j (x))

THEOREM: in-fa-range-implies-a-fa-1
in-fa-range $(y) \rightarrow$ a (fa-1 (y))

THEOREM: j-1-range
b $(x) \rightarrow$ a (j-1 (x))

EVENT: Disable j.

EVENT: Disable j-1.

THEOREM: j-is-one-one
(a $(x1) \land$ a $(x2) \land (x1 \neq x2)) \rightarrow$ (j $(x1) \neq$ j $(x2)$)

```
;; we were able to conservatively extend the theory culminating in
;; definitions of a function j which maps a one-one into b:
```

DEFINITION:
J-ISO

$$
\begin{aligned}
\leftrightarrow \quad & (\forall\, x\ (\mathrm{a}(x) \rightarrow \mathrm{b}(\mathrm{j}(x))) \\
& \land \quad \forall\, x1,\, x2\ ((\mathrm{a}(x1) \land \mathrm{a}(x2) \land (\mathrm{j}(x1) = \mathrm{j}(x2))) \\
& \qquad\qquad \rightarrow \quad (x1 = x2)) \\
& \land \quad \forall\, y\ (\mathrm{b}(y) \rightarrow \exists\, x\ (\mathrm{a}(x) \land (\mathrm{j}(x) = y))))
\end{aligned}
$$

THEOREM: j-is-an-isomorphism
J-ISO

Index