COMBINATORICA
Akadémiai Kiadó – Springer-Verlag

COMBINATORICA **14** (4) (1994) 417–433

THE COMPLEXITY OF THE PIGEONHOLE PRINCIPLE

M. AJTAI

Received February 22, 1992

The Pigeonhole Principle for n is the statement that there is no one-to-one function between a set of size n and a set of size $n-1$. This statement can be formulated as an unlimited fan-in constant depth polynomial size Boolean formula PHP_n in $n(n-1)$ variables. We may think that the truth-value of the variable $x_{i,j}$ will be true iff the function maps the i-th element of the first set to the j-th element of the second (see Cook and Rechkow [5]). PHP_n can be proved in the propositional calculus. That is, a sequence of Boolean formulae can be given so that each one is either an axiom of the propositional calculus or a consequence of some of the previous ones according to an inference rule of the propositional calculus, and the last one is PHP_n. Our main result is that the Pigeonhole Principle cannot be proved this way, if the size of the proof (the total number or symbols of the formulae in the sequence) is polynomial in n and each formula is constant depth (unlimited fan-in), polynomial size and contains only the variables of PHP_n.

The classical proof of the Pigeonhole Principle (using induction on n) yields a propositional proof where the depth of the formulae will be large, or if we want to keep it constant we have to introduce new variables. It is easy to give a proof containing only constant depth polynomial size Boolean formulae but of exponential length.

The theorem described in the abstract solves an open problem of Paris and Wilkie [7], namely according to their results it implies that the Pigeonhole Principle cannot be proved in $I\Delta_0(f)$. The axiom system $I\Delta_0$ is a bounded version of Peano arithmetic where in the induction axioms we allow only bounded quantifiers of the type $\exists x \leq y$ or $\forall x \leq y$. We get $I\Delta_0(f)$ by adding a new function symbol f to the language (which can be used in the induction axioms). The Pigeonhole Principle is stated for the function f.

Definitions. 1. In this paper the Pigeonhole Principle means the statement that there is no one-to-one function of a set of size n onto a set of size $n-1$. The usual formulation "into a set of size $n-1$" is a stronger statement, but since we are proving negative results, everything remains true with the stronger form. Our proof gives the "onto" version so we will call this the Pigeonhole Principle unless explicitly stated otherwise. Cook and Rechkow gave a propositional formulation of the Pigeonhole Principle:

AMS subject classification code (1991): 03 F 20, 03 F 30, 03 H 15

$$PHP_n = \neg \left[\left(\bigwedge_{i \in n} \bigvee_{j \in n-1} x_{i,j} \right) \wedge \left(\bigwedge_{j \in n-1} \bigvee_{i \in n} x_{i,j} \right) \wedge \left(\bigwedge_{\substack{i \in n \\ j,k \in n-1 \; j \neq k}} \neg \left(x_{i,j} \wedge x_{i,k} \right) \right) \wedge \left(\bigwedge_{\substack{j \in n-1 \\ i,l \in n \; i \neq l}} \neg (x_{i,j} \wedge x_{l,j}) \right) \right]$$

2. A Frege system is a propositional proof system. First a finite set of axioms is given. E.g. $\phi \wedge \psi \rightarrow \phi$ is an axiom. It means that we may replace ϕ and ψ by any propositional formulae and the resulted formula will be accepted as true. Naturally we will use only axioms whose truth value is true if we substitute arbitrary true/false values for the formula symbols in it.

A finite set of rules of inference is also given. The rules of inference must be sound in the following sense: the premises of any instance of the rule logically entail the conclusion of the rule. E.g. modus ponens is such a rule: it says that from ϕ and $\phi \rightarrow \psi$ we may infer ψ. If we infer the truth of a formula according to these rules from the axioms or already proven formulae, then we consider it as proven.

A Frege proof is a sequence of propositional formulae whose each element is either an axiom or follows by one of the inference rules from some of the earlier elements of the sequence. We do not fix any specific set of axioms or set of inference rules, our nonprovability result hold for any finite set of sound axioms/inference rules.

In a Frege proof as described here it is not possible to introduce abbreviations for boolean formulae, so e.g. the step "denote $x \vee y$ by z" is not allowed. Practically it means that to prove a formula we may use only formulae which contain the same variables. There is a stronger version of this notion, where this type of abbreviation is allowed, called extended Frege proof system.

A weaker notion is the resolution proof system, where starting from an unsatisfiable boolean formula and using the resolution rule we try to get a contradiction. (We will not use this notion).

3. A formula of the language of Peano Arithmetic (that is containing the relation symbols $=, +, \times, \leq, 0, 1$ only) is called bounded if it has only quantifiers of the type $\forall x \leq y$ and $\exists x \leq y$, where these are abbreviations for $\forall x(x \leq y \rightarrow \ldots)$ and $\exists x(x \leq y \wedge \ldots)$.

$I\Delta_0$ is the axiom system consisting of a set of axioms describing the usual algebraic properties of the relations $=, +, \times, \leq, 0, 1$ like e.g $\forall x, y \;\; x + y = y + x$, and for each bounded formula $\phi(\vec{x}, y)$ the corresponding induction axiom $\forall \vec{x}((\phi(\vec{x}, 0) \wedge \forall(\phi(\vec{x}, y) \rightarrow \phi(\vec{x}, y+1))) \rightarrow \forall z \phi(\vec{x}, z))$. We get $I\Delta_0(f)$ by extending the language with one unary function symbol f and allowing to use it in the induction axioms. In $I\Delta_0(f)$ the Pigeonhole Principle is the following statement "for all x the function f is not a one-to-one map of the set $\{0, 1, \ldots, x-1\}$ onto the set $\{0, 1, \ldots, x-2\}$". Clearly this statement can be given by a firstorder formula.

The notion of Frege system was introduced by Cook and Rechkow [5]. They and Statman [10] discussed the connection between length of propositional proofs and unsolved questions of computational complexity (e.g. NP = co-Np).

Cook and Rechkow gave a propositional formulation of the Pigeonhole Principle and used as an example for a propositional formula which have a polynomial size proof in an extended Frege system but its only known Frege proof is of exponential size. (The proof in the extended Frege system actually describe a sequence of functions $f_n,\ldots,f_0$, so that f_i is a one-to-one map of $\{1,\ldots,i\}$ into $\{1,\ldots,i-1\}$. Each f_i is given by $i(i-1)$ variables which are defined from the variables for f_{i+1}. If we want to express every variable in terms of the original variables corresponding to f_n then we get formulae of exponential size.) S. Buss proved however the surprising result that the Pigeonhole Principle actually has a polynomial size Frege proof. (The depth of the formulae given in his construction is not bounded by any constant.)

A. Haken has shown that any resolution proof of the PHP must be of exponential size. Urquhart gave an other example which shows that resolution proofs may require exponential size even when there is a polynomial size Frege proof. S. Buss and Gy. Turán [4] gave exponential lower bounds for resolution proofs of generalized forms of the Pigeonhole Principle (where the range of the function f is essentially smaller than the domain).

As these results show the Pigeonhole Principle was the main target of the lowerbound proofs. It seems that all of the lowerbound results handle proof systems weaker then the Frege system, (resolution proof systems). Our theorem gives a lowerbound for a proof in the Frege system, although with the additional restriction that the formulae has to be of constant depth. (As Buss' theorem about the existence of polynomial size Frege proof shows a restriction of this type is necessary in the case of the Pigeonhole Principle). The following theorem is the main result. A preliminary version of its proof was given in [2]. In the present version we give a more detailed and explicit description of the forcing method used in the proof.

