Review

- Number Theory
- Natural Numbers with Successor
- Natural Numbers with Successor and Less-Than
- Presburger Arithmetic

Outline

- A Subtheory of Number Theory
- Representable Relations
- Church's Thesis Revisited
- Representable Functions
- A Catalog of Representable Sets

A Subtheory of Number Theory

Let us now add $\times$ and E to our set of symbols. We now have the full language of number theory.

The intended model is $N = (\mathcal{N}; 0, S, <, +, \times, E)$.

We could do with fewer symbols. For example, 0, S, $<$, and E are all definable in $(\mathcal{N}; +, \times)$. However, having all these parameters will simplify some of the proofs.

As we will see, $Th\, N$ is niether decidable nor axiomatizable. This is not at all obvious and will require new and clever techniques to show.

We begin with a finitely axiomatizable subtheory.

Consider the following set A_E of axioms.

- S1. $\forall x\, \mathbf{S}x \neq \mathbf{0}$.
- S2. $\forall x \forall y\, (\mathbf{S}x = \mathbf{S}y \rightarrow x = y)$.
- L1. $\forall x \forall y\, (x < \mathbf{S}y \leftrightarrow x \leq y)$
- L2. $\forall x\, x \not< \mathbf{0}$
- L3. $\forall x \forall y\, (x < y \vee x = y \vee y < x)$
- A1. $\forall x\, x + \mathbf{0} = x$
- A2. $\forall x \forall y\, x + \mathbf{S}y = \mathbf{S}(x + y)$
- M1. $\forall x\, x \times \mathbf{0} = \mathbf{0}$
- M2. $\forall x \forall y\, x \times \mathbf{S}y = x \times y + x$
- E1. $\forall x\, xE\mathbf{0} = \mathbf{S0}$
- E2. $\forall x \forall y\, xE(\mathbf{S}y) = (xEy) \times x$

Lemma

1. $A_E \vdash \forall x\, x \not< \mathbf{0}$.
2. $A_E \vdash \forall x\, (x < \mathbf{S}^{k+1}\mathbf{0} \leftrightarrow x = \mathbf{S}^0\mathbf{0} \vee \ldots \vee x = \mathbf{S}^k\mathbf{0})$.

Proof

(1) is from L2. For (2), we use regular mathematical induction. For the base case, we must show

$$x < \mathbf{S0} \leftrightarrow x = \mathbf{0}$$

which follows from L1 and L2.

For the inductive step, apply L1 to get

$$x < \mathbf{S}^{k+1}\mathbf{0} \leftrightarrow x < \mathbf{S}^{k}\mathbf{0} \vee x = \mathbf{S}^{k}\mathbf{0}.$$

The result then follows from the inductive hypothesis.

Lemma

For any variable-free term t, there is a unique natural number n such that $A_E \vdash t = \mathbf{S}^n\mathbf{0}$.

Proof

Uniqueness is by S1 and S2. Existence is a simple induction argument on t.

Theorem

For any quantifier-free sentence τ true in N, $A_E \vdash \tau$.

Proof

Homework!

A Subtheory of Number Theory

To simplify things, we introduce the following notation for substitution:

$\phi(t) = \phi_t^{v_1}$,

$\phi(t_1, t_2) = \phi_{t_1\ t_2}^{v_1\ v_2}$,

etc.

In cases where x is not substitutable for v_1 in ϕ, we assume $\phi(x) = \psi_x^{v_1}$ where ψ is a suitable alphabetic variant of ϕ.

Also, we will make use of the following fact:

For a formula ϕ in which at most $v_1, \ldots, v_n$ occur free and for natural numbers $a_1, \ldots, a_n$,

$\models_N \phi[[a_1, \ldots, a_n]]$ iff $\models_N \phi(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_n}\mathbf{0})$.

We can now extend our results about what formulas are deducible in A_E. An *existential* formula is one of the form $\exists\, x_1 \ \cdots \exists\, x_k\ \theta$ where θ is quantifier-free.

Corollary

If τ is an existential sentence true in N, then $A_E \vdash \tau$.

Proof

If $\exists\, v_1\ \exists\, v_2\ \theta$ is true in N, then for some $m, n \in \mathcal{N}$, $\theta(\mathbf{S}^m\mathbf{0}, \mathbf{S}^n\mathbf{0})$ is true in N. By the previous theorem, this formula is deducible from A_E. But it in turn derives $\exists\, v_1\ \exists\, v_2\ \theta$, so $A_E \vdash \exists\, v_1\ \exists\, v_2\ \theta$.

