universität wien

DIPLOMARBEIT

Titel der Diplomarbeit

Propositional Logic, Complexity Theory And A Nontrivial Hierarchy Of Theories Of Weak Fragments Of Peano Arithmetic

angestrebter akademischer Grad

Magister der Naturwissenschaften (Mag.rer.nat)

Wien, im May 2011

Verfasser:	Christoph Schöller
Matrikel-Nummer:	9908625
Studienkennzahl lt. Studienblatt:	A 405
Studienrichtung lt. Studienblatt:	Mathematische Logik und Grundlagen
Betreuer:	Sy David Friedman

Contents

1. Introduction

Frege systems are the typical "incarnations" of propositional proof systems. They are not only of interest in logic but also in computer science because of their relationship to exhaustive search problems. This relationship basically states that the complexity of a Frege proof is equivalent to the complexity of a calculation of a Turing machine that runs an exhaustive search algorithm. So for the class of NP-complete problems, where only exhaustive search heuristics are known, the runtime of such a search is equivalent to the size of the corresponding Frege proof. A consequence of Ajtai's work is that an algorithm for finding a Frege proof for PHP cannot have sub-exponential runtime. As indicated in the abstract, an analogous proposition holds for the Parity Principle: the runtime cannot be sub-exponential even considering Turing machines with PHP as an oracle. As a conclusion one can consider a hierarchy of stronger and stronger tautologies that cannot be computed in sub-exponential time relative to an oracle lower in the hierarchy. Later Ajtai's results were improved even further [BIKPPW, BPU, KPW, BP] by eliminating the need for nonstandard models and by giving a more exact super-exponential lower bound to PHP in a more constructive way. Lower bounds to Frege proof systems have consequences for even broader complexity issues. The important, still open problem "$NP? = co - NP$", that is, the question whether the class of predicates accepted by a non-deterministic polynomial time Turing machine is closed under complementation, is equivalent to: "Is there a Frege proof system in which the correctness of a derivation can be checked in polynomial time and which admits polynomial size proofs of all tautologies?"

2. Paris & Wilkie's Work

In this section I present the required definitions and use them to give a general understanding of the subject (most of these are from [K]).

Definition 1. (*language of arithmetic* L_{PA}):
$L_{PA} = \{0, 1, +, \times, <, =\}$, where 0, 1 are constants, $<$, $=$ are binary relations and $+$, $\times$ are tertiary relations.

Definition 2. *(bounded arithmetical formulas* Δ_0):

(1) $E_0 = U_0$ is the class of quantifier free formulas.
(2) Class E_{i+1} is the class of formulas logically equivalent to a formula of the form
$$\exists x_1 < t_1(\bar{a}) \dots \exists x_k < t_k(\bar{a}) \phi(\bar{a},\bar{x})$$
with $\phi \in U_i$ and $t_i(\bar{a})$'s terms of the language L_{PA}.
(3) U_{i+1} is the class of formulas logically equivalent to a formula of the form
$$\forall x < t_1(\bar{a}) \dots \forall x_k < t_k(\bar{a}) \phi(\bar{a},\bar{x})$$
with $\phi \in E_i$ and $t_i(\bar{a})$'s terms of the language L_{PA}.
(4) Class Δ_0 of bounded arithmetic formulas is the union of classes E_i and U_i
$$\Delta_0 = \bigcup_i E_i = \bigcup_i U_i$$

Definition 3. (*theory of bounded arithmetic* $I\Delta_0$):
The theory of bounded arithmetic is a first order theory in the language L_{PA} is axiomatized by the axioms

(1) PA^-:
  (a) $a + 0 = a$
  (b) $(a + b) + c = a + (b + c)$
  (c) $a + b = b + a$
  (d) $a < b \to \exists x, a + x = b$
  (e) $0 = a \vee 0 < b$
  (f) $0 < 1$

(g) $0 < a \to 1 \leq a$

(h) $a < b \to a + c < b + c$

(i) $a + 0 = 0$

(j) $a \times 1 = a$

(k) $(a \times b) \times c = a \times (b \times c)$

(l) $a \times b = b \times a$

(m) $(a < b \wedge c \neq) \to a \times c < b \times c$

(n) $a \times (b + c) = (a \times b) + (a \times c)$

(2) and the Δ_0-*induction scheme* Δ_0-IND

$$(\phi(0) \wedge \forall(\phi(x) \to \phi(x+1))) \to \forall x \phi(x)$$

where ϕ is a Δ_0-formula, which may have other free variables beside x.

Definition 4. (*least number principle LNP scheme*):

$$\phi(x) \to \exists b \forall a(\phi(b) \wedge (a < b \to \neg\phi(a)))$$

where ϕ is a Δ_0-formula, which may have other free variables beside x.

Definition 5. (*induction up to n* IND_n):

$$(\phi(0) \wedge \forall(\phi(x) \to \phi(x+1))) \to \forall x \leq n \phi(x)$$

.

Definition 6. (*theory of existential arithmetic* $I\exists_1$):

(1) consist of the axioms PA^-

(2) and the $\exists_1$-induction scheme:

$$(\phi(0) \wedge \forall(\phi(x) \to \phi(x+1))) \to \forall x \phi(x)$$

where ϕ is a E_1-formula, which may have other free variables beside x.

Definition 7. ($[A]^n$):

For any set A and any natural number $0 < n \in \omega$

$$[A]^n = \{X \subset A || X| = n\}$$

is the set of all subsets of A that have exactly n elements.

Definition 8. (*the Pigeonhole Principle PHP*):
Fix $k \in \omega$. For every

$$F : [\omega]^1 \to \{1, \ldots, k\}$$

there exists an infinite $H \subset \omega$ s.t. F is constant on $[H]^1$

Definition 9. (*the propositional Pigeonhole Principle PHP_n by Cook and Rechkov*):

$$\begin{aligned} PHP_n \quad = \quad & \neg[(\bigwedge_{i\in n} \bigvee_{j\in n-1} x_{i,j}) \wedge \\ & (\bigwedge_{j\in n-1} \bigvee_{i\in n} x_{i,j}) \wedge \\ & (\bigwedge_{i\in j,k\in n-1, j\neq k} \neg(x_{i,j} \wedge x_{i,k}) \wedge \\ & (\bigwedge_{j\in n-1 i,l\in n i\neq l} \neg(x_{i,j} \wedge x_{l,j})))] \end{aligned}$$

To show the consistency of $I\exists_1(F) + \exists x F : x \mapsto x - 1$, Paris and Wilkie applied a simple forcing argument to a non-standard model $\mathcal{M}$ of $I\exists_1$ to get an extended model $\mathcal{M}[F]$ with $\mathcal{M}[F] \models I\exists_1(F) + \exists x F : x \to x - 1$. Because this is the first important technique for understanding the following arguments, it is worth discussing the origins of forcing.

The general idea of forcing was introduced by Paul Cohen in his proofs that the *Continuum Hypothesis* and the *Axiom of Choice* are independent of ZF. In the following I give those definitions, that are appropriate for applications to bounded arithmetic.

Definition 10. (*Initial segment of a model of PA*):
If $\mathcal{M} =: < M, 0, 1, +, \times, <, = >$ is a model of Peano Arithmetic and $n \in M$ then

$$M_n =: \{x \in M | \mathcal{M} \models x < n\}$$

.

Definition 11. Let A be an i-ary relation symbol and R a binary relation symbol, then $L = L_{PA} \cup \{A\}$ and $L' = L \cup \{B\}$.

Definition 12. ($\mathcal{M}$-*definability*):

Let $i \in \omega$, $R \subseteq M^i$ (a i-ary relation on M),

then R is definable in $\mathcal{M}$

if there exists a 1st-order formula $\phi(x_1, \ldots, x_i, y)$ of L_{PA} with free variables $x_1, \ldots, x_i$, y and there exists a $c \in M$ s.t. for all $a_1, \ldots, a_i \in M$ we get $R(a_1, \ldots, a_i)$ iff $\mathcal{M} \models \phi(a_1, \ldots, a_i, c)$.

Definition 13. ($\mathcal{M}$-*definability* on M_n):

Let $i, n \in \omega$, $R \subseteq M_n^i$ (a i-ary relation on M_n),

then R is $\mathcal{M}$-definable on M_n

iff there exists a single 1st-order formula $\phi(x_1, \ldots, x_i, y)$ of L_{PA} with free variables $x_1, \ldots, x_i, y$ and there exists $c_R \in M$ s.t. for all $a_1, \ldots, a_i \in M_n$ we get $R(a_1, \ldots, a_i)$ iff $\mathcal{M} \models \phi(a_1, \ldots, a_i, c_R)$.

Remark 14. So we can treat definable relations on M_n as elements of M, by coding R as above as $2^{\#(\phi)}3^{c_R} \in M$.

Definition 15. (ω-*definability in* $\mathcal{M}$):

Let $i \in \omega, R \subseteq M^i$,

then R is ω-definable in $\mathcal{M}$

iff there exists a 1st-order formula $\phi(x_1, \ldots, x_i, y, z)$ of L_{PA} with free variables $x_1, \ldots, x_i, y, z$ and there exists $b \in M$ s.t. for all $a_1, \ldots, a_i \in M$ we get $R(a_1, \ldots, a_i)$ iff (there is $c_R \in \omega$ s.t. $\mathcal{M} \models \phi(a_1, \ldots, a_i, c_R, b)$).

Definition 16. (*Forcing*):

(1) Let $\mathcal{M}$ be a countable model of PA^-.

(2) notion of forcing:

(a) Let $P \subseteq M$ be nonempty, definable in $\mathcal{M}$ and $\leq_P$ a partial, $\mathcal{M}$-definable ordering on P,

then $< P, \leq_P >$ is definable in $\mathcal{M}$ and called an $\mathcal{M}$-*definable notion of forcing*.

(b) Let $P \subseteq M$ be nonempty, ω-definable in $\mathcal{M}$ and $\leq_P$ a ω-definable in $\mathcal{M}$, partial ordering on P,

then $< P, \leq_P >$ is ω-definable in $\mathcal{M}$ and called an *$\mathcal{M}$-ω-definable notion of forcing*.

(3) The elements $p \in P$ are called *forcing conditions*.

