1.3. Complementation Theorems.

Recall the Complementation Theorem from section 1.1. It first appeared in print in [Fr92], Theorem 3, p. 82, (in a slightly different form), where we presented some precursors of BRT.

The Complementation Theorem is closely related to the standard Contraction Mapping Theorem. We discuss the connection below.

The Complementation Theorem is also closely related to a well known theorem, due to von Neumann in [VM44], and subsequent developments in graph theory. We discuss this at the end of this section.

COMPLEMENTATION THEOREM. For all $f \in SD$ there exists $A \in INF$ such that $fA = N\backslash A$.

COMPLEMENTATION THEOREM (with uniqueness). For all $f \in SD$ there exists a unique $A \subseteq N$ with $fA = N\backslash A$. Moreover, $A \in INF$.

Before giving the proof of the Complementation Theorem (with uniqueness), we discuss some alternative formulations.

The Complementation Theorem (without uniqueness) is written above as a statement of EBRT in A,fA on (SD,INF). Strictly speaking, we cannot express the uniqueness within BRT.

DEFINITION 1.3.1. $A \dot\cup B$ is the disjoint union of A and B, and is defined as $A \cup B$ if A,B are disjoint; undefined otherwise. E.g., $A \dot\cup B = C$ if and only if $A \cup B = C \wedge A \cap B = \emptyset$.

Note that there are other equivalent ways of writing $fA = N\backslash A$. E.g., we can write

$$fA = N\backslash A.$$
$$A = N\backslash fA.$$
$$A \dot\cup fA = N.$$

The first evaluates the action of f on A.

The second asserts that A is a fixed point (of the operator that sends each B to $N\backslash fB$.

The third asserts that N is partitioned into A and fA.

Proof: Let $f \in SD$. Note that for all $A \subseteq N$, $n \in fA$ if and only if $n \in f(A \cap [0,n))$.

We inductively define a set $A \subseteq N$ as follows. Suppose $n \geq 0$ and we have defined membership in A for all $0 \leq i < n$. We then define $n \in A$ if and only if $n \notin f(A \cap [0,n))$. Since $f \in SD$, we have for all n, $n \in A \leftrightarrow n \notin fA$ as required.

Now suppose $fB = N\backslash B$. Let m be least such that A,B differ. Then $m \in B \leftrightarrow m \notin fB \leftrightarrow m \notin f(B \cap [0,m))$, and $m \in A \leftrightarrow m \notin f(A \cap [0,m))$. Since $A \cap [0,m) = B \cap [0,m)$, we have $m \in A \leftrightarrow m \in B$. This is a contradiction. Hence A = B.

If A is finite then fA is finite and $N\backslash A$ is infinite. Hence A is infinite. QED

It will be convenient to use the following terminology. Let $f:X^k \to X$.

DEFINITION 1.3.2. Let f be a multivariate function with domain X (see Definitions 1.1.8 - 1.10). A complementation of f is a set $A \subseteq X$ such that $fA = X\backslash A$.

Thus we can restate the Complementation theorem (with uniqueness) as follows.

COMPLEMENTATION THEOREM (with uniqueness). Every $f \in SD$ has a unique complementation.

Note that we have proved the Complementation Theorem (with uniqueness) within the base theory RCA_0 of Reverse Mathematics. See [Si99].

The Complementation Theorem is obviously a particularly simple way of encapsulating the essence of recursion along the natural numbers. It appears to have significant educational value.

We now state a Complementation Theorem for well founded relations. We will be using this generalization in section 4.2.

DEFINITION 1.3.3. A binary relation is a set R of ordered pairs. We place no restriction on the coordinates of the elements of R. We write $\mathrm{fld}(R) = \{x: (\exists y \in R)(x \text{ is a coordinate of } y)\}$.

DEFINITION 1.3.4. We say that a binary relation R is well founded if and only if for all nonempty $S \subseteq \mathrm{fld}(R)$, there exists $y \in S$ such that for all $x \in S$, $(x,y) \notin R$. Thus well founded relations are irreflexive.

DEFINITION 1.3.5. We say that $f:\mathrm{fld}(R)^k \to \mathrm{fld}(R)$ is strictly dominating if and only if for all $x \in \mathrm{fld}(R)^k$, $(x_1,f(x)),\ldots,(x_k,f(x)) \in R$.

DEFINITION 1.3.6. We write SD(R) for the set of all strictly dominating functions whose domain is a Cartesian power of fld(R) and whose range is a subset of fld(R).

THEOREM 1.3.1. COMPLEMENTATION THEOREM (for well founded relations, with uniqueness). If R is a well founded relation, then every $f \in SD(R)$ has a unique complementation.

