

Philosophy 532 and Philosophy 536 were the two seminars I presented while on leave at the Princeton University Philosophy Department, Fall, 2002.

Harvey M. Friedman

PHILOSOPHY 536
PHILOSOPHY OF MATHEMATICS
LECTURE 1
9/25/02

1. LOGIC.

What are we trying to do with logic?

In this seminar, we concentrate on mathematical reasoning. It appears that certain reasoning principles are used not only in mathematics, but in a very wide variety of contexts outside mathematics.

On the other hand, certain other principles of mathematical reasoning seem peculiar to mathematics.

These are normally in the form of principles of set existence.

This distinction between logic and mathematics is subject to various criticisms and can be given various defenses. Nevertheless, the division seems natural enough and is commonly adopted in presentations of the standard foundations for mathematics.

In particular, when presenting the crucial formal system ZFC of Zermelo Frankel set theory with the axiom of choice, one writes down 9 axioms (some are axiom schemes), and says "the axioms and rules of first order predicate calculus with equality and epsilon are understood".

What we try to do in logic (of the sort under consideration) is to first identify a family of statement forms. In a statement form, certain components are identified with special names referring to "logical operations", and other components are identified as atomic, with no internal structure.

The idea is that the meaning of a statement depends, uniformly, on the meaning of the atomic components and the way in which the logical operations operate on meanings.

Two primary examples of "logics" stand out in f.o.m. so much that in this seminar we will avoid the serious difficulties involved in talking about "logics" in any substantial generality.

These are propositional calculus and predicate calculus. The first is subsumed by the second, but there are good reasons to discuss it first.

Incidentally, sometimes the so called higher order predicate calculus is considered rather than what we mean by (first order) predicate calculus. For our purposes, this should be reduced to (first order) predicate calculus together with a dose of set theory. Because of the set theoretic aspect, it is extremely ill behaved in comparison with (first order) predicate calculus.

There is another brand of propositional calculus and predicate calculus called intuitionistic propositional calculus and intuitionistic predicate calculus. Current mathematics is far from intuitionistic, although there is no doubt that significant fragments of mathematics are intuitionistic, and that it is quite interesting to see what can or cannot be proved intuitionistically. This has ramifications for the existence of algorithms associated with mathematical theorems. We will only briefly touch on this today, and it will play no (little) role later in the seminar.

Since propositional calculus, PROP, is a primary example of a logic, it has a syntactic side and a semantic side which must not be confused.

On the syntactic side, we need to specify the vocabulary. The symbols of PROP are taken to be

- i) the "connectives" \neg \wedge \vee \rightarrow \leftrightarrow ;
- ii) the "atoms" p_n , where $n \geq 0$.

These five connectives are read: not, and, or, if then, iff.

We have to describe what the statements look like. They are defined inductively as follows.

- 1) any atom is a formula of PROP;
- 2) if A,B are formulas of PROP, then so are $\neg(A)$, $(A \vee B)$, $(A \wedge B)$, $(A \supset B)$, $(A \equiv B)$;
- 3) the only way to be a formula of PROP is through 1),2).

This kind of definition is completely typical of the grammar of formal languages. Such grammars have been treated systematically in great generality in the formal language world (principally part of the computer science community).

There are two standard ways of making this rigorous, one from "above", and one from "below".

From above, we define the formulas of PROP as the elements of the least set of finite strings of symbols of PROP that reflect 1) and 2). One proves that there is such a least set.

From below, we consider finite rooted trees whose terminal vertices are labeled with atoms, and whose nonterminal vertices are suitably labeled with connectives. The formulas of PROP are those finite strings of symbols of PROP that correspond to such "parse trees" in the obvious way.

A unique parsing theorem needs to be proved. In fact, there is a well understood theory concerning conventions for the reduction of parentheses needed in order to have unique parsing - so called precedence grammar theory.

So far we have only discussed the syntactic side. Coming now to the semantic side, we want to discuss what it means for a given set of formulas of PROP to logically imply a given formula of PROP.

This is defined in terms of truth assignments. A truth assignment is a mapping from the set of atoms to the two element set $\{T,F\}$.

We inductively define $\text{Sat}(A,f)$, which means that A is satisfied under the truth assignment f. Truth assignments are thought of as interpretations of PROP.

The inductive definition proceeds as follows.

$\text{Sat}(p_n, f)$ iff $f(p_n) = T$.
 $\text{Sat}(\neg A, f)$ iff not $\text{Sat}(A, f)$.
 $\text{Sat}(A \wedge B, f)$ iff $\text{Sat}(A, f)$ and $\text{Sat}(B, f)$.
 $\text{Sat}(A \vee B, f)$ iff $\text{Sat}(A, f)$ or $\text{Sat}(B, f)$.
 $\text{Sat}(A \supset B, f)$ iff not $\text{Sat}(A, f)$ or $\text{Sat}(B, f)$.
 $\text{Sat}(A \equiv B, f)$ iff $(\text{Sat}(A, f) \text{ and } \text{Sat}(B, f))$ or $(\text{not } \text{Sat}(A, f)$
 and not $\text{Sat}(B, f))$.

Let X be a set of formulas of PROP and A be a formula of PROP. We write $\text{Sat}(X, f)$ to indicate that $\text{Sat}(B, f)$ holds for all $B \in X$. We say that X logically implies A iff for all f , if $\text{Sat}(X, f)$ then $\text{Sat}(A, f)$.

We say that A is a tautology iff for all f , $\text{Sat}(A, f)$.

There is a set of axioms and rules of inference which is complete in the following sense.

WEAK COMPLETENESS. Every tautology is provable using these axioms and rules.

WEAK SOUNDNESS. Every formula of PROP provable using these axioms and rules is a tautology.

STRONG COMPLETENESS. If a given set of formulas of PROP logically implies a given formula of PROP then that formula can be derived from the set using these axioms and rules.

STRONG SOUNDNESS. If a given formula of PROP can be derived from a given set of formulas of PROP using these axioms and rules, then that set logically implies that formula.

Weak and strong completeness are equivalent because of a purely semantic fact.

SEMANTIC FINITENESS. A given set of formulas of PROP logically implies a given formula of PROP iff some finite subset of the set does.

There are other logical relations between these standard facts.

There are a number of such axioms and rules of inferences for PROP in textbooks and elsewhere, none of which are all that memorably neat. But here is a (new?) twist on this axiomatization problem.

We will give a Hilbert style axiomatization. We use two rules:

- a. Modus ponens. From A and $A \rightarrow B$ derive B .
- b. Substitution. From any axiom A derive every substitution instance of A .

But what of the axioms?

- c. All tautologies with at most 6 occurrences of atoms.

It would be interesting to see just how small a number we can use instead of 6.

We now move on to predicate calculus. Here we use variables x_n , $n \geq 0$, constant symbols c_n , $n \geq 0$, relation symbols R_m^n of arity $n \geq 1$, where $m \geq 0$, and function symbols F_m^n of arity $n \geq 1$, where $m \geq 0$.

Terms are inductively defined using the constant and function symbols as follows.

1. Each c_n is a term.
2. If t_1, \dots, t_n are terms then $F_m^n(t_1, \dots, t_n)$ is a term.

Atomic formulas are of the form

$$R_m^n(t_1, \dots, t_n).$$

In predicate calculus with equality, the atomic formulas are of the forms

$$R_m^n(t_1, \dots, t_n)$$

$$s = t$$

where s, t, t_1, \dots, t_n are terms.

The formulas are inductively defined as follows.

- a. Every atomic formula is a formula.
- b. If A, B are formulas then so are $(\neg A)$, $(A \rightarrow B)$, $(A \wedge B)$, $(A \vee B)$, $(A \leftrightarrow B)$, $(\forall x_n) (A)$, $(\exists x_n) (B)$.

The usual semantics is in terms of relational structures. A relational structure is a system $M = (D, c_n^*, R_m^n, F_m^n)$, where D is a nonempty set and the c_n^* are elements of D , the R_m^n are n -ary relations on D , and the F_m^n are n -ary functions from D into D .

To give the usual semantics, we need to use M -assignments. These are functions f from the set of all variables into $D = \text{dom}(M)$.

What we are after is the definition of $\text{Sat}(M, A, f)$. I.e., the formula A holds in the structure M with the M -assignment f .

We first have to define $\text{Val}(M, t, f)$, where t is a term and f is an M -assignment.

- i. $\text{Val}(M, x_n, f) = f(x_n)$;
- ii. $\text{Val}(M, c_n, f) = c_n^*$;
- iii. $\text{Val}(M, F_m^n(t_1, \dots, t_n)) = F_m^n(\text{Val}(M, t_1, f), \dots, \text{Val}(M, t_n, f))$.

We can now define $\text{Sat}(M, A, f)$ for atomic formulas A , as follows.

$$\text{Sat}(M, R_m^n(t_1, \dots, t_n), f) \text{ iff } R_m^n(\text{Val}(M, t_1, f), \dots, \text{Val}(M, t_n, f)).$$

$$\text{Sat}(M, s = t, f) \text{ iff } \text{Val}(M, s, f) = \text{Val}(M, t, f).$$

Finally, we define $\text{Sat}(M, A, f)$ for all formulas A as follows.

- a. $\text{Sat}(M, (\neg A), f) \text{ iff not } \text{Sat}(M, A, f)$;
- b. $\text{Sat}(M, (A \wedge B), f) \text{ iff } \text{Sat}(M, A, f) \text{ and } \text{Sat}(M, B, f)$;
- c. $\text{Sat}(M, (A \vee B), f) \text{ iff } \text{Sat}(M, A, f) \text{ or } \text{Sat}(M, B, f)$;
- d. $\text{Sat}(M, (A \rightarrow B), f) \text{ iff not } \text{Sat}(M, A, f) \text{ or } \text{Sat}(M, B, f)$;
- e. $\text{Sat}(M, (A \leftrightarrow B), f) \text{ iff } (\text{Sat}(M, A, f) \text{ and } \text{Sat}(M, B, f)) \text{ or } (\text{not } \text{Sat}(M, A, f) \text{ and not } \text{Sat}(M, B, f))$;
- f. $\text{Sat}(M, (\forall x_n)(A), f) \text{ iff for all } y \in A, \text{Sat}(M, A, f[n/y])$;
- g. $\text{Sat}(M, (\exists x_n)(A), f) \text{ iff there exists } y \in A, \text{Sat}(M, A, f[n/y])$.

Here $f[n/y]$ is the same as f except that at x_n it is y (instead of $f(x_n)$).

Let X be a set of formulas and A be a formula. A is valid if and only if for all structures M and M -assignments f , $\text{Sat}(M, A, f)$.

We write $\text{Sat}(M, X, f)$ if and only if for all $B \in X$, $\text{Sat}(M, B, f)$.

We say that X logically implies A if and only if for all structures M and M -assignments f , if $\text{Sat}(M, X, f)$ then $\text{Sat}(M, A, f)$.

There are nice axioms and rules of inference for predicate calculus with or without equality. Again we provide a new twist.

WEAK COMPLETENESS. Every valid formula is provable using these axioms and rules.

WEAK SOUNDNESS. Every formula provable using these axioms and rules is valid.

STRONG COMPLETENESS. If a given set of formulas logically implies a given formula then that formula can be derived from the set using these axioms and rules.

STRONG SOUNDNESS. If a given formula can be derived from a given set of formulas using these axioms and rules, then that set logically implies that formula.

We will give a Hilbert style axiomatization. We use two rules:

- a. Modus ponens. From A and $A \rightarrow B$ derive B .
- b. Substitution. From any axiom A derive every substitution instance of A .
- c. Universal generalization. From any axiom A derive $(\forall x_n)(A)$.

Here we have to be much more careful about what we mean by substitution. I will clarify this carefully later (not today).

What axioms?

- d. All valid formulas with at most n occurrences of signs other than parentheses.

I have to experiment to see just what are the most appropriate forms of d to use.

The point is that very simple formulas for d will do, and one can then take all formulas of small size. This is now a recurrent theme in a number of things I work on now. E.g., in

Phil 532, I alluded to using this idea to try to uniformly associate axiomatic theories to concepts or objects.

As opposed to the case with PROP, here we know that there is no algorithm for determining whether or not a formula is valid.

The usual move is to look for significant subclasses of formulas for which there is an algorithm, and then study the computational complexity of such algorithms. This is normally done for classes with infinitely many elements. Normally one runs into recursive unsolvability - no algorithm. A small dose of flexibility in the formulas will cause this unsolvability, where nobody knows what to say beyond that.

I have been proposing that one proceed differently as follows. Look at all kinds of unsolvable classes, including the entire class of formulas. But don't try to do anything with the whole class - which you can't. Rather look at successively larger small initial segments of these classes.

You might say - "but any finite set is recursively solvable, and so what is there to do?"

But here is the paradigm shift. Deciding membership in a large finite set is, in actuality, very much like deciding membership in an infinite set. You want the algorithm to be of reasonable size. You want to have, as a consequence of your decision procedure, that every instance of the membership problem is provably true or provably false in (a weak fragment of) ZFC (the standard axioms for mathematics). The fact that the sample set may be finite is no assurance that this can be done, or that if it can be done, it can be done easily. In fact, these finite decision problems are probably much harder than infinite ones that go positively.

Tricky philosophical issues arise regarding just how you want to say that a large finite set is "intractable". From Gödel, we know that if you start with any recursively unsolvable set of finite strings, then for some n , the set of elements of length at most n is in some sense intractable. For instance, there is a particular string such that membership in the set is neither provable nor refutable in ZFC.

2. FORMAL SYSTEMS.

3. CONSISTENCY.

4. RELATIVE CONSISTENCY.
5. CONSERVATIVE EXTENSION.
6. INTERPRETATION.

PHILOSOPHY 536
 PHILOSOPHY OF MATHEMATICS
 LECTURE 2
 10/02/02
 10/11/02

In this lecture, we discuss formal systems from logic to Presburger arithmetic.

COMPARISON OF FORMAL SYSTEMS.

In this seminar, we climb up the now standard hierarchy of formal systems that have emerged in f.o.m. from logic to the highest of the large cardinal axioms.

By a formal system, we will usually mean a system with the following ingredients, as discussed in seminar 536, lecture 1.

0. Choice of constants, relations, and functions.
1. Logical axioms.
2. Rule of substitution applied to all logical axioms.
3. Rule of universal generalization, applied to all theorems.
4. rule of modus ponens, applied to all theorems.
5. Nonlogical axioms.

We consider 1,2,3,4 as fixed, where 1,2 are restricted to the formulas in the language given by 0. The crucial choice is that of 0 and 5.

Usually 0 is finite, and often 5 is also finite. When infinite, it is most often the closure of a finite set under substitution.

However, some important sets of nonlogical axioms that are not handled in this way. I am thinking of schemes where restrictions are placed on the formulas to be substituted such as on the number of quantifiers, or that all quantifiers be relativized by some particular formulas, or restrictions are placed on terms, etc.

This flexibility is normally handled by simply requiring that the set of all nonlogical axioms is "recursively decidable".

However, this is clearly much too general, and one would like to have a general framework for presenting formal systems with finitely many nonlogical axiom "schemes", with some suitably general notion of "scheme".

An attractive approach in many contexts is to bite the bullet and move over to many sorted predicate calculus, with all of its complications over single sorted predicate calculus. Perhaps this is worth doing. Then we can do things like insist that only quantifiers over certain sorts are present in a scheme, etc. However, this solves some of the problems but not all of the problems. That is, the problem of reflecting that in any reasonable case where infinitely many nonlogical axioms are used, the nonlogical axioms are "essentially finite" in number. However, even this move to many sorted predicate calculus does not handle all useful cases.