(4) For $p, q \in P$ we say q is *stronger than* p iff $q \leq_P p$.

(5) If $p, q \in P$ and there is r s.t. $r \leq_P p$ and $r \leq_P q$ then p and q are called *compatible*.

(6) A set $D \subseteq P$ is *dense in* P if for every $p \in P$ there is $q \in D$ s.t. $q \leq_P p$.

Definition 17. (*Filter*):

A set $F \subseteq P$ is called a *filter on* P if the following holds:

(1) $F \neq \emptyset$.

(2) If $p \leq_P q$, $p \in F, q \in P$, then $q \in F$.

(3) If $p, q \in F$, then there is $r \in F$ s.t. $r \leq_P p$ and $r \leq_P q$.

Definition 18. (*P-genericity*):

Let P be an $\mathcal{M}$-definable forcing notion,

then a set $G \subseteq P$ is called *P-generic over $\mathcal{M}$* if the following holds:

(1) G is a filter on P .

(2) If D is dense in P and D $\mathcal{M}$-definable, then $G \cap D \neq 0$.

Definition 19. (*P-ω-genericity*):

Let P be an $\mathcal{M}$-ω-definable forcing notion,

then a set $G \subseteq P$ is called *P-ω-generic over $\mathcal{M}$* if the following holds:

(1) G is a filter on P .

(2) If D is dense in P and D ω-definable, then $G \cap D \neq 0$.

Definition 20. (*Forcing relation*):

Suppose $< P, \leq_P >$ is a notion of forcing, $\phi(\overrightarrow{x})$ a 1st-order formula with a new relation symbol, $\overrightarrow{a} \in M$, $p \in P$. We say $p \Vdash \phi(\overrightarrow{a})$ (p forces ϕ) iff for any G P-generic over $\mathcal{M}$ s.t. $p \in G$ we get $\mathcal{M}[G] \models \phi(\overrightarrow{a})$.

Here $\mathcal{M}[G]$ is the model (the *generic extension*) obtained from $\mathcal{M}$ (the *ground model*) by adjoining the generic set G as a new unary relation to get a richer model.

What is important for the definition of the forcing relation is that the "external" definition of $p \Vdash \phi$ is equivalent to its "internal" definition. This is done to ensure that the properties definable in $\mathcal{M}[G]$ are "expressible" in $\mathcal{M}$. To get a nontrivial case where $\mathcal{M}[G]$ is a model of a theory T' stronger than T, the forcing conditions have to be understood as "partial examples" of the new properties denoted by T'. Using the partial ordering $< P, \leq_P >$ of the forcing conditions defined in the ground model, we can understand a filter $F \subset P$ as a consistent sequence of such partial examples that each belong to the ground model. So a generic $G \subset P$, consisting of forcing conditions in the ground model, can arbitrarily approximate this new property. This approximation further fully defines what else is true in the generic extension and can be formalized by the following three conditions:

Definition 21.

(1) Truth: $\mathcal{M}[G] \models \phi$ iff there is some condition $p \in G, p \Vdash \phi$.

(2) Definability: For every ϕ fixed the relation $p \Vdash \phi$ must be definable in $\mathcal{M}$.

(3) Coherence: If $p \Vdash \phi$ and $q \leq_P p$, then $q \Vdash \phi$.

Paris and Wilkie defined their forcing conditions this way:

Definition 22.

Suppose $\mathcal{M}$ is a countable nonstandard model of $I\exists_1$, $n \in M$ and n nonstandard. A forcing condition p is a finite set of the form

$$p = \{R(x_1) = y_1, R(x_2) = y_2, \ldots, R(x_i) = y_i\}$$

with $\overrightarrow{x} \leq n, \overrightarrow{y} < n$ and $R \subset n \times n - 1$ is one-to-one and for two forcing conditions p, q is $q \leq_P p$ iff $q \supseteq p$.

Remark 23. In this case P, the set of forcing conditions p, can be regarded as an $\mathcal{M}$-definable notion of forcing, by coding the forcing conditions using elements of M.

Theorem 24.

$$I\exists_1(F) + \exists x F : x \to x - 1 + F \textit{ is one-to-one}$$

is consistent.

Proof.

Remark 25. Suppose p is a forcing condition, $\phi(\overrightarrow{x})$ a formula from L_{PA} (i.e. ϕ does not involve R) and $\overrightarrow{a} \in M$, then

$$p \Vdash \phi(\overrightarrow{a}) \Longleftrightarrow \mathcal{M} \models \phi(\overrightarrow{a}) \text{ and } p \Vdash R(a) = b \Longleftrightarrow (R(a) = b) \in p$$

.

Claim 26. ("Decision Lemma") Suppose $\phi(x) = \exists \overrightarrow{y} \theta(x, \overrightarrow{y}) \in \exists_1(R)$ in the language $L_{PA}(R) =: L_{PA} \cup R$, then there is a fixed $j_\theta \in \omega$ depending only on θ s.t. for any condition p and $a \in M$, either $p \Vdash \neg\phi(a)$ or $\exists p' \leq_P p$, $p' \Vdash \phi(a)$ and $|p' - p| \leq j_\theta$.

Proof. To decide $\theta(x, y_1, \ldots, y_m)$ we need to know the values of $R^i(x)$,$R^i(y_1)$,..., $R^i(y_m)$,$R^i(e_1)$,...,$R^i(e_k)$ where $e_1, \ldots, e_k$ are the constants in θ and $i \leq j$, j fixed. Suppose there exist j_θ such values, then either $p \Vdash \neg\phi(a)$ or $\exists p' \leq_P p$, $\overrightarrow{b} \in ran(R)$ s.t. $p' \Vdash \theta(a, \overrightarrow{b})$. Since $|p|$ is finite and n is nonstandard we can pick a p'' compatible to p' (i.e. $p'' \cup p' \Vdash \theta(a, \overrightarrow{b})$) s.t. p'' extends p by defining $R^i(x), R^i(y_1), \ldots, R^i(y_m), R^i(e_1), \ldots, R^i(e_k)$ for $i \leq j$ and hence p'' decides $\theta(a, \overrightarrow{b})$. Then also $p'' \Vdash \theta(a, \overrightarrow{b})$ and $p'' \Vdash \phi(a)$, $|p'' - p| \leq j_\theta$. □

Now we can pick a generic set G of forcing conditions p s.t. $F =: \bigcup G$ and $< \mathcal{M}, F > \models \exists \alpha F : \alpha \to \alpha - 1 + F$ is one-to-one.

To show that $< \mathcal{M}, F > \models I\exists_1(F)$, we have to show that every nonempty $\exists_1(F)$ set has a least element:
Suppose that p a forcing condition, $\phi(x) \in \exists_1(F)$ and $j_\theta \in \omega$ are as in the Claim, $p \Vdash \phi(a)$. Then

$$\{a' \leq a | \text{ there is a forcing condition } p' \leq_P p, |p' - p| \leq j_\theta \text{ and } p' \Vdash \phi(a)\}$$

is definable in $\mathcal{M}$ and has a least element l. By the Claim above $p \Vdash \neg\phi(a)$ for all $a < l$, hence p' forces that l is the least element satisfying $\phi(x)$ in $< \mathcal{M}, F >$ □

The second important idea of Paris and Wilkie was the connection between bounded arithmetic and Frege systems in their consistency result for $I\Delta_0(F) + \exists x, F : x \to x - 1$, under the assumption of the Cook-Reckhov Conjecture:

Definition 27. (Frege system [U]):

(1) A *Frege Rule* is defined to be a sequence of propositional formulas of the form $A_1, \ldots, A_k \vdash A_0$.

(2) If $A_1 = ... = A_k = \emptyset$ then $\vdash A_0$ is called an *axiom scheme.*

(3) A rule is *sound* if ever truth-assignment satisfying $A_1, \ldots, A_k$ also satisfies A_0 ($A_1, \ldots, A_k \models A_0$).

(4) C_0 is *inferred from* $C_1, \ldots, C_k$ by a Frege rule $A_1, ..., A_k \vdash A_0$, if there is a sequence of formulas $B_1, \ldots, B_m$ and variables $x_1, \ldots, x_m$ s.t. for all i, $0 \leq i \leq k, C_i = A_i[B_1/x_1, \ldots, B_m/x_m]$. B_i/x_i refers to the substitution of the variable x_i by the formula B_i.

(5) If $\mathfrak{F}$ is a set of Frege rules and A a formula, then a *proof of A in $\mathfrak{F}$ from* $A_1, ..., A_k$ is a finite sequence of formulas s.t. every formula in the sequence is either one of the $A_1, ..., A_k$ or inferred by a rules in $\mathfrak{F}$ and the last formula is A.

(6) The *length* of a Frege proof is number of formulas in this sequence.

(7) The *size* of a Frege proof is the number of its symbols.

(8) A set $\mathfrak{F}$ of Frege rules is *implicationally complete* if whenever $A_1, \ldots, A_k \models A_0$, then there is a proof of A in $\mathfrak{F}$ from $A_1, \ldots, A_k$.

(9) A *Frege system* is a finite, sound, implicationally complete set of Frege rules.

Definition 28. (*Cook-Rechkov Conjecture*):

$\forall k \exists n$ s.t. every Frege proof of

$$CR \equiv \bigwedge_{i \leq n} \bigvee_{j < n} p_{i,j} \to \bigvee_{i < e \leq n} \bigvee_{j < n} (p_{i,j} \wedge p_{e,j})$$

has size bigger than n^k.

Theorem 29. *(Paris, Wilkie):*

Suppose the Cook-Reckhov Conjecture holds,

then

$$I\Delta_0(F) + \exists n, F : n \to n-1$$

is consistent.

Proof.

Suppose $\mathcal{M}$ is a countable, nonstandard model of $I\Delta_0$. Take $n, k \in M$ and nonstandard s.t. every proof of

$$\bigwedge_{i\leq n} \bigvee_{j<n} p_{i,j} \to \bigvee_{i<e\leq n} \bigvee_{j<n} (p_{i,j} \wedge p_{e,j})$$

has size bigger than n^k.