Proof: We want to be particularly careful because we are not assuming that R is transitive. Let the arity of f be $k \geq 1$.

For all $b \in \mathrm{fld}(R)$, define b^* to be the set of all x which ends a backward R chain of length ≥ 1 that starts with b. Thus $b \in b^*$.

We first make a coherence claim. Let $b,b' \in \mathrm{fld}(R)$, and $S,T \subseteq \mathrm{fld}(R)$, where

$$S \subseteq b^* \wedge (\forall c \in b^*)(c \in S \leftrightarrow c \notin fS).$$
$$T \subseteq b'^* \wedge (\forall c \in b'^*)(c \in T \leftrightarrow c \notin fT).$$

Then

$$(\forall c \in b^* \cap b'^*)(c \in S \leftrightarrow c \in T).$$

Suppose this is false. By well foundedness, fix c such that

$$c \in b^* \cap b'^* \wedge (c \in S \leftrightarrow c \notin T)$$
$$(\forall d)(R(d,c) \to \neg(d \in b^* \cap b'^* \wedge (d \in S \leftrightarrow d \in T)))$$

and obtain a contradiction.

We now claim that $c \in fS \leftrightarrow c \in fT$. For the forward direction, let $c = f(d_1,\ldots,d_k)$, $d_1,\ldots,d_k \in S$. By $f \in SD(R)$, we have $R(d_1,c),\ldots,R(d_k,c)$. Hence $d_1,\ldots,d_k \in T$, and so $c \in fT$. The reverse direction is proved in the same way.

Since $c \in S \leftrightarrow c \notin T$, we have $c \notin fS \leftrightarrow c \in fT$. This contradicts the above claim, and the coherence claim is established.

We now claim that for all $b \in fld(R)$, there exists $S_b \subseteq b^*$ such that $(\forall c \in b^*)(c \in S_b \leftrightarrow c \notin f(S_b))$. To see this, suppose this is false, and fix $b \in fld(R)$ such that

$$(\forall x)(R(x,b) \rightarrow (\exists S \subseteq x^*)(\forall c \in x^*)(c \in S \leftrightarrow c \notin fS)).$$
$$\neg(\exists S \subseteq b^*)(\forall c \in b^*)(c \in S \leftrightarrow c \notin fS).$$

By the coherence claim, for each x such that $R(x,b)$, there is a unique set $S_x \subseteq x^*$ such that $(\forall c \in x^*)(c \in S_x \leftrightarrow c \notin f(S_x))$.

Furthermore, by the coherence claim, we have

$$(\forall x,y)((R(x,b) \wedge R(y,b)) \rightarrow (\forall c \in x^* \cap y^*)(c \in S_x \leftrightarrow c \in S_y)).$$

Let V be the union of the S_x such that $R(x,b)$. We claim that

$$(\forall c \in b^*\backslash\{b\})(c \in V \leftrightarrow c \notin fV).$$

To see this, let $c \in b^*\backslash\{b\}$. First assume $c \in V$, $c \in fV$. Fix x such that $c \in S_x$, $R(x,b)$. Let $c = f(d_1,\ldots,d_k)$, $d_1,\ldots,d_k \in V$. Then $R(d_1,c),\ldots,R(d_k,c)$. Hence $d_1,\ldots,d_k \in x^*$. By coherence, $d_1,\ldots,d_k \in S_x$, since $d_1,\ldots,d_k \in V$. Hence $c \in S_x$, $c \in f(S_x)$, which contradicts the definition of S_x.

Now assume $c \notin fV$. Since $c \in b^*\backslash\{b\}$, let $c \in x^*$, $R(x,b)$. Then $c \in S_x \leftrightarrow c \notin f(S_x)$. Now $c \notin f(S_x)$. Hence $c \in S_x$. Therefore $c \in V$.

The set V is not quite the same as the set S_b that we are looking for. We let $S_b = V$ if $b \in fV$; $V \cup \{b\}$ otherwise. Then

$$\neg(\exists S \subseteq b^*)(\forall c \in b^*)(c \in S \leftrightarrow c \notin fS).$$

and so we have a contradiction. Hence the claim is established.

To complete the proof, let S be the union of all S_b, b ∈ fld(R). By the same argument, we see that

$$(\forall c \in fld(R))(c \in S \leftrightarrow c \notin fS).$$

and so S is a complementation of f. S is unique by the argument given above for the coherence claim. QED

DEFINITION 1.3.7. Let (V,K) be a BRT setting (see Definition 1.11). The Complementation Theorem for (V,K) asserts that $(\forall f \in V)(\exists A \in K)(fA = U\backslash A)$. The Complementation Theorem for (V,K) (with uniqueness) asserts that $(\forall f \in V)(\exists! A \in K)(fA = U\backslash A)$.