Theorem 1. *For all natural numbers c_1, c_2 if the integer n is sufficiently large, then there is no Frege proof for the boolean formula PHP_n (Pigeonhole Principle for n) of size smaller then n^{c_1}, so that each formula in the proof is at most of depth c_2.*

A. Woods proved (see [13] or [9]) that the existence of infinitely many prime numbers can be proved in a system that we get from $I\Delta_0$ by adding an axiom which essentially guarantees the existence of $x^{\log x}$ for any natural number x, if the Pigeonhole Principle is a theorem of this system. A. Wilkie [12] has found a weaker version of the Pigeonhole Principle which indeed can be proved in $I\Delta_0$ and still implies the existence of an infinite number of primes, but the question about PHP remained unsolved. Paris and Wilkie [7] 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). They have shown that if PHP can be proved in $I\Delta_0(f)$ then there is a polynomial size constant depth Frege proof for PHP_n. So Theorem 1 implies the following:

Corollary. *The Pigeonhole Principle cannot be proved in $I\Delta_0(f)$.*

Although the proof of our theorem is mostly combinatorial and probabilistic, ideas from axiomatic set theory, namely Cohen's method of forcing, play an im-

portant role. We prove our nonprovability result, in the following way. Let n be a nonstandard natural number in a nonstandard model K of Peano Arithmetic. Assume that contrary to our assumption there is a constant depth polynomial size propositional proof of the Pigeonhole Principle with the required properties. We may suppose that there is such a proof in K for the number n. We consider the structure M consisting of all numbers less than n from K with some relations like the ordering, arithmetic operations and possibly others which are definable in K. One of these relations will code the mentioned polynomial length proof of the Pigeonhole Principle.

Now we extend our structure M by adding to it a one-to-one function f which maps the set $\{0,1,\ldots,n-1\}$ into the set $\{1,\ldots,n-2\}$. The essential part of the proof is to show that there is an f so that in the extended structure the axiom of complete induction up to n remains valid, that is if we define a subset of the set $\{0,1,\ldots,n-1\}$ by a firstorder formula then it will have a smallest element. This will imply that we may check our polynomial length proof for f, that is, we may find the first formula in the proof which is not valid for f and this way we reach a contradiction with the soundness of our inference rules.

The construction of f is done according to the general ideas of Cohen's method of forcing but without its specific details concerning infinite axiomatic set theory. There is a striking similarity to the technique of "cardinal collapsing", here the cardinal n collapsed onto $n-1$. In both cases a one-to-one function f is constructed between two sets of different cardinality. (Of course f will be outside of the original model). f is constructed by giving a set of partial one-to-one maps in the original model then choosing a compatible family of them outside the model so that the domains of the functions in the family cover the whole set. The common extension of the functions in the family will be f. Our partial one-to-one maps will be the common extension of the functions in the family. Paris and Wilkie [7] have used a forcing argument of this kind to prove that if we weaken $I\Delta_0(f)$ by allowing only existential formulae in the induction axiom then the Pigeonhole Principle indeed cannot be proved.

As we have indicated earlier our proof uses the extensions of initial fragments of models Peano Arithmetic where the axiom of complete induction remains true in the extended model. In the following we describe the intuitive meaning of such extensions.

When we are proving theorems in Peano Arithmetic we accept the existence of natural numbers and certain properties of them (e.g. complete induction). However the most often used models for computational complexity (e.g. polynomial time hierarchy) suggest that we really accept only the existence of natural numbers up to a certain large natural number n and larger numbers (for example, subsets of a set of size n) "exist" only if we can compute them with some kind of algorithm. Therefore it is natural to consider a system of axioms where the universe is the set of natural numbers from 0 to n and the relations are the arithmetic operations and ordering up to 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.) It is also natural to accept the axiom of complete induction up to n or, which is the same, up to a fixed power of n. How strong is this system of axioms? We will show that the Pigeonhole Principle

cannot be proved in it, (this is an other formulation of our result), in other words we prove that if we add a function symbol f to the system and we allow f in the axioms of complete induction still it is consistent that f is a one-to-one map of $0,1,\ldots,n-1$ onto $0,1,\ldots,n-2$. Actually this consistency result will remain valid in a much stronger form. We may add arbitrary axioms to the system which do not contain f but are consistent to Peano Arithmetic or we may add arbitrary new relation and function symbols and new axioms about them not containing f but consistent to Peano Arithmetic, and we may add the axioms of complete induction up to n containing all of the relation and function symbols together with f, and still the Pigeonhole Principle remains unprovable. These latter results show that the initial choice of the arithmetic relations has really no significance.

The mentioned consistency result is proved by constructing a model where both the axiom-schema of complete induction (up to n) and the negation of the Pigeonhole Principle is valid. As we have told we will use the method of forcing. As a "notion of forcing" that is the set of compatible functions we use partially defined one-to-one maps of n into $n-1$, namely we will use maps which are defined on a set of size $n-n^{\varepsilon}$ where n is nonstandard element of a nonstandard model of Peano Arithmetic and ε is a positive rational in the world. Our terminology will be similar to the terminology of forcing but we actually do not use any result from it. The most difficult part of our proof is to show that in the model what we get by the mentioned construction the axiom-schema of complete induction (up to n) is valid. The proof of this fact is essentially combinatorial. Some of the ideas of this part of the proof was used already in [1] for the proof of the following theorem:

Theorem. *For each k let d_k be the smallest positive integer so that for infinitely many n there is a depth d_k size n^{d_k} unlimited fan-in Boolean circuit which decides for any graph G on n vertices and for any pair of vertices u, v in G whether the distance of u, v is smaller than k. Then $\lim_{k\to\infty} d_k=\infty$.*

Actually the same theorem holds if the input is k permutations of a set of size n containing a point p and we are looking for circuits which decide whether the product of the k permutations takes p into itself.

We are not able to use any of the results proved there but a part of the proof can be modified to our present needs.

If M is a model of Peano Arithmetic and $n\in M$ then M_n will denote the set $\{x\in M \mid M\models x<n\}$. Suppose that X is a k-ary relation defined on M where k is a natural number. We say that X is *definable* in M if there is a firstorder formula $\phi(x_1,\ldots,x_k,y)$ of Peano Arithmetic with the free variables $x_1,\ldots,x_k,y$ and there is a $c\in M$ so that for all $x_1,\ldots,x_k\in M$ we have $X(x_1,\ldots,x_k)$ iff $M\models \phi(x_1,\ldots,x_k,c)$. If X is a k-ary relation on M_n then there exists a single firstorder formula $\phi(x_1,\ldots,x_k,y)$ (which does not depend on X) so that if X is defined on M_n if and only if there exists a $c_X\in M$ so that for all $x_1,\ldots,x_k\in M_n$ we have $X(x_1,\ldots,x_k)$ iff $M\models\phi(x_1,\ldots,x_k,c_X)$. We will suppose that for each X a c_X is fixed (e.g. the smallest one with the required properties). This makes it possible to treat the relations on M_n as elements of M.

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

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 number 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 $\{0,1,\ldots,n-1\}$ (for some natural number k) which is definable in M so that with the universe $M_n = \{0,\ldots,n-1\}$ and the interpretation τ; $\tau(\mathcal{A}) = A$, $\tau(+) = +_M|_{M_n}$, $\tau(\times) = \times_M|_{M_n}$, $\tau(\leq) = \leq_M|_{M_n}$ we have $M_n \models_\tau T$.

Assume that we have an interpretation τ with the properties described in the previous definition, that is a structure $\mathcal{M} = \langle M_n, +, \times, \leq, A\rangle$ where M is a countable nonstandard model of Peano Arithmetic and n is a nonstandard integer in M. We want to add a new binary relation ρ. (We are speaking about only binary relations but everything remains the same for j-ary relations too where j is standard.) We want to add the relation ρ so that the new structure $\mathcal{M}[\rho]$ satisfies certain firstorder properties. E.g. we will give a ρ which is a one-to-one map of M_n onto M_{n-1} (this is trivial in itself since both sets are infinite), but we will do it in a way that induction remains true in the structure. In other words, each subset of M_n which is definable by a firstorder formula from ρ and the other relations of the structure will have a smallest element.