What do we mean by going up or climbing up, as in the first sentence of this section?

There is a quasi ordering on formal systems, discussed in 536, lecture 1. This is the quasi ordering under interpretability. (A quasi ordering is a transitive reflexive relation).

Frequently, but not always, as we go up, we will have that the weaker system is a subsystem of the stronger system. When this is not the case, we always have that every sentence of a certain general kind provable in the weaker system is provable in the stronger system. The latter will hold in both directions for systems that are mutually interpretable.

It is nice to know that asserting the interpretability of one formal system into another is in principle incontrovertible, in the case of formal systems with finitely many nonlogical axioms (no nonlogical axiom schemes). This is because such an interpretation is given by finite data, and asserts the provability of finitely many statements in the target system. If we had nonlogical schemes, we are still talking about finite data, but also we are talking about infinitely many assertions being provable.

The reason it is nice to know that we have incontrovertibility here is that in general we will be considering interpretations of one not obviously consistent system into another not obviously consistent system. The interpretation of the first into the second establishes that if the second is consistent then the first is consistent. Since consistency is the sensitive issue, particularly as we move up the hierarchy of systems, we would like such a comparison tool to be as free of controversy as possible.

In the case of where the first formal system is given by finitely many nonlogical axiom schemes, and not just finitely many nonlogical axioms, the interpretations, when they exist, are still satisfactorily incontrovertible in that very little in the way of epistemic or ontological commitments are needed in order to establish that one has given an interpretation - at least in practice.

Moreover, there appears to be, in practice, quite a robust associated finitely axiomatized extension of any natural theory arising with finitely many axiom schemes. This is the system obtained by adding a new sort for "subsets of the universe", and adding a comprehension axiom which does not allow quantification over the new sort. This produces a formal system extending the original one which, under certain general conditions, is finitely axiomatizable - and very demonstrably so. Then one can to some extent have one's cake and eat it too by always passing to such a finitely axiomatizable extension when confronted with finitely many axiom schemes. Use the notation T' for this extension of T .

This immediately leads to the question: what precisely is the relationship between a given formal system axiomatized by finitely many axiom schemes, or even an outright finitely axiomatized system, and T' ?

The answer is that we have a conservative extension, in the sense that every sentence in the language of the original system is provable in T if and only if it is provable in T' .

However, in general, this requires some epistemic (ontological?) commitment involving the indefinite iteration of exponentiation. There is a blowup involved in going from a proof in T' of a sentence in the original language, to a proof in T .

There appears to be a number of detailed issues concerning blowups of this kind when passing to extensions of this sort. One can consider various weaker and stronger such extensions, with lesser and greater blowups expected. Also, the blowup one gets in general, or in certain standard cases, may be greater than the blowups one gets if the original system is weak; e.g., too weak to interpret a fair amount of formal arithmetic.

Typically, we will encounter the following situation. We have two fundamentally important formal systems S, T . We have

- i) T proves the consistency of S ; or
- ii) S proves the consistency of T ; or
- iii) S, T are "equiconsistent".

As an immediate consequence of i), we have S is interpretable in T but not vice versa (provided T interprets a reasonable amount of arithmetic). As an immediate consequence of ii), we have the other way around: T is interpretable in S but not vice versa (provided S interprets a reasonable amount of arithmetic).

The exact meaning of iii) is usually kept fluid. But it normally means that one can prove with very little epistemic commitments that

S is consistent if and only if T is consistent.

Often, but not always, we will have that S, T are mutually interpretable.

We proved a very general theorem to the effect that S, T are "equiconsistent" if and only if S, T are mutually interpretable, in the case of finitely axiomatized S, T which interpret a certain small amount of arithmetic.

The usual statement of this theorem asserts that for finitely axiomatized systems S, T interpreting a small amount of arithmetic,

S is inconsistent \square
 T is inconsistent

is provable in a suitably explicit way in a suitably weak system if and only if

S is interpretable in T.

The reverse direction is immediate since interpretations explicitly map inconsistencies into inconsistencies.

Moreover,

$$\begin{array}{l} S \text{ is inconsistent} \square \\ T \text{ is inconsistent} \end{array}$$

is provable in a suitably weak system if and only if

S is interpretable in T'.

There are small changes that can be made in the definition of interpretation - e.g., does equality have to be interpreted as equality or not, and can objects be interpreted as tuples of objects, etc. Such theorems as above, relating interpretability to relative consistency proofs, can be used to show that under quite general conditions, such small modifications in the notion of interpretation are inconsequential.

Recently, we thought about what is the strongest thing that can be said in the case that S,T are equiconsistent, or mutually interpretable. We believe that under quite general conditions, including the situations that we will be concerned with, S,T are in fact synonymous. Again there are several notions that differ in detail, but the idea is that there is a pair of interpretations, one from S into T, one from T into S, such that the interpretation of an interpretation of a sentence is equivalent to the sentence (with the sentence from any of the two sources S,T).

Perhaps this way of talking about synonymy is a bit confusing and does not directly enough get at the essence of the idea of synonymy, which is "talking about the same thing in two different equivalent ways".

It should be possible to make an honest philosophical analysis of this phrase "talking about the same thing in two different equivalent ways", and lead to the above formal notion of synonymy, or at least a closely related one or ones.

The Theorem to look for is that whenever two finitely axiomatizable theories satisfying quite general conditions (including interpreting a certain amount of arithmetic) are mutually interpretable, they are synonymous. The proof would pass through the relative consistency formulations that we know are equivalent.

Such results should then be adapted to the situation where we have finitely many nonlogical axiom schemes.

THE SYSTEM $T(=)$.

Our first system with nonlogical axioms in this Seminar, is $T(=)$, in the language with just equality. We have the axioms that assert there are at least n objects, for each $n \geq 2$. The case $n = 1$ is provable.

Thus the n -th axiom is

$$A_n = (\exists x_1) \dots (\exists x_n) (B)$$

where B is the conjunction of all $x_i \neq x_j$, $1 \leq i, j \leq n$.

The most striking thing about the n -th axiom is its length. It has n^2 conjunctions of negated equations.

This leads to the following question. Let C be a sentence in this language which is equivalent to A_n . What can we say about the structure of C ?

First of all, we can considerably shorten A_n by writing it in the logically equivalent form

$$A_n = (\exists x_1) \dots (\exists x_{n-1}) (\exists x_n) (x_n \neq x_1 \wedge \dots \wedge x_n \neq x_{n-1}).$$

It would appear that A_n is the simplest way of asserting that there are at least n distinct objects, in various senses. Presumably, one can show that one needs at least n quantifiers. It would also seem that if we use n quantifiers in prenex form, then the last quantifier must be existential.

In fact, one can study which quantifier forms can be used in prenex form, to assert that there are at least n distinct objects. Note that for some quantifier combinations, the matrix appears to have to be quite long (say with the first

A_n), and with others, the matrix can be comparatively short (say with the second A_n).

I am not sure if such a detailed and sharp analysis of various aspects of this system has been done.

The elimination of quantifiers shows that every formula is equivalent in $T(=)$ to a formula without quantifiers. The usual way to prove such things is to show that every formula starting with a single existential quantifier followed by a quantifier free part is equivalent in $T(=)$ to a quantifier free formula.

One then shows that every sentence is equivalent to $x = x$ or equivalent to $x \neq x$. I.e., every sentence is either provable or refutable in $T(=)$.

In particular, this means that $T(=)$ is a complete theory. I.e., every sentence in its language can be proved or refuted. It is provable if and only if it is true in the infinite structures.

Suppose we are given a sentence with at most n quantifiers. We should be able to get sharp information on the "size" of a "smallest" proof of the sentence or its negation. For lower bounds, we may have to assume the fundamental conjecture on the lengths of proofs in propositional proof systems (that they may have exponential size).

It is my impression that there has been definitive work on the computational complexity of determining whether a sentence is provable or refutable in $T(=)$, and for several stronger systems than $T(=)$. But the issue of sizes of proofs seems to have been neglected.

If a sentence is provable in $T(=)$ then it holds in all structures of at least some particular size. One should be able to get sharp information as to the sufficient size in terms of the number of quantifiers in the given sentence. More detailed information involving the pattern of quantifiers in prenex form should also be obtainable.

It would be interesting to present reasonably short provable sentences whose proofs are all very long. This may or may not involve solving presently intractable problems related to computational complexity.

THE SYSTEM $T(0,S)$.

Here we will have equality, the constant 0, and the unary function symbol S. The axioms are:

1. $S(x) \neq 0$.
2. $S(x) = S(y) \implies x = y$.
3. $x \neq 0 \implies (\exists y)(x = S(y))$.
4. $S(x) \neq x$.
5. $S(S(x)) \neq x$.
- ...

The "standard" model of $T(0,S)$ is $(N,0,S)$, where $S(x) = x+1$.

Note that $T(0,S)$ proves $T(=)$. In fact, $T(=)$ is provable with just 1,2 of $T(0,S)$. To see this, for each $n \geq 0$, let n^* be $S \dots S(0)$, where there are n S's. From $n^* = m^*$ one gets $(n-1)^* = (m-1)^*$, etc. If $n \neq m$, one eventually gets $r^* = 0$, where $r \neq 0$, which is a contradiction.

Again, one has elimination of quantifiers, where every formula is provably equivalent to a quantifier free formula. From this, we again get completeness - every sentence is provable or refutable. We also obtain that a sentence is provable if and only if it is true in the "standard" model of T_2 , which is $(N,0,S)$, where N is the set of all nonnegative integers and $S(x) = x+1$.

We can again raise the same issues regarding sizes of proofs.

We can also ask about bounds associated with sentences of the form

$$(\exists x_1) \dots (\exists x_n) (\exists y) (A(x_1, \dots, x_n, y))$$

that are true in $(N,0,S)$, where A is a formula. The bounds we are talking about depend on x_1, \dots, x_n and the size of A , and upper bounds the y .

It is clear that every sentence in the language of $T(=)$ provable in $T(0,S)$ is already provable in $T(=)$. I.e., $T(0,S)$ is a conservative extension of $T(=)$. This is because if provable in $T(0,S)$ then it is true in $(N,0,S)$, and hence in N . Therefore it is provable in $T(=)$.

What can we say about the relationship between a proof in $T(=)$ of a sentence and a proof in $T(0,S)$ of that same sentence? It might be that the size of some proof in $T(0,S)$ is significantly shorter than the size of any proof in $T(=)$. We don't know if this has been thoroughly investigated.

$T(0,S)$ cannot be interpreted in $T(=)$. We can use the elimination of quantifiers in T_0 to show that no relation can serve as an interpretation of S .

$T(0,S)$ is not finitely axiomatizable. One can show that there are models of $T(0,S)$ with no loops of size $\leq n$ but with a loop of size $n+1$, for any given positive integer n .

THE SYSTEM $T(0,S,<)$.

$T(0,S,<)$ has primitives $0,S,<$. The axioms of $T(0,S,<)$ are

1. $x \neq 0 \rightarrow (\exists y)(x = S(y))$.
2. $x < S(y) \rightarrow (x < y \vee x = y)$.
3. $\exists x < 0$.
4. $<$ is a linear ordering.

The "standard" model of $T(0,S,<)$ is $(N,0,S,<)$.

Note that $T(0,S,<)$ is finitely axiomatizable, unlike $T(0,S)$. Also note that $T(0,S)$ is a subsystem of $T(0,S,<)$.

Again, we have quantifier elimination, in the usual sense that every formula is provably equivalent to a quantifier free formula in $T(0,S,<)$. So we get that every sentence is provable or refutable in $T(0,S,<)$. This means that a sentence is provable in $T(0,S,<)$ if and only if it is true in $(N,0,S,<)$.

Thus a sentence in $0,S$, if provable in $T(0,S,<)$, must be true in $(N,0,S)$, and hence provable in $T(0,S)$. Therefore $T(0,S,<)$ is a conservative extension of $T(0,S)$.

We can ask our usual questions about lengths of proofs, and bounds on existential quantifiers.

Is there a significant size reduction for proofs of sentences in the language of $T(0,S)$ if we allow a proof in $T(0,S,<)$? This should be explored.

Can $T(0, S, <)$ be interpreted in $T(0, S)$? The answer is no. Use the quantifier elimination for $T(0, S)$ to show that no relation can serve as an interpretation of $<$.

$T(0, S, <)$ has no finite models. $T(0, S, <)$ has a model whose complete diagram is recursive - namely $(\mathbb{N}, 0, S, <)$.

THE SYSTEM $T(0, S, +)$.

$T(0, S, +)$ is Presburger arithmetic. The axioms are rather long. So we bring in a unifying idea for $T(0, S)$, $T(0, S, <)$, $T(0, S, +)$.

Let us go back to $T(0, S)$. Consider the following axiomatization.

1. $S(x) \neq 0$.
2. $S(x) = S(y) \rightarrow x = y$.
3. $(A[x/0] \rightarrow (\forall x)(A \rightarrow A[x/S(x)])) \rightarrow A$, where A is any formula in $0, S$.

Thus we are using the induction scheme for all formulas in the language of $T(0, S)$.

It can be easily verified that $T(0, S)$ is a subsystem of 1-3. However, every sentence provable in 1-3 is true in $(\mathbb{N}, 0, S)$, and therefore provable in $T(0, S)$. Hence 1-3 is an axiomatization of $T(0, S)$.

Now go back to $T(0, S, <)$. Consider the following axiomatization.

1. $S(x) \neq 0$.
2. $S(x) = S(y) \rightarrow x = y$.
3. $x < S(y) \rightarrow (x < y \vee x = y)$.
4. $\forall x < 0$.
5. $(A[x/0] \rightarrow (\forall x)(A \rightarrow A[x/S(x)])) \rightarrow A$, where A is any formula in $0, S, <$.

It can be easily verified that $T(0, S, <)$ is a subsystem of 1-5.

Of course, since $T(0, S, <)$ is finitely axiomatized, something is lost in using the axiomatization 1-5.

An interesting question is to what extent are proofs shortened by using the induction scheme both in the case of $T(0,S)$ and in the case of $T(0,S,<)$.

We now use this unifying induction idea to give an axiomatization of what we call Presburger arithmetic, or in our notation, $T(0,S,+)$. The axioms of $T(0,S,+)$ are

1. $S(x) \neq 0$.
2. $S(x) = S(y) \implies x = y$.
3. $x + 0 = x$.
4. $x + S(y) = S(x + y)$.
5. $(A[x/0] \implies (\forall x)(A \implies A[x/S(x)])) \implies A$, where A is any formula in $0,S,+$.

In the version with $0,S,<,+$, we simply add the definition of $<$ as follows:

6. $x < y \iff (\exists z)(z \neq 0 \implies x + z = y)$.

We write this as $T(0,S,+,<)$.

The elimination of quantifiers for Presburger arithmetic is more difficult than for $T(=)$, $T(0,S)$, $T(0,S,<)$. First of all, it is false if taken literally - i.e., that every formula in $0,S,+$ is equivalent to a quantifier free formula in $0,S,+$, or even that every formula in $0,S,+,<$ is equivalent to a quantifier free formula in $0,S,+,<$.

The correct elimination of quantifiers must be done for an expanded language. The expanded language consists of $0,S,<,+$, and for each $n \geq 2$, a binary relation \equiv_n , whose intended meaning is "congruent modulo the standard integer n ". Here we view \equiv_n as defined by

$$x \equiv_n y \iff ((x \leq y \iff (\exists z)(y = x + nz)) \quad (y < x \iff (\exists z)(x = y + nz))$$

where nz abbreviates $z + \dots + z$, where there are n z 's.