We use POW(E) for the power set of E.

Let < be a binary relation. Then (SD(<),POW(fld(<))) is a BRT setting, and its universal set U = fld(<). See Definition 1.13 for the definition of U.

THEOREM 1.3.2. Let < be an irreflexive transitive relation with the upper bound condition $(\forall x,y)(\exists z)(x,y < z)$. The following are equivalent.
1. The Complementation Theorem holds on (SD(<),POW(fld(<))).
2. The Complementation Theorem (with uniqueness) holds on (SD(<),POW(fld(<))).
3. < is well founded

Proof: Obviously 3 → 2 → 1 follows immediately from Theorem 1.3.1, even for arbitrary relations <. Thus we have only to assume that < is non well founded, and give a counterexample to 1.

Since < is irreflexive and transitive, < has no cycles. Since < is non well founded, < must have an infinite descending sequence.

Let $x_1 > x_2 > x_3 > \ldots$ be an infinite descending sequence. Let f ∈ SD(<) have arity 2, where for all $0 < i < j$, $f(x_{2i},x_{2j-1}) = x_{2i-1}$. For all other pairs y,z ∈ fld(<), let $f(y,z) > x_1,y,z$. Then f ∈ SD(<). Let A ⊆ fld(<), fA = fld(<)\A.

Clearly each $x_{2i} \notin fA$, and so each $x_{2i} \in A$. Hence for all $i > 0$, $x_{2i-1} \in fA \leftrightarrow (\exists j > i)(x_{2j-1} \in A)$. Hence for all $i > 0$, $x_{2i-1} \in A \leftrightarrow (\forall j > i)(x_{2j-1} \notin A)$.

Let $i > 0$. Suppose $(\forall j > i)(x_{2j-1} \notin A)$. Then $(\forall j > i+1)(x_{2j-1} \notin A)$, and so $x_{2i+1} \in A$. This is a contradiction, using $j = i+1$.

Hence for all $i > 0$, $x_{2i-1} \notin A$. But then $x_1 \notin fA$, $x_1 \in A$. This is a contradiction. Hence $fA \neq fld(<)\backslash A$. QED

Transitivity cannot be removed from the hypotheses of Theorem 1.3.2, as indicated by the following example.

THEOREM 1.3.3. Let R be the non well founded irreflexive binary relation on Z with the upper bound condition, given by $x \; R \; y \leftrightarrow (x+1 = y \vee (x < y \wedge y \geq 0))$. Then every $f \in SD(R)$ has a complementation.

Proof: Let $f \in SD(R)$. We first define $A \cap Z^-$ as follows. Let $B = Z^-\backslash rng(f)$. We first put $B \subseteq A$.

Now define membership in A in the open interval between any two numerically successive elements of B by induction. I.e., if $n < m$ are two numerically successive elements of B, then for all $1 \leq i \leq m-n-1$, put $n+i$ in A if and only if $n+i \notin fA$. This is well defined because the truth value of $n+i \in fA$ depends only on the truth value of $n+i-1 \in A$.

If $\max(B) < 0$ then define membership in A in the open interval between $\max(B)$ and 0 by induction in the same way.

Now suppose that B has a least element, t. Put $t-1 \notin A$, $t-2 \in A$, $t-3 \notin A$, ..., alternating in the obvious way. If $B = \emptyset$, put $-1 \notin A$, $-2 \in A$, $-3 \notin A$, ...

This completes the definition of $A \cap Z^-$. Note that for all $n < 0$, $n \in A \leftrightarrow n \notin fA$.

We can now define $A \cap N$ recursively as follows. For $n \in N$, take $n \in A$ if and only if $n \notin fA$. Then for all $n \geq 0$, $n \in A \leftrightarrow n \notin fA$. Since for all $n < 0$, $n \in A \leftrightarrow n \notin fA$, A is a complementation of f. QED

We now consider the structure of the unique complementations, for various simple $f \in SD$.

From examination of the construction of the unique complementation A, given in the proof of the Complementation Theorem above, we see that as more numbers are placed in A, more numbers appear in fA, and so fewer numbers are placed in A later. And as fewer numbers are placed in A later, fewer numbers appear in fA, and so more numbers are placed in A latter. So there is a tension between numbers going in and numbers staying out.

There is the expectation that even for very simple $f \in SD$, the unique complementation A of f can be very complicated - and have an intricate structure well worth exploring.

Let us consider some very basic examples.

DEFINITION 1.3.8. We define $Res(n,m)$ as the residue of n modulo $m \geq 1$.