We will construct ρ in the following way. We take a partially ordered set, whose elements are definable in M. E.g. in the case when we want ρ to be a one-to-one function from M_n onto M_{n-1} the elements of this partially ordered set will be partial one-to-one maps between the two sets, which are defined in M and their domain is of size at most $n - n^\varepsilon$ for some standard ε. We will pick a sequence (outside M) from these functions, so that ε tends to 0 and the latter elements of the sequence are extensions of the earlier ones. Since M_n is countable we will be able to pick this sequence so that the common extension of the functions is defined everywhere on M_n, takes every value in M_{n-1} and so it is a one-to-one map of M_n onto M_{n-1}. To prove that induction remains true will be much more complicated.

We return now to the general case. First we define a partially ordered set. We may think of the elements of this set as approximations of the relation ρ. As in the previous example we will pick a sequence from this partially ordered set and the union of the relations in the sequence will be ρ.

We will frequently deal with sets which are not definable in M but still they are the union of a uniform sequence of definable sets. E.g. the set of all one-to-one maps from a subset of M_n of size at most $n - n^\varepsilon$ into M_{n-1} for some standard $\varepsilon > 0$. The following definition describes this situation.

Definition. If k is a natural number and X is a k-ary relation on M we say that X is ω-definable in M iff there exists a firstorder formula $\psi(x_1,\ldots,x_k,y,z)$ of Peano Arithmetic, and a $b \in M$ so that for all $a_1,\ldots,a_k \in M$ we have: $X(a_1,\ldots,a_k)$ iff "there exists a standard natural number y, so that $M \models \psi(a_1,\ldots,a_k,y,b)$". (The standardness of y is the essence of this definition.)

Definition. Suppose that $\langle \wp, \leq\rangle$ is a partially ordered set, whose elements are binary relations on M_n and the ordering is: $p \leq q$ iff $q \subseteq p$. Assume further that

(1) each element $p \in \wp$ is definable in M,
(2) the set $\wp$ is ω-definable in M,
(3) $\wp$ has a greatest element $1_\wp$, and
(4) $\wp$ has no minimal elements.

We will call such a partially ordered set a notion of forcing.

Remarks. 1. Although the elements of $\wp$ are relations on M_n, we may treat them as elements of M, so requirement (2) is meaningful. (See remark in the definition in the definition of definability).

2. Since $\wp$ has no minimal elements but it is covered by a set which is finite in M, it cannot be definable in M.

Example. Let $\wp_\varepsilon = \{f | f \in M,\ f$ is a one-to-one map of M_n into $M_{n-1}\ \ M \models$ "$|\mathrm{dom}(f)| \leq [n - n^\varepsilon]$"$\}$. $\wp^{\leftrightarrow} = \bigcup_{1/k}\{\wp_{1/k} | k$ is a standard natural number$\}$. $\wp^{\leftrightarrow}$ is a notion of forcing.

Definition. Assume that T is a subset of $\wp$, where $\wp$ is an arbitrary notion of forcing. We say that T is dense iff for all $g \in \wp$ there is a $h \in T$ with $h \leq g$. (We will be mainly interested in those dense subsets which are ω-definable in M.)

Example. In $\wp^{\leftrightarrow}$ the following sets are ω-definable dense sets. (These sets are not definable in M since $\wp^{\leftrightarrow}$ itself is not definable in M).

1. For each fixed standard rational $\delta > 0$, $T_\delta = \wp^{\leftrightarrow} - \wp_\delta$.
2. For each fixed $x \in M_n$, $T_x = \{p \in \wp^{\leftrightarrow} \mid p$ is defined at $x\}$.
3. For each fixed $y \in M_{n-1}$, $T^{(y)} = \{p \in \wp^{\leftrightarrow} \mid y$ is in the range of $p\}$.

Definition. Let G be a subset of $\wp$, where $\wp$ is an arbitrary notion of forcing. We say that G is $\wp$ generic over M iff the following three conditions are satisfied:

(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 T is a dense subset of $\wp$, which is ω-definable in M, then $G \cap T$ is non-empty.

Since M is countable it is possible to pick (outside M) a decreasing sequence $p_1, p_2, \ldots$ form the elements of $\wp$ so that the sequence contains at least one element from every dense subset of $\wp$ which is ω-definable in M. The filter generated by this sequence is a generic subset of $\wp$ over M. In the example with the partial one-to-one functions $f \leq g$ iff f is an extension of g. $p_1, p_2, \ldots$ is the sequence mentioned whose common extension is the required function. This will be also the common extension of all of the functions in the filter G generated by $p_1, p_2, \ldots$.

Example. Assume that G is $\wp^{\leftrightarrow}$ generic over M and let $\rho = \bigcup_{p \in G} p$. Clearly ρ is a one-to-one map of a subset M_n into M_{n-1}. We claim that it is actually a one-to-one map of M_n onto M_{n-1}. Indeed as we have remarked earlier for each fixed $x \in M_n$, $T_x = \{p \in \wp^{\leftrightarrow} \mid p$ is defined in $x\}$ is dense and therefore according to the definition of generic sets contains an element from G. Thus ρ is defined in x. In a similar way using the dense set $\{p \in \wp^{\leftrightarrow} \mid y$ is in the range of $p\}$ we can show that the range of ρ contains y for any $y \in M_{n-1}$. To show that in $\mathcal{M}[\rho]$ the induction holds we need to know something about the truth value of firstorder formulae in $\mathcal{M}[\rho]$. We will prove essentially the following: if $\mathcal{M}[\rho] \models \phi$, where ϕ is a firstorder sentence, then there is a $p \in G$ so that for all $\wp^{\leftrightarrow}$-generic G' with $p \in G'$ and $\rho' = \bigcup G' = \bigcup_{p \in G'} p$ we have $\mathcal{M}[\rho'] \models \phi$. We will need to know something about the truth value of firstorder formulae $\phi(x)$ depending on a parameter $x \in M_n$. Naturally, as a consequence of the previous statement, we know that for each fixed $a \in M_n$ there is a p_a which decides $\phi(a)$ in the sense that either for all generic G' containing p_a we have $\mathcal{M}[\rho] \models \phi(a)$ or for all such G' we have $\mathcal{M}[\rho] \models \neg\phi(a)$. We will show that if a

generic G is fixed then there is a $p \in G$ so that for all $a \in M_n$ there is a $p_a \in G$, $p_a \leq p$ so that p_a decides $\phi(a)$ in the previous sense and moreover $|\mathrm{dom}(p_a) - \mathrm{dom}(p)| \leq j$ for some standard j. We will also show that it is possible to assign to each $a \in M_n$ a set $U(a) \subseteq M_n$, $|U(a)| \leq k$ for some standard k, so that any $q \leq p$ with $U(a) \subseteq \mathrm{dom}(q)$ and $U(a) \cap M_{n-1} \subseteq \mathrm{range}(q)$, q decides $\phi(a)$. The significance of this will be the following. If we know already that $p \in G$ then the truth value of any fixed $\phi(a)$ can be decided by looking at the values of ρ and ρ^{-1} on $U(a)$ which contains only a small (standard) number of elements. For the proof of this statement we will use essentially the structure of $\wp^{\leftrightarrow}$.

The following definitions are necessary to formulate the results sketched above.

Definitions. 1. Suppose that $\phi(y_0, \ldots, y_i)$ is a firstorder formula of L', $a_0, \ldots, a_i \in M_n$, $g \in \wp$. We say that $g \Vdash \phi(a_0, \ldots, a_i)$ iff for any generic subset G of $\wp$ with $g \in G$ we have that $\rho = \bigcup G$ implies $\mathcal{M}[\rho] \models \phi(a_0, \ldots, a_i)$.

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

We will be interested in the properties of those relations on M_n which can be defined by a firstorder formula from ρ and the relations given in $\mathcal{M}$.

