Feasible Mathematics

Samuel R. Buss Philip J. Scott
Editors

Feasible Mathematics

A Mathematical Sciences Institute Workshop, Ithaca, New York, June 1989

1990

Birkhäuser
Boston · Basel · Berlin

Samuel R. Buss
Department of Mathematics
University of California, San Diego
La Jolla, CA 92093-0114
USA

Philip J. Scott
Department of Mathematics
University of Ottawa
Ottawa, Ontario
Canada K1N 6N5

Library of Congress Cataloging-in-Publication Data
Feasible mathematics : a Mathematical Sciences Institute workshop, Ithaca, New York, June 1989 / edited by Samuel R. Buss, Philip J. Scott.
p. cm.
Papers presented at the Workshop on Feasible Mathematics, held at Cornell University, sponsored by the Mathematical Sciences Institute.
1. Computational complexity--Congresses. 2. Mathematics--Congresses. I. Buss, Samuel R. II. Scott, Philip J.
III. Workshop on Feasible Mathematics (1989 : Cornell University)
IV. Cornell University. Mathematical Sciences Institute.
QA267.7.F43 1990
510—dc20 90-918

Printed on acid-free paper.

ISBN 0-8176-3483-5
ISBN 3-7643-3483-5

Camera-ready text supplied by the authors.
Printed and bound by Edwards Brothers, Inc., Ann Arbor, Michigan.
Printed in the U.S.A.

9 8 7 6 5 4 3 2 1

Preface

A so-called "effective" algorithm may require arbitrarily large finite amounts of time and space resources, and hence may not be practical in the real world. A "feasible" algorithm is one which only requires a limited amount of space and/or time for execution; the general idea is that a feasible algorithm is one which may be practical on today's or at least tomorrow's computers. There is no definitive analogue of Church's thesis giving a mathematical definition of feasibility; however, the most widely studied mathematical model of feasible computability is polynomial-time computability.

Feasible Mathematics includes both the study of feasible computation from a mathematical and logical point of view and the reworking of traditional mathematics from the point of view of feasible computation. The diversity of Feasible Mathematics is illustrated by the contents of this volume which includes papers on weak fragments of arithmetic, on higher type functionals, on bounded linear logic, on subrecursive definitions of complexity classes, on finite model theory, on models of feasible computation for real numbers, on vector spaces and on recursion theory.

The Workshop on Feasible Mathematics was sponsored by the Mathematical Sciences Institute and was held at Cornell University, June 26-28, 1989. The principal speakers were M. Ajtai, L. Blum, S. Buss, P. Clote, S. Cook, J. Crossley, J.-Y. Girard, Y. Gurevich, K.-I Ko, D. Leivant, A. Nerode, J. Remmel, A. Scedrov, G. Takeuti, and A. Urquhart. There were shorter talks by J.C.E. Dekker, F. Ferriera, J. Foy and J. Krajíček. H. J. Hoover did not speak at the workshop but contributed a paper to the proceedings.

These proceedings illustrate the diversity of talks at the meeting. We would like to thank the speakers for the lively exchange of ideas during the talks. The editors would also like to thank the Mathematical Sciences Institute of

Cornell University , and especially Anil Nerode, for their financial and logistic help in making this meeting possible. We would also like to thank the staff of MSI for their help in organizing this meeting.

Most of the papers in this volume have been refereed; however, four of the speakers, L. Blum, Y. Gurevich, D. Leivant, and A. Urquhart submitted abstracts of their talks which were not refereed. We would like to thank the referees for their consciencious efforts in reviewing the rest of the articles.

Samuel R. Buss and Philip J. Scott

Table of Contents

PARITY AND THE PIGEONHOLE PRINCIPLE

M. Ajtai

INTRODUCTION. The Pigeonhole Principle is the statement that there is no one-to-one map of a set of size n into a set of size $n-1$. This is a theorem of Peano Arithmetic that is it can be proved using the axioms of complete induction. A weaker version of Peano Arithmetic is $I\Delta_0$ where we allow only bounded formulas in the induction axioms, that is for each bounded formula $\phi(\vec{x}, y)$ the corresponding induction axiom $\forall\vec{x}((\phi(\vec{x},0) \wedge \forall(\phi(\vec{x},y) \rightarrow \phi(\vec{x},y+1))) \rightarrow \forall z\phi(\vec{x},z))$, where a formula is called bounded if it contains only quantifiers of the type $\forall x < y$ or $\exists x < y$.