The background fact is that $T(0,S,+)$ proves the crucial quotient remainder theorem, which asserts that for all standard integers $n \geq 2$,

$$(\exists y)(\exists z)(x = ny + z \wedge z < n)$$

where again ny is $y + \dots + y$, where there are n y 's.

This expansion of the language is by definable relations. So it is clear what we mean by quantifier elimination for Presburger arithmetic for this language.

As a Corollary to the quantifier elimination, we get that every sentence of $T(0,S,+)$ is provable or refutable (for any of the languages under consideration).

We ask our usual questions about bounds and sizes of proofs. Also to what extent proofs are shortened by using $T(0,S,+,<)$ over the different axiomatizations of $T(0,S,<)$.

It is possible to give a much more explicit set of mathematically clear axioms for $T(0,S,+)$ and $T(0,S,+,<)$, and even $T(+)$, although this is at the cost of having quite a large number. Presumably axioms with at most one existential quantifier will suffice (with free variables allowed). The axioms can be given in the following form: the quotient remainder theorem as a scheme for each divisor ≥ 2 , together with finitely many axioms.

Presburger arithmetic represents a very significant portion of important mathematics with a complete axiomatization, where the axiomatization is by finitely many axiom schemes in the usual sense. "Integral semilinear geometry".

PHILOSOPHY 536
PHILOSOPHY OF MATHEMATICS
LECTURE 3
10/16/02

1. Structure of definable structures.

We first discuss a somewhat new kind of problem for structures. We have considered a number of structures where the definable sets are well behaved; e.g.,

$$(N,=), (N,0,S), (N,0,S,<), (N,<), (N,+)$$

Last lecture, we gave complete axiomatizations for all of them except $(N,<)$. This can be given in terms of the complete axiomatization given for $(N,0,S)$, since $0,S$ are definable in $(N,<)$. We have quantifier elimination for the first three structures without expanding the language. We have quantifier

elimination for the last two structures in a suitably expanded language.

We can ask for rather strong information about the definable sets. In one dimension, the definable sets are particularly simple, and the kind of information we will talk about doesn't surface. The family of definable subsets of N in the five structures above are, respectively,

- i) $(N,=)$. The finite and cofinite sets;
- ii) $(N,0,S)$. The finite and cofinite sets;
- iii) $(N,0,S,<)$. The finite and cofinite sets;
- iv) $(N,<)$. The finite and cofinite sets.
- v) $(N,+)$. The ultimately periodic sets.

Let M be a structure. By an M -definable set we will always mean a multidimensional M -definable set.

We can consider all structures that are M -definable. This means a structure in a finite relational type whose domain is an M -definable set, and whose relations and functions are M -definable. In this context, the relations and functions are treated as multidimensional sets in the relevant dimension.

The strong info that we are talking about consists of getting detailed information about the M -definable structures up to isomorphism.

To illustrate the depth of this problem even for $(N,<)$, let alone $(N,+)$, consider just linear orderings. Some of them are well orderings. E.g., we have the lexicographic orderings $x <_k y \iff (x,y \in N^k \iff (x_i < y_i, \text{ where } i \text{ is least such that } x_i \neq y_i))$.

The decidability of whether or not one has presented a well ordering definable in $(N,<)$ follows from the known decidability of the monadic second order theory of $(N,<)$. In monadic second order logic, one has the usual first order predicate calculus, but one can also quantify over subsets of the domain.

However, the monadic second theory of $(N,+)$ is undecidable, since multiplication can be monadic second order defined. So you have to go back to the salt mines to prove the decidability of whether or not one has presented a well ordering definable in $(N,+)$.

In any case, one wants to prove that the sup of the well orderings definable in $(\mathbb{N}, <)$, or even $(\mathbb{N}, +)$, is \aleph_1 . This should be true.

PROPOSITION 1.1. The monadic second order theory of $(\mathbb{N}, +)$ is undecidable.

Proof: To see this, first recall that $<$ is definable in $(\mathbb{N}, +)$. Let E be the set of all squares. We claim that the set of first order sentences true in $(\mathbb{N}, +, E)$ is undecidable. This is because squaring can be defined in $(\mathbb{N}, +, E)$ by

$$r = n^2 \iff r \in E \text{ and the next element of } E \text{ is } r+2n+1.$$

Also multiplication can be defined from squaring by

$$t = nm \iff 2t = (n+m)^2 - n^2 - m^2.$$

We claim that E is the unique solution to a first order predicate $\phi(E)$ in $(\mathbb{N}, +)$. We just say that $0, 1 \in E$, and for all successive $n < m < r$ from E , $m-r = m-n+2$.

We can convert any first order sentence ϕ in $(\mathbb{N}, +, E)$ to a monadic second order sentence ϕ^* in $(\mathbb{N}, +)$, such that ϕ is true in $(\mathbb{N}, +, E)$ if and only if ϕ^* is true in $(\mathbb{N}, +)$, by taking $\phi^* = (\exists E)(\forall E) \phi(\mathbb{N}, +, E)$ satisfies ϕ . But we can convert any first order sentence in $(\mathbb{N}, +, \bullet)$ to a first order sentence in $(\mathbb{N}, +, E)$. QED

I can show that the problem of whether or not one definable structure over $(\mathbb{N}, <)$ is embeddable into another is undecidable. In fact, I am working on a proof that this problem is complete \aleph_1 .

I lean towards the opinion that the problem of whether or not two definable structures over even $(\mathbb{N}, <)$ are isomorphic is undecidable. I'm working on a proof of this, using the undecidability of Hilbert's 10th problem. This should be easier to pull off for $(\mathbb{N}, +)$.

2. Complexity of axiomatizations.

A second somewhat new kind of problem relates to the complexity of axiomatizations. The aim is to find the "simplest" axiomatization, or "a simplest" axiomatization of

familiar theories. We have already touched on this earlier, in connection with the complexity of sentences equivalent to "there are at least k objects".

For instance, one can look at the total number of quantifiers used for an axiomatization with sentences, and attempt to minimize it. Of course, even more delicate is issues surrounding the pattern of universal and existential quantifiers in prenex form.

As an example, let us consider the axioms for strict linear ordering, as sentences. In the usual axiomatization, we can combine universal quantifiers to get an axiomatization using 3 universal quantifiers. Presumably it is a theorem that one needs 3 quantifiers. In fact, that one needs 3 universal quantifiers, when restricting attention to prenex sentences.

Recall the finite complete axiomatization we discussed of $(\mathbb{N}, 0, S, <)$. Even more elemental is the complete axiomatization of $(\mathbb{N}, <)$ that can be derived from it. It would appear that 4 quantifiers are necessary for this, including, in the prenex case, three universal and 1 existential quantifier.

One can continue this study completely systematically.

3. Axiomatizations for the rationals.

$(\mathbb{Q}, <)$ is completely axiomatized by the axioms of dense linear order without endpoints. This has quantifier elimination.

Presumably, $(\mathbb{N}, <)$ and $(\mathbb{N}, 0, S)$ are not isomorphic to definable structures over $(\mathbb{Q}, <)$, and $(\mathbb{Q}, <)$ is not isomorphic to a definable structure over $(\mathbb{N}, 0, S, <)$, or even over $(\mathbb{N}, +)$. I am a little bit queasy about this second statement, though.

In any case, it seems almost clear that formal system $T(\mathbb{Q}, <)$ is not interpretable in $T(\mathbb{N}, +)$, and $T(\mathbb{N}, 0, S)$ is not interpretable in $T(\mathbb{Q}, <)$.

We now consider $(\mathbb{Q}, +)$. This also has quantifier elimination, without going to an expanded language. This is different than the case of $(\mathbb{N}, +)$, where in order to have quantifier elimination, we must introduce infinitely many new unary relations. It seems likely that $(\mathbb{Q}, +)$ is not isomorphic to any definable structure over $(\mathbb{N}, +)$, and vice versa. Also, it

seems almost clear that $T(Q,+)$ and $T(N,+)$ are not interpretable in each other.

Now consider $(Q,+,<)$. Obviously, $<$ is definable in $(N,+)$. However, $<$ is not definable in $(Q,+)$. We have quantifier elimination for $(Q,+,<)$ without expanding the language.

Presumably, $(Q,+,<)$ is not isomorphic to any structure definable in $(Q,+)$, and $T(Q,+,<)$ is not interpretable in $T(Q,+)$.

The one dimensional definable sets in $(Q,<)$ are exactly the finite unions of intervals, where the intervals can have endpoints on one side or the other, or be infinite on one side or the other. This is also true of $(Q,+,<)$.

In $(Q,+)$, the one dimensional definable sets are finite or cofinite.

5. Axiomatizations for the integers.

Just as we have considered, $(N,=)$, $(N,0,S)$, $(N,0,S,<)$, $(N,<)$, $(N,+)$, we can also consider $(Z,=)$, $(Z,0,S)$, $(Z,0,S,<)$, $(Z,<)$, $(Z,+)$, $(Z,+,<)$.

All of these have simple complete axiomatizations. The one for $(Z,=)$ is the same as the one for $(N,=)$ since they are isomorphic.

For $(Z,0,S)$, we can take two numbers have the same successors iff they are equal, no loops, and every number has a predecessor. The constant 0 serves no purpose, and so we can use (Z,S) instead, and have quantifier elimination. Note that (N,S) does not have quantifier elimination without adding, say, 0.

For $(Z,0,S,<)$, we have a simple finite axiomatization, and also quantifier elimination. Unlike the case for N , we don't need 0 for the quantifier elimination.

For $(Z,<)$, we can get an axiomatization via $(Z,S,<)$.

$(Z,+)$ does not admit quantifier elimination unless we add infinitely many new unary predicates for divisibility, as in the case of $(N,+)$. Only in the case of $(N,+)$, we also had to

add $<$. Here we do not need $<$, and in fact $<$ is not definable in $(\mathbb{Z}, +)$. Moreover, \mathbb{N} is not definable in $(\mathbb{Z}, +)$.

$(\mathbb{Z}, +, <)$ admits quantifier elimination if we add infinitely many new unary predicates for divisibility, and the complete axiomatization can be obtained from that for $(\mathbb{N}, +, <)$.

6. Axiomatizations for the reals.

Here we can go much further, and bring in multiplication. Let's proceed in steps.

$(\mathbb{R}, <)$ has quantifier elimination, and $(\mathbb{R}, <)$, $(\mathbb{Q}, <)$ are elementarily equivalent; i.e., satisfy the same sentences. In fact, $(\mathbb{Q}, <)$ is an elementary substructure of $(\mathbb{R}, <)$. This means that any formula with parameters from \mathbb{Q} holds in $(\mathbb{Q}, <)$ if and only if it holds in $(\mathbb{R}, <)$.

$(\mathbb{R}, +)$ has quantifier elimination, and $(\mathbb{Q}, +)$ is an elementary substructure of $(\mathbb{R}, +)$.

$(\mathbb{R}, +, <)$ has quantifier elimination, and $(\mathbb{Q}, +, <)$ is an elementary substructure of $(\mathbb{R}, +, <)$. The one dimensional definable sets are exactly the finite unions of intervals.

We now come to a main event. $(\mathbb{R}, +, \cdot)$ has quantifier elimination. We have to use the expanded language $(\mathbb{R}, <, +, \cdot, 0, 1)$. Of course, $<$ is definable in $(\mathbb{R}, <, +, \cdot, 0, 1)$, but not in $(\mathbb{R}, +)$.

I have my own pet treatment of this quantifier elimination, but I asked Dave Marker at University of Illinois at Chicago for his favorite references. He responded:

The book "Real Algebraic Geometry" by Bochnak, Coste and Roy presents a geometric proof of quantifier elimination for real closed fields.

The book "Quantifier Elimination and Cylindric Algebraic Decomposition", Springer-Verlag, 1998. B. F. Caviness and J. R. Johnson (eds.), is a "reader" on qe. It contains original papers by Tarski, Collins paper describing cylindric decomposition and some of the more modern papers in the subject.

In my Model Theory of Fields book I prove quantifier elimination using model theory and the Robinson/Blum style methods for proving qe from embedding results. I am in the process of writing a introductory model theory text book. Chapter 3 discusses the model theoretic approach to qe and studies algebraically closed and real closed fields. A first draft of the book is available on [Marker's] web page:

<http://www.math.uic.edu/~marker/CIMT-9-01.ps>

I think Marker's book is now out, published by Springer.

As a consequence of the quantifier elimination for $(\mathbb{R}, <, +, \cdot, 0, 1)$, we get that the one dimensional definable sets are again just the finite unions of intervals.

There are a number of important complete axiomatizations for $(\mathbb{R}, <, +, \cdot, 0, 1)$. The first one is given by the so called "real closed ordered field" axioms, written RCOF:

A. Ordered field axioms.

1. $+$ is commutative and associative.
2. \cdot is commutative and associate.
3. $x(y+z) = xy + xz$.
4. $x+0 = x$, $x \cdot 1 = x$.
5. $<$ is a strict linear ordering, $0 < 1$.
6. $x < y \implies x+z < y+z$.
7. $(x < y \implies 0 < z) \implies xz < yz$.
8. $(\exists y)(x + y = 0)$.
9. $x \neq 0 \implies (\exists y)(x \cdot y = 1)$.

B. Completeness axioms.

10. Every nonnegative element has a square root.
11. Every polynomial of odd degree has a root.

Note that 11 is an axiom scheme, which can be written as

$$(\exists x)(x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0)$$

where n is an odd positive integer.

Obviously RCOF holds in $(\mathbb{R}, <, +, \cdot, 0, 1)$. The only issue is 11, but since n is odd, we see that the polynomial must take on a negative value for negative enough x , and a positive value for positive enough x . So by the intermediate value theorem, it has a root.

That, however, is a consistency proof using ideas embedded in real analysis. We address the issue of consistency proofs later.

Another axiomatization of RCOF is as follows.

- A. Ordered field axioms.
- B. Intermediate value. Every polynomial that takes on a negative value at the left endpoint of a closed interval, and a positive value at the right endpoint of that closed interval, has a zero in the interior of that closed interval.

It is obvious that the first axiomatization is a subsystem of this second axiomatization. The reverse follows the completeness (discussed below), but one would like a more elementary proof of the logical equivalence of these two systems. This can be done.

We now give another kind of axiomatization.

- A. Ordered field axioms.
- B. Least upper bound scheme. For any formula in the language, with one free variable and parameters allowed, there is a least nonnegative element which is at least as large as any solution to the formula.

It is clear how the earlier axiomatizations of RCOF are a subsystem of this axiomatization, but again the obvious proof of the reverse goes through completeness. One can get an elementary proof of the logical equivalence of all three axiomatizations.

We now take up the matter of axiomatizations that do not use $<$. I.e., just for $(R, +, \cdot, 0, 1)$.

The most well known one is the so called axioms for real closed fields (RCF).

- A. Field axioms.
- B. Realness. -1 is not the sum of finitely many squares.
- C. Square roots. For all x , x has a square root or $-x$ has a square root.
- D. Zeros. Every polynomial of odd degree has a root.

The above is the most "bare bones" axiomatization known of $(\mathbb{R}, +, \cdot, 0, 1)$. But what does that mean?

It is easy to see that this latter axiomatization is complete for $(\mathbb{R}, +, \cdot, 0, 1)$ if and only if the first axiomatization is complete for $(\mathbb{R}, <, +, \cdot, 0, 1)$.

It is easy to show that realness is a consequence of the first axiomatization, since squares can be proved to be nonnegative. So the first axiomatization is, from the algebraic point of view, simply the real closed field axioms.