Definition. Definition (bounded arithmetic $\leftrightarrow$ propositional calculus)

For ϕ formula from $L_{PA}(R) =: L_{PA} \cup R$, R a new binary relation symbol and $\overrightarrow{a} \leq n$ we define a formula $\Phi(\overrightarrow{a})$ of a Frege system

ϕ	Φ
$R(a_1, a_2)$	r_{a_1,a_2}
$a_1 + a_2 = a_3$	s_{a_1,a_2,a_3}
$a_1 \times a_2 = a_3$	t_{a_1,a_2,a_3}
$a_1 = a_2$	e_{a_1,a_2}
$\phi_1 \wedge \phi_2$	$\Phi_1 \wedge \Phi_2$
$\neg\phi$	$\neg\Phi$
$\exists x\phi(x)$	$\bigvee_{a\leq n} \Phi(a)$
$\forall x\phi(x)$	$\bigwedge_{a\leq n} \Phi(a)$

, with p, s, t new propositional variables.

Now we define a sets of propositional formulas T such that any proof of inconsistency uses more than n^k symbols:

$$T \equiv CR \cup$$

$$\{\Phi | \phi \text{ is an atomic sentence or negation of an atomic sentence of } L_{PA}$$

$$\text{and } n+1 \models \phi\}$$

Define an increasing sequence of sets of propositional formulas

$$T = T_0 \subseteq T_1 \subseteq T_2 \subseteq ...$$

s.t.

(1) each T_i is coded in $\mathcal{M}$,

(2) there is no proof of inconsistency in $\mathcal{M}$ from T_i using less than $n^{k/2^i}$ symbols,

(3) for each $\phi(\overrightarrow{x}) \in L_{PA}(R)$ and $\overrightarrow{a} \leq n$ there is an $i \in \mathbb{N}$ s.t. $\Phi(\overrightarrow{a}) \in T_i$ or $\neg\Phi(\overrightarrow{a}) \in T_i$,

(4) if $\bigvee_{a \leq n} \Phi(\overrightarrow{a}) \in T_i$ then there is $\exists j, m \in \omega, j \geq i$ and $m \leq n$ s.t. $\Phi(\overrightarrow{m}) \wedge \bigwedge_{a \leq m} \neg\Phi(\overrightarrow{a}) \in T_j$.

Define a new relation

$$\bar{R} \subseteq (n+1) \times (n+1) \Longleftrightarrow r_{a_1,a_2} \in \bigcup_{i \in \omega} T_i$$

then

$$< n+1, \bar{R} > \models \Delta_0\text{-}IND + \{\phi | \Phi \in \bigcup_{i \in \omega} T_i\}$$

For $a \leq n$ define

$$F(a) = \text{the least } b \text{ s.t. } \bar{R}(a,b)$$

then F is an one-to-one map from $n+1$ into n, because $CR \in T_i$ for all i and

$$< n^\omega, F > \models \Delta_0\text{-}IND(F) + F : n+1 \to n$$

where n^ω denotes the substructure of $\mathcal{M}$ with universe $\{m | m \leq n^{\overset{e}{}}, e \in \omega\}$.

□

3. Ajtai

Ajtai combined the ideas of forcing on nonstandard models and the connection of Frege systems with the provability in bounded arithmetic to prove that $I\Delta_0(F)+\exists nF : n \to n-1$ is consistent, if we consider only Frege proofs of polynomial size and constant depth [AJ2]. As the existence of such a function F is a simple application of the ideas of forcing, the consistency gives deep insight into the complexity of the construction of this function.

The argument is the following: The Paris-Wilkie proof above shows that PHP can only be proven if we have a model where a polynomial size and constant depth Frege proof of PHP_n exists. Now assume that there is such a model $\mathcal{M}$ where a polynomial size and constant depth proof for PHP_n exists for some nonstandard n. We restrict our model to the initial segment containing only elements less than n. We add the function $\rho : n-1 \to n-2$, ρ one-to-one via forcing. Furthermore by a combinatorial argument, IND_n also holds in this extended model and with this we can check the proof of PHP_n for ρ. This contradicts our assumption, by finding a formula in the proof that contradicts the injectivity of ρ.

Thus the consistency proof splits into two main parts:

First we define a model $\mathcal{M}$ and special notion of forcing $< \mathcal{P}^{\leftrightarrow}, \leq_{\mathcal{P}^{\leftrightarrow}} >$ and show that for any generic subset G, $\mathcal{M}[G] \models \neg PHP_n$.

The second part, showing that induction holds in the generic extension, is the more difficult part. To decide the truth value of a 1st-order formula $\phi(a)$ for a fixed $a \in M_n$ in the new model, means that there exists a p_a s.t. either for all generic G containing p_a $\mathcal{M}[G] \models \phi(a)$ or $\mathcal{M}[G] \models \neg\phi(a)$. We have to show that this can be done by looking at the values of ρ and ρ^{-1} on a small, standard number of elements and taking into account the combinatorial structure of the notion of forcing. We essentially show:

If ϕ is a 1st-order formula and G $\mathcal{P}^{\leftrightarrow}$-$\omega$-generic over $\mathcal{M}$ and $p \in G$, then

(1) $\forall a{\in}M_n\, \exists p_a{\in}G\, \exists j{\in}\omega\ p_a{\leq_{\mathcal{P}^{\leftrightarrow}}}p \wedge |dom(p_a) - dom(p)| \leq j \wedge p_a$ decides $\phi(a)$

(2) $\forall a{\in}M_n\, \exists U(a){\subseteq}M_n\, \exists w{\in}\omega\ |U(a)|{\leq_{\mathcal{P}^{\leftrightarrow}}}w$ and $\forall q{\leq_{\mathcal{P}^{\leftrightarrow}}}p\ U(a) \subseteq dom(q){\wedge}U(a){\cap}$ $M_{n-1} \subseteq ran(q) \to q$ decides $\phi(a)$

The meaning of (1) is, if we already know $p \in G$ then there exists a p_a only a "little" stronger (at most "j-much" stronger) than this and p_a decides $\phi(a)$. The meaning of (2) is, if we already know $p \in G$ then the truth value of any fixed $\phi(a)$ can be decided by looking only at the values of ρ and ρ^{-1} on $U(a)$ which contains only w many elements.

Now I give a rigorous definition of these ideas:

3.1. **Forcing** $< \mathcal{M}, \rho > \models \neg PHP$.

Definition 30. Let T be a theory of the language L,
then T describes a large initial segment of Peano Arithmetic,
if for each $l \in \omega$ then there is a model $\mathcal{M}$ of PA and an $n \in M$ s.t. $\mathcal{M} \models n > l$ and there is an $i \in \omega$ and an i-ary relation $A \subseteq M_n^i$ definable in $\mathcal{M}$ s.t. with the interpretation τ defined by, $\tau(+) = +_{\mathcal{M}} \restriction M_n, \tau(\times) = \times_{\mathcal{M}} \restriction M_n, \tau(<) = <_{\mathcal{M}} \restriction M_n$, we get $\mathcal{M}_n =: < M_n, \tau(+), \tau(\times), \tau(<), =, A > \models T$.

Definition 31. Let $\tau' \supset \tau$ be an interpretation of the language L'.

Let T describe a large initial segment of PA and let $\mathcal{M} \models PA$ and $n \in M$ s.t. $\mathcal{M}_n \models T$ with n nonstandard. To get Ajtai's result we have to extend $\mathcal{M}_n$ by adding a generic set G via forcing s.t. the extended structure $\mathcal{M}[G]$ satisfies a new binary relation ρ:

(1) ρ is an one-to-one map of M_n onto M_{n-1}

(2) if $\tau'(R) = \rho$, then $< \mathcal{M}, \rho > \models IND_n(\rho)$.

We will define a notion of forcing $< \mathcal{P}^{\leftrightarrow}, \leq_{\mathcal{P}^{\leftrightarrow}} >$ where its elements $p \in \mathcal{P}^{\leftrightarrow}$ will consist of partial one-to-one maps between two sets definable in $\mathcal{M}$, with domain of size at most $n - n^{\epsilon}, \epsilon > 0, \epsilon$ standard rational which are definable in $\mathcal{M}$ and ordered by set-inclusion. We take a filter $G \subseteq \mathcal{P}^{\leftrightarrow}$ which is $\mathcal{P}^{\leftrightarrow}$-$\omega$-generic over $\mathcal{M}$. Since M_n is countable, $\bigcup G$ is defined everywhere on M_n, takes every value in M_{n-1}, is one-to-one and onto. Thus $\rho := \bigcup G$ will serve as the desired new binary relation.

Definition 32. (Ajtai forcing)
Let $\epsilon > 0$, standard, $\mathcal{P}_\epsilon := \{p \in \mathcal{M} | p$ is one-to-one from M_n into $M_{n-1} \wedge \mathcal{M} \models |dom(p)| \leq (n - n^{\epsilon})\}$, $\mathcal{P}^{\leftrightarrow} := \bigcup_{1/t} \{\mathcal{P}_{1/t} | t \in \omega\}$ and $q \leq_{\mathcal{P}^{\leftrightarrow}} p$ iff $q \supseteq p$,
then $< \mathcal{P}^{\leftrightarrow}, \leq_{\mathcal{P}^{\leftrightarrow}} >$ is a notion of forcing which is ω-definable in $\mathcal{M}$.

Fact 33.

The following hold:

(1) *each* $p \in \mathcal{P}^{\leftrightarrow}$ *is definable in* $\mathcal{M}$ *(because of the remark above every definable relation on* M_n *is an element of* M*).*

(2) $\mathcal{P}^{\leftrightarrow}$ *is not definable in* $\mathcal{M}$*, because* $\mathcal{P}^{\leftrightarrow}$ *has no minimal elements.*

(3) $\mathcal{P}^{\leftrightarrow}$ *is* ω*-definable in* $\mathcal{M}$*, because for every* $p \in \mathcal{P}^{\leftrightarrow}$ *there is a* $t \in \omega$*,* $p \in \mathcal{P}_{1/t}$*.*

(4) $\mathcal{P}^{\leftrightarrow}$ *has a greatest element* $1_{\mathcal{P}}$*, that is the empty function.*

(5) *for each fixed* $x \in M_n$*,* $D_x := \{p \in \mathcal{P}^{\leftrightarrow} | p \text{ is defined at } x\}$ *is dense in* $\mathcal{P}^{\leftrightarrow}$ *and* ω*-definable in* $\mathcal{M}$*:* D_x *has no minimal elements; for all* $p \in D_x$ *there is* $t \in \omega$*,* $p \in \mathcal{P}_{1/t}$*.*

(6) *for each fixed* $y \in M_{n-1}$*,* $D^y := \{p \in \mathcal{P}^{\leftrightarrow} | y \text{ is in the range of } p\}$ *is dense in* $\mathcal{P}^{\leftrightarrow}$ *and* ω*-definable in* $\mathcal{M}$*:* D^y *has no minimal elements; for all* $p \in D^y$ *there is* $t \in \omega$*,* $p \in \mathcal{P}_{1/t}$*.*

Lemma 34.

