2.7. IBRT in $A_1,...,A_k,fA_1,...,fA_k,\subseteq$.

In this section, we analyze IBRT in $A_1,...,A_k,fA_1,...,fA_k,\subseteq$ on (SD,INF), (ELG $\cap$ SD,INF), (ELG,INF), (EVSD,INF), and (MF,INF). We show that for all $k \geq 1$, IBRT in $A_1,...,A_k,fA_1,...,fA_k,\subseteq$ on each of (SD,INF), (ELG $\cap$ SD,INF), (ELG,INF), (EVSD,INF) is RCA_0 secure. We show that IBRT in $A_1,...,A_k,fA_1,...,fA_k,\subseteq$ on (MF,INF) is ACA' secure (see Definition 1.4.1). We also show that the only correct format for IBRT in $A_1,...,A_k,fA_1,...,fA_k,\subseteq$ on (SD,INF), (ELG $\cap$ SD,INF), (ELG,INF), (EVSD,INF) is $\emptyset$. This is not true on (MF,INF).

We begin with (MF,INF), for some fixed $k \geq 1$. We need to analyze all statements of the form

#) $(\exists f \in MF)(\forall A_1,...,A_k \in INF)(A_1 \subseteq ... \subseteq A_k \rightarrow \varphi)$.

where φ is an $A_1,...,A_k,fA_1,...,fA_k,\subseteq$ format. Recall that the instances of #) are Boolean equivalent to the assertions of IBRT in $A_1,...,A_k,fA_1,...,fA_k,\subseteq$, and the negations of the statements in IBRT in $A_1,...,A_k,fA_1,...,fA_k,\subseteq$.

Recall the list of all $A_1,...,A_k,fA_1,...,fA_k,\subseteq$ elementary inclusions that were used in section 2.6:

1. $A_i = \emptyset$.
2. $fA_i = \emptyset$.
3. $A_i \cap fA_j = \emptyset$.
4. $A_i = N$.
5. $fA_i = N$.
6. $A_i \cup fA_j = N$.
7. $A_i \subseteq A_j$, $j < i$.
8. $A_i \subseteq fA_j$.
9. $A_i \subseteq A_j \cup fA_p$, $j < i$.
10. $fA_i \subseteq A_j$.
11. $fA_i \subseteq fA_j$, $j < i$.
12. $fA_i \subseteq A_j \cup fA_p$, $p < i$.
13. $A_i \cap fA_j \subseteq A_p$, $p < i$.
14. $A_i \cap fA_j \subseteq fA_p$, $p < j$.
15. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < i$ and $q < j$.

For each of these elementary inclusions, ρ, we will provide a useful description of the witness set for ρ, in the following sense: The set of all $f \in MF$ such that

$$(\forall A_1,...,A_k \in INF)(A_1 \subseteq ... \subseteq A_k \rightarrow \rho).$$

To analyze formats, we analyze the intersections of these witness sets, determining which intersections are nonempty. I.e., a format is correct if and only if the intersection of the set of witnesses of each element is nonempty (in IBRT in $A_1,\ldots,A_k,fA_1,\ldots,fA_k,\subseteq$ on (MF,INF)).

We also use this technique for the other four BRT settings. Thus a format is correct if and only if the intersection of the set of witnesses of each element meets V (in IBRT in $A_1,\ldots,A_k,fA_1,\ldots,fA_k,\subseteq$ on (V,INF), $V \subseteq MF$)).

Each numbered entry in the list represents several inclusions. In some numbered entries, all of the inclusions will have the same witness set. We call such an entry uniform. Unfortunately, some of the numbered entries are not uniform.

We shall see that entries 1-7,11 are uniform. We now determine their witnesses sets.

LEMMA 2.7.1. The inclusions in clauses 1-7 each have no witnesses. I.e., their witness sets are $\emptyset$.

Proof: Let $f \in MF$. We show that f is not a witness. For 1,2,3, let $A_1 = \ldots = A_k = N$. For 4,5,6 take $A_1 = \ldots = A_k = \emptyset$. For 7, take each $A_i = \{i\}$. QED

LEMMA 2.7.2. Let $f \in MF$ and $j < i$. f witnesses $fA_i \subseteq fA_j$ if and only if $(\forall B \in INF)(fB = fN)$.

Proof: Let f,j,i be as given. Let f witness $fA_i \subseteq fA_j$. Let $B \in INF$. Set $A_1 = \ldots = A_j = B$, $A_{j+1} = \ldots = A_k = N$. Then $fN = fB$. For the converse, assume $(\forall B \in INF)(fB = fN)$. Let $A_1 \subseteq \ldots \subseteq A_k \subseteq N$, where A_1 is infinite. Then $fA_i = fN = fA_j$. QED

We now break the remaining numbered entries into uniform parts as follows.