The normal way of doing the quantifier elimination for the first axiomatization, and thereby deriving completeness as a consequence, is to first derive the second axiomatization. However, this is normally done purely algebraically, thereby passing through the completeness theorem for predicate calculus. One goes through the Artin theory of real closed fields. One first proves that if you adjoin $\sqrt{-1}$ to a real closed field, then the field becomes algebraically closed. Then one has the theory of algebraically closed fields available, including factoring of polynomials. One then shows that every polynomial over the real closed field can be factored into linear and quadratic factors. From there, one derives the intermediate value property for polynomials.

After this step, the quantifier elimination is fairly straightforward, but still has to be done carefully.

7. Conservative extension.

There is a very important conservative extension result.

THEOREM 5.1. Tarski?. Every purely universal sentence provable in RCOF is provable in OF (the ordered field axioms).

I have not seen a careful study of the blowups involved in Theorem 5.1. However, it appears that they are roughly on the order of a double exponential.

Normally this is proved algebraically via the classical result that every real field can be embedded in a real closed field. This proof does not readily give any bounds.

It would be very interesting to give a set of striking simple examples of sentences in RCOF whose proof in RCOF is far shorter than its proof in OF.

8. Consistency proof.

We have given a detailed sketch of a consistency proof of all of the real closed (ordered) field axioms within a weak fragment of arithmetic. The most natural fragment to do such a consistency proof is the system EFA of exponential function arithmetic. The proof is a somewhat big deal, requiring novel formalizations of classical algebraic arguments.

9. A combined system.

Consider $(\mathbb{R}, \mathbb{Q}, \mathbb{Z}, <, +)$. This is well behaved, with a complete axiomatization, and quantifier elimination, provided one adds divisibility predicates.

10. An axiomatization of euclidean plane geometry based on distance comparison.

In the algebraic approach to geometry, one defines the plane and its Euclidean metric in the usual first order way in the field of real numbers. In this way, the first order Euclidean plane geometry reduces to the first order algebra of real numbers.

Under the geometric approach, we consider structures such as (\mathbb{R}^2, E) , where $E(x, y, z, w)$ holds if and only if $d(x, y) = d(z, w)$; i.e., the Euclidean distance between x and y is the same as the Euclidean distance between z and w .

We can define the field of real numbers in (\mathbb{R}^2, E) . This is done by equivalence classes of pairs of elements of \mathbb{R}^2 . In fact, much more is true. This is almost surely known - but I don't know a reference.

THEOREM 10.1. The sets definable in (\mathbb{R}^2, E) are exactly the semialgebraic subsets of \mathbb{R}^2 . By Tarski, these are also the subsets of \mathbb{R}^2 definable in $(\mathbb{R}, 0, 1, +, \cdot)$. The sets definable in (\mathbb{R}^2, E) with only the three parameters $(0, 0), (0, 1), (1, 0)$ are exactly the semialgebraic subsets of \mathbb{R}^2 presented with rational coefficients, or the subsets of \mathbb{R}^2 that are 0-definable in $(\mathbb{R}, 0, 1, +, \cdot)$.

(Here definable means definable with any number of parameters. And 0-definable means definable with no parameters).

We also consider interpretability.

THEOREM 10.2. $(\mathbb{R}, 0, 1, +, \cdot)$ is interpretable in (\mathbb{R}^2, E) and vice versa.

Here, interpretations are allowed to be via equivalence relations of tuples, which is allowed in a well known general form of interpretability.

According to Tarski, the first order theory of $(\mathbb{R}, 0, 1, +, \cdot)$ has a beautiful axiomatization via the real closed field axioms:

- 1) the usual field axioms;
- 2) -1 is not the sum of squares;
- 3) for all x , x or $-x$ is a square;
- 4) every polynomial of odd degree has a root.

Tarski showed that these axioms are complete. Thus a sentence is true in $(\mathbb{R}, 0, 1, +, \cdot)$ if and only if it is derivable from these axioms.

Think of (\mathbb{R}^2, E) as corresponding to the geometric approach to Euclidean plane geometry, and $(\mathbb{R}, 0, 1, +, \cdot)$ as corresponding to the algebraic approach to Euclidean plane geometry.

The following question arises. Can we give a similarly elegant and basic axiomatization of the first order theory of (\mathbb{R}^2, E) involving only \mathbb{R}^2, E ?

We also consider a related matter. According to Tarski, the real algebraic numbers are the 0-definable elements of $(\mathbb{R}, 0, 1, +, \cdot)$. But they have a very algebraic definition (hence the name "real algebraic"): the solutions to nontrivial polynomials in one variable with integer coefficients. In fact, this is the usual definition of real algebraic numbers.

Fundamental to all aspects of this theory is the concept of ****equality condition****. An equality condition is a formula in the language of (\mathbb{R}^2, E) of the following special form: a conjunction of one or more atomic formulas of the form $E(x, y, z, w)$, where x, y, z, w are variables.

We can think of an equality condition in variables x_1, \dots, x_k as a Euclidean plane geometric diagram. There are k labeled points x_1, \dots, x_k in the diagram. There is an indication that for various pairs of points x_1, \dots, x_k , we have equality of distance. Thus we could mark the line segments joining various pairs in such a way that pairs that are to have the same distance have their line segments marked with the same marking.

Of course, here one must be entirely noncommittal about degeneracies; e.g., about which of the x 's are equal or unequal, which line segments cross or don't cross, which triples of points are or are not colinear, etc.

THEOREM 3. Let $x \in \mathbb{R}^2$. The following are equivalent:

- a) x is definable in (\mathbb{R}^2, E) with parameters $(0,0), (1,0), (0,1)$;
- b) x is 0-definable in $(\mathbb{R}, 0, 1, +, \cdot)$;
- c) x is real algebraic (i.e., its components are real algebraic numbers);
- d) x is a coordinate in some solution of some equality condition in (\mathbb{R}^2, E) with parameters $(0,0), (1,0), (0,1)$ that has at most finitely many solutions;
- e) x is a coordinate in some solution of some equality condition in (\mathbb{R}^2, E) with parameters $(0,0), (1,0), (0,1)$ all of whose solutions are permutations of each other.

We can alter the notion of equality condition to incorporate various commitments. E.g., we can consider modified equality conditions which consist of a conjunction of one or more atomic formulas without equality and the conjunction asserting that all points used are distinct. This eliminates the most basic of degeneracies, although there are other important degeneracies still allowed. Then Theorem 3 still holds.

Furthermore, various other modifications with regard to the elimination of degeneracies can be made, with the same result.

We now come to the more delicate matter of the complete axiomatization of geometry in terms of diagrammatic axioms.

For this purpose it is very convenient to use the 4-ary relation $LE(x, y, z, w)$ on \mathbb{R}^2 , meaning that the distance between

x, y is less than or equal to the distance between z, w . This relation can be defined nicely from $E(x, y, z, w)$. We give such a definition below.

First of all, we want to nicely define the midpoint between two points x, y . Note that there are points z, w (or w, z), such that x, y, z, w forms a square with diagonal x, y (degenerate if and only if $x = y$). This is defined using equidistance - the sides are all equal and the two diagonals are equal. The unique point equidistant to the four corners is the desired midpoint.

Now we are in a position to define $LE(x, y, z, w)$ as follows. Let p be the midpoint between z, w . Then $LE(x, y, z, w)$ if and only if there exists u such that $d(x, u) = d(u, y) = d(z, p)$.

Since we are now admitting the ordering directly, it is appropriate to consider ordered fields and real closed fields using $<$. We assume familiarity with the usual ordered field axioms. In this context, the real field axiom 2) is superfluous. Thus in this context, real closed fields are given by

- 1) the usual ordered field axioms;
- 2) every all $x \geq 0$ has a square root;
- 3) every polynomial of odd degree has a root.

It is very useful to separate out what we call basic Euclidean plane geometry and quadratic Euclidean plane geometry.

Basic Euclidean plane geometry consists of the set of all sentences of (\mathbb{R}^2, LE) that become provable from the axioms of ordered fields under the obvious translation of (\mathbb{R}^2, LE) into $(\mathbb{R}, <, 0, 1, +, \cdot)$. The quadratic ordered field axioms consist of just axioms 1) - 2) above. Quadratic Euclidean plane geometry consists of the set of all sentences of (\mathbb{R}^2, LE) that become provable from the quadratic real ordered axioms under the obvious translation of (\mathbb{R}^2, LE) into $(\mathbb{R}, 0, 1, +, \cdot)$.

One can give reasonably elegant axiomatizations of basic Euclidean plane geometry and quadratic Euclidean plane geometry staying within the language of (\mathbb{R}^2, LE) . The latter corresponds closely to ruler and compass constructions. This much is well known.

We now come to the main issue of giving a geometric form of axiom scheme 3) - that every polynomial of odd degree has a root - within the language of (\mathbb{R}^2, LE) .

We certainly don't want to simulate this axiom scheme 3) directly. E.g., odd degree appears to be geometrically meaningless. But we are looking for a kind of geometric construction principle.

For this purpose, we define a comparison condition as the conjunction of finitely many atomic formulas $LE(x, y, z, w)$, where x, y, z, w are variables.

Let $\square(x_1, \dots, x_n, y_1, \dots, y_m)$ be a comparison condition, where $n, m \geq 0$.

I. Suppose $\square(x_1, \dots, x_n, y_1, \dots, y_m)$. Then we can adjust y_1, \dots, y_m so that $\square(x_1, \dots, x_n, y_1, \dots, y_m)$ and the maximum distance from x_1 to the points y_1, \dots, y_m is minimized.

Think of x_1 as the center of a closed disk in which the new points y_1, \dots, y_m to be constructed are to lie. We want to minimize the radius of that closed disk.

THEOREM 4. A sentence is true in (\mathbb{R}^2, LE) if and only if it is provable from the axioms of basic Euclidean geometry plus the axiom scheme I.

There are a number of variants of * where related quantities are minimized. Here are some examples.

II. Suppose $\square(x_1, \dots, x_n, y_1, \dots, y_m)$. Then we can adjust y_1, \dots, y_m so that $\square(x_1, \dots, x_n, y_1, \dots, y_m)$ and the maximum distance from x_1 to the points $x_1, \dots, x_n, y_1, \dots, y_m$ is minimized.

III. Suppose $\square(x_1, \dots, x_n, y_1, \dots, y_m)$. Then we can adjust y_1, \dots, y_m so that $\square(x_1, \dots, x_n, y_1, \dots, y_m)$ and the diameter of y_1, \dots, y_m is minimized.

IV. Suppose $\square(x_1, \dots, x_n, y_1, \dots, y_m)$. Then we can adjust y_1, \dots, y_m so that $\square(x_1, \dots, x_n, y_1, \dots, y_m)$ and the diameter of $x_1, \dots, x_n, y_1, \dots, y_m$ is minimized.

Theorem 4 holds for any of I - IV.

PHILOSOPHY 536
 PHILOSOPHY OF MATHEMATICS
 LECTURE 4
 10/23/02

We have finished discussion of the tame systems, and we now take up the interval from Presburger arithmetic to Peano arithmetic.

The best source for this material is the book

Peter Hajek, Pavel Pudlak, *Metamathematics of First-Order Arithmetic*, Springer, 1998.

1. The main language, and formulas.

The main language that we use is $L_0 = 0, S, +, \cdot, \square, =$. We use the abbreviations

$$\begin{aligned} x < y &\square x \square y \square \square x = y. \\ x \geq y &\square x \square y. \\ x > y &\square y > x. \\ x \neq y &\square \square x = y. \end{aligned}$$

Let $\square_0 = \square_0$ the class of bounded formulas, which are the formulas in L whose quantifiers are bounded; i.e., whose quantifiers are of the form

$$(\square x \square y), (\square x \square y)$$

where x, y are distinct variables, and this is expanded out using the definition of \square .

\square_{n+1} is the class of formulas $(\square x) (\square)$, where \square is \square_n . \square_{n+1} is the class of formulas $(\square x) (\square)$, where \square is \square_n .

We always let $n^* = SS\dots S(0)$, where there are n S 's.

2. R.M. Robinson's system Q .

The language is $0, S, +, \cdot, =$. The axioms are

1. $S(x) \neq 0$.
2. $S(x) = S(y) \square x = y$.
3. $x \neq 0 \square (\square y) (x = S(y))$.
4. $x+0 = x$.

5. $x+S(y) = S(x+y)$.
6. $x \cdot 0 = 0$.
7. $x \cdot S(y) = (x \cdot y) + x$.
8. $x \leq y \iff (\exists z)(x+z = y)$.

THEOREM 1.1. A Σ_0 sentence is true iff it is provable in Q .

Proof: By induction on the Σ_0 sentence. This needs some basic facts about Σ_0 provable in Q . E.g., $x \leq n$ iff $x = 0 \vee \dots \vee x = n$. QED

THEOREM 1.2. Q is essentially undecidable. I.e., no consistent extension of Q is decidable.

Proof: Let A, B be two r.e. recursively inseparable sets. Let $(\exists x)(\exists y)$ define A and $(\exists x)(\exists y)$ define B , where \exists, \exists are bounded. Consider $\exists(y) = (\exists x)(\exists y) \wedge (\exists z \leq x) (\exists w(x, z))$, $\exists(y) = (\exists x)(\exists y) \wedge (\exists z \leq x) (\exists w(x, z))$. These still define A, B , and also for every $n \geq 0$, Q proves $\exists(\exists(n^*)) \wedge \exists(n^*)$. Let T be a consistent extension of Q . Then $\{n: T \text{ proves } \exists(n^*)\}$ contains A and is disjoint from B . Therefore it is not recursive. QED

Q was set up to be a kind of minimal natural finitely axiomatized system in L_0 which is essentially undecidable. Can we make sense of "minimal natural" here?

Q is known not to prove the commutativity of $+$. Presumably it cannot prove the associativity of $+$, the commutativity of \cdot , the associativity of \cdot , the transitivity of \leq , the connectedness of \leq .

It is perhaps somewhat surprising that stronger than expected extensions of Q are interpretable in Q .

An appropriate form of Gödel's second incompleteness theorem can be given for consistent extensions of Q . One needs only a Σ_1 definition of the set of all formulas provable in T satisfying the provability conditions.

3. I_{open} .

I_{open} is Q together with the induction scheme

$$(\exists[x/0] \wedge (\exists x)(\exists y \wedge \exists[x/S(x)])) \wedge \exists$$

where ϕ is a formula in L_0 without quantifiers.

This definitely allows us to go much farther in terms of elementary mathematical theorems. E.g., the axioms of discretely ordered commutative semiring with unit. Also, the appropriate quotient remainder theorem. So we can formally construct the discretely ordered commutative semiring with unit of integers, with its quotient remainder theorem. I_{open} proves the existence of a very specific one-one onto quadratic pairing function (using multiplication by $1/2$).

I don't know of any interesting theorem that characterizes what is provable in I_{open} in an interesting class of sentences. For example, what can we say about the class of Diophantine equations that can be proved to have no solutions in I_{open} ? Is it even decidable? This might be known.

It is known that I_{open} does not prove $(\exists x)(x \cdot x \neq 2)$, and does not prove Fermat's last theorem for exponent 3. Such independence results are proved via the proof of the following.

THEOREM 3.1. I_{open} has a recursive nonstandard model.

I.e., one whose domain is \mathbb{Q} , and where $S, +, \cdot, \lfloor \rfloor$ are recursive.

Presumably, I_{open} does not suffice to prove FLT for any given exponent. Also presumably not the existence of a gcd, or that if $x, y \geq 1$ are relatively prime, then we can write $nx + my = 1$, where n, m are integers.

Because of the appropriately provable pairing function, we see that for any extension T of I_{open} (in L_0), the formulas that are provably equivalent in T to ϕ_n (\exists_n) formulas are closed under disjunction, conjunction, and existential (universal) quantification.

I_{open} is interpretable in \mathbb{Q} .

4. $I_{\mathbb{Q}_0}$.