THEOREM 1.3.4. Let $f:N^k \to N$ be given by $f(n_1,\ldots,n_k) = n_1+\ldots+n_k+c$, where c is a constant ≥ 1. Then the complementation of f is $\{n \geq 0: Res(n,k(c-1)+c+1) < c\}$. Thus A is periodic with period $k(c-1)+c+1$.

Proof: Let k,f,c be as given. Let $A = \{n \geq 0: Res(n,k(c-1)+c+1) < c\}$. Suppose $n_1,\ldots,n_k \in A$. Then $Res(n_1,k(c-1)+c+1),\ldots,Res(n_k,k(c-1)+c+1) < c$. Hence $Res(n_1+\ldots+n_k+c,k(c-1)+c+1) \in [c,k(c-1)+c]$, because when we add the residues of n1,...,nk,c, we stay below the modulus $k(c-1)+c+1$. Therefore $n_1+\ldots+n_k+c \notin A$.

Suppose $n \notin A$, $n \geq 0$. Then $p = Res(n,k(c-1)+c+1) \in [c,k(c-1)+c]$ and $n \geq c$. Hence $p-c \in [0,k(c-1)]$, and so write $p-c$ as a sum of k elements of $[0,c-1]$. Hence write $p = t_1+\ldots+t_k+c$, where $t_1,\ldots,t_k \in [0,c-1]$. Write $n = (n-p+t_1)+t_2+\ldots+t_k+c$.

By the definition of p, we have $p \leq n$, and so $n-p+t_1 \geq 0$ and $Res(n-p+t_1,k(c-1)+c+1),Res(t_1,k(c-1)+c+1),\ldots,Res(t_k,k(c-1)+c+1) \in [0,c-1]$. Hence $n-p+t_1,t_2,\ldots,t_k \in A$. QED

We now come to a basic example where the function is unary and one-one. This is a very special case, and it lends itself to a general result of independent interest.

Let $f:X \to X$ be one-one and k be an integer. For $k \geq 0$ and $x \in X$, let $f^k(x) = f\ldots f(x)$, where there are k f's. Let $f^{-k}(x)$

be the unique y such that $f^k(y) = x$, if y exists; undefined otherwise.

LEMMA 1.3.5. Let $f:X \to X$ be one-one. Assume that for all $x \in X$ there exists $k \geq 1$ such that $f^{-k}(x)$ does not exist. Then the unique complementation of f is $X\backslash fX \cup f^2(X\backslash fX) \cup f^4(X\backslash fX) \cup \ldots$.

Proof: Let f be as given. We first claim that every $x \in X$ can be written as $f^i(y)$, where $i \geq 0$ and $y \in X\backslash fX$. Suppose this is false for x. We show that by induction on $i \geq 1$ that for all $i \geq 1$, $f^{-i}(x)$ exists, contrary to the hypothesis on f. Clearly $x \in fX$, and so the case $i = 1$ is verified.

Suppose $f^{-i}(x)$ exists. If $f^{-i-1}(x)$ does not exist then $f^{-i}(x) \in X\backslash fX$, and so $x \in f^i(X\backslash fX)$. This is a contradiction. Hence $f^{-i-1}(x)$ exists, completing the induction argument.

We next claim that X is partitioned by the infinite disjoint union

$$1)\quad X\backslash fX \cup. f(X\backslash fX) \cup. f^2(X\backslash fX) \cup. \ldots .$$

We have just shown that the union is X. To see that these sets are disjoint, let $f^i(x) = f^j(y)$, where $0 \leq i < j$, and $x,y \in X\backslash fX$. Since f is one-one, we have $x = f^{j-i}(y)$, and so $x \in fX$. This is a contradiction.

We now see that X is partitioned by the two disjoint sets

$$X\backslash fX \cup. f^2(X\backslash fX) \cup. f^4(X\backslash fX) \cup. \ldots .$$
$$f(X\backslash fX) \cup. f^3(X\backslash fX) \cup. f^5(X\backslash fX) \cup. \ldots .$$

Also note that the forward image of f on the first set is the second set. Therefore the first set is a complementation of f.

For uniqueness, suppose E is a complementation of f. Then obviously $X\backslash fX \subseteq E$. Hence $f(X\backslash fX) \subseteq X\backslash E$. Therefore $f^2(X\backslash fX) \subseteq X$. Continue in this way. This determines membership in X for all of 1), which is all of X. QED

THEOREM 1.3.6. Let $f:N \to N$ be given by $f(n) = an+b$, where $a \geq 2$ and $0 < b < a$. Then the unique complementation of f is a finite union of ranges of two variable expressions involving addition, subtraction, multiplication, unnested base a exponentiation, and constants. In particular, the unique complementation of f is $\{(an+k)a^{2i} + b(a^{2i}-1)/(a-1): n,i \geq 0 \wedge k \in [0,a-1]\backslash\{b\}\}$.