8a. $A_i \subseteq fA_j$, $i \leq j$.
8b. $A_i \subseteq fA_j$, $j < i$.
9a. $A_i \subseteq A_j \cup fA_p$, $j,p < i$.
9b. $A_i \subseteq A_j \cup fA_p$, $j < i \leq p$.
10a. $fA_i \subseteq A_j$, $i \leq j$.
10b. $fA_i \subseteq A_j$, $j < i$.
12a. $fA_i \subseteq A_j \cup fA_p$, $p,j < i$.
12b. $fA_i \subseteq A_j \cup fA_p$, $p < i \leq j$.

13a. $A_i \cap fA_j \subseteq A_p$, $p < i,j$.
13b. $A_i \cap fA_j \subseteq A_p$, $j \leq p < i$.
14a. $A_i \cap fA_j \subseteq fA_p$, $p < i,j$.
14b. $A_i \cap fA_j \subseteq fA_p$, $i \leq p < j$.
15a. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < i \leq q < j$.
15b. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < q < i \leq j$.
15c. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $q \leq p < i \leq j$.
15d. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < q = i < j$.
15e. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < q < j \leq i$.
15f. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $q \leq p < j \leq i$.
15g. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $q < j \leq p < i$.
15h. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $q < p = j < i$.

We need to show that this list includes all of 8-10,12-15 from the original list. This is evident by inspection for all but 15 = 15a-15h. Here we need Lemma 2.7.4 below.

LEMMA 2.7.3. Suppose $p < i$ and $q < j$. Then at least one of the following holds.
$p \leq i \leq q \leq j$.
$p \leq q \leq i \leq j$.
$q \leq p \leq i \leq j$.
$p \leq q \leq j \leq i$.
$q \leq p \leq j \leq i$.
$q \leq j \leq p \leq i$.

Proof: Let $p < i$ and $q < j$. Obviously, at least one of the $4! = 24$ four term inequalities with $\leq$ separating the four variables i,j,p,q, must hold. In any such true four term inequality with $\leq$, p must come before i and q must come before j. Of the $4! = 24$ permutations of the letters i,j,p,q, exactly 1/4 of them have p before i and q before j. Since the above lists 6 such, the above list must be complete. QED

LEMMA 2.7.4. Suppose $p < i$ and $q < j$. Then at least one of the following holds.
$p < i \leq q < j$
$p < q < i \leq j$
$q \leq p < i \leq j$
$p < q = i < j$
$p < q < j \leq i$
$q \leq p < j \leq i$
$q < j \leq p < i$
$q < p = j < i$.

Proof: We use Lemma 2.7.3, which provides six cases.

Suppose $p \leq i \leq q \leq j$. Then $p < i \leq q < j$.

Suppose $p \leq q \leq i \leq j$. If $p < q$ then $p < q < i \leq j \vee p < q = i < j$. If $p = q$ then $p = q < i \leq j$, and so $q \leq p < i \leq j$.

Suppose $q \leq p \leq i \leq j$. Then $q \leq p < i \leq j$.

Suppose $p \leq q \leq j \leq i$. If $p < q$ then $p < q < j \leq i$. If $p = q$ then $p = q < j \leq i$, and so $q \leq p < j \leq i$.

Suppose $q \leq p \leq j \leq i$. If $p < j$ then $q \leq p < j \leq i$. If $p = j$ then $q \leq p = j < i$, and hence $q < p = j < i$ (using $q < j$).

Suppose $q \leq j \leq p \leq i$. Then $q < j \leq p < i$. QED

We are now prepared to make the determination of witnesses for each of the entries 8a - 15h.