Let G *be* $\mathcal{P}^{\leftrightarrow}$*-*$\omega$*-generic over* $\mathcal{M}$ *and* $\rho := \bigcup G$*, then* ρ *is an one-to-one map of* M_n *onto* M_{n-1}*.*

(1) *for all* $x \in M_n$ ρ *is defined in* x*:*

for each fixed $x \in M_n$ D_x *is dense in* $\mathcal{P}^{\leftrightarrow}$ *and so by definition of genericity* $D_x \cap G \neq \emptyset$*.*

(2) *for all* $y \in M_{n-1}$ y *is in the range of* ρ*:*

for each fixed $y \in M_{n-1}$ D^y *is dense in* $\mathcal{P}^{\leftrightarrow}$ *and so by definition of genericity* $D^y \cap G \neq \emptyset$*.*

(3) ρ *is one-to-one:*

for all $p, q \in G$ p, q *are compatible, partial one-to-one maps of* M_n *into* M_{n-1}*.*

Corollary 35. $< \mathcal{M}, \rho > \models \neg PHP$

3.2. **Truth of 1st-order formulas in** $< \mathcal{M}, \rho >$**.**

Lemma 36.

Let $j \in \omega$, G $\mathcal{P}^{\leftrightarrow}$-$\omega$-generic, $\rho := \bigcup G$ and $R \subseteq M_n^j$ s.t. R is definable in $< \mathcal{M}, \rho >$, then the following holds:

(1) *for all $a_1, \ldots, a_j \in M_n$ there is a $p \in G$ s.t. $p \Vdash R(a_1, \ldots, a_j)$ or $p \Vdash \neg R(a_1, \ldots, a_j)$*

(2) *for all $p \in \mathcal{P}^{\leftrightarrow}$ there is a $p' \in \mathcal{P}^{\leftrightarrow}$, $p' \leq_{\mathcal{P}^{\leftrightarrow}} p$ s.t.*

- *the relation $q \Vdash R(a_1, \ldots, a_j)$ restricted to $q \leq_{\mathcal{P}^{\leftrightarrow}} p', q \in \mathcal{P}^{\leftrightarrow}$, $a_1, \ldots, a_j \in M_n$ is ω-definable*

  and

- *for all standard $\epsilon > 0$ the relation $q \Vdash R(a_1, \ldots, a_j)$ restricted to $q \leq_{\mathcal{P}^{\leftrightarrow}} p', q \in \mathcal{P}^{\leftrightarrow}_{\epsilon}, a_0, \ldots, a_j \in M_n$ is definable in $\mathcal{M}$.*

(3) *for all $p \in \mathcal{P}^{\leftrightarrow}$ there is a $p' \in \mathcal{P}^{\leftrightarrow}$,$q \leq_{\mathcal{P}^{\leftrightarrow}} p'$, $w \in \omega$ and a function $U : M_n^j \to M_{n-1}$ that is definable in $\mathcal{M}$ s.t. for all $a_1, \ldots, a_j \in M_n$ $U(a_1, \ldots, a_j) \subseteq M_n \cup M_{n-1}, |U(a_1, \ldots, a_j)| = w$, and for all $q \in \mathcal{P}^{\leftrightarrow}$ if $q \leq_{\mathcal{P}^{\leftrightarrow}} p', U(a_1, \ldots, a_j) \cap M_n \subseteq dom(q)$ and $U(a_1, \ldots, a_j) \cap M_{n-1} \subseteq ran(q)$ then either $q \Vdash R(a_1, \ldots, a_j)$ or $q \Vdash \neg R(a_1, \ldots, a_j)$.*

To prove this, we introduce:

3.2.1. *Unlimited fan-in Boolean formulae.*

Definition 37. (unlimited fan-in Boolean formulae):

Let X be a set of Boolean variables.

By induction on $c \in \omega$ we define B_c:

(1) $B_0 = X \cup \{0, 1\}$.

(2) Induction step:

(a) If $H \subset \omega$, $|H| < \omega$, $h : H \to B_{c-1}$,
then $\bigvee_{x \in H} h(x) \in B_c$ and $\bigwedge_{x \in H} h(x) \in B_c$.

(b) If $\Phi \in B_{c-1}$,
then $\Phi, \neg\Phi \in B_c$.

$\mathcal{B} =: \bigcup_c B_c$ is the set of unlimited fan-in Boolean formulae with variables in X.

Definition 38. (depth of a formula):

Let $\Phi \in \mathcal{B}$,

then the $depth(\Phi)$ is the smallest $c \in \omega$ s.t. $\Phi \in B_c$.

Definition 39. (size of a formula):

Let $\Phi \in \mathcal{B}$,

then $|\Phi|$ (the size of Φ) is defined by induction on $d = depth(\Phi)$:

(1) $d = 0$: If $\Phi \in B_0$, then $|\Phi| = 1$.

(2) define $|\neg\Phi| =: |\Phi| + 1$

(3) Let $|h(x)|$ be defined for all $h(x) \in B_{k-1}$. Then
$|\bigwedge_{x\in H} h(x)| = \sum_{x\in H} |h(x)| = |\bigvee_{x\in H} h(x)|$.

Definition 40.

Let D_0, D_1 be arbitrary sets s.t. $D_0 \cap D_1 = \emptyset$. $|D_0| = n < \omega$, $|D_1| = n - 1 < \omega$, $D := D_0 \cup D_1$,

then define the set of Boolean variables indexed by D_0, D_1: $X_{D_0,D_1} =: \{x_{a,b}|$ for all $a \in D_0$, $b \in D_1\}$.

Remark 41. In the following we consider $\mathcal{B}_{D_0,D_1} =: \{\Phi \in \mathcal{B}|$ for all $x_{a,b}$ which appear in Φ we have $x_{a,b} \in X_{D_0,D_1}\}$.

Notation 42. For simplicity we will denote $\mathcal{B}_{D_0,D_1}$ as B. And X_{D_0,D_1} as X.

3.2.2. *(Partial-)Truth assignments and evaluations of Boolean formulae.* Now we define an assignment of truth values on the Boolean variables. We'll start with an ϵ-partial assignment R_ϵ on $X_{D_0^\epsilon,D_1^\epsilon} \subset X_{D_0,D_1}$ s.t. $D_1^\epsilon \subset D_1$, $D_0^\epsilon \subset D_0$, $n - n^\epsilon = |D_0^\epsilon|$ for $0 < \epsilon \leq 1$. Then we'll define an $\delta-$partial assignment Q_δ on D_0^δ, D_1^δ that acts as a kind of complement to R_ϵ. The common extension $R_\epsilon \circ Q_\delta$ will be a $\delta-$partial assignment on D_0 in a natural way.

Definition 43.

Let p be an one-to-one map of $D_0^\epsilon \subseteq D_0$ onto $D_1^\epsilon \subseteq D_1$, $Q_\epsilon : X' \subseteq X \to \{0, 1\}$,

then Q_ϵ is an *ϵ-partial assignment (on $D_0^\epsilon, D_1^\epsilon$)*,

if the following holds:

(1) $n - n^\epsilon = |D_0^\epsilon|$

(2) $(Q_\epsilon(x_{a,b}) = 0$ or $Q_\epsilon(x_{a,b}) = 1)$ iff $(a \in dom(p)$ or $b \in ran(p))$

(3) $Q_\epsilon(x_{a,b}) = 1$ iff $p(a) = b$.

Notation 44. $map(Q_\epsilon) =: p$, $val_p =: Q_\epsilon$ and $set(Q_\epsilon) =: dom(p) \cup ran(p)$.

Definition 45.

Let $\Phi \in B$ and Q_ϵ an ϵ-partial assignment,

then Φ^{Q_ϵ} denotes the Boolean formula that we get

if we apply the truth assignment Q_ϵ on Φ, i.e replace the $x_{a,b}$ appearing in Φ by $Q_\epsilon(x_{a,b})$.

Definition 46.

Let p be an one-to-one map of $D_0^{|dom(p)|}$ into D_1, $|dom(p)| < n - n^{\epsilon_0}$, $\epsilon_0 > 0$ and $\epsilon < \epsilon_0$,

then $R_\epsilon^{(p)}$ is a random element of $\{Q_\epsilon | Q_\epsilon$ is an ϵ-partial assignment and $p \subseteq map(Q_\epsilon)\}$.

Definition 47.

Let R_ϵ be a random, ϵ-partial assignment, $D_0^\delta \subseteq D_0 - dom(R_\epsilon)$, $D_1^\delta \subseteq D_1 - ran(R_\epsilon)$ and Q_δ a δ-partial assignment on D_0^δ, D_1^δ,

then $R_\epsilon \circ Q_\delta$ is the common extension of the assignments R_ϵ and Q_δ.

Fact 48. *Each $R_\epsilon \circ Q_\delta$ is a δ-partial assignment on D_0, D_1 and the probability of choosing a particular common extension $R_\epsilon \circ Q_\delta$ is the same as choosing a particular δ-partial assignment.*

Definition 49. (evaluation of a Boolean variable):

Let ρ be an one-to-one map of D_0 onto D_1, $x_{a,b} \in X$ a Boolean variable,

then define a Boolean evaluation $e_\leftrightarrow : X \to \{0, 1\}$ by:

$e_\leftrightarrow(x_{a,b}) = 1$ iff $\rho(a) = b$.

Notation 50. We denote this evaluations $e_\leftrightarrow$ defined by ρ as val_ρ.