A. Woods (see [Wo] or [PWW]) proved that the existence of infinitely many prime numbers can be proved in $I\Delta_0$ if the pigeonhole principle is a theorem of this system. A. Wilkie (see [Wi] or [PWW]) has found a weaker version of the Pigeonhole Principle which indeed can be proved, and still implies the existence of infinite number of primes, in a system which is somewhat stronger than $I\Delta_0$, but the question about PHP remained unsolved. Paris and Wilkie [PW] asked whether PHP can be proved in $I\Delta_0(f)$. (If it can be proved in this extended system then it can be proved in $I\Delta_0$ too. We get $I\Delta_0(f)$ from $I\Delta_0$ by adding a unary function symbol f and allowing to use it in the induction axioms. Now the Pigeonhole Principle is the statement that for any x the restriction of f onto x is not a one-to-one map of x into $x-1$). The answer is negative (c.f. Ajtai [Aj2]), the Pigeonhole Principle cannot be proved in $I\Delta_0(f)$, actually it is possible

to add to any nonstandard initial segment $(\{0, 1, ..., n-1\}, +, \times, \leq)$ of Peano arithmetic a function f violating the Pigeonhole Principle for n in a way that the axiom-schema of complete induction (upto n and so upto any fixed power of n) remains true in the extended model. This result shows that the Pigeonhole Principle for the number n is in some sense stronger than complete induction upto n.

In this paper we show that the assertion that the cardinality of a set cannot be even and odd at the same time is stronger than the Pigeonhole Principle in the same sense. More precisely let PAR_n be the following statement:

the set $2n + 1 = \{0, 1, ..., 2n\}$ has no partition into subsets with two elements.

We show that PAR_n is stronger then the Pigeonhole Principle in the following sense:

Let $PHP\Delta_0$ be the axiom-system what we get from $I\Delta_0$ by adding for each bounded formula $\psi(\vec{x}, z, u, v)$ the following axiom "for all $\vec{x}$ and z if $u = f(v) \leftrightarrow \psi(\vec{x}, z, u, v)$ is a function defined on z with values in $z - 1$ then there are two different elements of z where it takes the same value". (Obviously this can be expressed by a firstorder formula).

$PHP\Delta_0(R)$ will be the axiom-system what we get from $PHP\Delta_0$ if we allow to use the binary relation symbol R in the bounded formula ψ in the PHP axioms. Our main result is that the following statement cannot be proved in $PHP\Delta_0(R)$

"$\forall x$ if R restricted to the set $2x + 1$ is a partition of $2x + 1$ then there is at least one class of it which does not contain exactly two elements".

We will not work directly with the $PHP\Delta_0(R)$, but, like in [Aj2], we will consider an axiom-system which describes the following structure: the universe is the set of natural numbers from 0 to n and the relations are the arithmetic operations and ordering upto n. Addition and multiplication will be only partial functions. (The choice of these relations is somewhat arbitrary but as we will see for our present purposes it has essentially no importance at all.) Now we accept the Pigeonhole Principle for n, that is an axiom-schema which asserts that if a map of n into $n - 1$ can be defined by a firstorder formula in this structure, then it will not be one-to-one. We

will show that PAR_n cannot be proved in this axiom-system in other words we prove that if we add a relation symbol R to the system and we allow R in the Pigeonhole Principle axioms, still it is consistent that R is a partition of the set $2n+1 = \{0, 1, ..., 2n\}$ into subsets each with two elements. Like in the case of PHP versus complete induction, this consistency result remains valid in a much stronger form. We may add arbitrary axioms to the system which do not contain R and consistent to Peano Arithmetic (that is axioms which hold in an initial segment of some model of Peano Arithmetic) or we may add arbitrary new relation and function symbols and new axioms about them not containing R but consistent to Peano Arithmetic (in the above sense), and we may add the PHP-axiom for n containg all of the relation and function symbols together with R, and still PAR_n remains unprovable.

There is one difficulty which did not arise in the case of induction/PHP. Namely complete induction had the nice property that if it is true up to n than it is also true upto any fixed power of n. This can be proved by reapeatedly applying the induction axioms. We do not know whether the Pigeonhole Principle has this property, actually it seems more likely that e.g. PHP_{2n} cannot be proved from PHP_n. We will prove however, (and this is necessary for the independence concerning $I\Delta_0(R)$), that PAR_n cannot be proved even using PHP_{n^c} where c can be an arbitrarily large constant.