WITNESS SET ASSIGNMENT LIST

1-7. None. Lemma 2.7.1.
8a. $A_i \subseteq fA_j$, $i \leq j$. $(\forall B \in INF)(B \subseteq fB)$. Lemma 2.7.5.
8b. $A_i \subseteq fA_j$, $j < i$. None. Lemma 2.7.6.
9a. $A_i \subseteq A_j \cup fA_p$, $j,p < i$. None. Lemma 2.7.7.
9b. $A_i \subseteq A_j \cup fA_p$, $j < i \leq p$. $(\forall B \in INF)(B \subseteq fB)$. Lemma 2.7.8.
10a. $fA_i \subseteq A_j$, $i \leq j$. $(\forall B \in INF)(fB \subseteq B)$. Lemma 2.7.9.
10b. $fA_i \subseteq A_j$, $j < i$. None. Lemma 2.7.10.
11. $fA_i \subseteq fA_j$, $j < i$. $(\forall B \in INF)(fB = fN)$. Lemma 2.7.2.
12a. $fA_i \subseteq A_j \cup fA_p$, $p,j < i$. $(\forall B \in INF)(fB = fN)$. Lemma 2.7.11.
12b. $fA_i \subseteq A_j \cup fA_p$, $p < i \leq j$. $(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$. Lemma 2.7.12.
13a. $A_i \cap fA_j \subseteq A_p$, $p < i,j$. None. Lemma 2.7.13.
13b. $A_i \cap fA_j \subseteq A_p$, $j \leq p < i$. $(\forall B \in INF)(fB \subseteq B)$. Lemma 2.7.14.
14a. $A_i \cap fA_j \subseteq fA_p$, $p < i,j$. $(\forall B \in INF)(fB = fN)$. Lemma 2.7.15.
14b. $A_i \cap fA_j \subseteq fA_p$, $i \leq p < j$. $(\forall B \in INF)(B \cap fN \subseteq fB)$. Lemma 2.7.16.
15a. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < i \leq q < j$. $(\forall B \in INF)(B \cap fN \subseteq fB)$. Lemma 2.7.17.
15b. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < q < i \leq j$. $(\forall B \in INF)(fB = fN)$. Lemma 2.7.18.
15c. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $q \leq p < i \leq j$. $(\forall B \in INF)(fN \subseteq B \cup fB)$. Lemma 2.7.19.

15d. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < q = i < j$. $(\forall B \in INF)(B \cap fN \subseteq fB)$. Lemma 2.7.20.
15e. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < q < j \leq i$. $(\forall B \in INF)(fB = fN)$. Lemma 2.7.21.
15f. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $q \leq p < j \leq i$. $(\forall B \in INF)(fN \subseteq B \cup fB)$. Lemma 2.7.22.
15g. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $q < j \leq p < i$. $(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$. Lemma 2.7.23.
15h. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $q < p = j < i$. $(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$. Lemma 2.7.24.

LEMMA 2.7.5. Let $f \in MF$ and $i \leq j$. f witnesses $A_i \subseteq fA_j$ if and only if $(\forall B \in INF)(B \subseteq fB)$.

Proof: Let f,i,j be as given. Assume f witnesses $A_i \subseteq fA_j$. Let $B \in INF$. Set $A_1 = \ldots = A_k = B$. Then $B \subseteq fB$. For the converse, assume $(\forall B \in INF)(B \subseteq fB)$ and let $A_1 \subseteq \ldots A_k \subseteq N$, where A_1 is infinite. Then $A_i \subseteq fA_i \subseteq fA_j$. QED

LEMMA 2.7.6. $A_i \subseteq fA_j$, $j < i$, has no witnesses.

Proof: Let f witness $A_i \subseteq fA_j$, $j < i$. By the Thin Set Theorem, let $fB \neq N$. Set $A_1 = \ldots = A_j = B$, $A_{j+1} = \ldots = A_k = N$. Then $A_i \subseteq fA_j$ is false. QED

LEMMA 2.7.7. $A_i \subseteq A_j \cup fA_p$, $j,p < i$, has no witnesses.

Proof: Let f witness $A_i \subseteq A_j \cup fA_p$, $j,p < i$. By the Thin Set Theorem (variant), let $B \in INF$ where $B \cup fB \neq N$. Set $A_1 = \ldots = A_{i-1} = B$, $A_i = \ldots = A_k = N$. Then $A_i \subseteq A_j \cup fA_p$ is false. QED

LEMMA 2.7.8. Let $f \in MF$ and $j < i \leq p$. f witnesses $A_i \subseteq A_j \cup fA_p$ if and only if $(\forall B \in INF)(B \subseteq fB)$.

Proof: Let f,i,j,p be as given. Let f witness $A_i \subseteq A_j \cup fA_p$. Let $B \in INF$. Suppose $B \subseteq fB$ fails, and let $r \in B\backslash fB$. Set $A_1 = \ldots = A_j = B\backslash\{r\}$, $A_{j+1} = \ldots = A_k = B$. Then $B \subseteq B\backslash\{r\} \cup fB$, which contradicts the choice of r. Hence $B \subseteq fB$. For the converse, assume $(\forall B \in INF)(B \subseteq fB)$. Let $A_1 \subseteq \ldots \subseteq A_k \subseteq N$, where A_1 is infinite. Then $A_i \subseteq fA_i \subseteq fA_p \subseteq A_j \cup fA_p$. QED

LEMMA 2.7.9. Let $f \in MF$ and $i \leq j$. f witnesses $fA_i \subseteq A_j$ if and only if $(\forall B \in INF)(fB \subseteq B)$.