3. Suppose that i is a natural number and X is a relation on M_n^i. We say that X is in $\mathcal{M}[\rho]$ (or definable in $\mathcal{M}[\rho]$), if there exists a natural number j and a firstorder formula $\phi(x_0, \ldots, x_{i-1}, y_0, \ldots, y_{j-1})$ so that for some $b_0, \ldots, b_j \in M_n$ we have that for all $a_0, \ldots, a_{i-1} \in M_n$: $X(a_0, \ldots, a_{i-1})$ iff $\mathcal{M}[\rho] \models \phi(a_0, \ldots, a_{i-1}, b_0, \ldots, b_j)$.

Now we are able to give a precise (and somewhat more general) formulation of the results mentioned about the truth values of a set of formulae $\phi(x)$, $x \in M_n$.

Lemma 2. *Suppose that i is a natural number and X is a relation on M_n^i so that X is in $\mathcal{M}[\rho]$, where $\rho = \bigcup G$ and G is $\wp^{\leftrightarrow}$ generic over M, then the following hold:*

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

(2.2) for each $q \in \wp^{\leftrightarrow}$ there is a $q' \in \wp^{\leftrightarrow}$, $q' \leq q$ so that the relation $p \Vdash X(a_0, \ldots, a_{i-1})$ restricted to the set $p \leq q'$, $p \in \wp^{\leftrightarrow}$, $a_0, \ldots, a_{i-1} \in M_n$ is ω-definable, and for any standard rational $\varepsilon > 0$ the relation $p \Vdash X(a_0, \ldots, a_{i-1})$ restricted to the set $p \leq q'$, $p \in \wp_\varepsilon^{\leftrightarrow}$, $a_0, \ldots, a_{i-1} \in M_n$ is definable in M

(2.3) for all $q \in \wp^{\leftrightarrow}$ there exists a $q' \in \wp^{\leftrightarrow}$, $q' \leq q$, standard natural numbers k, i and a function U which is definable in M so that for all $a \in M_n^i$, $U(a)$ is a subset of M_n with k elements, and for all $p \in \wp^{\leftrightarrow}$ if $p \leq q'$ and $U(a) \subseteq \mathrm{dom}(p)$ and $U(a) \cap M_{n-1} \subseteq \mathrm{range}(p)$, then either $p \Vdash X(a)$ or $p \Vdash \neg X(a)$.

Remark. Since $\wp^{\leftrightarrow}$ is not definable in M the relation $p \Vdash X(a_0, \ldots, a_{i-1})$ is not definable in M. However if we restrict p to a $\wp_\varepsilon^{\leftrightarrow}$ as described in (2.2) it will be definable. (2.3) shows that it is enough to consider this restricted relation since already in such a $\wp_\varepsilon^{\leftrightarrow}$ we will find an element p with $p \Vdash X(a)$ or $p \Vdash \neg X(a)$.

As we have explained earlier, (2.3) means that if a set of formulae is given with parameters in M_n then they can be almost decided simultaneously, that is there is a $p \in G$ so that for each fixed formula there is a set $(U(a))$ containing a standard number of elements so that if we give the values of ρ and its inverse ρ^{-1} there, it decides already whether the formula is true or false in $\mathcal{M}[\rho]$.

Using Lemma 2 we may prove easily that induction holds in the structure $M[\rho]$. First we show that induction holds up to $\log n$, that is, any nonempty subset of natural numbers less than $\log n$ which is definable in $M[\rho]$ has a smallest element. Actually we will show that any such set is also definable in M so our assertion will follow from the validity of induction in M. The second part i.e., to show that induction up to $\log n$ (in $\mathcal{M}[\rho]$) implies induction up to n is easier, for this part we do not use anything from the specific properties of the relation ρ.

Lemma 3. *If G is a $\wp^{\leftrightarrow}$ generic set over M, $\rho = \bigcup G$ and X is a unary relation on M_n which is in $\mathcal{M}[\rho]$ (definable by a first-order formula in this structure), and for all $a \in M_n$, $X(a)$ implies $a \leq \log n$, then X is definable in M.*

Proof. Lemma 2 implies that there exists a $q' \in \wp^{\leftrightarrow}$ so that for each $a \leq \log n$ there is a $U(a), |U(a)| \leq k$ so that if $p \leq q'$, $U(a) \subseteq \mathrm{dom}(p)$, $U(a) \cap M_{n-1} \subseteq \mathrm{range}(p)$ then either $p \Vdash X(a)$ or $p \Vdash \neg X(a)$, moreover the function U is definable in M. Assume that $q' \in \wp^{\leftrightarrow}_{\varepsilon}$ with some standard rational $\varepsilon > 0$. $|\bigcup_{a \leq \log n} U(a)| \leq k \log n$ where k is standard. Therefore the definition of $\wp^{\leftrightarrow}$ implies that the set $T = \{p \in \wp^{\leftrightarrow} | p \leq q', \bigcup_{a \leq \log n} U(a) \subseteq \mathrm{dom}(p)$ and $\bigcup_{a \leq \log n}(U(a) \cap M_{n-1}) \subseteq \mathrm{range}(p)\}$ is dense in $\wp^{\leftrightarrow}$. Consequently there is a $g \in G \cap T$. Clearly we may assume that $g \in \wp^{\leftrightarrow}_{\varepsilon/2}$. According to (2.3) for all $a \leq \log n$, we have either $g \Vdash X(a)$ or $g \Vdash \neg X(a)$. By (2.2) the relation $p \Vdash X(a)$ is definable on $\wp^{\leftrightarrow}_{\varepsilon/2}$, therefore $X(a)$ is definable in M. ∎

Lemma 4. *If induction up to $\log n$ is true in $\mathcal{M}[\rho]$ then induction up to n is also true in $\mathcal{M}[\rho]$*

Remark. This Lemma remains true if instead of $\mathcal{M}[\rho]$ we take any extension of the structure $\mathcal{M}$.

Proof. Suppose that there is a nonempty set $H \subseteq M_n$ definable in $\mathcal{M}[\rho]$ which has no smallest element. We will show that there is also a nonempty subset of $\{1, \ldots, [\log n]\}$, definable in $\mathcal{M}[\rho]$ without a smallest element.

We may clearly assume that H is upward closed, that is $x \leq y, x \in H$ implies $y \in H$. Let $H' = \{x - y \in M_n | x \in H, y \in M_n, y \notin H\}$. Clearly H' is an upward closed subset of M_n which has no smallest element. We claim that if $w \in H'$ then $[w/2] \in H'$. Indeed if $w = x - y$, $x \in H$, $y \notin H$ then let $z = y + [w/2]$. If $z \in H$ then clearly $[w/2] \in H'$. If $z \notin H$ then $x - z \in H'$. Since $x - z$ may differ from w at most by one this means that $w \in H'$.

Let $H'' = \{x | 2^x \in H'\}$. Since H' is closed under the division by 2 we have that H'' has no smallest element and clearly for each $x \in H''$, $x \leq \log n$. Our definitions show that H'' is definable in $\mathcal{M}[\rho]$ which completes our proof. (Here we use that the relation $y = 2^x$ is definable in the structure $\langle M_n, +, \times, \leq, = \rangle$, see [8]. We may avoid this, or using anything about the properties of exponentiation, by including the relation $y = 2^x$ in our basic structure either as a separate new relation or as a part of the relation A.) ∎

Proof of Lemma 2. As we have seen the relation $\rho = \bigcup G$ where G is $\wp^{\leftrightarrow}$ generic over M is a one-to-one map of M_n onto M_{n-1}. In the following definitions $\tilde{f}$ will be an arbitrary one-to-one map of M_n onto M_{n-1} but it will be of interest in the $\tilde{f} = \rho$ case. We will consider such a function $\tilde{f}$ as an evaluation of certain Boolean variables. This motivates the following definitions.

Definition. Suppose that D_0 and D_1 are disjoint finite sets $D = D_0 \cup D_1$. For each $a \in D_0$ and $b \in D_1$ let $x_{a,b}$ be a Boolean variable.