$I_{\mathbb{Q}_0}$ is \mathbb{Q} together with

$$(\exists [x/0] \exists (\exists x) (\exists \lfloor \rfloor \exists [x/S(x)])) \exists \lfloor \rfloor$$

where φ is a Σ_0 formula. This is also called polynomially bounded arithmetic.

$I\Sigma_0$ is sufficient to prove that there is no square root of 2, the existence of gcd's, and the basic theory of gcd's and lcm's.

Also, $I\Sigma_0$ is sufficient to prove that a specific Σ_0 formula of three variables acts as the graph of the binary exponential function, which the usual elementary properties and inequalities, but without proving that exponentiation defined this way is total. That is known to be an impossible additional requirement. $I\Sigma_0$ can prove that any two such Σ_0 formulas must be provably equivalent.

In the same vein, assuming that n^n exists (which can be formalized using the previous paragraph), we have a coding system for length n sequences from $[0, n]$ with all of the usual properties. Also assuming that n^n exists, $I\Sigma_0$ is sufficient to state and prove the fundamental theorem of arithmetic on $[0, n]$.

Presumably, $I\Sigma_0$ is sufficient to prove a lot of number theory on $[0, n]$, assuming n^n exists. E.g., between any positive integer and its double (closed interval) there is a prime. Also, presumably, FLT with exponent n on $[0, n]$, assuming n^n exists. In fact, these are strong forms of a conjecture that we later make about $I\Sigma_0 + \text{exp}$ and $I\Sigma_0(\text{exp})$.

THEOREM 4.1. There is no recursive nonstandard model of $I\Sigma_0$. In fact, in any nonstandard model M of $I\Sigma_0$ whose domain is a subset of \mathbb{N} , whose addition and multiplication are not recursive.

Somewhat surprisingly, $I\Sigma_0$ is interpretable in \mathcal{Q} .

THEOREM 4.2. Every Σ_2 sentence provable in $I\Sigma_0$ has a Skolem function that is everywhere bounded by a polynomial.

We can formulate $I\Sigma_0$ using the least number principle instead of induction. We get a logically equivalent system. The same is true of order induction (course of values induction).

5. $I\Sigma_0(\text{exp})$ and $I\Sigma_0 + \text{exp}$.

The system $I\Delta_0(\text{exp})$ is defined by first expanding the language L_0 with $S, +, \cdot, \square, =$ to $L_0(\text{exp})$ with $S, +, \cdot, \text{exp}, \square, =$. The $\Delta_0(\text{exp})$ formulas are defined the same way as the Δ_0 formulas; the formulas of $L_0(\text{exp})$ with all quantifiers bounded (to variables).

The axioms of $I\Delta_0(\text{exp})$ consist of Q , induction with respect to all formulas in $L_0(\text{exp})$, and the axioms for exponentiation,

$$2^0 = S(0), \quad 2^{S(x)} = 2^x + 2^x.$$

The system $I\Delta_0 + \text{exp}$ of course is in the language L_0 . Exp is defined in terms of the formula of three variables discussed above that codes the exponential function, provably in $I\Delta_0$. Recall its uniqueness property provably in $I\Delta_0$.

THEOREM 5.1. $I\Delta_0(\text{exp})$ and $I\Delta_0 + \text{exp}$ prove the same sentences in L_0 .

Here is a nonobvious fact about this system.

THEOREM 5.2. $I\Delta_0(\text{exp})$ and $I\Delta_0 + \text{exp}$ are finitely axiomatizable.

In $I\Delta_0(\text{exp})$, we can freely do finite sequence coding without worrying about the existence of exponentials. In a sense, $I\Delta_0(\text{exp})$ appears to be the weakest system with genuine metamathematical freedom.

$I\Delta_0(\text{exp})$ is an extremely powerful theorem from the point of view of finite mathematics. I have conjectured that every published finite theorem highly valued within the current core mathematical culture, with a robust formulation in $L_0(\text{exp})$, is provable in $I\Delta_0(\text{exp})$.

This conjecture would encompass things like Wiles' FLT, Falting's Mordell conjecture, and many other landmarks.

However, one theorem that is definitely not provable there is the following.

THEOREM 5.2. The finite Ramsey theorem is unprovable in $I\Delta_0(\text{exp})$.

By this I mean that every sufficiently large coloring of the unordered n tuples by r colors has a monochromatic set with p elements. I.e., sufficiently large relative to p, r .

The reason for this is the following.

THEOREM 5.3. Every Σ_2 sentence provable in $I\Sigma_0(\text{exp})$ has a Skolem function that is everywhere bounded by an iterated exponential.

THEOREM 5.4. The finite Ramsey theorem is a Σ_2 sentence that does not have a Skolem function that is everywhere bounded by an iterated exponential.

THEOREM. 5.5. The finite Ramsey theorem is a Σ_2 sentence that is not provable in $I\Sigma_0(\text{exp})$.

Another important theorem of a metamathematical nature that is not provable in $I\Sigma_0(\text{exp})$ is cut elimination.

THEOREM 5.6. The cut elimination theorem for predicate calculus is a Σ_2 sentence that does not have a Skolem function that is everywhere bounded by an iterated exponential.

THEOREM 5.7. The cut elimination theorem for predicate calculus is a Σ_2 sentence that is not provable in $I\Sigma_0(\text{exp})$.

In fact, we can be more specific in the form of a reversal.

Let superexp be the sentence in $L_0(\text{exp})$ that asserts that for all n, k , the k -fold exponential to base 2 of n exists. This is formulated in terms of finite sequences, which we are now comfortable with in $I\Sigma_0(\text{exp})$.

Alternatively, we could formulate superexp as a sentence in L_0 . In fact, we can consider the obvious systems $I\Sigma_0 + \text{superexp}$, $I\Sigma_0(\text{exp}) + \text{superexp}$, and $I\Sigma_0(\text{superexp})$. Then all three systems prove the same sentences in L_0 .

THEOREM 5.8. The following are provably equivalent in $I\Sigma_0(\text{exp})$.

- i) finite Ramsey theorem;
- ii) cut elimination for predicate calculus;
- iii) superexp .

THEOREM 5.9. $I\Delta_0(\text{exp})$ is not interpretable in Q .

Here is an important theorem of Wilkie.

THEOREM 5.10. Let A be a Δ_1 sentence in $L(\text{exp})$. Then $I\Delta_0(\text{exp})$ proves A iff $Q + A$ is interpretable in Q .

THEOREM 5.11. $I\Delta_0(\text{exp})$ does not prove $\text{Con}(Q)$. $I\Delta_0(\text{exp})$ proves cut free $\text{Con}(Q)$.

THEOREM 5.12. $I\Delta_0(\text{exp}) + \text{superexp}$ proves $\text{Con}(I\Delta_0(\text{exp}))$.

The second incompleteness theorem for consistent extensions of Q works for cut free consistency.

Under very general conditions, if one system proves the consistency of another, then the former cannot be interpreted in the other. Therefore $I\Delta_0(\text{exp}) + \text{superexp}$ is not interpretable in $I\Delta_0(\text{exp})$.

$I\Delta_0(\text{exp})$ is exactly the right place in arithmetic to be developing the theory of finite sets of natural numbers. One can easily prove all of the elementary facts about them, based on any reasonable coding of them as natural numbers. In particular, one can handle union, intersection, set difference, Cartesian product, sum set, and power set, and appropriately formalize and prove that the set of all (codes for) subsets of $[1, n]$ has cardinality 2^n . The same remarks apply to the elementary theory of relations, finite sequences, finite functions, domains, ranges, etc.

If we formulate $I\Delta_0(\text{exp})$ with the least number principle instead of the axiom of induction, then we get a logically equivalent system. The same is true of order induction (course of values induction).

In fact, we have worked on set theories that correspond to $I\Delta_0(\text{exp})$ and some weaker fragments as well. These set theories all have the first ω stages of the cumulative hierarchy as their intended interpretations; i.e., $V(\omega)$.

6. PRA.

PRA is primitive recursive arithmetic. There are a few formulations. All of the ones that we consider have the axioms for successor, and the defining equations.

The language consists of $=, 0, S$, and symbols for each primitive recursive function as they are introduced by defining equations.

1. $S(x) \neq 0, S(x) = S(y) \iff x = y$.
2. $Z(x) = 0$.
3. $U_m^n(x_1, \dots, x_n) = x_m$, where $1 \leq m \leq n$.
4. $F(x_1, \dots, x_n) = G(H_1(x_1, \dots, x_n), \dots, H_m(x_1, \dots, x_n))$, where G, H_1, \dots, H_m have been previously introduced.
4. $F(0) = k^*$, $F(S(x)) = G(x, F(x))$, where $k \geq 0$ and G has been previously introduced.
5. $F(x_1, \dots, x_n, 0) = G(x_1, \dots, x_n)$, $F(x_1, \dots, x_n, S(y)) = H(x_1, \dots, x_n, y, F(x_1, \dots, x_n, y))$, where G, H have been previously introduced.

We present three versions of PRA.

1. 1-5 plus the axiom scheme

$$(A[x/0] \iff (\exists x)(A \iff A[x/S(x)])) \iff A$$

where A is quantifier free, in the context of first order predicate calculus for our language.

2. 1-5 plus the rule

$$\text{from } A[x/0] \text{ and } A \iff A[x/S(x)], \text{ derive } A$$

where A is quantifier free, in the context of first order predicate calculus for our language.

3. 1-5 plus the rule

$$\text{from } A[x/0] \text{ and } A \iff A[x/S(x)], \text{ derive } A$$

where A is quantifier free, in the context of free variable predicate calculus for our language.

In the case of 3, all theorems are quantifier free (of course, interpreted universally).

THEOREM 6.1. All three versions of PRA prove the same sentences without quantifiers. The \exists_2 sentences provable in 1, 2 and the \exists_2 sentences that are provable from the theorems of 3 in predicate calculus are the same (even if blocks of

like quantifiers are used in the Σ_2 sentences). This is provable in $I\Sigma_0(\text{exp})$.

THEOREM 6.2. Under any adequate formalization of provability in PRA, we have that PRA proves the consistency of every particular finite fragment of PRA. In fact, the 1-consistency (every provable Σ_1 sentence is true). PRA proves the 1-consistency of $I\Sigma_0(\text{exp}) + \text{superexp}$. In particular, PRA is not interpretable in $I\Sigma_0(\text{exp}) + \text{superexp}$, or in any of its finite fragments. This is provable in $I\Sigma_0(\text{exp})$.

THEOREM 6.3. If PRA proves a sentence $(\forall n)(\exists m)(A)$, A quantifier free, then there is a function symbol F such that PRA proves $(\forall n)(A[m/F(n)])$. This is provable in $I\Sigma_0(\text{exp})$.

A streamlined version of the Ackermann hierarchy is defined as follows. We define functions $A_k: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ as follows. $A_1(n) = 2n$, $A_{k+1}(n) = A_k A_k \dots A_k(1)$, where there are n A_k 's.

More formally, $A(1, n) = 2n$, $A(k+1, n+1) = A(k, A(k+1, n))$.

We can ask whether each of the functions A_k exist in PRA. How is this formalized? One way is to see that for any $k \geq 1$, there is a Turing machine algorithm corresponding to A_k , which is constructed inductively on k by a primitive recursion. We can then state " A_k exists" as

for all n , the algorithm
corresponding to A_k halts at input n .

We can also formalize "the Ackermann function exists" in an analogous way, that the algorithm corresponding to our definition of A halts at any two arguments.

THEOREM 6.4. PRA does not prove "for all $k \geq 1$, the function A_k exists". PRA does not prove "the function A exists". The equivalence between these two statements is provable in $I\Sigma_0(\text{exp})$. In fact, over $I\Sigma_0(\text{exp})$, these two statements are provably equivalent to the 1-consistency of PRA.

We can alternatively present PRA with the language L_0 at the base, using Q , while we still introduce new symbols for primitive recursive functions in the same way. If we do this, then we get the same systems in the usual sense, and also we can use the least number principle instead of induction.

7. $I\Delta_1$.

$I\Delta_1$ is in the language L_0 with $0, S, +, \cdot, =, \Delta$. $I\Delta_1$ is \mathcal{Q} together with the induction scheme for Δ_1 formulas. Obviously $I\Delta_1$ contains $I\Delta_0$, and hence the development of the graph of exponentiation and finite sequence coding where there are exponentials. But then using Δ_1 induction, we can obviously prove that the exponential graph is total. These ideas create a standard interpretation of $I\Delta_0(\text{exp})$ in $I\Delta_1$. This interpretation preserves the domain, and $0, S, +, \cdot, =, \Delta$.

We can also view PRA as a subsystem of $I\Delta_1$. This is because the algorithms associated with every primitive recursive function can be proved to be total (halt at all inputs) within $I\Delta_1$. This fact can be proved in $I\Delta_0(\text{exp})$.

As remarked before, we can view the language of PRA as including L_0 .

THEOREM 7.1. $I\Delta_1$ and PRA prove the same Δ_2 sentences. In particular, a Turing machine can be proved in $I\Delta_1$ to halt everywhere iff it can be proved in PRA to halt everywhere. This fact cannot be proved in $I\Delta_0(\text{exp})$. Moreover, this fact is provably equivalent to superexp over $I\Delta_0(\text{exp})$.

THEOREM 7.2. $I\Delta_1$ remains logically equivalent if we make any of the following changes in formulation. Using order induction for Δ_1 formulas. Using least number principle for Δ_1 formulas. Using order induction for Δ_1 formulas. Using least number principle for Δ_1 formulas.

THEOREM 7.3. $I\Delta_1$ is finitely axiomatizable. The result of applying bounded quantification to a Δ_1 formula is provably equivalent to a Δ_1 formula over $I\Delta_1$.

8. $I\Delta_n$, $n \geq 2$.

$I\Delta_n$ is \mathcal{Q} together with induction for all Δ_n formulas.

THEOREM 8.1. $I\Delta_n$ remains logically equivalent if we make any of the following changes in formulation. Using order induction for Δ_n formulas. Using least number principle for Δ_n formulas. Using order induction for Δ_n formulas. Using least number principle for Δ_n formulas.

THEOREM 8.2. $I\Box_n$ is finitely axiomatizable. The result of applying bounded quantification to a \Box_n formula is provably equivalent to a \Box_n formula over $I\Box_n$.

THEOREM 8.3. $I\Box_{n+1}$ proves the 1-consistency of $I\Box_n$. In fact, $I\Box_{n+1}$ proves "every \Box_{n+1} sentence provable in $I\Box_n$ is true".

Theorem 8.3 needs a discussion of the development of truth predicates in $I\Box_{n+1}$, although there is an obvious version of it without this.

9. PA.

PA is Peano arithmetic, which is the union of the $I\Box_n$.

THEOREM 9.1. PA is not finitely axiomatizable. For all $n, m \geq 0$, PA proves "every \Box_m sentence provable in $I\Box_n$ is true".

We end the lecture with a discussion of provably recursive functions and \Box_0 , $<\Box_0$ recursive functions, and \Box_0 recursive functions. The provably recursive functions are exactly the $<\Box_0$ recursive functions. See

H. Friedman and M. Sheard, Elementary descent recursion and proof theory, *Annals of Pure and Applied Logic* 71 (1995), pp. 1-45.

PHILOSOPHY 536
PHILOSOPHY OF MATHEMATICS
LECTURE 5
11/6/02
11/7/02

As promised, we begin with our preferred independence result from PA (Peano Arithmetic). The original one of a serious mathematical flavor was that of Paris and Harrington in 1977, published as an Appendix in the Barwise handbook for mathematical logic, Springer.