The structure of the proof is similar to the proof given in [Aj2]. Actually there is a part of the proof which can be done by modifying the arguments given there in a nonessential way. We will describe the necessary changes, but will not repeat the proof. (This concerns the combinatorial part of the proof given there).

A part of the proof is extending a model by adding a new relation to it. As in [Aj2] this is done by some finite version of forcing exactly the same way.

The essential new part of the proof is to reduce the question of unporvability to a combinatorial lemma and the proof of this lemma. This combinatorial question is of completely different character than the one's handled in [Aj2] or [Aj1].

1. In this section we give a rigorous formulation of our main result and explain the model theoretic part of the construction. We essentially follow the same way as in [Aj2] with the obvoius necessary changes.

If M is a model of Peano Arithmetic and $n \in M$ then M_n will denote the set $\{x \in M | M \models x < n\}$. Suppose that A is a k-ary relation defined on M_n where k is a natural number. We say that A is definable in M if there is a firstorder formula $\phi(x_1, ..., x_k, y)$ of Peano Arithmetic with the free variables $x_1, ..., x_k, y$ and there is a $c \in M$ so that for all $x_1, ..., x_k \in M$ we have $A(x_1, ..., x_k)$ iff $M \models \phi(x_1, ..., x_k, c)$. If g is a function defined on a subset of M_n whose values are in M_n, then we say that the function g is definable in M if the relation "$x_1 = g(x_2)$" is definable in M. Obviously there exists a single firstorder formula $\phi(x_1, x_2, y)$ so that for each $g \in {}^{M_n}M_n$, if g is definable in M then there exists a $c_g \in M$ so that for all $x_1, x_2 \in M$ we have $x_1 = g(x_2)$ iff $M \models \phi(x_1, x_2, c_g)$. We will suppose that for each g a c_g is fixed (e.g. the smallest one with the required properties).

Definition. Let L_0 be the language with the binary relation symbols $=, \leq$ and the ternary relation symbols $+, \times$. Let A be a k-ary relation symbol, let R be a new binary relation symbol, $L = L_0 \cup \{A\}$, $L' = L \cup \{R\}$.

Definition. Suppose that T is a theory of the language L. We say that T describes a large initial segment of Peano Arithmetic if the following holds:

For all natural numbers l there is a model M of Peano Arithmetic and an $n \in M$ so that $M \models n > l$ and there is a k-ary relation A on the set $\{0, 1, ..., n-1\}$ which is definable in M so that with the universe $M_n = \{0, ..., n-1\}$ and the interpretation τ; $\tau(A) = A$, $\tau(+) = +_M|_{M_n}$, $\tau(\times) = \times_M|_{M_n}$, $\tau(\leq) = \leq_M|_{M_n}$ we have $M_n \models_\tau T$.

Now we want to give an axiom-schema which describes the Pigeonhole Principle. As we have mentioned in the introduction it will not be enough to prove that PAR_n is independent of PHP_n but we want to prove independency from PHP_{n^c} for any constant c. In the present situation this means that, when working with M_n, it is not enough to assume that there is no firstorder definable one-to-one function which maps the universe into a proper subset of it but we need this statement for the set of c-tuples taken from the universe, for any natural number c. So in our axiom-schema the

axioms will have two parameters, one is the firstorder formula which defines the map, and the other is the natural number c.

Definition. Let c be a natural number. In the following definition $\vec{u}$, $\vec{v}$ and $\vec{y}$ will be abbreviation for $u_0, ..., u_{c-1}$, $v_0, ..., v_{c-1}$ and $y_0, ..., y_{i-1}$, where i can be an arbitrary natural number. Let $\phi(\vec{u}, \vec{v}, \vec{y})$ be a firstorder formula of the language L'. We will write $\vec{u} = f^{\vec{y}}(\vec{v})$ for $\phi(\vec{u}, \vec{v}, \vec{y})$. We will call the following sentence the Pigeonhole Principle with parameters ϕ, c:

$PHP^{\phi,c} \equiv \forall \vec{y}(\forall \vec{u} \exists! \vec{v}\ \vec{v} = f^{\vec{y}}(\vec{u})) \rightarrow ((\exists \vec{v} \forall \vec{u}\ \neg \vec{v} = f^{\vec{y}}(\vec{u})) \rightarrow$
$\rightarrow (\exists \vec{u} \vec{v}\ \vec{u} \neq \vec{v} \wedge f^{\vec{y}}(\vec{u}) = f^{\vec{y}}(\vec{v})))$.

The theory consisting of the sentences $PHP^{\phi,c}$ for all firstorder formula ϕ and natural number c is called the axiom-schema for the Pigeonhole Principle.