Proof: Let f,a,b be as given. Note that f is one-one. We apply Lemma 1.3.5.

Let $S = N\backslash fN$. Note that $S = \{an+k: n \geq 0 \wedge k \in [0,a-1]\backslash\{b\}\}$.

We claim that for all $i \geq 0$,

$$f^i S = \{(an+k)a^i + b(a^i-1)/(a-1): n \geq 0 \wedge k \in [0,a-1]\backslash\{b\}\}.$$

We prove this by induction. For $i = 0$, we must verify that

$$f^0 S = S = \{an+k: n \geq 0 \wedge k \in [0,a-1]\backslash\{b\}\}$$

which is obvious. Suppose

$$f^i S = \{(an+k)a^i + b(a^i-1)/(a-1): n \geq 0 \wedge k \in [0,a-1]\backslash\{b\}\}.$$

Then

$$f^{i+1}S = \{a[(an+k)a^i + b(a^i-1)/(a-1)] + b: n \geq 0 \wedge k \in [0,a-1]\backslash\{b\}\} =$$

$$\{(an+k)a^{i+1} + ab(a^i-1)/(a-1) + b: n \geq 0 \wedge k \in [0,a-1]\backslash\{b\}\} =$$

$$\{(an+k)a^{i+1} + b(a(a^i-1)/(a-1) + 1): n \geq 0 \wedge k \in [0,a-1]\backslash\{b\}\} =$$

$$\{(an+k)a^{i+1} + b(a^{i+1}-1)/(a-1): n \geq 0 \wedge k \in [0,a-1]\backslash\{b\}\}.$$

Obviously, the first disjoint union from Lemma 1.3.5, which is the unique complementation of f, is

$$\{(an+k)a^i + b(a^i-1)/(a-1): n \geq 0 \wedge k \in [0,a-1]\backslash\{b\} \wedge i \in 2N\} =$$

$$\{(an+k)a^{2i} + b(a^{2i}-1)/(a-1): n,i \geq 0 \wedge k \in [0,a-1]\backslash\{b\}\}.$$

QED

We would like to consider any affine function f from a Cartesian power of N into N. The problem is that affine functions may not be in SD.

DEFINITION 1.3.9. Let f be a multivariate function and A be a set. We define the “upper image” of f on A by

$$f_{<}A = \{f(x_1,\ldots,x_k): f(x_1,\ldots,x_k) > \max(x_1,\ldots,x_k) \text{ and } x_1,\ldots,x_n \in A\}$$

where f has arity k. Obviously, if $f \in SD$ then $f_{<}A = fA$.

DEFINITION 1.3.10. Let < be a binary relation and f be a multivariate function with domain fld(R). An upper complementation of f is a set $A \subseteq X$ such that $f_{<}A = \mathrm{fld}(R)\setminus A$.

For upper complementations of $f \in MF$, it is understood that < is the usual ordering on N.

UPPER COMPLEMENTATION THEOREM. Every $f:N^k \to Z$ has a unique upper complementation. This unique upper complement is infinite.

In fact, this was the first form of the Complementation Theorem in print. See [Fr92], Theorem 3, p. 82.

We continue with two more examples.

THEOREM 1.3.7. Let $f:N^k \to N$ be given by $f(n_1,\ldots,n_k) = n_1+\ldots+n_k$, $k \geq 2$. Then the unique upper complementation of f is $\{n \geq 0: \mathrm{Res}(n,k) = 1\} \cup \{0\}$. Thus the unique upper complementation is periodic with period k. If k = 1 then the unique upper complementation is N.

Proof: Let k,f be as given. Let $A = \{n \geq 0: \mathrm{Res}(n,k) = 1\} \cup \{0\}$. Let $n = f_{<}(n_1,\ldots,n_k)$, $n_1,\ldots,n_k \in A$. Then $\mathrm{Res}(n_1+\ldots+n_k,k) = 0$, and so $n = f_{<}(n_1,\ldots,n_k)$ has residue 0 mod k and is > 0 if defined. Hence $n \notin A$ if defined.

Suppose $n \notin A$, $n \geq 0$. Then $n > 1$. Let p be largest such that $p < n$ and $\mathrm{Res}(p,k) = 1$. Since $\mathrm{Res}(n,k) \neq 1$, we have $0 < n-p \leq k-1$. Let $n_1,\ldots,n_{k-1} \in \{0,1\}$ be such that $n_1 + \ldots + n_{k-1} = n-p$. Then $n = p + n_1 + \ldots + n_{k-1}$, and $p,n_1,\ldots,n_{k-1} \in A$. Also $n > p,n_1,\ldots,n_{k-1}$. Hence $n \in f_{<}(p,n_1,\ldots,n_k)$. Therefore $n \in f_{<}A$. QED

Robert Lubarsky considered the case of binary multiplication (private communication). Here is his result.