We will use this definition in the case $D_0 = M_n$, $D_1 = M_{n-1}$, (more precisely D_1 is a copy of M_{n-1} disjoint from M_n.) If $\tilde{f}$ is a one-to-one map of M_n onto M_{n-1}, then we may associate with it the following 0, 1-evaluation e of the Boolean variables $x_{a,b}$, $a \in M_n$, $b \in M_{n-1}$: $e(x_{a,b}) = 1$ iff $\tilde{f}(a) = b$. (We will also denote this evaluation by $\mathrm{val}(\tilde{f})$.)

Lemma 2 is an assertion about a firstorder formula $\phi(\vec{a})$ of the language L'. Suppose that $\vec{a}$ is fixed. The truth value of ϕ is a function of the map $\tilde{f}$. It is easy to see that there is a constant depth Boolean formula $\Gamma \in M$ on the variables $x_{a,b}$ whose value at the evaluation e is the same as the truth value of ϕ. (The evaluation e is not in M but since the Boolean formula is of constant depth an evaluation can be defined in the natural way outside M). We will try to replace Γ by a simpler Boolean formula Γ' so that $\Gamma(e) = \Gamma'(e)$ for all of the possible $\tilde{f}$. We will construct Γ' in M but since the evaluation e is not in M, Γ' cannot be any Boolean formula which is equivalent to Γ in M. Still there are possibilities to construct a good Γ'. For example we may apply one of the Boolean identities (commutativity, associativity, distributivity, etc.) to Γ. If Γ' is the new formula what we get this way, clearly $\Gamma(e) = \Gamma'(e)$. Even if we perform such transformations on a set of disjoint subformulae of Γ still we get a good Γ', or we may perform a finite number of transformations one after the other of this type. (The number of transformations is counted in the world, not in M). To describe these things in a rigorous way first we define formally what is a constant depth, unlimited fan-in Boolean formula, then we define the mentioned operations on them.

Definition. Suppose that X is a set of Boolean variables. We define the unlimited fan-in Boolean formulae in the following way. We define the formulae recursively according to their complexity. Let $F_0 = X \cup \{0,1\}$. Suppose that F_{k-1} is already defined. If H is a finite set of natural numbers and h is a function defined on H with values in F_{k-1} then let $\bigvee_{x \in H} h(x)$ and $\bigwedge_{x \in H} h(x)$ be elements of F_k. Moreover if g is an element of F_{k-1} then let both g and $\neg g$ be elements of F_k. We define F_k as the set of all elements that we can get through one of the described ways. $F = \bigcup_{k=0,1,\ldots} F_k$ is the set of unlimited fan-in Boolean formulae with variables in X. In the following Boolean formula will mean always an unlimited fan-in Boolean formula. The depth of a Boolean formula g will be the smallest integer k with $g \in F_k$. We may define the size of the formula by induction on its depth k. For $k = 0$ the size is 1 and $\mathrm{size}(\bigwedge_{x \in H} h(x)) = \sum_{x \in H} \mathrm{size}(h(x))$ (and similarly for $\bigvee$), moreover $\mathrm{size}(\neg s) = \mathrm{size}(s) + 1$. This definition of the size is not the same as the corresponding notion for Boolean circuits. However if we want only to define constant depth polynomial size circuits/formulae the two notions are the same.

We will call two Boolean formulae equivalent if their value is the same under any 0,1-evaluation of the variables. We will consider Boolean formulae in a non-standard model M of Peano Arithmetic, whose depth is a standard natural number. For such formulae it is possible to define the value of the formula even for an evaluation which is not in M. It is possible that two such formulae are equivalent in M still there is an evaluation (not in M) so that the corresponding values of the formulae are different. In the following we will define relations in M which will be finer

than the equivalence of formulae, and will have the property that if two formulae are in relation with each other than their values are the same for any evaluations (not necessarily in M).

Definition. In the following we give some of the usual Boolean identities for unlimited fan-in formulae. (For our purposes it is important that they are given in the unlimited fan-in form.) Each identity has a dual form that we get by changing the role of the operations $\bigvee$ and $\bigwedge$. Although we will give here only one of the two forms later referring to these identities we will mean both of them.

(B1) If the ranges of the functions h and g coincide then

$$\bigwedge_{x\in H} h(x) \equiv \bigwedge_{x\in G} g(x).$$

(B2) If $H=\bigcup_{i\in I} H_i$ where $\{H_i\}$ is a family of pairwise disjoint sets, h_i is a function defined on H_i for all $i\in I$, h is the common extension of all h_i to H and $\bigwedge_{x\in H} h(x)\in F$ then

$$\bigwedge_{x\in H} h(x) \equiv \bigwedge_{i\in I}\left(\bigwedge_{x\in H_i} h_i(x)\right).$$

(B3) suppose that h is defined on $H\cup G$ and $\{h(x)|x\in G\}$ is a subset of $\{h(x)|x\in H\}$. Then $\bigwedge_{x\in H\cup G} h(x)\equiv\bigwedge_{x\in H} h(x)$.

(B4) if $s\in F$ and $\bigwedge_{x\in H} h(x)\in F$ then

$$s\vee\bigwedge_{x\in H} h(x) \equiv \bigwedge_{x\in H}(s\vee h(x)).$$

(B5) if $\bigwedge_{x\in H} h(x)\in F$ then $\neg\bigwedge_{x\in H} h(x)\equiv\bigvee_{x\in H}\neg h(x)$.

Apart from these identities for unlimited fan-in formulae we will need the usual Boolean identities fixing the role of $0,1$ and the operation $\neg$.

(B6) if $s\in F$ then $0\vee s\equiv s$, $0\wedge s\equiv 0$, $1\vee s\equiv 1$, $1\wedge s\equiv s$, $s\vee\neg s\equiv 1$, $s\wedge\neg s\equiv 0$, $\neg\neg s\equiv s$.

As we mentioned before we want to define a relation $\Rightarrow$ between Boolean formulae so that $\Gamma\Rightarrow\Gamma'$ implies $\Gamma(e)=\Gamma'(e)$ for any $\tilde{f}$ where e is the evaluation corresponding to $\tilde{f}$. Since $\tilde{f}$ is a one-to-one map, there will be Boolean equations between the variables $x_{a,b}$ which do not follow from the general Boolean identities given in (B1)-(B6) still they hold for all of the evaluations of type e.

Definitions. 1. Let $B=B(D_0,D_1)$ denote the set of unlimited fan-in Boolean formulae with the variables $\{x_{u,v}\}$, $u\in D_0, v\in D_1$. A $\kappa\in B$ is called a k-map if there is a one-to-one function g of a set $D_0(\kappa)\subset D_0$ onto a subset of D_1 so that $\kappa=\bigwedge x_{u,g(u)}$ and $|D_0(\kappa)|=k$. (We may visualize a k-map as bipartite graph between D_0 and D_1 with k vertex-disjoint edges.) We will use the notation $D_0(\kappa)=$ domain(g), $D_1(\kappa)=$ range(g), $D(\kappa)=D_0(\kappa)\cup D_1(\kappa)$, $g=g_\kappa$, $k=|\kappa|$. We define a function $\pi=\pi_\kappa$ on D by $\pi(x)=g(x)$ if $x\in D_0(\kappa)$ and $\pi(x)=g^{-1}(x)$ if $x\in D_1(\kappa)$.

We say that a set $V\subset D$ covers the map $\kappa\in B$ if for each $x\in D(\kappa)$ either $x\in V$ or $\pi_\kappa(x)\in V$.

Assume that κ, κ' are k, resp. k' maps. We say that κ and κ' are contradictory if there is an $x \in D(\kappa) \cap D(\kappa')$ with $\pi_\kappa(x) \neq \pi_{\kappa'}(x)$.

2. We call a formula $h \in B$ a k-disjunction if $h = \bigvee_{\kappa \in K} \kappa$, where each $\kappa \in K$ is a k'-map for some $k' \leq k$.

The set V covers the k-disjunction $h = \bigvee_{\kappa \in K} \kappa$, if it covers all $\kappa \in K$. We will say that the weight of the k-disjunction h is at most l if there is a set with l elements which covers h.