Definition 51. (evaluation of a Boolean formula):

Let ρ be an one-to-one map of D_0 onto D_1, $\Phi \in B$,

then $e(\Phi)$ is the truth value of Φ

where each Boolean variable $x_{a,b}$ appearing in Φ is replaced by its evaluation $val_\rho(a, b)$.

Remark 52. By Lemma 36 and definition 51 we can understand the truth value of a 1st-order formula $\phi(a_1, \ldots, a_k)$ in the language L' by an evaluation of a corresponding Boolean formula Φ by the map ρ.

In the following we will just consider Boolean formulae Γ s.t. $depth(\Phi) \in \omega$. For these it is possible to define the truth value $e(\Phi)$ even if $\rho \notin \mathcal{M}$, our non-standard model of PA.

3.2.3. *Equivalence of Boolean formulae.*

Definition 53. (Equivalence of Boolean Formulae):
Two Boolean formulae Φ, Ψ are equivalent ($\Phi \equiv_{eval} \Psi$),
iff for all evaluations e, $e(\Phi) = e(\Psi)$.

Definition 54. (Equivalence of Boolean Formulae in $\mathcal{M}$):
Two Boolean formulae Φ, Ψ are equivalent in $\mathcal{M}$ ($\Phi \equiv_{\mathcal{M}} \Psi$),
iff for all evaluations $e \in \mathcal{M}$, $e(\Phi) = e(\Psi)$.

Fact 55. *For every $\phi(a_1, \ldots, a_k) \in L'$, $a_1, \ldots, a_i \in M_n$ there is a $d \in \omega$ and $\Phi \in B$ s.t. $depth(\Phi) \leq d$ and $< \mathcal{M}, \rho > \models \phi(a_1, \ldots, a_k)$ iff $e(\Phi) = 1$, $e = val_\rho$.*

Remark 56. We want to replace Φ by a "simpler" Ψ s.t. $\Phi \equiv_{eval} \Psi$. The construction of Ψ will be in $\mathcal{M}$ but since there are evaluations $e \notin \mathcal{M}$, Ψ needs not to be in $\mathcal{M}$. However, there is one problem: If two Boolean formulae Φ, Ψ s.t. $\Phi \equiv_{\mathcal{M}} \Psi$, then still there may exist an evaluation $e' \notin \mathcal{M}$ s.t. $e'(\Phi) \neq e'(\Psi)$. So we need to define a stronger kind of equivalence relation $L \in \mathcal{M}$ s.t. $\Phi L \Psi \Rightarrow e(\Phi) \equiv_{eval} e(\Psi)$.

Definition 57. (Boolean identity):
We define the syntactic equivalence of Boolean formulae ($\equiv_s$) as follows:

(1) If $H \subset \omega$, $|H| < \omega$, $g, h : H \to B$ and $ran(g) = ran(h)$,
then $\bigwedge_{x \in H} g(x) \equiv_s \bigwedge_{x \in H} h(x)$.

(2) If $H_i \subset \omega$, $|H_i| < \omega$, pairwise disjoint, $h_i : H_i \to B$, $H = \bigcup_{i \in I} H_i$, $h_i \subseteq h : H \to B$ and $\bigwedge_{x \in H} h(x) \in B$,
then $\bigwedge_{x \in H} h(x) \equiv_s \bigwedge_{i \in I} \bigwedge_{x \in H_i} h_i(x)$.

(3) If $\Phi \in B$ and $\bigwedge_{a \in H} h(a) \in B$,
then $\Phi \vee \bigwedge_{x \in H} h(x) \equiv_s \bigwedge_{x \in H} (\Phi \vee h(x))$.

(4) If $\bigwedge_{x\in H} h(x) \in B$,

then $\neg \bigwedge_{x\in H} h(x) \equiv_s \bigvee_{x\in H} \neg h(x)$.

(5) If $\Phi \in B$,

then $0 \vee \Phi \equiv_s \Phi$, $0 \wedge \Phi \equiv_s 0$, $1 \vee \Phi \equiv_s 1$, $1 \wedge \Phi \equiv_s \Phi$, $\Phi \vee \neg\Phi \equiv_s 1$, $\Phi \wedge \neg\Phi \equiv_s 0$, $\neg\neg\Phi \equiv_s \Phi$.

Remark 58. Each identity in the above definition has a dual form that we get by replacing $\bigwedge$ with $\bigvee$ and vice versa.

Definition 59. (k-map):

$K \in B$ is called a k-map,

if there is an one-to-one map p_K of $D_0(K) \subset D_0$ onto $D_1(K) \subset D_1$ s.t. $K = \bigwedge_{(a,b)\in p_K} x_{a,b}$, $|D_0(K)| = k$.

Definition 60. $D(K) = D_0(K) \cup D_1(K)$.

Fact 61. $D_0(K) \cap D_1(K) = \emptyset$.

Fact 62. $|K| = k$.

Definition 63.

Let $K \in B$ be a k-map,

then define a function $\pi_K : D \to D$ by

$$\pi_K(x) = \begin{cases} p_K(x)\ x \in D_0(K) \\ p_K^{-1}(x)\ x \in D_1(K) \end{cases}$$

Definition 64. (cover of a k-map):

Let $K \in B$ be a k-map and $V \subset D$,

then V covers K,

if for all $x \in D(K) \Rightarrow x \in V$ or $\pi_K(x) \in V$.

Definition 65.

Let $K \in B$ be a k-map and $K' \in B$ a k'-map,

then K and K' are contradictory,

if there is a $x \in D(K) \cap D(K')$ s.t. $\pi_K(x) \neq \pi_{K'}(x)$.

Definition 66. (k-disjunction)

Let $\Delta \in B$,

then Δ is a k-disjunction

if there is a set $\kappa = \{K|$ there is a $k' \leq k$ s.t K is a k'-map$\}$ and $\Delta = \bigvee_{K \in \kappa} K$.

Definition 67. (cover of a k-disjunction):

Let $V \subset D$, and a k-disjunction $\Delta = \bigvee_{K \in \kappa} K$,

then V covers Δ

if V covers all $K \in \kappa$.

Definition.

Let $u \in D$,

then we define

$$F_u =: \begin{cases} \bigvee\limits_{v \in D_1} x_{u,v} \wedge \bigwedge\limits_{s,t \in D_1,\ s \neq t} (x_{u,s} \to \neg x_{u,t}) & u \in D_0 \\ \bigvee\limits_{v \in D_0} x_{v,u} \wedge \bigwedge\limits_{s,t \in D_0,\ s \neq t} (x_{s,u} \to \neg x_{t,u}) & u \in D_1 \end{cases}$$

and

$$O_{D_0,D_1} =: \bigwedge_{u \in D} F_u$$

.

Fact 68.

If there is a $0,1$*-assignment for* $x_{u,v}$, *s.t* $O_{D_0,D_1} = 1$,

then the function ρ *defined by* $\rho(a) = b$ *iff* $x_{a,b} = 1$ *is an one-to-one map of* D_0 *onto* D_1.

Fact 69. *If* $|D_0| \neq |D_1|$,

then the equation $O_{D_0,D_1} = 1$ *has no solution.*

Definition 70.

Let $\Delta = \bigvee_{K \in \kappa} K$ be a k-disjunction, $V \subset D$ covers Δ, $|V| = l$,

then the l-disjunction $c(\Delta, V)$ is defined,

if $\mu =: \{M|$ there is a $l' \leq l$ s.t M is a l'-map, V covers M and for all $K \in \kappa$, M and K are contradictory$\}$, and $c(\Delta, V) =: \bigvee_{M \in \mu} M$.

Remark 71. $c(\Delta, V)$ serves as a complement of Δ, if restrict the evaluations of the Boolean variables $x_{a,b}$ to $val_p(a,b)$ s.t p is an one-to-one map on V.

Even if V is a minimal cover of Δ, it is possible that $l > k$.

Fact 72. *If ρ is an one-to-one map of D_0 onto D_1 , $\Delta \in B$ a k-disjunction and e the evaluation defined by ρ, then $e(\neg\Delta) = e(c(\Delta, V))$.*

Notation 73. We say $\neg\Delta$ and $c(\Delta, V)$ are k-equivalent.

Definition 74. (L_w)

Let $w \in \omega$, $\Phi, \Psi \in B$,

then define the binary relation $\Phi L_w \Psi$,

if there is a set S of pairwise disjoint sub-formulae of Φ s.t.

if we replace each formula $\Lambda \in S$ by a formula Λ' that is either $\equiv_s$-equivalent or a k-equivalent k-disjunction Δ, $k \leq w$, then we get Ψ.

Definition 75. $(L_{w,r})$

Let $w, r \in \omega$, $\Phi, \Psi \in B$,

then define the binary relation $\Phi L_{w,r} \Psi$,

if there is a sequence $\Phi = \Phi_0, \Phi_1, \ldots \Phi_r = \Psi$ s.t. for all $0 \leq j \leq r-1$ $\Phi_j L_w \Phi_{j+1}$.

Definition 76.

Let Δ, Δ' be k-disjunctions,

then $\Delta \mathcal{L} \Delta'$,

if $\Delta = \bigvee_{x \in H} h(x)$, $\Delta' = \bigvee_{x \in H'} h(x)$, $H' = \{x \in H |$ for all $y \in H$, $h(x) \neq h(y) \rightarrow map(h(x)) \not\subseteq map(h(y))\}$.

Remark 77. We get Δ' from Δ by deleting $h(x)$ with non-minimal $map(h(x))$'s.

Fact 78. *There are $w, r \in \omega$ constant for all Δ, Δ' k-disjunctions s.t. $\Delta \mathcal{L} \Delta' \rightarrow \Delta L_{w,r} \Delta'$.*

Notation 79. For $\Delta \mathcal{L} \Delta'$ the unique Δ' is denoted by $min(\Delta)$.

Fact 80. *If Q is an assignment of the Boolean variables in Δ,*

then $min(\Delta^Q) = min(min(\Delta^Q))$.

3.2.4. *Properties of k-disjunctions.* We'll now state what a property of a k-disjunction is, what it means that a property holds and how one property can be reduced to another one:

Remark 81. The following two Lemma are from [AJ1]

Lemma 82.