THEOREM 1.3.8. Let $f:N^2 \to N$ be given by $f(n,m) = nm$. Then the unique upper complementation of f is $\{n: n = 0 \vee n = 1 \vee n$ is the product of an odd number of primes$\}$.

Proof: Let f be as given. Let $A = \{n: n = 0 \vee n = 1 \vee n$ is the product of an odd number of primes$\}$. Let $n \in A$, $n \in f_<A$. Write $n = mr$, $m,r \in A$, $n > m,r$. Then $m,r \geq 2$, and so m,r are each the product of an odd number of primes. Therefore $n = mr$ is the product of an even number of primes, and hence $n = mr \notin A$. This establishes that $(\forall n \in N)(n \in f_<A \to n \notin A)$.

Now let $n \notin A$, $n \geq 0$. Then $n \geq 2$ and n is not the product of an odd number of primes. Hence n is the product of an even number, 2t, of primes, $t \geq 1$. We can obviously write $n = mr$, where m,r are each the product of t primes. Hence we have written $n = mr$, where $m,r \in A$, and $m,r \geq 2$. Therefore $n \in f_<A$. QED

To understand the complementation of a function like nm+1 appears to be difficult.

A challenge would be to understand the structure of the unique upper complementation of every affine function $f:N^k \to Z$ with integer coefficients. In particular, can we estimate the number of elements below n of these unique upper complementations? Can we algorithmically determine whether there are arbitrarily long blocks?

Can we algorithmically determine the cardinalities of all finite Boolean combinations of the unique upper complementations of these f's?

We now wish to generalize the Complementation Theorem (for SD) in a different direction that will be used in section 2.4. Recall the definition of BRT term in Definition 1.1.5.

Note that one of the three forms of $fA = N\setminus A$ is $A = N\setminus fA$, which converts the Complementation Theorem into a fixed point theorem.

BRT FIXED POINT THEOREM. Let t be a BRT term in several set variables and several function variables, in which all occurrences of the set variable A lie within the scope of a function variable. Let us assume that the function variables have been assigned elements of SD, and the set variables other than A have been assigned subsets of N. Then there is a unique set $A \subseteq N$ such that the BRT equation $A = t$ holds.

Proof: We first claim that if t is any BRT term, and an assignment for t is as stated, and $A,A' \subseteq N$ agree on $[0,n)$, then $n \in t(A) \leftrightarrow n \in t(A')$. This claim is proved by induction on the BRT term t. We now follow the proof given above of the Complementation Theorem, building sets $A_0 \subseteq A_1 \subseteq \ldots$ by induction, and setting $A = \cup_n A_n$. We use the claim to verify that $A = t$ holds. Uniqueness is easily verified as before. QED

The BRT fixed point theorem is closely associated with the standard contraction mapping theorem.

CONTRACTION MAPPING THEOREM. Let (X,d) be a compact metric space, $c \in [0,1)$, and $T:X \to X$ be continuous. Assume that for all $x,y \in X$, $d(T(x),T(y)) \leq c \bullet d(x,y)$. Then T has a unique fixed point.

We can apply the Contraction Mapping Theorem to prove the BRT Fixed Point Theorem, using the usual compact metric space on POW(N). This metric is given by

$$d(B,C) = 2^{-\min(B\Delta C)} \text{ if } B \neq C;\ 0 \text{ otherwise.}$$

The claim in the proof of the BRT Fixed Point Theorem establishes the required inequality for the mapping t(A) with constant $c = 1/2$.

We now present a useful sufficient condition on $f:X^k \to X$ so that f has a unique complementation. The sufficiency of the criterion follows immediately from the Complementation Theorem (for well founded relations, with uniqueness) proved earlier in this section.

DEFINITION 1.3.11. Define the relation R(f) on X by

R(f)(x,y) if and only if
y is the value of f at some arguments that include x.

THEOREM 1.3.9. Every $f:X^k \to X$, where R(f) is well founded, has a unique complementation.

Proof: Let $f:X^k \to X$, where $R(f)$ is well founded. We claim that $f \in SD(R)$. To see this, note that for all $1 \le i \le k$, $f(x_1,\ldots,x_k)$ is the value of f at some arguments that include x_i. Hence f has a unique complementation by Theorem 1.3.1. QED

Note that in Lemma 1.3.5, the f has a (very) well founded $R(f)$. Hence the existence of a unique complementation in Lemma 1.3.5 follows immediately from Theorem 1.3.9.