Arguably more mathematically natural ones were published in my 1998 *Annals of Mathematics* paper, which is mostly concerned with other matters. Also the one of Kanamori and McAloon is arguably more natural, and an account of it has appeared in Dave Marker's recent model theory book, Springer.

A number of quite different arguably more natural ones related to the Kruskal tree theorem has appeared in my article "Internal tree embeddings" in the Feferfest volume, published by the ASL, 2002.

Let $S(A)$ be the set of all subsets of A and $S_k(A)$ be the set of all subsets of A of cardinality k . Write $|A|$ for the cardinality of A . Let $[n] = \{1, \dots, n\}$.

THEOREM 1. For all $k \geq 1$ there exists $n \geq 1$ such that the following holds. For every $F: S[n] \rightarrow [n]$ there exists $E \subseteq S_k[n]$ such that $|F[S(E)] \cap [\min(E)+k]| \leq k$.

THEOREM 2. Theorem 1 cannot be proved in PA. It is provably equivalent to the 1-consistency of PA over EFA. The growth rate of the least n as a function of k is an Σ_0 -recursive function that eventually dominates every $< \Sigma_0$ -recursive function.

We now discuss subsystems of second order arithmetic. We follow the notation and treatment of Simpson's authoritative book, *Subsystems of Second Order Arithmetic*, Springer, 1999.

1. Z_2 .

Z_2 is so called second order arithmetic, but it is not a second order system. It is a two sorted first order system. Lower case letters range over $\mathbb{N} = \{0, 1, 2, \dots\}$. Upper case letters range over the subsets of \mathbb{N} . The former are the numerical variables, and the latter are the set variables.

The numerical terms are built up from the numerical variables, the constant symbols $0, 1$, and the binary function symbols $+, \cdot$. The atomic formulas are of the forms

$$\begin{aligned} t_1 &= t_2 \\ t_1 &< t_2 \\ t_1 &\in X \end{aligned}$$

where t_1, t_2 are numerical terms and X is a set variable.

Formulas are built up from atomic formulas by means of the connectives $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$, the number quantifiers $\exists n, \forall n$, and the set quantifiers $\exists X, \forall X$. A sentence is a formula with no free variables. L_2 is this language of second order arithmetic.

There is a standard Hilbert style logically complete system appropriate for L_2 .

The intended model for L_2 is $(\mathbb{N}, S(\mathbb{N}), +, \cdot, 0, 1, <)$. An \mathbb{N} -model is any model for L_2 of the form $(\mathbb{N}, E, +, \cdot, 0, 1, <)$, $E \subseteq S(\mathbb{N})$. By usual conventions it is required that E be nonempty.

We now present the system Z_2 . It is understood that we have the usual axioms and rules of logic for L_2 .

1. Numerical axioms.

$$\begin{aligned} \mathbb{N} + 1 &= 0 \\ m + 1 &= n + 1 \iff m = n \\ m + 0 &= m \\ m + (n + 1) &= (m + n) + 1 \\ m \cdot 0 &= 0 \\ m \cdot (n + 1) &= (m \cdot n) + m \\ \mathbb{N} &< 0 \\ m < n + 1 &\iff (m < n \vee m = n) \end{aligned}$$

2. Induction axiom.

$$(0 \in X \wedge (\forall n)(n \in X \implies n + 1 \in X)) \implies \mathbb{N} \subseteq X.$$

3. Comprehension axioms.

$(\exists X)(\forall n)(n \in X \iff \varphi)$, where φ is a formula of L_2 in which X is not free.

Z_2 is very powerful. However, Z_2 is not the most powerful system one can naturally write down of a "logical" character that is in the language L_2 . There is the axiom of countable choice, and the stronger axiom of dependent choice.

$$\begin{aligned} (\forall n)(\exists X)(\exists \varphi) \implies (\exists Y)(\forall n)(\exists X)(\exists \varphi \varphi \implies Y = X_n) \\ (\exists X)(\exists Y)(\exists \varphi) \implies (\exists W)(\forall n)(\exists X)(\exists Y)(\exists \varphi \varphi \implies X = W_n \wedge Y = W_{n+1}) \end{aligned}$$

where the displayed equations are suitable abbreviations.

One can attempt to prove that in some sense dependent choice is the strongest "simple" principle in L_2 . There are a lot of difficulties in carrying out such a program, but let me mention something that seems particularly promising.

Note how simple the comprehension axiom scheme is. One can define the general notion of a scheme. Note that the comprehension axiom scheme is a scheme with 2 quantifiers in

which the only nonlogical symbol is \exists (and one schematic letter). One can attempt to analyze all such schemes, and determine their status in various senses. In the general notion of scheme, one uses \exists syntactically as a unary relation symbol, writing

$$(\exists X) (\exists n) (n \leq X \leq \exists(n))$$

to indicate that among the variables displayed, only n is allowed to be free when substituting formulas for the schematic letter \exists . This provides a general framework for free variable restrictions such as in the comprehension axiom scheme.

I have done classifications like this which are much more difficult. See "Three quantifier sentences" on the preprint server that I use. It will appear in *Fundamenta*. I would try to classify all \exists schemes in L_2 with three quantifiers.

THEOREM 1.1. Z_2 without induction interprets Z_2 .

2. Restricted comprehension.

The most obvious way to obtain important fragments of Z_2 is to restrict the formulas \exists in comprehension. The most simpleminded of these restrictions is to require that \exists be arithmetical; i.e., have no set quantifiers. Then we get what is called ACA_0 , for arithmetic comprehension. The naught is because, historically, ACA was considered, where induction was formulated as a scheme involving all formulas. For a number of good reasons, the systems with the induction axiom rather than the induction scheme now predominate. It is known that under very general circumstances, the scheme is stronger than the axiom, both in terms of outright provability and in terms of interpretation power and consistency strength.

THEOREM 2.1. Z_2 is not finitely axiomatizable. ACA_0 is finitely axiomatizable.

The system ACA_0 is particularly important in light of its connection with PA. Note that PA is a subsystem of ACA_0 in the sense that every axiom of PA is a theorem of ACA_0 .

THEOREM 2.2. ACA_0 is a conservative extension of PA for all arithmetic sentences. This fact is equivalent to

"exponentiation can be indefinitely iterated" over $EFA = I\Delta_0(\exp)$.

It is natural to consider the extension of PA in L_2 that has no comprehension but allows induction for all arithmetic formulas of L_2 ; i.e., free set variables. Call this PA_2 .

THEOREM 2.3. ACA_0 is a conservative extension of PA_2 for arithmetic formulas of L_2 .

THEOREM 2.4. The Δ_1 -models of ACA_0 are those where $E \subseteq S(\Delta_1)$ is nonempty and closed under relative arithmeticity. The arithmetic sets form the minimum Δ_1 -model of ACA_0 .

A Δ_1^k formula, $k \geq 1$, is a formula of L_2 which starts with a universal set quantifier followed by at most $k-1$ set quantifiers, followed by an arithmetic formula. The first mentioned quantifier is allowed to be omitted.

A Δ_1^k formula, $k \geq 1$, is defined analogously.

Δ_1^0 and Δ_0^1 is identified with the arithmetic formulas.

Δ_1^k - CA_0 results from Z_2 by restricting Δ_1 in comprehension to Δ_1^k formulas. Δ_1^k - CA_0 is defined analogously.

THEOREM 2.5. Let $k \geq 0$. Δ_1^k - CA_0 and Δ_1^{k+1} - CA_0 are equivalent and finitely axiomatizable. Δ_1^k - CA_0 does not derive Δ_1^{k+1} - CA_0 . In fact, Δ_1^{k+1} - CA_0 is not interpretable in Δ_1^k - CA_0 , and proves the consistency of Δ_1^k - CA_0 . These results hold even if we replace Δ_1^k - CA_0 with Δ_1^k - $CA_0 + IND$.

Here IND is the induction scheme for all formulas of L_2 .

THEOREM 2.6. There is no minimal Δ_1 -model of Z_2 . For $k \geq 1$, there is no minimum Δ_1 -model of Δ_1^k - CA_0 . In fact, no minimal Δ_1 -model of Δ_1^k - CA_0 .

We had published a proof that there is no minimal Δ_1 -model of Z_2 apparently without pushing the generality. Quinsey is credited with showing the following.

THEOREM 2.7. Let S be a recursive set of L_2 -sentences which includes the axioms of ATR_0 (a fragment of Δ_1^1 - CA_0). Then S has no minimal Δ_1 -model.

All this is in Simpson's book in detail.

A Σ^1_k -model is a Σ^1_k -model such that every Σ^1_1 formula with parameters from the Σ^1_k -model that holds in the Σ^1_k -model is true. This turns out to be an important notion.

THEOREM 2.8. For all $k \geq 0$, there is a minimum Σ^1_k -model of $\Sigma^1_k\text{-CA}_0$. The minimum Σ^1_k -model of $\Sigma^1_k\text{-CA}_0$ is properly included in the minimum Σ^1_{k+1} -model of $\Sigma^1_{k+1}\text{-CA}_0$, and in fact has an enumeration there.

There is another set of simpleminded restriction of Z_2 of importance. These are $\Sigma^1_k\text{-CA}_0$. Here comprehension takes the form

$$(\exists n) (\exists x) (\exists y) \phi(x, y) \rightarrow (\exists x) (\exists y) (n \leq x \wedge \phi(x, y))$$

where ϕ is Σ^1_k and ψ is Σ^1_k and X is not free in ϕ .

THEOREM 2.9. For all $k \geq 1$, $\Sigma^1_k\text{-CA}_0 \not\equiv \Sigma^1_{k+1}\text{-CA}_0 \not\equiv \Sigma^1_{k+1}\text{-CA}_0$, and $\Sigma^1_k\text{-CA}_0$ is finitely axiomatizable. The first proper inclusion is weak in that we have equiconsistency and conservative extension for Σ^1_1 sentences. The second proper inclusion is strong in that we have provable consistency.

THEOREM 2.10. $\Sigma^1_1\text{-CA}_0$ has a minimum Σ^1_1 -model, and this is the hyperarithmetical subsets of \mathbb{N} . For $k \geq 2$, $\Sigma^1_k\text{-CA}_0$ has no minimal Σ^1_k -model by Quinsey's theorem.

3. Fragments of $\Sigma^1_1\text{-CA}_0$.

It turns out that in the appropriate formalization of mathematics, the vast bulk is provable in $\Sigma^1_1\text{-CA}_0$, and in fact even further down. The next lecture is about Reverse Mathematics, which concerns the logical analysis of mathematics, and the main systems are subsystems of $\Sigma^1_1\text{-CA}_0$.

The most commonly encountered of the proper subsystems of $\Sigma^1_1\text{-CA}_0$ is the system ATR_0 , or arithmetic transfinite recursion.

ATR_0 replaces the comprehension axiom scheme by a single axiom that says the following. Let X be a well ordering of \mathbb{N} , coded in terms of a standard pairing function on \mathbb{N} . Let $\phi(n, Y)$ be an arithmetic formula with set and number parameters allowed. Note that ϕ provides what is called an arithmetic operator

that sends Y to $\{n: \exists (n, Y)\}$. We assert that we can iterate this operation along the well ordering X starting with any $Y \in \mathcal{P}$. This construction is given in terms of a set W , using its cross sections W_n , $n \in \mathcal{P}$. At limits, these are combined into a single set in a standard way, and one then continues.

ATR_0 is also the weakest of the most commonly encountered systems for which the hyperarithmetical subsets of \mathcal{P} do not form an \mathcal{P} -model.

THEOREM 3.1. ATR_0 is finitely axiomatizable and is a proper fragment of $\Sigma^1_1\text{-CA}_0$. In fact, ATR_0 is provably consistent within $\Sigma^1_1\text{-CA}_0$.

We proved the following.

THEOREM 3.2. ATR_0 is equiconsistent with the Feferman Schutte analysis of predicativity in terms of the proof theoretic ordinal Γ_0 . ATR_0 is a conservative extension of the versions of predicativity that are in L_2 , for all Σ^1_1 sentences. This is true even for the latter systems with IND.

The strongest of the most commonly encountered proper subsystems of ATR_0 is ACA_0 which we have discussed earlier.

THEOREM 3.3. ATR_0 proves the consistency of ACA_0 . This is true even for $ACA = ACA_0 + \text{IND}$. ATR_0 proves $\Sigma^1_1\text{-CA}_0$.

We now come to fragments of ACA_0 . Two very important ones have emerged, RCA_0 and WKL_0 . RCA_0 is based on a comprehension axiom scheme, but the situation is more delicate. WKL_0 is an extension of RCA_0 by an important principle that is not like comprehension at all.

RCA_0 is recursive comprehension axiom naught. We need to define the bounded arithmetic formulas of L_2 . We have encountered this in the previous lecture. We will do this using terms:

$$\begin{aligned} (\exists n < t) (\varphi) &= (\exists n) (n < t \wedge \varphi) \\ (\exists n < t) (\varphi) &= (\exists n) (n < t \wedge \varphi) \end{aligned}$$

where φ is a formula of L_2 , t is a numerical term, and n does not appear in t .

The bounded arithmetic formulas are the arithmetic formulas all of whose quantifiers are so bounded.

The Σ_1^0 formulas are the arithmetic formulas of L_2 which begin with an existential number quantifier followed by a bounded arithmetic formula. Analogously for Σ_1^0 .

The axioms of RCA_0 consist of

1. Numerical axioms. As in Z_2 .
2. Σ_1^0 induction.
 $(\exists n/0) \varphi \rightarrow (\exists n) (\varphi \wedge \varphi[n/n+1]) \rightarrow \varphi$, where φ is Σ_1^0 .
3. Σ_1^0 comprehension.
 $(\exists n) (\varphi \wedge \psi) \rightarrow (\exists X) (\exists n) (n \leq X \wedge \varphi)$, where φ is Σ_1^0 , ψ is Σ_1^0 , and X is not free in φ .

THEOREM 3.4. RCA_0 is finitely axiomatized. RCA_0 has the minimum Σ_1^0 -model consisting of the recursive subsets of \mathbb{N} . RCA_0 is a proper subsystem of ACA_0 . ACA_0 proves the consistency of RCA_0 but not of $RCA = RCA_0 + IND$.

THEOREM 3.5. RCA_0 is a conservative extension of $I\Sigma_1^0$ for all arithmetic sentences, which is in turn a conservative extension of PRA for Σ_2^0 sentences.

We now come to WKL_0 . This is RCA_0 augmented with "weak Konig's lemma". This asserts that any infinite tree of finite sequences of 0's and 1's has an infinite path. Using standard coding mechanisms, this is easily stated in RCA_0 .

THEOREM 3.6. WKL_0 is a subsystem of ACA_0 , which proves its consistency. WKL_0 has no minimal Σ_1^0 -model. WKL_0 has an Σ_1^0 -model consisting of some of the subsets of \mathbb{N} recursive in $0'$ (i.e., Σ_2^0). WKL_0 is conservative over RCA_0 for Σ_1^1 sentences.

4. TI.

TI consists of ACA_0 together with the axiom scheme

$$WF(X) \rightarrow TI(X; \varphi)$$

where $WF(X)$ means that X codes a well ordering of \mathbb{N} , and $TI(X; \varphi)$ is transfinite induction on X with respect to the arbitrary formula φ .

THEOREM 4.1. For all $k \geq 1$, TI is not provable in $\Sigma^1_k\text{-CA}_0$. $\Sigma^1_1\text{-CA}_0$ proves the consistency of TI, and even the existence of a Σ^1_1 model of TI. TI is not finitely axiomatizable.

THEOREM 4.2. TI proves ATR_0 , and the existence of an Σ^1_1 -model of ATR_0 . TI has no minimal Σ^1_1 model. Neither does ATR_0 .