Definition. The expression "the cardinality of the universe is odd" will be an abbreviation of the firstorder sentence: "$\exists x, y$ x is the largest element of the universe and $x = 2y$". (The universe has n elements and the greatest one is $n - 1$) "The parity principle for R" will mean the following sentence of L': "if the cardinality of the universe is odd then R is not a partition of the universe into subsets with two elements."

Theorem A1. *Suppose that T is a theory of the language L which describes a large initial segment of Peano Arithmetic. Then the following theory in L' is consistent: T + "the axiom-schema for the Pigeonhole Principle" + $\neg$ "the parity principle for R".*

The proof of Theorem A1 actually gives the following:

Theorem A1'. *Assume that M is a model of Peano Arithmetic, n is an odd nonstandard element of M and A is a k-ary relation on the set $M_n = \{0, 1, ..., n - 1\}$ definable in M where k is a standard natural number. Then there exists a partition $\tilde{R}$ of n into subsets of size 2 so that in the structure $\langle M_n, A, \tilde{R}\rangle$ the "axiom-schema for the Pigeonhole Principle" holds.*

Defintion. If P is a partition of the set S we call P a 2-partition iff every class of P contains exactly two elements. If P is a 2-partition of some subset of S then we call P a partial 2-partition of S. We will consider partitions as the set of their classes, so e.g. $P \subseteq Q$ means that each class of P is a class of Q too. We call the partial 2-partitions P, Q compatible if every class of P is either a class of Q too, or disjoint from every class of Q.

Assume that P is a partial 2-partition of the set S and V is a subset of S. V covers P iff each class of P contains at least one element of V. V is inside P iff $V \subseteq \bigcup P$. V supports P iff it is inside P and covers P.

Proof of Theorem A1. Suppose that T is given. Then there exists a countable nonstandard model of Peano Arithmetic M, so that n is an odd element of M, $M_n = \{0, ..., n-1\}$ is infinite and $M_n \models_\tau T$, where $\tau(\mathcal{A}) = A$, and A is a k-ary relation on $\{0, 1, ...n-1\}$ which is definable in M.

Suppose $\tilde{R}$ is a 2-partition of M_n.

Let $\sigma = \sigma_{\tilde{R}}$ be an interpretation of the language L' on the universe M_n so that σ is an extension of τ and $\sigma(R) = \tilde{R}$.

Obviously $\models_\sigma T \wedge \neg$ "the parity principle for $\tilde{R}$".

It is sufficient to prove that for a suitable choice of $\tilde{R}$ we have $\models_\sigma$ "the axiom-schema of the Pigeonhole Principle".

2. THE CONSTRUCTION OF $\tilde{R}$

Definitions 1. Let $H_n = \{g | g$ is a partial 2-partition of M_n and g is definable in $M\}$.

2. If $\epsilon > 0$ is rational then let

$\wp_\epsilon = \{g \in H_n | \ M \models$ "$|\bigcup g| \leq n - n^\epsilon$"$\}$, (since g is definable in M, $|\bigcup g|$ is also definable in M. Although n^ϵ is not necessarily defined in M still the inequality "$a \geq b^\epsilon$" can be defined in the natural way in M for all $a, b \in M$ and rational $\epsilon > 0$).

$\wp = \bigcup\{\wp_\epsilon | \epsilon > 0, \epsilon$ is rational $\}$. (It is important in this definition that we take all rational ϵ in the world, not in M.)

We will consider $\wp$ as a partially ordered set with the partial ordering: $\forall g, h \in \wp \ g \leq h$ iff $h \subseteq g$.

3. Suppose that D is a subset of $\wp$. We say that D is dense iff for all $g \in \wp$ there is a $h \in D$ with $h \leq g$.

We say that the dense set D belongs to M iff there exists a firstorder formula of Peano Arithmetic $\psi(x, y, z)$ and a $b \in M$ so that for all $g \in \wp$ we have: $g \in D$ iff (there exists a natural number k so that $M \models \psi(c_g, k, b)$).

4. Let G be a subset of $\wp$. We say that G is generic over M iff

(1) $g \in G$, $h \in \wp$, $g \leq h$ implies $h \in G$,

(2) for all $g, g' \in G$ there is a $h \in G$ with $h \leq g$ and $h \leq g'$,

(3) if D is a dense subset of $\wp$, which belongs to M then $G \cap D$ is nonempty.