We now prove a Continuous Complementation Theorem.

We say that $f:E^k \to \Re$, $E \subseteq \Re$, is strictly dominating if and only if for all $x \in E^k$, $|f(x)| > |x|$. Here we take $|\ |$ to be the sup norm.

CONTINUOUS COMPLEMENTATION THEOREM (with uniqueness). Every strictly dominating continuous $f:E^k \to E$, where $E \subseteq \Re$ is closed, has a unique complementation.

Proof: Let f be as given. By Theorem 1.3.9 it suffices to prove that $R(f)$ is well founded. Let $\ldots\ x_3\ R(f)\ x_2\ R(f)\ x_1$ be an infinite backwards chain living in E. Then $|x_1| > |x_2| > \ldots$. Let $w_1,w_2,\ldots \in E^k$, where for all $i \ge 1$, $x_i = f(w_i)$ and x_{i+1} is a coordinate of w_i. Then for all $i \ge 1$, $|x_i| > |w_i| \ge |x_{i+1}|$. In particular, $|w_1| > |w_2| > \ldots$. Note that the $|x_i| = |f(w_i)|$ and the $|w_i|$ are both strictly decreasing and have the same inf, α. Note that α is the unique limit point of the $|f(w_i)|$ and of the $|w_i|$. Since the w_i are bounded, let w be a limit point of the w_i. Since E is closed, $w \in E^k$. Clearly $|w| = \alpha$. By continuity, $f(w)$ is a limit point of the $f(w_i)$. Hence $|f(w)|$ is a limit point of the $|f(w_i)|$. Therefore $|f(w)| = \alpha$. I.e., $|f(w)| = |w| = \alpha$. This violates that f is strictly dominating. QED

If we strengthen strictly dominating, then we no longer need continuity.

DEFINITION 1.3.12. We say that $f:E^k \to \Re$, $E \subseteq \Re$, is shift dominating if and only if there exists a constant $c > 0$ such that for all $x \in E^k$, $|f(x)| > |x| + c$.

SHIFT DOMINATING COMPLEMENTATION THEOREM (with uniqueness). Every shift dominating $f:E^k \to E$, $E \subseteq \Re$, has a unique complementation.

Proof: Let f be as given. A backwards chain in R(f) creates vectors $x_1,x_2,\ldots$ such that each $|x_i| > |x_{i+1}| + c$. This is obviously impossible. Hence R(f) is well founded. Apply Theorem 1.3.9. QED

The Complementation Theorem is closely related to an important development in digraph theory.

DEFINITION 1.3.13. A digraph (directed graph) is a pair G = (V,E), where V = V(G) is a set of vertices and E = E(G) is a set of edges. $E(G) \subseteq V^2$ is required. We say that x is G connected to y if and only if $(x,y) \in E(G)$.

The key definition is that of a kernel (see [Be85]) and its dual notion, dominator.

DEFINITION 1.3.14. A kernel K of G is a subset of V(G) such that

i. There is no edge connecting any two elements of K. In particular, there is no loop with vertex from K.
ii. Every element of V(G)\K is G connected to an element of K.

DEFINITION 1.3.15. A dominator D of G is a subset of V(G) such that

i. There is no edge connecting any two elements of D. In particular, there is no loop with vertex from D.
ii. Every element of D is G connected to an element of V(G)\D.

It is obvious that K is a kernel of G if and only if the following holds:

$x \in K$ if and only if
x is not G connected to any element of K.

Also D is a dominator of G if and only if the following holds:

$x \in D$ if and only if
no element of D is G connected to x.

Also let G be a digraph and G* be the dual of G; i.e., the same digraph with the arrows reversed. Then the kernels of

G are the same as the dominators of G*, and the dominators of G are the same as the kernels of G*.

Dominators are explicitly connected with the Complementation Theorem in the unary case $f:X \to X$. We can think of f as a graph G whose vertex set is X and whose edges are the $(x,f(x))$. Then the complementations of f are the same as the dominators of G.

DEFINITION 1.3.16. A dag is a directed acyclic graph. I.e., a digraph with no cycles. A cycle (in a digraph) is a finite path which starts and ends at the same place.

The following is due to von Neumann in [VM44]. Also see [Be85].

THEOREM 1.3.10. Every finite dag has a unique kernel and a unique dominator.

Proof: Since the dual of an acyclic graph is acyclic, it suffices to prove that there is a unique kernel.