Proof: Let f,i,j be as given. Let f witness $fA_i \subseteq A_j$. Let $B \in INF$. Set $A_1 = ... = A_k = B$. Then $fB \subseteq B$. For the converse, assume $(\forall B \in INF)(fB \subseteq B)$. Let $A_1 \subseteq ... \subseteq A_k \subseteq N$, where A_1 is infinite. Then $fA_i \subseteq A_i \subseteq A_j$. QED

LEMMA 2.7.10. $fA_i \subseteq A_j$, $j < i$, has no witnesses.

Proof: Let f witness $fA_i \subseteq A_j$, $j < i$. Let $r \in fN$. Set $A_1 = ... = A_j = N\backslash\{r\}$, $A_{j+1} = ... A_k = N$. Then $fA_i \subseteq A_j$ is false. QED

LEMMA 2.7.11. Let $p,j < i$. f witnesses $fA_i \subseteq A_j \cup fA_p$ if and only if $(\forall B \in INF)(fB = fN)$.

Proof: Let f,i,j,p be as given. Let f witness $fA_i \subseteq A_j \cup fA_p$. Let $B \in INF$. Suppose $fB \subseteq fN$ fails. Let $r \in fN\backslash fB$. Set $A_1 = ... = A_{i-1} = B\backslash\{r\}$, $A_i = ... = A_k = N$. Then $fN \subseteq B\backslash\{r\} \cup f(B\backslash\{r\})$, which is a contradiction. For the converse, assume $(\forall B \in INF)(fB = fN)$. Let $A_1 \subseteq ... \subseteq A_k \subseteq N$, where A_1 is infinite. Then $fA_i = fN \subseteq A_j \cup fN = A_j \cup fA_p$. QED

LEMMA 2.7.12. Let $f \in MF$ and $p < i \leq j$. f witnesses $fA_i \subseteq A_j \cup fA_p$ if and only if $(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$.

Proof: Let f,i,j,p be as given. Let f witness $fA_i \subseteq A_j \cup fA_p$. Let $B \subseteq C \subseteq N$, where B is infinite. Set $A_1 = ... = A_p = B$, $A_{p+1} = ... = A_k = C$. Then $fC \subseteq C \cup fB$. For the converse, assume $(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$. Let $A_1 \subseteq ... \subseteq A_k \subseteq N$, where A_1 is infinite. Then $fA_i \subseteq A_i \cup fA_p \subseteq A_j \cup fA_p$. QED

LEMMA 2.7.13. $A_i \cap fA_j \subseteq A_p$, $p < i,j$, has no witnesses.

Proof: Let $p < i,j$. Let f witness $A_i \cap fA_j \subseteq A_p$. Let $r \in fN$. Let $A_1 = ... = A_p = N\backslash\{r\}$, $A_{p+1} = ... = A_k = N$. Then $A_i \cap fA_j \subseteq A_p$ is false. QED

LEMMA 2.7.14. Let $f \in MF$ and $j \leq p < i$. f witnesses $A_i \cap fA_j \subseteq A_p$ if and only if $(\forall B \in INF)(fB \subseteq B)$.

Proof: Let f,i,j,p be as given. Let f witness $A_i \cap fA_j \subseteq A_p$. Let $B \in INF$. Set $A_1 = ... = A_{i-1} = B$, $A_i = ... = A_k = N$. Then $fB \subseteq B$. For the converse, assume $(\forall B \in INF)(fB \subseteq B)$. Let $A_1 \subseteq ... \subseteq A_k \subseteq N$, where A_1 is infinite. Then $A_i \cap fA_j \subseteq A_i \cap A_j = A_j \subseteq A_p$. QED

LEMMA 2.7.15. Let $f \in MF$ and $p < i,j$. f witnesses $A_i \cap fA_j \subseteq fA_p$ if and only if $(\forall B \in INF)(fB = fN)$.

Proof: Let f,i,j,p be as given. Let f witness $A_i \cap fA_j \subseteq fA_p$. Let $B \in INF$. Set $A_1 = ... = A_p = B$, $A_{p+1} = ... = A_k = N$. Then $fN \subseteq fB$. For the converse, assume $(\forall B \in INF)(fB = fN)$. Let $A_1 \subseteq ... \subseteq A_k \subseteq N$, where A_1 is infinite. Then $A_i \cap fA_j \subseteq fN = fA_p$. QED

LEMMA 2.7.16. Let $f \in MF$ and $i \leq p < j$. f witnesses $A_i \cap fA_j \subseteq fA_p$ if and only if f witnesses $A_i \cap fA_j \subseteq fA_p$ if and only if $(\forall B \in INF)(B \cap fN \subseteq fB)$.