If $0 < \epsilon < \frac{1}{2}$, $0 < \delta < \frac{\epsilon}{4}$, g *is a function,* $dom(g) = H$, $|H| = n$, *for all* $x \in H$ $g(x) \subseteq H$, $|g(x)| \leq |H|^{1-\epsilon}$, $x \notin g(x)$, $j < |H|^{\delta}, H'$ *random subset of* H, $|H'| = j$ *then for all* $t > 0$, $P(|\{y | y \in H' \text{ there is } x \in H', y \in g(x)\}| \geq t) < n^{-c_1 t + c_2}$.

Lemma 83.

If $0 < \epsilon < \frac{1}{2}$, $k \in \omega$,

then there are $\delta > 0$ *for all* H, $|H| = n$, $x =< x_1, \ldots, x_k > \in H^k$,

if g *is a function,* $dom(g) = H^k$, $g(x) \subseteq H$, $|g(x)| \leq |H|^{1-\epsilon}$, $g(< x_1, \ldots, x_k >) \cap \{x_1, \ldots, x_k\} = \emptyset$, H' *random subset of* H, $|H'| = |H|^{\delta}$,

then for all $t > 0$ $P(|\{y \in H' | \text{ there is } x \in H'^k, y \in g(x)\}| \geq t) < n^{-c_1 t + c_2}$, $c_1 > 0$, c_1, c_2 depend only on ϵ and k.

Definition 84.

Let $k \in \omega$ and $\Delta \in B$ be a k-disjunction,

then $P_k(\Delta, w)$ is a property of Δ,

if it is a binary relation defined on all pairs Δ, w, all elements $a \in D$ are $a \in \omega$:

$$P_k \subseteq \{(\Delta, w) | \Delta \text{ is a } k\text{-disjunction for some } D_0, D_1 \text{ and } w \in \omega\}$$

Definition 85.

Let $k, w \in \omega$, $\Delta \in B$ be a k-disjunction and $\Omega_k(\Delta, w)$ be a property,

then Ω_k is the trivial property,

iff $\Omega_k(\Delta, w)$ holds for all Δ and w.

Definition 86.

Let $k, w \in \omega$ and $\Delta \in B$ be a k-disjunction,

then we say that the property $\Pi_k(\Delta, w)$ of the k-disjunction Δ holds (we say that the weight of Δ is at most w),

iff there is a set $V \subseteq D$ s.t. V covers Δ and $|V| \leq w$.

Definition 87.

Let R_ϵ be a random ϵ-partial assignment, $k \in \omega$, Δ a k-disjunction and P_k, P'_k properties of k-disjunctions,

then $P_k \lhd P'_k$ (P_k can be reduced to P'_k),

if for all w' there are $\epsilon > 0$, $w_0 \in \omega$, $h \in^\omega \omega$ with $lim_{x\to\infty} h(x) = \infty$ s.t. for all $w > w_0$, n sufficiently large, $|D_0| = n$, $|D_1| = n-1$ and $P_k(\Delta, w')$,

then with a probability$\geq 1 - n^{-h(w)}$ there is a k-disjunction Δ' s.t. $\Delta^{R_\epsilon} \mathcal{L} \Delta'$ and $P'_k(\Delta', w)$.

Fact 88. *$\lhd$ is transitive.*

Theorem 89. *Let R_ϵ be a random ϵ-partial assignment. For any $k \in \omega$ $\Omega_k \lhd \Pi_k$.*

Proof. (Theorem 89 for $k = 1$):

If Δ is a 1-disjunction, Δ is of the form $\bigvee_{(a,b)\in W} x_{a,b}$ s.t. $W \subseteq D_0 \times D_1$, then $\bigvee_{(a,b)\in W}$ is an abbreviation for $\bigvee_{a\in D_0} \bigvee_{b\in W_a} x_{a,b}$ s.t. for all $a \in D_0$, $W_a \subseteq D_1$. Let $\epsilon > 0$ and $G = \{a \in D_0 |\ |W_a| \geq n^{1-\epsilon}\}$.

Case 1. $|G| \geq n^{2\epsilon}$

With a probability of a least $(1 - (1 - \frac{n^\epsilon}{2}))^{n^{2\epsilon}} > 1 - n^{-n^{\frac{\epsilon}{2}}}$, there is at least one $val_{R_\epsilon}(a, b) = 1$ s.t, $b \in W_a$. So the empty set covers $min(\lambda^{R_\epsilon})$.

Case 2. $|G| < n^{2\epsilon}$

We apply Lemma 82 with D in the role of H, then we define a function

$$f(x) = \begin{cases} W_x\ x \in D_0 - G \\ \\ 0\ else \end{cases}$$

. Let $D' = D - set(R_\delta)$. Strictly speaking D' is not a random subset of D with uniform distribution since $|D' \cap D_0|$ is the same for all R_δ.

Fact 90. *There is a random assignment D'' s.t. with an uniform probability we choose D'' as the subsets of D with $4[n^\delta]$ elements and with high probability $D' \subseteq D''$.*

This implies that Lemma 82 holds for D' too. Let $V = \{y \in D' |$ there is $x \in D'$ s.t. $y \in f(x)\}$, then V covers the 1-disjunction Δ^{R_ϵ} and Lemma 82 implies that with high probability $|V| \leq w$.

□

Now we want to prove Theorem 89 for $k > 1$:

We prove if Δ is a k-disjunction then there is a k-disjunction E and a $k-1$-disjunction E' s.t. $\Delta^{R_\epsilon} \mathcal{L}(E \vee E')$ and $\Pi(E, w)$. Then applying the induction hypothesis to E' we get the wanted result:

Definition 91.

Let $\Delta = \bigvee_{x \in H} h(x)$ be a k-disjunction s.t. each $h(x)$ is an k'-map, $k' \leq k$ and $min(\Delta) = \bigvee_{x \in H'} h(x)$ for some $H' \subseteq H$,

then we define the k-disjunction $(\Delta)_k$,

if there is a set $H'' = \{x \in H' | map(h(x))$ is a k-map$\}$ and $(\Delta)_k = \bigvee_{x \in H''} h(x)$.

Definition 92.

Let P_k be a property of k-disjunctions,

then we define $(P)_k$,

if $P_k(\Delta, w)$ iff $P_k((\Delta)_k, w)$.

Definition 93. Let $\Delta = \bigvee_{x \in H} h(x)$ be a k-disjunction and $a \in D_0$, $b \in D_1$,

then $\Delta^{a,b}$ denotes a k-disjunction,

if there is a set $H' = \{x \in H | map(h(x))(a) = b\}$ and $\Delta^{a,b} = \bigvee_{x \in H'} h(x)$.

Claim 94. Let P_k be the property " for all $a \in D_0$, $b \in D_1$ $\Pi_k(\Delta^{a,b}, w)$" , then $\Omega_k \lhd (P)_k$.

Proof.

Let $a \in D_0$, $b \in D_1$ be fixed, $\Delta^{a,b} = \bigvee_{i \in H'} h(i)$. For each fixed $i \in H'$, $h(i)$ is a k'-map, $k' \leq k$. Let $h'(i)$ be the $k-1$-map that we get from $h(i)$ by deleting the term $x_{a,b}$. Let $E = \bigvee_{i \in H'} h(i)$ be a $k-1$-disjunction, then by induction hypothesis with high probability there is $k-1$-disjunction Δ' s.t. $\Delta^{R_\epsilon} \mathcal{L} \Delta'$ and a set with $w-1$ elements covers Δ'. That implies the Claim. □

Claim 95. $P_k \lhd (\Pi)_k$.

Proof.

We apply Lemma 83 with D in the roll of H and 2 as k. If $a \in D_0$, $b \in D_1$, then according to P_k there is V, $|V| \leq w$ s.t. V covers $\Delta^{a,b}$. We define the function f:

$$f(< a, b >) = \begin{cases} V & a \in D_0, b \in D_1 \\ 0 & else \end{cases}$$

As in the proof of Case 1 for $k = 1$, Lemma 83 holds for an D', $D' = D - set(R_\epsilon)$. Let $V = \{y \in D' |$ there are $a, b \in D'$ s.t $y \in f(< a, b >)\}$, then by the Lemma $P(|V| > t) < n^{-c_1 t + c_2}$, $c_1 > 0$, c_1, c_2 depend just on ϵ. V covers $(\Delta^{R_\epsilon})_k$:

Let $\Delta = \bigvee_{i \in H} h(i)$ and for each fixed $i \in H$ $map(h(i))(x) = y$. It is sufficient to prove that if $|dom(h(i)) - set(R_\epsilon)| = k$ then either $x \in V$ or $y \in V$ $k \geq 2$ implies there are $a, b \in D$, $a \neq x$ s.t. $map(h(i))(a) = b$. So V covers $\Delta^{a,b}$. □

Lemma 96.

For all $k, u \in \omega$ there are $\epsilon > 0, w \in \omega$ for all sufficiently large n,
if $|D_0| = n$, $|D_1| = n - 1$, $\Delta \in B$ is a k-disjunction and R_ϵ a random ϵ-partial assignment,
then with probability $\geq 1 - n^{-u}$ there is $V \subset D$ s.t. V covers $min(\Delta^{R_\epsilon})$ and $|V| \leq w$.

Proof. 96

Starting with an arbitrary k-disjunction Δ and $R_\epsilon =: R_{\epsilon(1)} \circ \cdots \circ R_{\epsilon(r)}$. We construct a sequence of k-disjunctions s.t. $\Delta = \Delta_1, \ldots, \Delta_r = min(\Delta^{R_\epsilon})$, $\Delta_j^{R_{\epsilon(j)}} \mathcal{L} \Delta_{j+1}$ for $0 \leq j \leq r-1$and r depending only on k, u. We construct this sequence in such a way that later k-disjunctions satisfy additional properties: If Δ_j is a k-disjunction and property $P_k(\Delta_j, w)$ holds for sufficiently large w (for all $w > w_0$, w depending just on k, u), then with a probability of at least $1 - n^{-u}$ we have $\Delta_j^{R_{\epsilon(j)}} \mathcal{L} \Delta_{j+1}$, where $\epsilon(j)$ depends just on k, u and Δ_{j+1} is k-disjunction with a property $P'_k(\Delta_{j+1}, w)$. This is sufficient as we know that Ω_k trivially holds for Δ and after r steps we reach $min(\Delta^{R_\epsilon})$ s.t Π_k holds for it with a high probability.