A *universal* formula is one of the form $\forall\, x_1 \ \cdots \forall\, x_k\ \theta$ where θ is quantifier-free. There are some universal sentences that are true in N, but are not deducible from A_E.

Representable Relations

Let R be an m-ary relation on $\mathcal{N}$.

R is definable in N iff there exists some formula ϕ in which only $v_1, \ldots, v_n$ occur free such that

$\langle a_1, \ldots, a_m \rangle \in R$ iff $\models_N \phi[[a_1, \ldots, a_m]]$.

Notice that this is equivalent to $\models_N \phi(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0})$.

So, if ϕ defines R, it follows that

$\langle a_1, \ldots, a_m \rangle \in R \Rightarrow \models_N \phi(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0})$, and
$\langle a_1, \ldots, a_m \rangle \notin R \Rightarrow \models_N \neg\phi(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0})$.

Representability is the dual notion of *definability* in which truth in a model is replaced by deducibility in a theory.

We say that ϕ *represents* R in a theory T (in a language including $\mathbf{0}$ and $\mathbf{S}$) iff for every $a_1, \ldots, a_m \in \mathcal{N}$:

$\langle a_1, \ldots, a_m \rangle \in R \Rightarrow \phi(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0}) \in T$, and
$\langle a_1, \ldots, a_m \rangle \notin R \Rightarrow (\neg\phi(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0})) \in T$.

A relation is *representable* in T iff there exists some formula that represents it in T.

A formula ϕ in which at most $v_1, \ldots, v_m$ occur free is *numeralwise determined* by A_E iff for every m-tuple $a_1, \ldots, a_m$ of natural numbers, either

$A_E \vdash \phi(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0})$, or $A_E \vdash \neg\phi(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0})$.

Theorem

A formula ϕ represents a relation R in *Cn* A_E iff

1. ϕ is numeralwise determined by A_E, and
2. ϕ defines R in N.

Proof

Suppose ϕ represents R in *Cn* A_E. (1) holds by definition. (2) holds by soundness and the fact that N is a model of A_E. On the other hand, given (1) and (2), we have

$$\begin{array}{lll} \langle a_1, \ldots, a_m \rangle \in R \quad \Rightarrow \quad \models_N \phi(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0}) & \text{by (2)} \\ \Rightarrow \quad A_E \nvdash \neg\phi(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0}) & \text{since } N \models A_E \\ \Rightarrow \quad A_E \vdash \phi(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0}) & \text{by (1)} \end{array}$$

The case for $\langle a_1, \ldots, a_m \rangle \notin R$ is similar.

Church's Thesis Revisited

Representability can be linked to decidability.

Theorem

If R is representable in a consistent axiomatizable theory, then R is decidable.

Proof

Suppose R is represented by ϕ in a consistent axiomatizable theory T. We know that T is effectively enumerable. Thus, a decision procedure is to enumerate T until either $\phi(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0})$ or $\neg\phi(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0})$ appears. Since one of these has to be in T by definition of representability, the procedure will eventually terminate.

We now define the fundamental notion of *recursive* relations.

A relation R on the natural numbers is *recursive* iff it is representable in some consistent finitely axiomatizable theory (in a language with $\mathbf{0}$ and $\mathbf{S}$).

Earlier, we gave Church's thesis as the assertion that all models of computation are either equivalent to or less powerful than what can be done on a computer with infinite time and memory. We can now be more precise.

Church's thesis

A relation is decidable iff it is recursive.

The definition of recursive relations is one of many equivalent formalizations of the notion of decidability.

Our goal is to show that recursiveness is equivalent to representability in $Cn\,A_E$. This is no small task and will require a significant amount of work. We begin with some basic facts about representability.

Numeralwise Determined Formulas

We just showed that a relation is representable in *Cn* A_E if we can find a formula that defines it in N and is numeralwise determined by A_E. The following theorem is helpful for establishing numeralwise determination.

Theorem

1. Any atomic formula is numeralwise determined by A_E.
2. If ϕ and ψ are numeralwise determined by A_E, then so are $\neg\phi$ and $\phi \to \psi$.
3. If ϕ is numeralwise determined by A_E, then so are the following formulas (obtained by "bounded quantification"):

   $\forall x\,(x < y \to \phi)$ and $\exists x\,(x < y \wedge \phi)$.