Let (V,G) be a finite dag. We can assume that V(G) is nonempty. We inductively define $V_0,V_1,V_2,\ldots$, where for every i, V_i is the set of vertices outside $V_0 \cup \ldots \cup V_{i-1}$ which G connect only to vertices in $V_0 \cup \ldots \cup V_{i-1}$. In particular, V_0 is the set of vertices that do not G connect to any vertex. Since G is a dag, V_0 is nonempty. Obviously the V's are eventually empty, and are pairwise disjoint. So we write $V_0,V_1,\ldots,V_n$, $n \geq 0$, where these V's are nonempty and $V_{n+1} = \emptyset$.

We claim that $V(G) = V_0 \cup \ldots \cup V_n$. Otherwise, let $x \notin V_0 \cup \ldots \cup V_n$. Since $x \notin V_{n+1}$, x G connects to some $y \notin V_0 \cup \ldots \cup V_n$. We can continue this process, obtaining an infinite chain of G connections. This contradicts that V(G) is finite.

Now define $K \cap V_i$ by induction on $i = 0,\ldots,n$. Take $x \in K \cap V_i$ if and only if x is not G connected to any element of $V_0 \cup \ldots \cup V_{i-1}$. By the construction of the V's, we see that $x \in K$ if and only if x is not G connected to any element of K. QED

This is not true for arbitrary dag's (as is well known).

THEOREM 1.3.11. There is a countable dag without a kernel and without a dominator.

Proof: We first construct a countable dag G without a kernel.

Let G be the digraph with V(G) = N and whose edges are the (n,m) where n < m. Let K be a kernel of G. We have $n \in K \leftrightarrow$ n is not connected to any element of K $\leftrightarrow$ K has no element > n. If K is empty then $0 \in K$. Hence K is nonempty. Let $n \in K$. Then K has no elements > n. In particular, $n+1 \notin K$. Hence n+1 is G connected to some element of K. Therefore K has an element > n+1. This is a contradiction.

For the final claim, let G* be the dual of G. Then G* has no dominator. Let H be the disjoint union of G and G*. I.e., $V(H) = V(G) \cup V(G^*)$ and $E(H) = E(G) \cup E(G^*)$, where we assume $V(G) \cap V(G^*) = \emptyset$. Then any kernel of H intersected with G is a kernel of G, and any dominator of H intersected with G* is a dominator of G. Therefore H is a countable dag without a kernel and without a dominator. QED

We mention an old but rather striking result of [Ri46].

THEOREM 1.3.12. Every finite graph without cycles of odd length has a kernel and a dominator.

Here we do not have uniqueness since the two vertex digraph with each vertex connected to the other, has no cycles of odd length, and two obvious kernels - the singletons – which are also dominators.

The book [HHS98a] has an extensive bibliography that includes many papers on kernels in graphs. Also see [HHS98b], [GLP98].

Theorem 1.3.10 has the following known extension to infinite digraphs.

THEOREM 1.3.13. Every digraph without an infinite walk $x_0 \to x_1 \to \ldots$ has a unique kernel.

Proof: We can either give a proof analogous to that of Theorem 1.3.1 (as a referee has done), or we can conveniently derive this from Theorem 1.3.1. Let G be a digraph with no infinite walk $x_0 \to x_1 \to \ldots$. Let R be the binary relation $R(x,y) \leftrightarrow (y,x) \in E(G)$; i.e., $y \to x$ in G. Then R is well founded.

In fact, we need to use an extension R' of R. We introduce a new copy of every vertex in G, and make all of these copies R' predecessors of every vertex in G. These copies have no R' predecessors. Also introduce new points $\infty,\infty+1,\infty+2,...$, each an R' predecessor of the next, all of which are R' successors of all vertices in G and their copies. Note that any two elements of fld(R') have a common successor.

Define $f:\text{fld}(R')^2 \to V(G)$ by cases.

case 1. $x \in V(G)$, y is a copy of some $z \in V(G)$ with $R(x,z)$. Then define $f(x,y) = z$.

case 2. otherwise. Define $f(x,y)$ to be any R' successor of x,y.

By Theorem 1.3.1, let A be a complementation of f. Note that all of the copies of vertices in G lie in A. Hence if x is G connected to an element of A then $x \in fA$, $x \notin A$.

On the other hand, suppose $x \in V(G)$ is not G connected to any element of A. Then $x \notin fA$, $x \in A$. This establishes that $A \cap V(G)$ is a kernel of G.

To show that all kernels of G are the same, let K,K' be kernels of G. Assume that $K \Delta K'$ is nonempty, and choose $x \in K \Delta K'$ such that x is not G connected to any element of $K \Delta K'$. By symmetry, we can assume that $x \in K$, $x \notin K'$. Then x is not G connected to any element of K, and x is G connected to some element y of K'. Clearly $y \notin K \Delta K'$, $y \in K$. This is a contradiction. QED