Proof: Let f,i,j,p be as given. Let f witness $A_i \cap fA_j \subseteq fA_p$. Let $B \in INF$. Set $A_1 = ... = A_{j-1} = B$, $A_j = ... = A_k = N$. Then $B \cap fN \subseteq fB$. For the converse, assume $(\forall B \in INF)(B \cap fN \subseteq fB)$. Let $A_1 \subseteq ... \subseteq A_k \subseteq N$, where A_1 is infinite. Then $A_i \cap fA_j \subseteq A_i \cap fN \subseteq fA_i \subseteq fA_p$. QED

LEMMA 2.7.17. Let $f \in MF$ and $p < i \leq q < j$. f witnesses $A_i \cap fA_j \subseteq A_p \cup fA_q$ if and only if $(\forall B \in INF)(B \cap fN \subseteq fB)$.

Proof: Let f,i,j,p,q be as given. Let f witness $A_i \cap fA_j \subseteq A_p \cup fA_q$. Let $B \in INF$. Suppose $B \cap fN \subseteq fB$ is false. Let $r \in B,fN$, $r \notin fB$. Set $A_1 = ... = A_{i-1} = B\backslash\{r\}$, $A_i = ... = A_{j-1} = B$, $A_j = ... = A_k = N$. Then $B \cap fN \subseteq B\backslash\{r\} \cup fB$. This is a contradiction. For the converse, assume $(\forall B \in INF)(B \cap fN \subseteq fB)$. Let $A_1 \subseteq ... \subseteq A_k \subseteq N$, where A_1 is infinite. Then $A_i \cap fA_j \subseteq A_i \cap fN \subseteq fA_i \subseteq fA_q$. QED

LEMMA 2.7.18. Let $f \in MF$ and $p < q < i \leq j$. f witnesses $A_i \cap fA_j \subseteq A_p \cup fA_q$ if and only if $(\forall B \in INF)(fB = fN)$.

Proof: Let f,i,j,p,q be as given. Let f witness $A_i \cap fA_j \subseteq A_p \cup fA_q$. Let $B \in INF$. Suppose $fB \neq fN$. Let $r \in fN\backslash fB$. Set $A_1 = ... = A_{q-1} = B\backslash\{r\}$, $A_q = ... = A_{i-1} = B$, $A_i = ... = A_k = N$. Then $fN \subseteq B\backslash\{r\} \cup fB$. This is a contradiction. Conversely, assume $(\forall B \in INF)(fB = fN)$. Let $A_1 \subseteq ... \subseteq A_k \subseteq N$, where A_1 is infinite. Then $A_i \cap fA_j \subseteq fN = fA_q \subseteq A_p \cup fA_q$. QED

LEMMA 2.7.19. Let $f \in MF$ and $q \leq p < i \leq j$. f witnesses $A_i \cap fA_j \subseteq A_p \cup fA_q$ if and only if $(\forall B \in INF)(fN \subseteq B \cup fB)$.

Proof: Let f,i,j,p,q be as given. Let f witness $A_i \cap fA_j \subseteq A_p \cup fA_q$. Set $A_1 = ... = A_{i-1} = B$, $A_i = ... = A_k = N$. Then $fN \subseteq B \cup fB$. Conversely, assume $(\forall B \in INF)(fN \subseteq B \cup fB)$. Let

$A_1 \subseteq \ldots \subseteq A_k \subseteq N$, where A_1 is infinite. Then $A_i \cap fA_j \subseteq fN \subseteq A_q \cup fA_q \subseteq A_p \cup fA_q$. QED

LEMMA 2.7.20. Let $f \in MF$ and $p < q = i < j$. f witnesses $A_i \cap fA_j \subseteq A_p \cup fA_q$ if and only if $(\forall B \in INF)(B \cap fN \subseteq fB)$.