Proof sketch The first two are easy. The $\forall$ case follows from the $\exists$ case. The $\exists$ case can be shown by using the fact that ϕ is numeralwise determined and considering two cases, one in which ϕ is true for some $x < y$ and one in which ϕ is false for every $x < y$.

Representable Functions

Often functions are more convenient than relations. Suppose $f : \mathcal{N}^m \to \mathcal{N}$ is an m-place function on the natural numbers.

A formula ϕ in which at most $v_1, \ldots, v_{m+1}$ occur free *functionally represents* f in the theory *Cn* A_E iff for every $a_1, \ldots, a_m$ in $\mathcal{N}$,

$$A_E \vdash \forall v_{m+1}\ \left[\phi(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0}, v_{m+1}) \leftrightarrow v_{m+1} = \mathbf{S}^{f(a_1,\ldots,a_m)}\mathbf{0}\right].$$

Theorem

If ϕ functionally represents f in $Cn\, A_E$, then it also represents f as a relation in $Cn\, A_E$.

Proof

Since ϕ functionally represents f, we have for any $a_1, \ldots, a_{m+1}$,

$$A_E \vdash \phi(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0}, \mathbf{S}^{a_{m+1}}\mathbf{0}) \leftrightarrow \mathbf{S}^{a_{m+1}}\mathbf{0} = \mathbf{S}^{f(a_1,\ldots,a_m)}\mathbf{0}.$$

Since we can easily deduce whether the right half is true or false, it follows that we can deduce the left half or the negation of the left half.

The converse of the previous theorem is not true in general. A formula ϕ may in fact represent a function f as a relation, but the stronger requirement of uniqueness may not be deducible.

However, by modifying ϕ, we can get a formula that works.

Theorem

If f is a function that is representable as a relation in $Cn\, A_E$, then we can find a formula ϕ that functionally represents f in $Cn\, A_E$.

Proof Idea

If θ represents f as a relation, then take ϕ to be

$$\theta(v_1, \ldots, v_m, v_{m+1}) \wedge \forall z\, (z < v_{m+1} \rightarrow \neg\theta(v_1, \ldots, v_m, z)).$$

Consider the equation $v_{m+1} = t$ where the free variables of t are among $v_1, \ldots, v_m$. If f is a function which denotes the value of t at $\langle a_1, \ldots, a_m \rangle$, then clearly the equation defines f in N.

Also, since we showed that any atomic formula is numeralwise determined by A_E, it follows that the equation represents f as a relation.

Finally, since $\forall v_{m+1}\ \left[v_{m+1} = t(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0}) \leftrightarrow v_{m+1} = \mathbf{S}^{f(a_1,\ldots,a_m)}\mathbf{0}\right]$ is logically equivalent to $t(\mathbf{S}^{a_1}\mathbf{0}, \ldots, \mathbf{S}^{a_m}\mathbf{0}) = \mathbf{S}^{f(a_1,\ldots,a_m)}\mathbf{0}$, which is easily deducible in N, the equation functionally represents f as well.

As a result, we have the following:

1. The successor function is functionally represented by $v_2 = \mathbf{S}v_1$.
2. The m-place constant function with value b is functionally represented by $v_{m+1} = \mathbf{S}^b\mathbf{0}$.
3. Projection on variable i is functionally represented by $v_{m+1} = v_i$.
4. Addition, multiplication, and exponentiation are represented by $v_3 = v_1 + v_2$, $v_3 = v_1 \times v_2$, and $v_3 = v_1 E v_2$.

Theorem

Let g be an n-place function, and let $h_1, \ldots, h_n$ be m-place functions, and let f be defined by

$f(a_1, \ldots, a_m) = g(h_1(a_1, \ldots, a_m), \ldots, h_n(a_1, \ldots, a_m))$. Then, given formulas functionally representing g and $h_1, \ldots, h_n$, we can find a formula that functionally represents f.

Proof Idea

Suppose g is functionally represented by ψ and h_i by θ_i. We can represent f as

$\forall y_1\ \ldots\ \forall y_n\ (\theta_1(v_1, \ldots, v_m, y_1) \rightarrow \ldots \rightarrow \theta_n(v_1, \ldots, v_m, y_n) \rightarrow \psi(y_1, \ldots, y_n, v_{m+1}))$

or

$\exists y_1\ \ldots\ \exists y_n\ (\theta_1(v_1, \ldots, v_m, y_1) \wedge \ldots \wedge \theta_n(v_1, \ldots, v_m, y_n) \wedge \psi(y_1, \ldots, y_n, v_{m+1}))$.