3. Suppose that ϕ, ψ are s disjunctions. We say that $\phi \mathcal{L} \psi$ if $\phi = \bigvee_{i \in I} d(i)$, $\psi = \bigvee_{i \in I'} d(i)$, $I' = \{i \in I | \forall j \in I \ d(i) \neq d(j)$ implies that $\mathrm{map}(d(i))$ is not an extension of $\mathrm{map}(d(j))\}$. (That is we get ψ from ϕ by deleting from ϕ those terms which are not "minimal").

We will denote the (essentially) unique ψ with $\phi \mathcal{L} \psi$ by $\min(\phi)$. It is easy to see that if Q is an evaluation of the variables then $\min(\phi^Q) = \min((\min(\phi))^Q)$. (More precisely the two formulae are equivalent according to (B1)).

4. For each fixed $u \in D_j$, $j = 0, 1$, we define a Boolean formula

$$F_u \equiv \left(\bigvee_{v \in D_{1-j}} x_{u,v} \right) \wedge \bigwedge_{s,t \in D_{1-j}, s \neq t} x_{u,s} \to \neg x_{u,t}.$$

That is F_u states that from the variables $x_{u,v}$, $v \in D_{j-1}$ there is exactly one whose value is 1.

$O(D_0, D_1)$ will denote the Boolean formula $\bigwedge_{u \in D} F_u$. Clearly if there is a 0,1 assignment for the variables $x_{u,v}$ so that the value of $O(D_0, D_1)$ is 1 then the function g defined by $g(u) = v$ iff $x_{u,v} = 1$ is a one-to-one map of D_0 onto D_1. So the equation $O(D_0, D_1) = 1$ has no solution if D_0 and D_1 are of different cardinalities.

5. Suppose that $h = \bigvee_{\kappa \in K} \kappa$ is a k-disjunction and V covers h, $|V| = l$. We define an l-disjunction $c(h, V)$. ($c(h, V)$ will act as a complement for h if we restrict our attention to evaluations of the variables which define a one-to-one map on V). Let $M = \{\mu |$ μ is a j-map for some $j \leq l$; μ is covered by V and $\forall \kappa \in K$ μ is contradictory to $\kappa\}$ and

$$c(h, V) = \bigvee_{\mu \in M} \mu.$$

Even if we assume that V is a minimal set covering h it is possible that $l > k$. Therefore $c(h, V)$ is only an l-disjunction and not necessarily a k-disjunction. It is easy to check that for any $\tilde{f}$ if e is the corresponding evaluation then the formulae $\neg h$ and $c(h, V)$ have the same value under the evaluation e. We say that the formulae $\neg h$ and $c(h, V)$ are k-equivalent.

6. If k is a natural number then we define a binary relation $\Rightarrow_k$ between Boolean formulae. We say that $\Gamma \Rightarrow_k \Gamma'$ if there is a set S of pairwise disjoint subformulae of Γ so that if we replace each formula in S by another which is equivalent to it according to (B1),...,(B6) or by a formula which is k'-equivalent to it for some $k' \leq k$, then we get the formula Γ'.

If k, r are both natural numbers we define the relation $\Rightarrow_{k,r}$ by $a \Rightarrow_{k,r} b$ iff there exists a sequence $a_0 = a, a_1, \ldots, a_r = b$ so that for all $j = 0, \ldots, r-1$ we have $a_j \Rightarrow_k a_{j+1}$.

7. Suppose now that $|D_0|=n$ and $|D_1|=n-1$, $\varepsilon>0$ and Q is a 0,1 assignment on a subset of X. We say that Q is an ε-partial assignment if there is a one-to-one map h of a subset of D_0 with $[n-n^{\varepsilon}]$ elements onto a subset of D_1 so that Q assigns a value to a variable $x_{u,v}$ iff either $u\in \mathrm{domain}(h)$ or $v\in \mathrm{range}(h)$, moreover $Q(x_{u,v})=1$ iff $h(u)=v$. We will use the notations $h=\mathrm{map}(Q)$, $Q=\mathrm{val}(h)$ and $\mathrm{set}(Q)=\mathrm{domain}(h)\cup\mathrm{range}(h)$.

If λ is a Boolean formula then we will denote by λ^Q the Boolean formula that we get from λ if we perform the substitutions prescribed in Q.

Let q be a one-to-one map of a subset of D_0 into D_1, and let $\varepsilon>0$.

We define a random variable $R=R_{\varepsilon}^{(q)}$ which takes its values with uniform distribution on the set of all ε-partial assignments Q satisfying the condition that $\mathrm{map}(Q)$ is extension of q.

Theorem 5. *$\forall s,d,u,\delta>0\exists\varepsilon>0,k,r$ so that for all sufficiently large n if $|D_0|=n$, $|D_1|=n-1$ and $\phi\in B(D_0,D_1)$ is a Boolean formula of size at most n^s and depth d, q is a one-to-one map of a subset of D_0 with at most $n-n^{\delta}$ elements into D_1 and $R=R_{\varepsilon}^{(q)}$ is the random assignment defined earlier, then with a probability of at least $1-n^{-u}$ the following holds. There exists a k-disjunction g and a set $V\subset D$ with k elements so that g is covered by V and $\phi^R\Rightarrow_{k,r} g$.*

In [1] a similar theorem is proved in a somewhat more complicated setting for the case $|D_0|=|D_1|$.

Using Theorem 5 we may complete the proof of Lemma 2. According to the original definition of $\wp^{\leftrightarrow}$ the elements of $\wp^{\leftrightarrow}$ are maps of subset of M_n into M_{n-1}. In order to conform with the notation of Theorem 5 we will assume now that the maps are between two disjoint sets D_0 and D_1. We may think that D_0 is M_n and D_1 is a copy of M_{n-1}, disjoint from M_n. Naturally (2.3) must be modified in the following way:

(2.3') *for all $q\in\wp^{\leftrightarrow}$ there exists a $q'\in\wp^{\leftrightarrow}$, $q'\le q$, standard natural numbers k,i and a function U which is definable in M so that for all $a\in M_n^i$, $U(a)$ is a subset of $D=D_0\cup D_1$ with k elements, and for all $p\in\wp^{\leftrightarrow}$ if $p\le q'$ and $U(a)\cap D_0\subseteq\mathrm{dom}(p)$, $U(a)\cap D_1\subseteq\mathrm{range}(p)$, then either $p\Vdash X(a)$ or $p\Vdash\neg X(a)$.*

First we define two relations W_0 and W_1. $W_0(p,a_0,\dots,a_{i-1})$ will imply $p\Vdash X(a)$, $W_1(p,a_0,\dots,a_{i-1})$ will imply $p\Vdash\neg X(a)$. For each fixed $a\in M_n^i$ let $\phi_a\in B(D_0,D_1)$ be the Boolean formula expressing the relation $X(a_0,\dots,a_1)$. (Since X is definable in $\mathcal{M}[\rho]$ and ρ can be considered as an evaluation of the variables $x_{s,t}, s\in D_n, t\in D_{n-1}$, there is such a formula ϕ_a.) We may assume that each ϕ_a is of depth at most d and size at most n^s, where the standard integers d,s depend only on the size of the first-order formula defining X but not on n or a. We apply Theorem 5 with $u=i+1$ for each fixed ϕ_a, $a\in M_n^i$. Let $\varepsilon>0,k,r$ be the numbers whose existence is guaranteed by Theorem 5 and let q' be a value of $R_{\varepsilon}^{(q)}$ satisfying the conclusion of Theorem 5 simultaneously for each fixed ϕ_a, $a\in M_n^i$. (Since $u>i$ there is such a q'.) We define a relation W_1 by $W_1(p,a_0,\dots,a_i)$ iff "there exists a standard j so that $p\in\wp^{\leftrightarrow}_{1/j}$ and $\phi^p\Rightarrow_{j,j}1$". (We get the definition of W_0 if we substitute the last formula by $\phi^p\Rightarrow_{j,j}0$). Clearly W_0, W_1 are ω-definable. The conclusion of Theorem 5 implies that W_1 is equivalent to the relation $p\Vdash X(a_0,\dots,a_1)$ if $p\le q'$. This implies the first part of (2.2).