Proof: Let f,i,j,p,q be as given. Let f witness $A_i \cap fA_j \subseteq A_p \cup fA_q$. Let $B \in INF$. Suppose $B \cap fN \subseteq fB$ is false. Let $r \in B,fN$, $r \notin fB$. Set $A_1 = \ldots = A_p = B\backslash\{r\}$, $A_{p+1} = \ldots = A_q = B$, $A_{q+1} = \ldots = A_k = N$. Then $B \cap fN \subseteq B\backslash\{r\} \cup fB$. This is a contradiction. For the converse, assume $(\forall B \in INF)(B \cap fN \subseteq fB)$. Let $A_1 \subseteq \ldots \subseteq A_k \subseteq N$, where A_1 is infinite. Then $A_i \cap fA_j \subseteq A_i \cap fN \subseteq fA_i = fA_q \subseteq A_p \cup fA_q$. QED

LEMMA 2.7.21. Let $f \in MF$ and $p < q < j \leq i$. f witnesses $A_i \cap fA_j \subseteq A_p \cup fA_q$ if and only if $(\forall B \in INF)(fB = fN)$.

Proof: Let f,i,j,p,q be as given. Let f witness $A_i \cap fA_j \subseteq A_p \cup fA_q$. Let $B \in INF$. Suppose $fN \neq fB$. Let $r \in fN\backslash fB$. Set $A_1 = \ldots = A_p = B\backslash\{r\}$, $A_{p+1} = \ldots = A_q = B$, $A_{q+1} = \ldots = A_k = N$. Then $fN \subseteq B\backslash\{r\} \cup fB$. This is a contradiction. For the converse, assume $(\forall B \in INF)(fN = fB)$. Let $A_1 \subseteq \ldots \subseteq A_k \subseteq N$, where A_1 is infinite. Then $A_i \cap fA_j \subseteq fN = fA_q \subseteq A_p \cup fA_q$. QED

LEMMA 2.7.22. Let $f \in MF$ and $q \leq p < j \leq i$. f witnesses $A_i \cap fA_j \subseteq A_p \cup fA_q$ if and only if $(\forall B \in INF)(fN \subseteq B \cup fB)$.

Proof: Let f,i,j,p,q be as given. Let f witness $A_i \cap fA_j \subseteq A_p \cup fA_q$. Let $B \in INF$. Set $A_1 = \ldots = A_{j-1} = B$, $A_j = \ldots = A_k = N$. Then $fN \subseteq B \cup fB$. For the converse, assume $(\forall B \in INF)(fN \subseteq B \cup fB)$. Let $A_1 \subseteq \ldots \subseteq A_k \subseteq N$, where A_1 is infinite. Then $A_i \cap fA_j \subseteq fN \subseteq A_q \cup fA_q \subseteq A_p \cup fA_q$. QED

LEMMA 2.7.23. Let $f \in MF$ and $q < j \leq p < i$. f witnesses $A_i \cap fA_j \subseteq A_p \cup fA_q$ if and only if $(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$.

Proof: Let f,i,j,p,q be as given. Let f witness $A_i \cap fA_j \subseteq A_p \cup fA_q$. Let $B \subseteq C \subseteq N$, where B is infinite. Set $A_1 = \ldots = A_q = B$, $A_{q+1} = \ldots = A_p = C$, $A_{p+1} = \ldots = A_k = N$. Then $fC \subseteq C \cup fB$. For the converse, assume $(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$. Let $A_1 \subseteq \ldots \subseteq A_k \subseteq N$, where A_1 is infinite. Then $A_i \cap fA_j \subseteq fA_j \subseteq A_j \cup fA_q \subseteq A_p \cup fA_q$. QED

LEMMA 2.7.24. Let $f \in MF$ and $q < p = j < i$. f witnesses $A_i \cap fA_j \subseteq A_p \cup fA_q$ if and only if $(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$.

Proof: Let f,i,j,p,q be as given. Let f witness $A_i \cap fA_j \subseteq A_p \cup fA_q$. Let $B \subseteq C \subseteq N$, where B is infinite. Set $A_1 = \ldots = A_q = B$, $A_{q+1} = \ldots = A_p = C$, $A_{p+1} = \ldots = A_k = N$. Then $fC \subseteq C \cup fB$. For the converse, assume $(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$. Let $A_1 \subseteq \ldots \subseteq A_k \subseteq N$, where A_1 is infinite. Then $A_i \cap fA_j \subseteq A_j \cup fA_q = A_p \cup fA_q$. QED

We now remove entries with no witnesses from the Witness Set Assignment List.