Theorem

If the $m+1$-place function g is representable and if for every $a_1, \ldots, a_m$ there is a b such that $g(a_1, \ldots, a_m, b) = 0$, then we can find a formula that represents the m-place function f, where $f(a_1, \ldots, a_m) =$ the least b such that $g(a_1, \ldots, a_m, b) = 0$.

Using traditional notation, we can write this as $f(\vec{a}) = \mu b\,[g(\vec{a}, b) = 0]$.

Proof

We have that $f(\vec{a}) = b$ iff $g(\vec{a}, b) = 0$ and for every $c < b, g(\vec{a}, c) \neq 0$. If ψ represents g, then a formula representing f is simply:

$$\psi(v_1, \ldots, v_m, v_{m+1}, \mathbf{0}) \wedge \forall\, y\, (y < v_{m+1} \rightarrow \neg\psi(v_1, \ldots, v_m, y, \mathbf{0})).$$

A Catalog of Representable Sets

1. A relation R is representable iff its characteristic function K_R is ($K_R(\vec{a}) = 1$ if $\vec{a} \in R$, 0 otherwise).
2. If R is a representable binary relation and f,g are representable functions, then $\{\vec{a} |\ \langle f(\vec{a}), g(\vec{a})\rangle \in R\}$ is representable.
3. If R is a representable binary relation, then so is $P = \{\langle a, b\rangle \mid \text{for some } c \leq b, \langle a, c\rangle \in R\}$.
4. The divisibility relation $\{\langle a, b\rangle \,|a \text{ divides } b \text{ in } \mathcal{N}\}$ is representable.
5. The set of primes is representable.
6. The set of pairs of adjacent primes is representable.
7. The function whose value at a is p_a, the $(a+1)^{st}$ prime, is representable.

We can use this last fact to encode a finite sequence of numbers into a single number as follows:

$$\langle a_0, \ldots, a_m\rangle = p_0^{a_0+1} \cdots p_m^{a_m+1}.$$

8. For each m, the function whose value at $a_0, \ldots, a_m$ is $\langle a_0, \ldots, a_m \rangle$ is representable.
9. There is a representable function (whose value at $\langle a, b \rangle$ is written $(a)_b$) such that for $b \leq m$, $(\langle a_0, \ldots, a_m \rangle)_b = a_b$.
10. Say that b is a *sequence number* iff for some $m \geq -1$ and some $a_0, \ldots, a_m$, $b = \langle a_0, \ldots, a_m \rangle$. The set of sequence numbers is representable.
11. There is a representable function lh such that $lh \langle a_0, \ldots, a_m \rangle = m + 1$.
12. There is a representable function (whose value at $\langle a, b \rangle$ is called the *restriction* of a to b, written $a \restriction b$) such that for any $b \leq m + 1$, $\langle a_0, \ldots, a_m \rangle \restriction b = \langle a_0, \ldots, a_{b-1} \rangle$.
13. (Primitive recursion) With a $k+1$-place function f we associate another function $\overline{f}$ such that $\overline{f}(a, b_1, \ldots, b_k)$ encodes the values of $f(j, b_1, \ldots, b_k)$ for all $j < a$. Specifically, let $\overline{f}(a, \vec{b}) = \left\langle f(0, \vec{b}), \ldots, f(a-1, \vec{b}) \right\rangle$.

Theorem

Let g and h be representable functions, and assume that $f(0, b) = g(b)$, $f(a+1, b) = h(f(a, b), a, b)$. Then f is representable.

14. For a representable function F, the function whose value at a, $\vec{b}$ is

$$\prod_{i<a} F(i, \vec{b})$$

is representable. Similarly for $\sum_{i<a} F(i, \vec{b})$

15. Define the *concatenation* of a and b, $a * b$, as

$$a * b = a \prod_{i<lh(b)} p_{i+lh(a)}^{(b)_i+1}.$$

This is a representable function of a and b, and $\langle a_1, \ldots, a_m \rangle * \langle b_1, \ldots, b_n \rangle = \langle a_1, \ldots, a_m, b_1, \ldots, b_n \rangle$.

16. Let $*_{i<a} f(i) = f(0) * f(1) * \cdots * f(a-1)$. For a representable function F, the function whose value at a, $\vec{b}$ is $*_{i<a} F(i, \vec{b})$ is representable.