□

Theorem 97.

For all $k, d, u \in \omega, \delta > 0$ there are $\epsilon > 0, w, r \in \omega$ s.t. for all sufficiently large n,

if $|D_0| = n$, $|D_1| = n-1$, $\Phi \in B$, $|\Phi| \leq n^k$, $depth(\Phi) = d$, p *an one-to-one map of* $D_0' \subseteq D_0$ *into* D_1, $|D_0'| = n - n^\delta$ *and* $R_\epsilon^{(p)}$ *a* ϵ*-partial assignment,*
then with probability $\geq 1 - n^{-u}$ *there is a* w*-disjunction* Δ *and* $V \subset D$ *s.t.* V *covers* Δ, $|V| = w$ *and* $\Phi^{R_\epsilon^{(p)}} L_{w,r}\Delta$.

Remark 98. Δ being a k-disjunction is replaced by Φ being an arbitrary Boolean Formula with $|\Phi| \leq n^k$ and $depth(\Phi) = d$, because the size of a k-disjunction on n variables can't exceed $2n^{2k}$.

Fact 99. $\delta \geq \epsilon$, *because the* ϵ*-partial assignment* $R_\epsilon^{(p)}$ *defined on an subset of* D_0 *with* $n - n^\epsilon$ *extends the map* p *that is defined on a subset of* D_0 *with* $n - n^\delta$ *elements.*

Proof. 97
Let

$$K_k =: \{\Phi \in B || \Psi| \leq n^k\}$$

Definition 100. Define $U_{d,l}^k$ by induction:

(1) For each $l \in \omega$ let

$$U_{0,l}^k =: \{\Delta \in K_k | \Delta \text{ is a } l - disjunction\}$$

(2) Suppose $U_{d-1,l}^k$ is already defined,
then let

$$\begin{aligned} U_{d,l}^k \quad =: \quad & \{\Delta \in K_k | \Delta = \bigvee_{x \in H} h(x),\ h(x) \in U_{d-1,l}^k \text{ for all } x \in H\} \\ & \cup \{\Phi \in K_k | \Phi = \neg\Delta,\ \Delta \in U_{d-1,l}^k\} \end{aligned}$$

.

Fact 101. *If* $\Phi \in K_k$ *and* $depth(\Phi) \leq d$, *then by the Boolean identities there is a* $\Delta \in U_{2d,l}^k$ *and there are* $w, r \in \omega$ *depending only on* d *s.t* $\Phi L_{w,r}\Delta$.

Suppose $\Phi \in U_{1,l}^k$ if Φ is of he form $\bigvee h(x)$ we can transform it into a formula in $U_{0,l}^k$ then Lemma 96 can be applied.

Suppose that h is of the form $\neg\Phi$ and $\Phi \in U_{0,l}^k$, then by Lemma 96 we have a high probability that $\Phi^{R_\epsilon}\mathcal{L}\Delta$ s.t. Δ is a w-disjunction covered by a set V, $|V| = w$. Δ is w-equivalent to $c(h, V)$, so $\Phi^{R_\epsilon} L_{w,r+1} c(h, V)$.

□

3.2.5. *Proof of the truth Lemma.* Proof of Lemma 36

Proof. (36.2) According to the definition of $\mathcal{P}^{\leftrightarrow}$ the $q \in \mathcal{P}^{\leftrightarrow}$ are maps of M_n into M_{n-1}. We define two relations W_0 and W_1 $W_1(q, a_1, \ldots, a_j)$ will imply $q \Vdash R(a_1, \ldots, a_j)$ and $W_0(q, a_1, \ldots, a_j)$ will imply $q \Vdash \neg R(a_1, \ldots, a_{ij})$. For each fixed $a \in M_n^j$ let $\Gamma_a \in B$ be the Boolean formula defining the relation $R(a_1, \ldots, a_j)$. There is such a formula Γ_a because R is definable in $< \mathcal{M}, \rho >$ and ρ can be seen as an evaluation of the variables $x_{a,b}$, $a \in D_0$, $b \in D_1$. We may assume that for each Γ_a $depth(\Gamma_a) \leq d$, $|\Gamma_a| \leq n^k$, where $d, k \in \omega$ depend only on $|\Gamma_a|$ and not on a or n. We apply Theorem 97 with $u = j + 1$ for each Γ_a, then $\epsilon > 0$, w, r, $R_\epsilon^{(p)}$, V_a , $|V_a| = w$ is as in the Theorem (Since $u > j$ there is such an $R_\epsilon^{(p)}$). We define $p' =: map(R_\epsilon^{(p)})$ s.t. $val_{p'}$ satisfies the conclusion of 97 for all Γ_a simultaneously, W_1 iff "there is a $t \in \omega$ s.t $q \in \mathcal{P}^{\leftrightarrow}_{1/t}$ and $\Gamma^{val_q} L_{t,t} 1$" and W_0 iff "there is a $t \in \omega$ s.t. $q \in \mathcal{P}^{\leftrightarrow}_{1/t}$ and $\Gamma^{val_q} L_{t,t} 0$".

Fact 102. *W_0 and W_1 are ω-definable.*

Theorem 97 concludes: If $q \leq p'$, then W_1 is equivalent to the relation $q \Vdash R(a_1, \ldots, a_j)$.

Let $\delta > 0$, then by Theorem 97 the relation W_1, $q \leq_{\mathcal{P}^{\leftrightarrow}} p'$ restricted to $q \in \mathcal{P}^{\leftrightarrow}_\delta$ is equivalent to $q \in \mathcal{P}^{\leftrightarrow}_\epsilon$ and $\Gamma^{val_q} L_{w,r} 1$ w, r depending just on j and $|\Gamma|$. So $q \Vdash R(a_0, \ldots, a_j)$ is definable in $\mathcal{M}$ if $q \leq_{\mathcal{P}^{\leftrightarrow}} p'$ and $q \in \mathcal{P}^{\leftrightarrow}_\epsilon$.

(36.3) We take V_a for $U(a)$.

(36.1) Follows from 36.2.

□

Using this Lemma we can prove that induction up to n holds, we'll do this by showing first that any nonempty subset of the natural numbers definable in $< \mathcal{M}, \rho >$ with less than $log(n)$ is already definable in $\mathcal{M}$. As a last step we'll show that induction up to $log(n)$ in $< \mathcal{M}, \rho >$ implies induction up to n:

3.3. $< \mathcal{M}, \rho > \models IND_n$.

Lemma 103.

If G is a $\mathcal{P}^{\leftrightarrow}$-$\omega$-generic over $\mathcal{M}$, $\rho = \bigcup G$, R an unary relation on M_n definable in $< \mathcal{M}, \rho >$ and for all $a \in M_n$ $R(a) \to a \leq log(n)$,

then R is definable in $\mathcal{M}$ and therefore the induction principle for R holds up to $log(n)$ in $< \mathcal{M}, \rho >$.

Proof.

By Lemma 36 there exists a $p' \in \mathcal{P}^{\leftrightarrow}$ s.t. for all $a \leq log(n)$ there is an $U(a)$, $|U(a)| \leq w$ s.t. if $q \leq_{\mathcal{P}^{\leftrightarrow}} p'$, $U(a) \subseteq dom(q)$, $U(a) \cap M_{n-1} \subseteq ran(q)$ then either $q \Vdash R(a)$ or $q \Vdash \neg R(a)$ and U is definable in $\mathcal{M}$. Let $p' \in \mathcal{P}^{\leftrightarrow}_{\epsilon}$, $\epsilon > 0$. $|\bigcup_{a \leq log(n)} U(a)| \leq w\ log(n)$, $w \in \omega$. So the definition of our notion of forcing implies that $T = \{q' \in \mathcal{P}^{\leftrightarrow} | q' \leq_{\mathcal{P}^{\leftrightarrow}} p',\ \bigcup_{a \leq log(n)} U(a) \subseteq dom(q') \wedge \bigcup_{a \leq log(n)} (U(a) \cap M_{n-1}) \subseteq ran(q')\}$ is dense in $\mathcal{P}^{\leftrightarrow}$. So there is a $q \in G \cap T$. We may assume $q \in \mathcal{P}^{\leftrightarrow}_{\epsilon/2}$ for a fitting ϵ. Also by Lemma 36 we have either $q \Vdash R(a)$ or $q \Vdash \neg R(a)$ for all $a \leq log(n)$ and the relation $p \Vdash R(a)$ is definable on $\mathcal{P}^{\leftrightarrow}_{\epsilon/2}$ therefore R is definable in $\mathcal{M}$. □

Lemma 104.

If the induction principle up to $log(n)$ holds in $< \mathcal{M}, \rho >$, then also induction up to n holds.

Proof. By contradiction

Let $H \subseteq M_n$, $H \neq \emptyset$, definable in $< \mathcal{M}, \rho >$ s.t H has no smallest element. We show there is also a nonempty subset of $\{0, \ldots, [log(n)]\}$ without a smallest element.

We may assume that for all $x \in H$ if $x \leq y$ then also $y \in H$. Let $H' = \{x - y \in M_n | x \in H,\ y \in M_n,\ y \notin H\}$, then H' is a cut too.

Claim 105. If $w \in H'$ then $[w/2] \in H'$.

Proof. If $w = x - y$, $x \in H$, $y \notin H$ then let $z = y + [w/2]$.

Case 1. If $z \in H$, then clearly $[w/2] \in H'$.

Case 2. If $z \notin H$, then $x - z \in H'$. Since $x - z$ may differ from w at most by one, $[w/2] \in H'$.

Let $H'' = \{x | 2^x \in H'\}$. Then H'' is definable in $< \mathcal{M}, \rho >$. Because H' is closed under division by 2, H'' has no smallest element and for each $x \in H''$, $x \leq log(n)$. That gives the desired contradiction.