PRUNED WITNESS SET ASSIGNMENT LIST

8a. $A_i \subseteq fA_j$, $i \leq j$. $(\forall B \in INF)(B \subseteq fB)$. Lemma 2.7.5.
9b. $A_i \subseteq A_j \cup fA_p$, $j < i \leq p$. $(\forall B \in INF)(B \subseteq fB)$. Lemma 2.7.8.
10a. $fA_i \subseteq A_j$, $i \leq j$. $(\forall B \in INF)(fB \subseteq B)$. Lemma 2.7.9.
11. $fA_i \subseteq fA_j$, $j < i$. $(\forall B \in INF)(fB = fN)$. Lemma 2.7.2.
12a. $fA_i \subseteq A_j \cup fA_p$, $p,j < i$. $(\forall B \in INF)(fB = fN)$. Lemma 2.7.11.
12b. $fA_i \subseteq A_j \cup fA_p$, $p < i \leq j$. $(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$. Lemma 2.7.12.
13b. $A_i \cap fA_j \subseteq A_p$, $j \leq p < i$. $(\forall B \in INF)(fB \subseteq B)$. Lemma 2.7.14.
14a. $A_i \cap fA_j \subseteq fA_p$, $p < i,j$. $(\forall B \in INF)(fB = fN)$. Lemma 2.7.15.
14b. $A_i \cap fA_j \subseteq fA_p$, $i \leq p < j$. $(\forall B \in INF)(B \cap fN \subseteq fB)$. Lemma 2.7.16.
15a. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < i \leq q < j$. $(\forall B \in INF)(B \cap fN \subseteq fB)$. Lemma 2.7.17.
15b. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < q < i \leq j$. $(\forall B \in INF)(fB = fN)$. Lemma 2.7.18.
15c. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $q \leq p < i \leq j$. $(\forall B \in INF)(fN \subseteq B \cup fB)$. Lemma 2.7.19.
15d. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < q = i < j$. $(\forall B \in INF)(B \cap fN \subseteq fB)$. Lemma 2.7.20.
15e. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $p < q < j \leq i$. $(\forall B \in INF)(fB = fN)$. Lemma 2.7.21.
15f. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $q \leq p < j \leq i$. $(\forall B \in INF)(fN \subseteq B \cup fB)$. Lemma 2.7.22.
15g. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $q < j \leq p < i$. $(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$. Lemma 2.7.23.
15h. $A_i \cap fA_j \subseteq A_p \cup fA_q$, $q < p = j < i$. $(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$. Lemma 2.7.24.

Exactly six sets of witnesses appear in the Witness Set Assignment List.

WITNESS SET LIST (FOR MF).

$(\forall B \in INF)(fB = fN)$.
$(\forall B \in INF)(fN \subseteq B \cup fB)$.
$(\forall B \in INF)(B \subseteq fB)$.
$(\forall B \in INF)(fB \subseteq B)$.
$(\forall B \in INF)(B \cap fN \subseteq fB)$.
$(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$.

We have only to determine which subsets of the above list have a common witness; i.e., which subsets have nonempty intersection. For this purpose, we use the "pure" application of the Tree Methodology mentioned at the very end of section 2.1.

WITNESS SET LIST*.
3

$(\forall B \in INF)(fB = fN)$.
$(\forall B \in INF)(fN \subseteq B \cup fB)$.
$(\forall B \in INF)(B \subseteq fB)$.
$(\forall B \in INF)(fB \subseteq B)$.
$(\forall B \in INF)(B \cap fN \subseteq fB)$.
$(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$.

LIST 1.

$(\forall B \in INF)(fB = fN)$:
$(\forall B \in INF)(fN \subseteq B \cup fB)$.
$(\forall B \in INF)(B \subseteq fB)$. $fN = N$. No. By the Thin Set Theorem, let $fB \neq N$. Hence $fN \neq N$.
$(\forall B \in INF)(fB \subseteq B)$. No. Let $B = N\backslash\{r\}$, $r \in fN$.
$(\forall B \in INF)(B \cap fN \subseteq fB)$.
$(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$.

LIST 1.*
0

$(\forall B \in INF)(fB = fN)$:
$(\forall B \in INF)(fN \subseteq B \cup fB)$.
$(\forall B \in INF)(B \cap fN \subseteq fB)$.
$(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$.

Nonempty intersection. Let $f(x) = 0$.

LIST 2.

$(\forall B \in INF)(fN \subseteq B \cup fB)$:
$(\forall B \in INF)(B \subseteq fB)$. $fN = N$. No. By the Thin Set Theorem (variant), let $B \cup fB \neq N$. Since $fN \subseteq B \cup fB$, we have $fN \neq N$.
$(\forall B \in INF)(fB \subseteq B)$. $(\forall B \in INF)(fN \subseteq B)$. No. Let $B = N\backslash\{r\}$, $r \in fN$.
$(\forall B \in INF)(B \cap fN \subseteq fB)$.
$(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$.