5. Proof theoretic measures of systems.

Two common measures of systems are the provably recursive functions and the proof theoretic ordinal.

Let T be a theory in L_2 that contains EFA. A provably recursive function is a recursive function $f: \mathbb{N} \rightarrow \mathbb{N}$ such that for some index e of a Turing machine,

- i) T proves $(\exists n) (\{e\}(n) \text{ halts})$;
- ii) for all n , $f(n) = \{e\}(n)$.

Suitable classifications of the provably recursive functions of subsystems of Z_2 has been a preoccupation of proof theorists for many decades.

RCA_0 Primitive recursive functions.
 WKL_0 Primitive recursive functions.
 ACA_0 $<\Sigma^1_0$ recursive functions.
 ATR_0 $<\Sigma^1_0$ recursive functions.
 $\Sigma^1_1\text{-CA}_0$ $<\Sigma^1_{\omega}$ recursive functions.
 TI $<\Sigma^1_{\omega^{\omega}}$ recursive functions.

The provable ordinal of T is the sup of all ordinals α such that for some index e of a Turing machine,

- i) T proves " e defines a well ordering of \mathbb{N} ";
- ii) the well ordering of \mathbb{N} that e defines has ordinal α .

RCA_0 ω^{ω} .
 WKL_0 ω^{ω} .
 ACA_0 ω^{ω} .
 ATR_0 ω^{ω} .
 $\Sigma^1_1\text{-CA}_0$ $\omega^{\omega^{\omega}}$.
 TI $\omega^{\omega^{\omega}}$.

Reverse Mathematics

11/13/02

11/17/2

1. The reverse mathematics program.

Here are the five main systems of reverse mathematics.

RCA_0

1. Numerical axioms.
2. Σ^0_1 induction.
3. Σ^0_1 comprehension.

WKL_0

1. Numerical axioms.
2. Σ^0_1 induction.
3. Σ^0_1 comprehension.
4. Weak Konig's Lemma.

ACA_0

1. Numerical axioms.
2. Induction axiom.
3. Comprehension axioms. For arithmetic formulas only.

ATR_0

1. Numerical axioms.
2. Induction axiom.
3. All arithmetic transfinite recursions along all well orderings of \mathbb{Q} .

$\Sigma^1_1\text{-CA}_0$

1. Numerical axioms.
2. Induction axiom.
3. Comprehension axioms. For Σ^1_1 formulas only.

These systems, as well as some others, are used to classify the logical structure of a substantial body of mathematics.

One strives for the following kind of result. Let T be a mathematical theorem. It is essential that there be a faithful formalization of T as a sentence in the language of Z_2 , which is the same as the two sorted language of these five systems, based on $0, 1, +, \cdot, <, \square$.

There are some fundamental issues regarding such faithful formalizations - the so called coding issues. It is important to have a small set of primitives for many reasons, but this comes with a cost. Obviously mathematics proceeds by building up very substantial layers of definitions, one on top of another, and this is not done with logical investigations in mind.

Often mathematics proceeds with notions for which standard unraveling into mathematical primitives involve implicit epistemic/ontological commitments that are sufficiently strong as to overwhelm any inherent logical structure we seek to uncover.

In practice, we seek to develop coding mechanisms, whereby complicated objects are reduced to the primitives of Z_2 in ways that do not destroy what we seek to uncover. This requires care.

In the present development of RM = reverse mathematics, a set of established coding mechanisms have emerged, which in many cases appear unassailable. However, in other cases they need to be justified in ways that they have not been.

I have been trying to develop some ideas about the justifications of coding. I haven't had the time to work out a general framework for this, but in section 3 I will present some justifications on a somewhat ad hoc basis of the principal coding mechanisms of RM.

Now let's come back to the main theme of RM. We start with a mathematical theorem T , the more fundamental the better. We assume that we have a faithful formalization of T in the language of Z_2 .

We seek to determine the "logical status" of T . The preferred way is to show that one of the logically fundamental finitely axiomatized fragments of Z_2 such as WKL_0 , ACA_0 , ATR_0 , $\square^1_1\text{-}CA_0$, is outright provably equivalent to T over RCA_0 . That is why we call RCA_0 the base theory for RM.

Why is this RM program illuminating? We mention two factors. One is the robustness of the formalization of the relevant mathematics in the language of Z_2 . The other is the number of equivalence classes.

What equivalence relation? The equivalence relation

$$RCA_0 \text{ proves } S \square T$$

where S, T are appropriately formalized mathematical theorems.

Such equivalence classes are generally named by the most logically fundamental formal system that has arisen which is provably equivalent, over RCA_0 , to the elements of the equivalence class.

As I said last week, the current bible of RM is Simpson's book, *Subsystems of Second Order Arithmetic*, Springer, 1999.

In there, I would venture to say that between 10 and 15 equivalence classes are represented.

It is true that there is a special situation with Kruskal's theorem, where there are numerical parameters which, when varied, lead to inequivalent statements over RCA_0 . So this is a way of generating a lot of equivalence classes. But this is highly unusual and can be isolated from the discussion as involving weakenings of a single theorem.

We now move on to the issue of linearity. The five main systems of RM are linearly ordered under derivability. However, there are several good examples of mathematical theorems classified under RM where neither is provable from the other over RCA_0 .

In all known cases arising out of ordinary mathematics, we have comparability in the weaker sense. Either $RCA_0 + S$ interprets $RCA_0 + T$ or vice versa.

In fact, we have observed a strong dichotomy. Either $RCA_0 + S$ and $RCA_0 + T$ are mutually interpretable, or one of these two proves the consistency of the other. We conjecture that this kind of dichotomy will continue to be the case in the development of RM.

A great deal of mathematics, when appropriately formalized in the language of Z_2 , is provable in RCA_0 . Therefore it is not subject to an RM analysis (except to the extent of proving it in RCA_0).

Therefore it is of great interest to weaken the base theory of RM from RCA_0 to something weaker, or much weaker.

If the base theory is dropped too far, then we may lose the robustness of the formalizations, where a given mathematical theorem may have a myriad of slightly different formalizations, no two of which are provably equivalent over the too weak base theory. This situation could be saved if some guiding principle about formalizations proved unifying and effective.

Research on weakening the base theory somewhat has already begun by Simpson's work on RCA_0^* . Here \square_1^0 induction is dropped in favor of induction for bounded formulas, where exponentiation is added. We have conservation over EFA = exponential function arithmetic = $I\Sigma_0(\text{exp})$. The results are somewhat encouraging, but it is still too early to tell how good an idea this really is, and how more radical weakenings will fare.

There is the objection that the axioms of RCA_0 , and even RCA_0^* , are of a logical nature, and should be replaced by purely mathematical principles. In fact, can one build up logical power starting only from logic and direct quotes from the fundamental mathematical literature? This would show in a new definitive way that logical strength and the Gödel phenomena are unremovable. They cannot be gotten around by any wholly new way to slice the pie.

I addressed this issue with some success in a paper called Reverse Arithmetic.

2. Some Reverse arithmetic.

The results of this section can be found in the paper Finite Reverse Mathematics, on the mathpreprints preprint server.

We introduce the system T_0 , and show that it corresponds to the system $I\Sigma_0$ of polynomially bounded arithmetic (presented below).

Let T_0 be the following system in the two sorted language with variables over integers and variables over finite sets of integers. For the integer sort, we use the language $0, 1, +, -, \cdot, <, =$ of linearly ordered rings. We use \subseteq between integers and sets. Equality is used only between integers.

The axioms of T_0 are:

1. Linearly ordered ring axioms.
2. Finite interval. $(\exists A)(\forall x)(x \in A \rightarrow (y < x \rightarrow x < z))$.
3. Boolean difference. $(\exists C)(\forall x)(x \in C \rightarrow (x \in A \rightarrow \neg(x \in B)))$.
4. Set addition. $(\exists C)(\forall x)(x \in C \rightarrow (\exists y)(\exists z)(y \in A \wedge z \in B \wedge x = y+z))$.
5. Set multiplication. $(\exists C)(\forall x)(x \in C \rightarrow (\exists y)(\exists z)(y \in A \wedge z \in B \wedge x = y \cdot z))$.
6. Least element. $(\forall x)(x \in A) \rightarrow (\exists x)(x \in A \wedge \neg(\exists y)(y \in A \wedge y < x))$.

THEOREM 2.1. T_0 can be reaxiomatized as follows.

1. Linearly ordered ring axioms.
2. $(\exists A)(\forall x)(x \in A \rightarrow (y < x \wedge x < z \rightarrow \varphi))$, where φ is a bounded formula of T_0 and A is not free in φ .
3. Least element.

We now introduce the system K_0 based on integers only. The language of K_0 is the same as that of T_0 , except no set variables are allowed.

A bounded formula of K_0 is a bounded formula of T_0 that has no set variables.

The axioms of K_0 are as follows.

1. Linearly ordered ring axioms.
2. $(\exists [x/0] \rightarrow (\forall x \geq 0)(\varphi \rightarrow \varphi[x/x+1])) \rightarrow (x \geq 0 \rightarrow \varphi)$, where φ is a bounded formula of K_0 .

THEOREM 2.2. T_0 and K_0 prove the same formulas without set variables.

THEOREM 2.3. A sentence in the language of $I\mathbb{N}_0$ is provable in $I\mathbb{N}_0$ if and only if the result of relativizing each quantifier to the nonnegative integers and replacing each $S(t)$ by $t+1$ is provable in K_0 (or T_0).

We now consider the system T_1 whose axioms are

1. The axioms of T_0 .
2. Multiples. $(\exists y)(0 < y \wedge (\exists z)((0 < z \wedge z < x) \wedge (\exists w)(y = z \cdot w)))$.

Informally, axiom 2 asserts that for all integers x , the positive integers $1, \dots, x$ have a common positive multiple. This axiom can be viewed as mathematically essential since it is an immediate consequence of having a usable discrete factorial function.

An obvious consequence of T_1 is

- 2'. $(\exists y)(y \neq 0 \wedge (\exists z)((z \neq 0 \wedge z \in A) \wedge (\exists w)(y = z \cdot w)))$.

Informally, 2' asserts that the nonzero elements of any finite set have a nonzero common multiple.

The axioms of K_1 are as follows.

1. Linearly ordered ring axioms.
2. $x, y \geq 0 \wedge (x^0 = 1 \wedge x^{y+1}) = x^y \cdot x$;
3. $(x < 0 \wedge y < 0) \wedge x^y = 0$;
4. $(\exists [x/0] \wedge (\exists x \geq 0)(\exists \square \square [x/x+1])) \wedge (x \geq 0 \wedge \square)$, where \square is a bounded formula in the language of K_1 .

THEOREM 2.4. T_1 and K_1 prove the same formulas without set variables and exponentiation.

THEOREM 2.5. A sentence in the language of $I \square_0(\text{exp})$ is provable in $I \square_0(\text{exp})$ iff the result of relativizing each quantifier to the nonnegative integers and replacing each $S(t)$ by $t+1$ is provable in K_1 . A sentence in the language of $I \square_0$ is provable in $I \square_0 + \text{exp}$ iff the result of relativizing each quantifier to the nonnegative integers and replacing each $S(t)$ by $t+1$ is provable in T_1 .

The axioms of $T_1(!)$ are

1. The axioms of T_0 .
2. $0! = 1$.
3. $x > 0 \wedge x! = x \cdot (x-1)!$.
4. $0 < x < y \wedge (\exists z)(0 < z \wedge z \cdot (x!) = y!)$.

THEOREM 2.6. T_1 is a subsystem of $T_1(!)$. T_1 and $T_1(!)$ prove the same formulas that do not mention $!$.

3. Coding mechanisms in RM.

Let us start with one of the most elemental coding mechanisms of all: the coding mechanism for ordered pairs from \mathbb{N} (the set of all natural numbers, or \mathbb{N}). The official pairing function of [Si99] is

$$(m, n) = (m+n)^2 + m.$$

The essential point about pairing is that there is an obvious extension of RCA_0 involving pairing, where every formula with all of whose free variables are of the sorts of RCA_0 , is provably equivalent to a formula with the same free variables of RCA_0 .

The coding mechanism in the case of pairing provides an interpretation of the extended theory in RCA_0 which is correct in the sense that this interpretation, when applied to any formula all of whose free variables are of the sorts of RCA_0 , provides a formula in the language of RCA_0 which is provably equivalent to it. Since any coding mechanism is taken to be the identity interpretation when applied to any formula of RCA_0 , as a consequence we see that the extension of RCA_0 is a conservative extension of RCA_0 .

In our case, the relevant extension of RCA_0 has new sorts for ordered pairs, and a binary function symbol F taking natural number arguments into ordered pair values, with the axiom

$$F(x, y) = F(z, w) \iff (x = z \iff y = w).$$

Let us call this extension of RCA_0 , $\text{RCA}_0(\text{pair})$. Let ϕ be a formula in $L(\text{RCA}_0(\text{pair}))$ all of whose free variables are in $L(\text{RCA}_0)$. It is clear that ϕ is provably equivalent to a formula in RCA_0 with the same free variables, since the only atomic formulas involving the new sort are of the form

$$F(s_1, s_2) = F(t_1, t_2)$$

where s_1, s_2, t_1, t_2 are terms in $L(\text{RCA}_0)$. Each such atomic subformula can be replaced by $s_1 = t_1 \iff s_2 = t_2$, and the resulting formula will be provably equivalent in $\text{RCA}(\text{pair})$.

The resulting formula will have the same free variables and be in $L(RCA_0)$.

Also, we can use the official pairing function of [Si99] and get a formula in $L(RCA_0)$ with the same free variables which is provably equivalent in $RCA(\text{pair})$.

We then want to add sets of ordered pairs. The crucial axiom that makes this work right is that for every set of ordered pairs, the forward image under any quadratic function, with natural number coefficients, of two variables is a set. Also, given any set of natural numbers, the inverse under any such quadratic function is a set of ordered pairs.

With sets of ordered pairs, we can introduce functions from N to N . The crucial axiom is the relationship between sets of ordered pairs.

Next let us consider the extension of RCA_0 , $RCA_0(Qofld)$, by the ordered field of rational numbers. We have the field operations on the new sort for rational numbers, together with a function symbol for the embedding of the natural numbers into the rational numbers. There are a number of obvious axioms including that the rational numbers are the same as or minus of the ratio between natural numbers (without dividing by zero). Also axioms asserting the ring operations on the natural numbers correspond to the ring operations on the nonnegative rational numbers.

From such axioms, one can prove that for each rational there is a unique two natural numbers, which are appropriately reduced, with a signed bit which corresponds to it. Also, for each two natural numbers, appropriately reduced, there is a unique rational number corresponding to it.

Using these ideas, one then sees that every formula in $L(RCA_0(Qofld))$ with free variables all from $L(RCA_0)$ is provably equivalent in RCA_0 to a formula in $L(RCA_0)$ with the same free variables. Also the standard coding of the field of rationals over RCA_0 witnesses this fact.

We then add on sequences from Q , building on earlier experience with sequences from N .

We now wish to add on the ordered field of real numbers. We have the obvious algebraic axioms, with inequalities. But we

also have the crucial axiom that to every real number there is an infinite sequence of rational numbers that converges to it with $1/n$ convergence. Also to every infinite sequence of rational numbers that is a $1/n$ Cauchy sequence, there is a real number to which it converges.

The key point is that every sentence involving real numbers, with free variables from earlier constructions, is provably equivalent to a formula with the same free variables that does not involve real numbers. The idea is to replace talk about real numbers with talk about Cauchy sequences, provably in the relevant theory.

We now come to a special case of continuous functions, where things get somewhat more delicate.