Let $\delta > 0$ be a standard rational. Then, according to Theorem 5 the relation W_1 with $p \leq q'$ restricted to $\wp_\delta^{\leftrightarrow}$ is equivalent to "$p \in \wp_\varepsilon^{\leftrightarrow}$ and $\phi^p \Rightarrow_{k,r} 1$" where k and r may depend only on i and the size of the formula defining X but do not depend on the choice of $a_0, \ldots, a_{i-1}$. That is, $p \| \vdash X(a_0, \ldots, a_{i-1})$ is indeed definable in M, if $p \leq q'$, $p \in \wp_\varepsilon^{\leftrightarrow}$.

If we pick $U(a)$ as the set V belonging to ϕ_a then our previous argument shows that (2.3) holds.

(2.1) follows from (2.2). ∎

Proof of Theorem 5. First we show that it is enough to prove the theorem for the special case when ϕ is an s-disjunction. In this case we may suppose that the size of ϕ is not more than $2n^{2s}$ so we may drop the condition about the size of the formula. In the the formulation of the result for s disjunctions we may substitute the relation $\Rightarrow_{k,r}$ by the relation $\mathcal{L}$ defined after the definition of s-disjunctions. Clearly there are absolute constants k, r so that for all ϕ, ψ $\phi \mathcal{L} \psi$ implies $\phi \Rightarrow_{k,r} \psi$.

Lemma 6. *$\forall s, u \exists \varepsilon > 0, k$ so that for all sufficiently large n if $|D_0| = n$, $|D_1| = n-1$ and $\phi \in B(D_0, D_1)$ is an s disjunction and $R = R_\varepsilon$ is the random ε partial assignment, then with a probability of at least $1 - n^{-u}$ we have: there exists a set $V \subset D$ so that $\min(\phi^R)$ is covered by V and $|V| \leq k$.*

We show that Lemma 6 implies Theorem 5. The proof is based on the fact, (stated earlier) that if an s disjunction h is covered by a set V of size k then it has a complement $c(h, V)$ which is an l-disjunction where l depends only on k. This will make it possible to prove the theorem by induction on the depth of ϕ. We assume that there are a polynomial number of disjoint subformulae of ϕ of the form of $\neg\eta$, where η is a k' disjunction, for some constant k', so that ϕ is built up from these formulae by using only the operations disjunctions and negations in a depth of $d-1$. Suppose now that $\varepsilon' > 0$ is sufficiently small. According to Lemma 6 each $(\eta)^{R_{\varepsilon'}}$ will be covered by some set V of size k'. Therefore it has a complement which is a k'' disjunction that is $(\neg\eta)^{R_{\varepsilon'}}$ is a k'' disjunction and so the depth of $(\phi)^{R_{\varepsilon'}}$ is only $d-1$ but otherwise it has the same structure as ϕ had (with k'' instead of k') therefore we may complete the proof by using the inductive hypothesis. Below we give a more formal description of this proof.

Let K_j be the set of formulae of size at most n^j from $B(D_0, D_j)$. For each positive integer let $U_{0,l}^j = U_{0,l}$ be the set of l disjunctions in K_j. Suppose now that $U_{d-1,l}$ is already defined then let $U_{d,l}$ be the set of all formulae from K_j which are either of the form $\bigvee_{x \in H} h(x)$ where $h(x) \in U_{d-1,l}$ for all $x \in H$ or of the form $\neg h$ where $h \in U_{d-1,l}$.

Claim 7. *If $g \in K_j$ and g is of depth at most d then there is a g' in $U_{2d,1}$ and there are positive integers k, r depending on only d so that $g \Rightarrow_{k,r} g'$.*

Proof. Using the identities in (B1),...,(B6) we may transform g into a formula which uses only $\bigvee$ and $\neg$ as logical connectives and still its depth is not greater than $2d$. A single variable $x_{a,b}$ may be considered as a 1 disjunction. ∎

Now we may continue the proof of Theorem 5 (accepting Lemma 6), by induction on d. We give the proof for $d = 1$. Suppose that $g \in U_{1,k}$ if g is of the

form $\bigvee h(x)$ then using (B1) and (B2) we may transform g into a formula in $U_{0,l}$ so Lemma 6 can be directly applied.

Assume now that h is of the form $\neg\phi$ where $\phi \in U(0,1)$. According to Lemma 6 with high probability we have $\phi^R \mathscr{L} g$ where g is a k disjunction covered by a set V, where $|V|=k$. g is k equivalent to $c(g,V)$ so we have $\phi^R \Rightarrow_{k,r+1} c(g,V)$.

Before we start the proof of Lemma 6 we formulate two combinatorial lemmas which will be repeatedly used throughout the proof. (The proofs of these lemmas are given in [1].) The first Lemma essentially states that if there is a function defined on a finite set H so that at each point x the value of the function is a small subset of H not containing x, then inside a small random subset H' the function will be almost trivial, that is H' will have only a constant number of points which are contained in a value of the function taken at a point in H'. The second Lemma is a generalization of the first, for functions with more than one variables.

Lemma C. *Suppose that $0<\varepsilon<1/2$, $0<\delta<\varepsilon/4$ and g is a function defined on the finite set H with n elements such that $g(x)\subseteq H$, $|g(x)|\leq |H|^{1-\varepsilon}$ and $x\notin g(x)$ for all $x\in H$. If $j<|H|^{\delta}$ and H' is a random subset of H with j elements, then for all $t>0$ we have*

$$P\Big(|\{y|y\in H' \text{ and } y\in g(x) \text{ for some } x\in H'\}|\geq t\Big) < n^{-c_1 t+c_2}$$

where $c_1>0$ and c_1, c_2 depend only on ε.

Lemma C'. *Suppose that $0<\varepsilon<1/2$ and k is a positive integer. Then there exists a $\delta>0$ such that for any finite set H with n elements if g is a function defined on the Cartesian product $\prod_k H$ with $g(x)\subseteq H$, $|g(x)|\leq |H|^{1-\varepsilon}$, $g(\langle x_0,\ldots,x_{k-1}\rangle)\cap \{x_0,\ldots,x_{k-1}\}=\emptyset$ for all $x=\langle x_0,\ldots,x_{k-1}\rangle\in\prod_k H$ and H' is a random subset of H with $\lfloor |H|^{\delta}\rfloor$ elements, then for all $t>0$ we have*

$$P\Big(|\{y\in H'|y\in g(x) \text{ for some } x\in \prod_k H'\}|>t\Big) < n^{-c_1 t+c_2}$$

where $c_1>0$ and c_1, c_2 depend only on ε and k. ∎

Now we continue the proof of Lemma 6.

Definition. Suppose R_ε is the random ε partial assignment and $D_0'=D_0-\mathrm{set}(R_\varepsilon)$, $D_1'=D_1-\mathrm{set}(R_\varepsilon)$. For each fixed value of D_0', D_1' let R_δ' be a δ partial assignment on the universe D_0', D_1'. Let $R_\varepsilon\circ R_\delta'$ be the common extension of the functions R_ε, and R_δ'. Each value of $R_\varepsilon\circ R_\delta'$ is a δ partial assignment on D_0, D_1, moreover the distribution of $R_\varepsilon\circ R_\delta'$ is the same as the distribution of R_δ that is the random variables R_δ, and $R_\varepsilon\circ R_\delta'$ are identical. (In the following we will use this several times without any extra warnings.)

We prove the lemma by induction on s.

$s=1$. According to the definition if ϕ is a 1 disjunction then $\phi=\bigvee_{\langle a,b\rangle\in W} x_{a,b}$ where $W\subseteq D_0\times D_1$. We may write ϕ in the form $\bigvee_{a\in D_0}\bigvee_{b\in W_a} x_{a,b}$ where $W_a\subseteq D_1$ for each $a\in D_0$. Let $\varepsilon>0$ be sufficiently small and let $G=\{a\in D_0|\ |W_a|\geq n^{1-\varepsilon}\}$

Case I. $|G| > n^{2\varepsilon}$.