LIST 2.*
0

$(\forall B \in INF)(fN \subseteq B \cup fB)$:
$(\forall B \in INF)(B \cap fN \subseteq fB)$.
$(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$.

Nonempty intersection. Let $f(x) = 0$.

LIST 3.

$(\forall B \in INF)(B \subseteq fB)$:
$(\forall B \in INF)(fB \subseteq B)$.
$(\forall B \in INF)(B \cap fN \subseteq fB)$.
$(\forall B,C \in INF)(B \subseteq C \rightarrow fC \subseteq C \cup fB)$.

Nonempty intersection. Let $f(x) = x$.

THEOREM 2.7.25. For all $k \geq 1$, IBRT in $A_1,\ldots,A_k,fA_1,\ldots,fA_k,\subseteq$ on (MF,INF) is ACA' secure.

Proof: Let S be a format in this BRT fragment α. Then S is a set of elementary inclusions in α, which are compiled in the first list of this section, 1-15. Correctness of S is equivalent to the existence of $f \in MF$ satisfying $(\forall A_1,\ldots,A_k \in INF)(A_1 \subseteq \ldots \subseteq A_k \rightarrow S)$. This can be rewritten in the following form:

the intersection of the witness sets
$$\{f \in MF: (\forall A_1,\ldots,A_k \in INF)(A_1 \subseteq \ldots \subseteq A_k \rightarrow \varphi)\},$$
$\varphi \in S$, is nonempty.

A complete analysis of the non emptiness of these intersection has been presented. This analysis is explicit, except for the use of the Thin Set Theorem and Thin Set Theorem (variant). Recall from section 1.4 that the Thin Set Theorem and the Thin Set Theorem (variant) are provable in ACA'. QED

We now consider IBRT in $A_1,\ldots,A_k,fA_1,\ldots,fA_k,\subseteq$ on (SD,INF), (ELG ∩ SD,INF), (ELG,INF), and (EVSD,INF). We shall see that it suffices to consider only (EVSD,INF).

This amounts to determining which subsets of the Witness Set List have a common element from EVSD. For this purpose, we repeat the Tree Methodology on the witness list, this time with reference to EVSD only.

WITNESS SET LIST. (FOR EVSD).

$(\forall B \in \text{INF})(fB = fN)$. No. By Theorem 2.2.1, let fN not be a subset of $B \cup fB$.
$(\forall B \in \text{INF})(fN \subseteq B \cup fB)$. No. Theorem 2.2.1.
$(\forall B \in \text{INF})(B \subseteq fB)$. No. By Theorem 2.2.1, let $B \cap fB = \emptyset$.
$(\forall B \in \text{INF})(fB \subseteq B)$. No. By Theorem 2.2.1.
$(\forall B \in \text{INF})(B \cap fN \subseteq fB)$. No. By Theorem 2.2.1, let $B \subseteq fN$, $B \cap fB = \emptyset$.
$(\forall B,C \in \text{INF})(B \subseteq C \rightarrow fC \subseteq C \cup fB)$. No. Lemma 2.7.26.

LEMMA 2.7.26. There is no $f \in$ EVSD such that $(\forall B,C \in \text{INF})(B \subseteq C \rightarrow fC \subseteq C \cup fB)$.

Proof: Let $f \in$ EVSD. By Theorem 2.2.1, let $C \in$ INF, where $C \cap fC = \emptyset$. We now apply Theorem 2.2.1, with A = C and D = fC. Let $B \subseteq C$, B infinite, where $fC \subseteq fB$ fails. Then $fC \subseteq C \cup fB$ also fails. QED

THEOREM 2.7.27. The following is provable in RCA_0. For all $k \geq 1$, IBRT in $A_1,\ldots,A_k,fA_1,\ldots,fA_k,\subseteq$ on (SD,INF), (ELG ∩ SD,INF), (ELG,INF), (EVSD,INF), have no correct formats other than ∅. They are all RCA_0 secure.

Proof: First note that EVSD contains SD, ELG ∩ SD, and ELG.

The above analysis is explicit, except for the use of the Thin Set Theorem and Thin Set Theorem (variant). But we need only apply the Thin Set Theorem (variant) to functions from EVSD. By Theorem 2.2.1, there exists infinite B such that $B \cap fB = \emptyset$, and so $fB \neq N$. Now use the fact that Theorem 2.2.1 is provable in RCA_0. QED

It is clear that IBRT in $A_1,...,A_k,fA_1,...,fA_k,\subseteq$ on (MF,INF) has correct formats other than $\emptyset$. In particular,

$$(\exists f \in MF)(\forall A \in INF)(fA = A)$$

by setting $f(x) = x$.