Let us see what is involved in adding continuous functions $F: [0,1] \rightarrow \mathbb{R}$. Aside from obvious axioms, we need the crucial axiom in the form of the Stone Weierstraas theorem. Specifically, that there exists an infinite sequence of polynomials from $[0,1] \rightarrow \mathbb{R}$ which $1/n$ uniformly converges to F . I.e., every such sequences converges to some such F , and for every such F there exists such a sequence that converges to F . This in turn depends on a prior development of infinite sequences of polynomials. This also in turn depends on a prior development of polynomials. All of these necessary prior developments must be worked out carefully.

Note that in order to pull this off for continuous functions from $[0,1]$ into \mathbb{R} , we needed to use a basic theorem of mathematics, Stone Weierstraas, as an axiom. This will be typical of how delicate coding issues will be resolved. I have not attempted to go much farther with this program.

PHILOSOPHY 536
PHILOSOPHY OF MATHEMATICS
LECTURE 7
11/20/02

1. Zermelo set theory.

We now discuss systems ranging from Z_2 to Z and ZC . Recall Z_2 is the system of full second order arithmetic that we discussed in the last two lectures. Z is Zermelo set theory with the axiom of choice. The language of Z is $\in, =$.

1. Extensionality.
2. Pairing.
3. Union.
4. Separation.
5. Infinity.
6. Power set.

ZC is Z together with the axiom of choice.

There is a delicate point about Z in connection with the axiom of infinity. The usual formulation of the axiom of infinity is

Infinity. $(\exists x)(\emptyset \in x \wedge (\forall y \in x)(y \in \{y\} \in x))$.

Since we have full separation, we can define ω as the intersection of all such sets A. This is standard.

There is something not very robust about this. It is perfectly sensible to take infinity in the form of the existence of a set A such that

Infinity'. $(\exists x)(\emptyset \in x \wedge (\forall y, z \in x)(y \in \{z\} \in x))$.

This form of the axiom of infinity has its advantages, since the least such A is V_ω , which is the set of all hereditarily finite sets.

THEOREM 1.1. Z, or even ZC, does not prove Infinity'. However, ZC with Infinity' is interpretable in Z. Infinity' is provable in ZF.

Proof: Define $S^n(\emptyset)$ for $n \geq 0$, as follows. $S^0(\emptyset) = \emptyset$, $S^{n+1}(\emptyset) = S(S^n)$. Define $S^*(\emptyset) = \text{the union over } n \text{ of } S^n(\emptyset)$. Here S is the power set operation. Note that each $S^n(\emptyset)$ is a transitive set. It is clear that $S^*(\emptyset)$ forms a model of ZC. It is easily proved by induction on $n \geq 0$ that for every $x \in S^n(\emptyset)$, $(\exists y_1, \dots, y_n)((y_1 \in y_2 \in \dots \in y_n \in x) \wedge y_1 \in \emptyset)$. Since this does not hold of any superset of V_ω , we see that no superset of V_ω is an element of $S^n(\emptyset)$. Hence no superset of V_ω lies in $S^*(\emptyset)$. Therefore $S^*(\emptyset)$ does not satisfy Infinity'. It is easy to manipulate the epsilon relation on \emptyset so that it behaves like the epsilon relation on V_ω , and then preserve epsilon with respect to sets that are not in \emptyset , in order to achieve an interpretation of ZC + Infinity' in ZC. It is well known that ZC is interpretable in Z via Gödel's constructible

universe, and how this argument can be developed over Z instead of the usual ZF . It is well known how to prove 'Infinity' in ZF , using replacement. QED

ZC is actually an extremely effective vehicle for the foundations of mathematics, in that it is so powerful that one has to go rather far to find mathematically natural examples of theorems provable in ZFC but not in ZC , by any reasonable standard of mathematically natural. We will discuss such examples in the next lecture.

2. Fragments of ZC .

We have not previously discussed set theories, but rather systems of first and second order arithmetic. In this section, we provide fragments of ZC that correspond to the levels of interpretation power represented by the previously considered systems.

We start with the two main systems, PA and Z_2 . In most cases, we list two versions, the first with a large number of axioms, the second with a small number of axioms. Each system and the one or two that come under it are mutually interpretable and equiconsistent in the appropriate sense.

We will not use equality as primitive.

PA .

1. Extensionality.
2. Pairing.
3. Union.
4. Separation.
5. Power set.
6. Replacement.
7. Choice.
8. Foundation.
9. Every set is finite.

1. Pairing.
2. Separation.

Z_2 .

1. Extensionality.
2. Pairing.
3. Union.
4. Separation.
5. Replacement.
6. Choice.
7. Foundation.
8. Infinity.

1. Pairing.
2. Separation.
3. Infinity.

$I\aleph_0$.

1. Extensionality.
2. Pairing.
3. Union.
4. \aleph_0 -separation.
5. Choice.
6. Set foundation.
7. Cartesian product.
8. Every set is finite.

1. $x \in \{y\}$ exists.

$I\aleph_0(\text{exp})$ or EFA (exponential function arithmetic).

1. Extensionality.
2. Pairing.
3. Union.
4. \aleph_0 -separation.
5. Choice.
6. Set foundation.
7. Power set.
8. Every set is finite.

1. Pairing.
2. \aleph_0 -separation.
3. Power set.

$I\aleph_n, n \geq 1$.

1. Extensionality.
2. Pairing.
3. Union.
4. \aleph_n -separation.

5. Choice.
6. Set foundation.
8. Power set.
9. Every set is finite.

1. Pairing.
2. Δ_n -separation.

RCA_0 . Mutually interpretable with $\text{I}\Delta_1$.

ACA_0 . Mutually interpretable with PA.

ATR_0 . Simpson has a set theory mutually interpretable with ATR_0 . Probably done much more neatly with a variant of KP = Kripke Platek set theory.

$\Delta_1^1\text{-CA}_0$.

1. Extensionality.
2. Pairing.
3. Union.
4. Δ_1 -separation.
5. Choice.
6. Set foundation.
7. Cartesian product.
8. Infinity.

1. Pairing.
2. Δ_1 -separation.
3. Infinity.

$\Delta_n^1\text{-CA}_0$, $n \geq 1$.

1. Extensionality.
2. Pairing.
3. Union.
4. Δ_n -separation.
5. Choice.
6. Set foundation.
7. Cartesian product.
8. Infinity.

1. Pairing.
2. Δ_n -separation.
3. Infinity.

3. Higher order arithmetic.

Let $n \geq 1$. The vocabulary of Z_n is

- i) variables x_m^i , $1 \leq i \leq n$, and $m \geq 1$, ranging over sort i , where sort 1 is the natural number sort;
- ii) $0, 1, <, =, +, \cdot$ all in sort 1;
- iii) \wedge, \vee , the usual connectives, and the usual quantifiers in each sort;
- iv) parentheses.

The atomic formulas are

- $s = t$ and $s < t$ for numerical terms s, t ;
- $t \leq x$, where t is a numerical term and x is a variable of sort 2;
- $y \leq z$, where y, z are variables, and the sort of z is one higher than the sort of y .

The formulas are built up as usual.

The axioms of Z_n are

1. Usual numerical axioms.
2. Usual set induction.
3. All formulas $(\forall x)(\exists y)(y \leq x \wedge \varphi)$ in $L(Z_n)$, where φ is a formula in which x is not free in φ .

THEOREM 3.1. Z proves the consistency of $\exists_n Z_n$.

There is a fragment of Z that corresponds to $\exists_n Z_n$. $BZ =$ bounded Z , has the axioms

1. Extensionality.
2. Pairing.
3. Union.
4. Separation.
5. Infinity.
6. Power set.

THEOREM 3.2. BZ and $\exists_n Z_n$ are equiconsistent. BZ is finitely axiomatizable. $\exists_n Z_n$ is interpretable in BZ , but BZ is not interpretable in $\exists_n Z_n$.

We can get a close correspondence between Z_n and fragments of Z as follows.

Let T_n be

1. Extensionality.
2. Pairing.
3. Union.
4. Separation.
5. Infinity.
6. The 0-th through n-th power set of \emptyset exist.

Here the 0-th power set of \emptyset is \emptyset , as given by Infinity (and separation).

THEOREM 3.3. For all $n \geq 0$, T_n and Z_{n+1} are mutually interpretable. They are not finitely axiomatizable.

4. Theory of types.

The theory of types, TT , is similar to $\bigcup_n Z_n$, except that we have no axiom of infinity and do not have any arithmetic primitives. The axiom of infinity has to be added.

The vocabulary of TT is as follows.

- i) variables x_m^n of type n , where $n, m \geq 0$;
- ii) the usual connectives, and quantifiers in each type.

The atomic formulas are of the form

$$x \in y$$

where x, y are variables, and the sort of y is one more than the sort of x .

The axioms are the comprehension axioms, which are formulas of $L(TT)$ of the form

$$(\exists x) (\exists y) (y \in x \wedge \phi)$$

where ϕ is a formula of $L(TT)$ in which x is not free.

The axiom of infinity, INF , is formulated with some care. The standard way of doing this

"there is a nonempty set of type 2, where every element has a proper superset that is an element".

THEOREM 4.1. $TT + INF, \prod_n Z_n$, are mutually interpretable. They are also equiconsistent with BZ.

We would like to match the $TT_n + INF$ with the Z_m . Here TT_n is TT except that one uses only sorts $0, \dots, n$.

THEOREM 4.2. For all $n \geq 2$, TT_n, Z_{n+1}, T_n are mutually interpretable and equiconsistent.

5. Some relevant mathematical independence results.

We discuss Borel diagonalization theory, as it relates to independence from Z_2 and the Z . We start with Cantor's theorem.

THEOREM 5.1. In any infinite sequence of real numbers, some real number is not a coordinate of the sequence.

One defines a sequence of nondegenerate closed intervals with rational endpoints, shrinking to a point that lies off of the sequence. One obtains:

THEOREM 5.2. There is a Borel measurable function $F: \mathbb{R} \rightarrow \mathbb{R}$ such that for all $x \in \mathbb{R}$, $F(x)$ is not a coordinate of x .

$F(x)$ may depend only on the (set of) coordinates of x .

THEOREM 5.3. There is no Borel measurable function $F: \mathbb{R} \rightarrow \mathbb{R}$ obeying $\text{rng}(x) = \text{rng}(y) \implies F(x) = F(y)$, such that for all $x \in \mathbb{R}$, $F(x)$ is not a coordinate of x .

Or put positively,

THEOREM 5.4. Let $F: \mathbb{R} \rightarrow \mathbb{R}$ be Borel measurable, where for all $x, y \in \mathbb{R}$, $\text{rng}(x) = \text{rng}(y) \implies F(x) = F(y)$. There exists $x \in \mathbb{R}$ such that $F(x)$ is a coordinate of x .

THEOREM 5.5. Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be a Borel function such that $\text{rng}(x) = \text{rng}(y) \implies \text{rng}(f(x)) = \text{rng}(f(y))$. There exists x such that $\text{rng}(f(x)) \not\subseteq \text{rng}(x)$.

For $x, y \in \mathbb{R}$, define $x \sim y$ iff y is a permutation of x .

THEOREM 5.6. Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be such that $x \sim y \implies f(x) \sim f(y)$. There exists $x \in \mathbb{R}$ such that $F(x)$ is a subsequence of x .

Let $2^{\mathbb{N}}$ be the usual Cantor space. Let $s:2^{\mathbb{N}} \rightarrow 2^{\mathbb{N}}$ be given by $s(x)(n) = x(n+1)$. $f:K \rightarrow K$ is called shift invariant iff $f(x) = f(sx)$.

THEOREM 5.7. Let $f:K \rightarrow K$ be a shift invariant Borel function. There exists $x \in K$ such that $f(x) = x^{(2)}$.

Here $x^{(2)} = (x_1, x_4, x_9, x_{16}, \dots)$.

Let T be the circle group. $f:T \rightarrow T$ is double invariant if and only if $T(2x) = T(x)$.

THEOREM 5.8. There is a Borel $f:T \rightarrow T$ which agrees with every double invariant $g:T \rightarrow T$ somewhere.

Let $\text{GRP}(N)$ be the groups with domain N .

THEOREM 5.9. Let $f:\text{GRP}(N) \rightarrow \text{GRP}(N)$ be an isomorphically invariant Borel function. There exists G such that $f(G)$ is embeddable in G .

All of the above Theorems 5.1 - 5.9 are provable in Z_3 but not in Z_2 . There is the question of how to treat Borel measurable functions on complete separable metric spaces in Z_2 . This is handled in terms of well founded trees. First Borel sets are handled using well founded trees. Then one assigns Borel sets to basic open sets, to be the inverse image of the basic open sets. This treatment avoids any use of the axiom of choice and other issues.

There is the question of coding and a direct third order treatment of Borel measurable functions. One wants to develop appropriate conservative extensions of Z_2 , and even of the weak fragments of Z_2 used in RM (reverse mathematics), such as RCA_0 . This needs to be explored carefully.

We now give a theorem of Z that cannot be proved in BZ .

Let $\text{FG}(N)$ be the space of all finitely generated groups whose domain is N . This is a Borel subspace of the Baire space $B(N)$ of binary functions from N into N .

THEOREM 5.10. Let $F:\text{FG}(N)^{\bullet} \rightarrow \text{FG}(N)$ be an isomorphically invariant Borel function. There exists $x \in \text{FG}(N)^{\bullet}$ such that $f(x)$ is embeddable in a coordinate of x .

Theorem 5.10 is provable in Z but not in $BZ + Ax^C, \prod_n Z_n,$ or $TT.$

We sketch a proof of a sharp form of Theorem 5.1. There is something exotic about it.

Let \mathbb{R}^* be the reals with the ***discrete topology***. Is the discrete topology is one of those worthless meaningless things from the new new new new math? We shall see.

Granted, \mathbb{R}^* is silly, but \mathbb{R}^* is not. The basic open sets in \mathbb{R}^* are the $V_x = \{f \in \mathbb{R}^* : f \text{ extends } x\}$, where $x \in FS(\mathbb{R}) =$ set of all finite sequences from \mathbb{R} . Obviously every open (Borel) subset of \mathbb{R}^* is an open (Borel) subset of \mathbb{R}^* but not vice versa.

In any topological space, a set is called meager iff it is contained in a countable union of nowhere dense sets; comeager iff its complement is meager; Borel iff it is in the least σ algebra containing all open sets.

LEMMA 5.11. In any topological space, every Borel set differs from an open set by a meager set.

Baire category for \mathbb{R}^* :

LEMMA 5.12. \mathbb{R}^* is not meager. In fact, no V_x is meager.

0,1 laws for \mathbb{R}^* :

LEMMA 5.13. Let $A \subseteq \mathbb{R}^*$ be Borel and permutation invariant. Then A is meager or comeager.

We say that $F: \mathbb{R}^* \rightarrow \mathbb{R}$ is Borel iff the inverse image of every open subset of \mathbb{R} is a Borel subset of \mathbb{R}^* .

LEMMA 5.14. Every permutation invariant Borel $f: \mathbb{R}^* \rightarrow \mathbb{R}$ is constant on a comeager set.

THEOREM 5.15. Every permutation invariant Borel $f: \mathbb{R}^* \rightarrow \mathbb{R}$ maps some argument to a coordinate of itself.

Obviously the use of the discrete topology to prove a statement living in standard separable spaces is highly unusual. Recall the standard well known 0,1 law:

Every permutation invariant Borel function $f: \mathbb{R}^n \rightarrow \mathbb{R}$ is constant on a comeager set of full measure.

But this does not allow us to derive Theorem 5.1 because

For all c , $\{x \in \mathbb{R}^n: c \text{ is a coordinate of } x\}$ is meager and null.