In this case with a probability of at least $(1-(1-n^{-\varepsilon})^{n^{\varepsilon}})^{n^{2\varepsilon}} > 1-e^{-n^{\varepsilon}}$ after we perform the substitutions according to R_ε the value of at least one $x_{a,b}$, $b \in W_a$ will be 1. So $\min((\phi)^R)$ is covered by the empty set.

Case II. $|G| < n^{1-\varepsilon}$. Let us apply Lemma C with $H \to D$. We define the function f by $f(x) = W_x$ if $x \in D_0 - G$ and $f(x) = \emptyset$ otherwise. Let $H' = D - \text{set}(R_\delta)$. Strictly speaking H' is not a random subset of D with uniform distribution since the size of $H' \cap D_0$ is always the same. However it is easy to see that there is a random variable H'' so that H'' has uniform distribution on the subsets of D with $4\lfloor n^{\delta} \rfloor$ elements and with high probability H' is a subset of H''. This implies that the conclusion of Lemma C, holds for H' too. Let $V = \{y \in H' | \exists x \in H'\ y \in f(x)\}$. Clearly V covers the 1 disjunction ϕ^{R_δ} and Lemma C implies that the requirement about the size of V is met with sufficiently large probability.

We assume now that Lemma 6 holds for $s-1$ and prove it for s. We actually will show that for all s and u $\exists \varepsilon > 0, k$ so that if n is sufficiently large and ϕ is an s disjunction then there is an s disjunction ψ of weight at most $k/2$ and an $s-1$ disjunction ψ' so that

$$(*) \qquad \phi^{R_\varepsilon} \mathcal{L}(\psi \vee \psi').$$

Then we will apply the inductive hypothesis to $s-1$ and get an R_δ so that $\psi'^{R_\delta} \mathcal{L} \psi''$ where ψ'' is of weight at most $k/2$ and therefore $\min((\phi)^{R_\delta})$ is of weight at most k with a sufficiently high probability.

Definitions. 1. Suppose that ϕ is an s disjunction $\phi = \bigvee_{i \in I} d(i)$ where each $d(i)$ is an s' map for some $s' \leq s$ and $\min(\phi) = \bigvee_{i \in I'} d(i)$ for some $I' \subseteq I$. Let $(\phi)_s = \bigvee_{i \in I''} d(i)$ where $I'' = \{i \in I' | \text{map}(d(i)) \text{ is an } s\text{map}\}$. (In other words we get $(\psi)_s$ from ψ by keeping only those terms which are exactly of size s and which are not consequences of any terms of smaller size).

2. Suppose that $\eta = \bigvee_{i \in I} d(i)$ is an s disjunction. If $a \in D_0$ and $b \in D_1$ then we will denote by $\eta^{x,y}$ the s disjunction $\bigvee_{i \in I'} d(i)$ where $I' = \{i \in I |\ \text{map}(d(i))(a) = b\}$.

Proof of (*). First we prove that under the conditions of (*) with a probability of at least $1 - n^{-u}$ there exists an s-disjunction η so that $\phi^{R(\varepsilon)} \mathcal{L} \eta$ and "for all $a \in D_0, b \in D_1$ the weight of $\eta^{a,b}$ is at most k. Then we will show that applying an other R_δ we get that with high probability $\eta^{R_\delta} \mathcal{L}(\psi \vee \psi')$ where ψ, ψ' have the properties given in (*).

Suppose that $a \in D_0$ and $b \in D_1$ are fixed, $\phi^{a,b} = \bigvee_{i \in I'} d(i)$. For each fixed $i \in I'$, $d(i)$ is an s' map for some $s' \leq s$. Let $d'(i)$ be the $s'-1$ map what we get from $d(i)$ by deleting the term $x_{a,b}$. Let $\psi = \bigvee_{i \in I' d'(i)}$. ψ is an $s-1$ disjunction, so by the inductive hypothesis with high probability there is an $s-1$ disjunction g so that $\psi^{R_\varepsilon} \mathcal{L} g$ and g is covered by a set of size $k-1$, which implies our assertion.

To finish the proof of (*) let η be the s disjunction with the properties described above. We apply Lemma C' with $H \to D$, $k \to 2$. The function f is defined in the following way: if $a \in D_0, b \in D_1$ then according to Y there is a set V of size of at most k so that V covers $\eta^{a,b}$. In this case let $f(\langle a,b \rangle) = V$. For all other $\langle a,b \rangle$ let $f(a,b) = \emptyset$. As in the proof of Case II for $s=1$ let $R = R_\varepsilon$, $H' = D - \text{set}(R)$. By

the same argument the conclusion of Lemma C' holds for H'. Let $X=\{y\in H' \mid y\in f(x,z)$ for some $x,z\in H'\}$. According to the Lemma $P(|X|>k)<n^{-c_1k+c_2}$, where $c_1>0$ and c_1,c_2 depends only on ε. We claim that X covers $(\eta)_s^{R_\varepsilon}$, where $(\eta)_s$.

Let $\eta=\bigvee_{i\in I} d(i)$, and suppose that for a fixed $i\in I$,we have $\mathrm{map}(d(i))(x)=y$. It is sufficient to prove that if $|\mathrm{domain}(d(i))-\mathrm{set}(R_\varepsilon)|=s$ then either $x\in X$ or $y\in X$. $s\geq 2$ implies that there are $a,b\in D$ with $a\neq x$ so that $\mathrm{map}(d(i))(a)=b$. As we have seen X covers $\eta^{a,b}$ which implies our statement and also completes the proof of Lemma 6. ∎

References

[1] M. Ajtai: Firstorder definability on finite structures, to appear in *Annals of Pure and Applied Logic* 1989.

[2] M. Ajtai: The complexity of the Pigeonhole Principle, *29-th FOCS*, 1988, 346–358.

[3] S. Buss: Polynomial size proofs of the propositional Pigeonhole Principle, to appear in *Journal of Symbolic Logic*.

[4] S. Buss, and Gy. Turán: Resolution proofs of Generalized Pigeonhole Principles, to appear in *Journal of Symbolic Logic*.

[5] S. Cook, and R. Rechkhow: The relative efficiency of propositional proof systems, *Journal of Symbolic Logic* **44** (1977), 36–50.

[6] A. Haken: The intractability of resolution, *Theoretical Computer Science* **39** (1985), 297–308.

[7] J. B. Paris, and A. J. Wilkie: Counting problems in bounded arithmetic, in: *Methods in Mathematical Logic, Proc. Caracas 1983*, Springer-Verlag Lecture Notes in Mathematics no. 1130. Eds.: A. Dold and B. Eckman, Springer-Verlag, 1985, pp. 317–340.

[8] J. B. Paris, and A. J. Wilkie: Counting Δ_0 sets, *Fund. Math.* **127** (1986), 67–76.

[9] J. B. Paris, A. J. Wilkie, and A. R. Woods: Provability of the pigeonhole principle and the existence of infinitely many primes, *Journal of Symbolic Logic* **53** (1988) 1235–1244.

[10] R. Statman: Complexity of derivations from quantifier-free Horn formulae, mechanical introduction of explicit definitions, and refinement of completeness theorems, in: *Logic Colloquium '76*, eds.: R. Gandy, M. Hyland, North Holland, 1977, 505–517.

[11] A. Urquhart: Hard examples for resolution, *Journal of the ACM*, **34** (1987) (1) 209–219.

[12] A. J. Wilkie: talk presented at the ASL Summer meeting in Manchester, England, 1984.

[13] A. R. Woods: *Some problems in logic and number theory and their connections*, Ph.D. dissertation, Department of Mathematics, Manchester University, 1981.

Miklós Ajtai

IBM Almaden Research Center

ajtai@almaden.ibm.com