5. Suppose that G is a generic subset of $\wp$. (Since M is countable it is easy to prove the existence of a generic subset G). Let $\tilde{R}$ be the union of all partial 2-partitions in G. Property (2) from the definition of a generic set implies that $\tilde{R}$ is a partial 2-partition of M_n. For each fixed $i \in M_n$ the set $D = \{g \in \wp | i \in \bigcup g\}$ is dense, moreover the definition of D and $\wp$ implies that D belongs to M. Therefore by property (3) of the definition of generic sets, $\bigcup(\tilde{R}) = M_n$, so $\tilde{R}$ is a 2-partiton of M_n.

We will prove that if $\sigma(R) = \tilde{R}$ then

$\models_\sigma$ "the axiom-schema of the Pigeonhole Principle".

Definitions. 1. Suppose that $\phi(y_0, ..., y_i)$ is a firstorder formula of L', $a_0, ..., a_i \in M_n$, $g \in \wp$. We say that $g \Vdash \phi(a_0, ..., a_i)$ iff for any generic subset G of $\wp$ with $g \in G$ we have $M_n \models_{\sigma_R} \phi(a_0, ..., a_i)$.

2. If i is a natural number then M_n^i will denote the set of i-tuples from M_n.

3. Suppose that i is a natural number and X is a relation on M_n^i. We say that X is in σ if there exists a natural number j and a firstorder formula $\phi(x_0, ..., x_{i-1}, y_0, ..., y_{j-1})$ so that for some $b_0, ..., b_{j-1} \in M_n$ we have that for all $a_0, ..., a_{i-1} \in M_n$: $X(a_0, ..., a_{i-1})$ iff $\models_\sigma \phi(a_0, ..., a_{i-1}, b_0, ..., b_{j-1})$. (We will sometimes write $X(a_0, ..., a_{i-1})$ where strictly speaking we mean the defining formula $\phi(a_0, ..., a_{i-1}, b_0, ..., b_{j-1})$.) If i, i' are natural numbers and Y is a (possibly partial) function defined on M_n^i with values in $M_n^{i'}$ then we say that Y is in σ iff the relation $u = Y(v)$ on $M_n^{i+i'}$ is in σ.

Lemma T1. *Suppose that i is a natural number, G is a generic set, and X is a relation on M_n^i so that X is in σ, then the following conditions hold*

(T1.1) for all $a_0, ..., a_{i-1} \in M_n^i$ there is a $g \in G$ so that $g \Vdash X(a_0, ..., a_{i-1})$ or $g \Vdash \neg X(a_0, ..., a_{i-1})$.

(T1.2) There is a relation "$g \Vdash X(a_0, ..., a_{i-1})$" definable in M such that for all $g \in \wp$ and all $a_0, ..., a_{i-1} \in M_n^i$, "$g \Vdash X(a_0, ..., a_{i-1})$" implies $g \Vdash X(a_0, ..., a_{i-1})$, and if $\exists g \in G\ g \Vdash X(a_0, ..., a_{i-1})$ then $\exists g \in G$ "$g \Vdash X(a_0, ..., a_{i-1})$".

(T1.3) for all $h' \in \wp$ there exist a $h \in \wp$, $h \leq h'$, a natural number k and a function d, which is definable in M so that for all $a \in M_n^i$, $d(a)$ is a subset of M_n with k elements, and for all 2-partitions Q, if Q is supported by $d(a)$ and compatible to h then either "$h \cup Q \Vdash X(a)$" or "$h \cup Q \Vdash \neg X(a)$".

(T1.4) If $i = 2e$ and $X(a)$ is of the form $v = Y(u)$, where $a = \langle u, v \rangle$, $u, v \in M_n^e$ and Y is a (partial) function inside σ, then the function d can be chosen with the property $\forall u, v, v' \in M_n^e\ d(\langle u, v \rangle) = d(\langle u, v' \rangle)$.

Remark. We may suppose that $d(a) \subseteq M_n - \bigcup h$ since those classes of Q which contain at least one point from $\bigcup h$ coincide with the corresponding classes of h.

We will prove this Lemma in section 4, more precisely we explain how the proof in [Aj2] can be modified to our present needs. The next section contains the essential new part of the proof, namely we show that Lemma T1 implies theorem A1 and A1'.

3.

Suppose that $\models_\sigma \neg$ "the axiom-schema of the Pigeonhole Principle". This implies that there is a natural number e and a one to one map of Y of M_n^e into, say, $M_n^e - \langle 0, ..., 0 \rangle$ so that Y is in σ. Let $h \in \wp$ and d be the function with the properties listed in (T1.4) and Y' be the inverse function of Y (Y' is not necessarily defined everywhere). According to (T1.1) we may

also suppose that $h \Vdash$ "Y is a one-to-one map of M_n^c into $M_n^c - \langle 0, ..., 0\rangle$, and Y' is the inverse of Y."

Let d' be the function corresponding to Y' as described in (T1.4) and $\mu(a) = d(a) \cup d'(a)$ for all $a \in M_n^c$. We may suppose that for all a the size of the set $\mu(a)$ is the same natural number. (If necessary we may increase some of them). We may also assume that h and h' corresponding to Y, Y' in Lemma T1 are the same. (Otherwise we may take a common lower bound of them in G.) Since both μ and the relation $\Vdash$ are definable in M there are functions f, g definable in M with the following properties.

If $a \in M_n^c$ then for any partial 2 partition Q supported by $\mu(a)$ and compatible to h we have

(i) $h \cup Q \Vdash Y(a) = f(a, Q)$ and

(ii) if $g(a, Q)$ is defined then $h \cup Q \Vdash Y'(a) = g(a, Q)$,

if $g(a, Q)$ is not defined then $h \cup Q \Vdash$ "$Y'(a)$ is not defined".

(i) and (ii) imply that the functions μ, f, g satisfy conditions (F0),...,(F4) listed below. We may suppose according to the remark after Lemma T1 that $\mu(a) \subseteq M_n - \bigcup h$. Assume that $M \models m = |n - \bigcup h|$. We will identify m and $n - \bigcup h$ so we will assume that $\mu(a) \subseteq m$. Since $|M_n^c| = n^c$ we will identify M_n^c and $n^c = \ell$. We will suppose that Y maps ℓ into $\ell - \{0\}$.

(F0) μ maps ℓ into the set T of (unordered) k-tuples formed from the elements of m. The domain of f is the set of all pairs x, P so that $x \in \ell$, P is a partial 2-partition of m and $\mu(x)$ supports P. The domain of g is a subset of the set of all pairs y, Q so that $y \in \ell$, Q is a partial 2 partition of m and $\mu(y)$ supports Q.

Conditions (F1)-(F4) must hold for all values of x, y, P, Q where $x, y \in \ell$, P, Q are compatible partial 2-partitions of the set m, $\mu(x)$ supports P and $\mu(y)$ supports Q:

(F1) $f(x, P) < \ell$, $f(x, P) \neq 0$.

(F2) if $g(x, P)$ is defined then $g(x, P) \in \ell$. ($g(x, P)$ is not necessarily defined for all x, P with the given property)

(F3) if x, y are different elements of ℓ, then $f(x, P)$ and $f(y, Q)$ are also different.

(F4) $y = f(x, P)$ iff ($g(y, Q)$ is defined and $x = g(y, Q)$).

(F0) repeats the definition of μ, f and g. (F1) follows from the fact that the range of Y is $\ell - \{0\}$, and (F2) holds since Y' is a partial function with range in ℓ. (F3) is true since Y is one-to-one and P, Q are compatible (so there is a $h'' \leq h \in G$ which contains both). If P, Q are compatible then by (T1.4) we have that for some $y \in \ell$; $P \cup Q \cup h \Vdash y = Y(x)$ which implies (F4).

Definition. Suppose that $k, \ell, m \in \omega$. We say that $W1(k, \ell, m)$ holds if there exist functions μ, f and g so that (F0),...,(F4) are satisfied.

Our previous observations imply the following:

Lemma M0. *If* $\models_\sigma \neg$ *"the axiom-schema of the Pigeonhole Principle", then there exists a (standard) natural number* k *and nonstandard elements* ℓ, m *of* M *so that* $M \models W1(k, \ell, m)$

To get a contradiction it is enough to show that Peano Arithmetic exludes the existence of numbers k, ℓ, m with the given properties.

Lemma M1. $\forall k \in \omega$ *if* m *is a sufficiently large natural number and* $\ell \in \omega$ *then* $W1(k, \ell, m)$ *does not hold, moreover this statement can be proved in Peano Arithmetic.*

Remark. The fact that the first statement of Lemma M1 can be proved in Peano Arithmetic is only important for showing that our consistency result is a theorem of Peano Arithmetic. If we know only that the first statement of Lemma M1 is a theorem of ZFC then we may work with a nonstandard model M of Peano Arithmetic which is elementary equivalent to ω and get the same result, now proved in ZFC.