□

□

4. The nontrivial Hierarchy

Later Ajtai used the same ideas in his search for further tautologies whose proofs are even more difficult than that of PHP. $PHP\Delta_0$ will be the axiom system that we obtain if we add to $I\Delta_0$ the axiom scheme $\forall n\ PHP_n$. These other tautologies arise in a natural way if we understand the Pigeonhole Principle as another formulation of the Parity Principle PAR, where the Parity Principle for n, PAR_n, states that the set $2n+1 = \{0, \ldots, 2n\}$ has no partition into subsets with exactly two elements. Clearly PAR implies PHP_n if we state it in the form that there is no one-to-one map of $\{0, \ldots, n-1\}$ onto $\{0, \ldots, n-2\}$. The other direction, that PAR_n cannot be proven relative to $PHP\Delta_0$ has one difficulty that did not arise in the last section. While in the last section one could use the nice property of induction that induction up to n implies induction up to n^c for any fixed c, no such property is known from PHP_n. As a consequence we have to prove that PAR_n cannot be proven even when assuming PHP_{n^c}. So the first part of this proof will essentially be the same as in the last, whereby we construct a new model by forcing where PAR_n holds in a natural way. The second part, showing that PAR_n cannot be proven from PHP_{n^c}, however must be reduced to a completely different combinatorial question.

Definition 106.

Let $c, i \in \omega$, $(p_1, \ldots, p_c)$, $(h_1, \ldots, h_c)$, $(y_1, \ldots, y_i)$ and $\phi((p_1, \ldots, p_c),(h_1, \ldots, h_c),$ $(y_1, \ldots, y_i))$ a 1st-order formula of the language L', written in the form $(h_1, \ldots, h_c) =$

$f^{(y_1,\ldots,y_i)}(p_1,\ldots,p_c)$, then

$$\begin{aligned} PHP^{\phi,c} \equiv\ & \forall(y_1,\ldots,y_i) \\ & (\forall(p_1,\ldots,p_c)\exists!(h_1,\ldots,h_c)\ (h_1,\ldots,h_c) = f^{(y_1,\ldots,y_i)}(p_1,\ldots,p_c)) \\ & \rightarrow ((\exists(h_1,\ldots,h_c)\forall(p_1,\ldots,p_c)\neg(h_1,\ldots,h_c) = f^{(y_1,\ldots,y_i)}(p_1,\ldots,p_c)) \\ & \rightarrow (\exists(p_1,\ldots,p_c),(p'_1,\ldots,p'_c)\ (p_1,\ldots,p_c) \neq (p'_1,\ldots,p'_c) \\ & \wedge f^{(y_1,\ldots,y_i)}(p_1,\ldots,p_c) = f^{(y_1,\ldots,y_i)}(p'_1,\ldots,p'_c))) \end{aligned}$$

is the Pigeonhole Principle with parameters ϕ, c.

Definition 107.

"$\exists x, y(\forall z\ z < x) \rightarrow x + 1 = 2y + 1$",

then "the cardinality of the universe is odd".

Definition 108. Let R be a binary relation and $\phi \equiv$ "if the cardinality of the universe is odd, then R is not a partition of the universe into subsets with two elements" of the language L',

then ϕ is the Parity Principle for R.

Theorem 109.

Let T be a theory of the language L that describes a large initial segment of Peano Arithmetic ,

then

$$T + \forall\phi, c\ PHP^{\phi,c} + \neg\ \text{"the Parity Principle for } R\text{"}$$

is consistent in L'.

Theorem 110.

Let $\mathcal{M}$ be a model of Peano Arithmetic, $n \in M$ odd, nonstandard, $i \in \omega$ and $A \subseteq M_n^i$ an i-ary relation definable in $\mathcal{M}$,

there is a partition R of n into subsets of size 2 s.t. $< M_n, A, R > \models PHP^{\phi,c}$.

Definition 111. (partition)

We consider partitions as the set of their classes, so e.g. $p' \subseteq p$ means each class of p' is a class of p

Definition 112. (2-partition)

If S is a set and p is a partition of S,

then we call p a 2-partition,

iff every class of p contains exactly two elements.

Definition 113.

Let p be a 2-partition of some $S' \subset S$,

then p is a partial 2-partition for S.

Definition 114.

Let p, p' be (partial) 2-partitions and $p \subseteq p'$,

then p and p' are compatible,

if every class of p is either in p' or disjoint from every class of p'.

Definition 115. (cover)

Let p be a (partial) 2-partition of S and $V \subseteq S$,

then V covers p,

iff every class of p contains at least one element of V (for all $(x, y) \in p \Rightarrow x \in V \vee y \in V$).

Remark 116. The definition of a cover of a 2-partition is very similar to the definition of the cover of a k-map.

Definition 117. (inside)

Let p be a (partial) 2-partition of S and $V \subseteq S$,

then V is inside p,

iff $V \subseteq \bigcup p$.

Definition 118. (support)

Let p be a (partial) 2-partition of S and $V \subseteq S$,

V supports p,

iff V is inside p and covers p.

4.1. **Forcing $< \mathcal{M}, \sigma > \models \neg PAR_n$.**

Definition 119.

Let $\epsilon > 0$ and $H_\epsilon = \{p \in M | p$ is a partial 2-partition of $M_n \wedge \mathcal{M} \models |\bigcup p| \leq$

$(n - n^{\epsilon})\}$, $\mathcal{P}^{\equiv} = \bigcup_{1/t}\{H_{1/t} | t \in \omega\}$ and $q \leq_{\mathcal{P}^{\equiv}} p$ iff $q \supseteq p$,
then $< \mathcal{P}^{\equiv}, \leq_{\mathcal{P}^{\equiv}} >$ is an $\mathcal{M}$-ω-definable notion of forcing.

Fact 120.

the following holds:

(1) each $p \in \mathcal{P}^{\equiv}$ is definable in $\mathcal{M}$, because every definable relation on M_n is an element of M.

(2) $\mathcal{P}^{\equiv}$ is not definable in $\mathcal{M}$, because $\mathcal{P}^{\equiv}$ has no minimal elements.

(3) $\mathcal{P}^{\equiv}$ is ω-definable in $\mathcal{M}$, because for every $p \in \mathcal{P}^{\equiv}$ follows there is a $t \in \omega$, $p \in \mathcal{P}_{1/t}$.

(4) $\mathcal{P}^{\equiv}$ has a greatest element $1_{\mathcal{P}^{\equiv}}$, that is the empty relation.

(5) For each fixed $x \in M_n$, $D_x = \{p \in \mathcal{P}^{\equiv} | x \in \bigcup p\}$ is dense in $\mathcal{P}^{\equiv}$ and ω-definable in $\mathcal{M}$: D_x has no minimal elements; for all $p \in D_x$ follows there is $t \in \omega$, $p \in \mathcal{P}^{\equiv}_{1/t}$.

Lemma 121.

Let G be $\mathcal{P}^{\equiv}$-ω-generic over $\mathcal{M}$ and $\sigma := \bigcup G$, then σ is a 2-partition of M_n.

(1) σ is a partial 2-partition of M_n:
for all $p, q \in G$ p, q are compatible partial 2-partitions of M_n.

(2) for all $x \in M_n$ $\bigcup \sigma = M_n$:
for each fixed $x \in M_n$ D_x is dense in $\mathcal{P}^{\equiv}$ and ω-definable in $\mathcal{M}$ and so by definition of genericity of $D_x \cap G \neq \emptyset$.

Corollary 122. *If $\tau'(R) = \sigma$, then $< \mathcal{M}, \sigma > \models \neg PAR$*

4.2. **The truth Lemma revised.**

Lemma 123.

Let $ij \in \omega$, $G \subseteq \mathcal{P}^{\equiv}$ $\mathcal{P}^{\equiv}$-generic, $\sigma := \bigcup G$ and $R \subseteq M_n^{ij}$ s.t. R is definable in $< \mathcal{M}, \sigma >$,

then the following holds:

(1) for all $a_1, \ldots, a_j \in M_n$ there is a $p \in G$ s.t. $p \Vdash R(a_1, \ldots, a_j)$ or $p \Vdash \neg R(a_1, \ldots, a_j)$

(2) the relation $q \Vdash R(a_1, \ldots, a_{ij})$, $q \in \mathcal{P}^{\equiv}, a_0, \ldots, a_j \in M_n$ is definable in $\mathcal{M}$.

(3) for all $p \in \mathcal{P}^{\equiv}$ there are $p' \in \mathcal{P}^{\equiv}$, $p' \leq_{\mathcal{P}^{\equiv}} p$, $w \in \omega$ and a function $U : M_n^j \to M_n$ that is definable in $\mathcal{M}$ s.t. for all $a_1, \ldots, a_j \in M_n$ $U(a_1, \ldots, a_j) \subseteq M_n, |U(a_1, \ldots, a_j)| = w$ s.t. if all 2-partitions p'' of M_n are compatible to p' and supported by $U(a_1, \ldots, a_j)$,
then either $p' \cup p'' \Vdash R(a_1, \ldots, a_j)$ or $p' \cup p'' \Vdash \neg R(a_1, \ldots, a_j)$.

(4) if $j = 2c$ and for all $x \in M_n^c$, there is exactly one $y \in M_n^c$ s.t. $R(x_1, \ldots, x_c, y_1, \ldots, y_c)$ is a function (That is $y = Y(x)$ iff $R(x_1, \ldots, x_c, y_1, \ldots, y_c)$) definable in $< \mathcal{M}, \sigma >$), then $U(x_1, \ldots, x_c, y_1, \ldots, y_c)$ can be chosen s.t. for all $x, y, y' \in M_n^c$ $U(x_1, \ldots, x_c, y_1, \ldots, y_c) = U(x_1, \ldots, x_c, y_1', \ldots, y_c')$.

Fact 124. *$U(a_1, \ldots, a_{ij}) \subseteq M_n - \bigcup p'$, because those classes of p'' that contain at least one element from $\bigcup p'$ coincide with the corresponding classes of p'*

Definition 125. Let D be an arbitrary set s.t. $|D| = n < \omega$,
then define another set of Boolean variables indexed by D: $X_D =: \{x_{a,b} |$ for all $a, b \in D$, $a \neq b\}$.

Remark 126. In the following we just consider $\mathcal{B}_D =: \{\kappa \in \mathcal{B} |$ for all $x_{a,b} \in \kappa$ it follows that $x_{a,b} \in X_D\}$.

Notation 127. From here on we will denote $\mathcal{B}_D$ as B and X_D as X for simplicity.

Definition 128. Let D be a finite set, $x_{a,b} \in X$ a Boolean variable,
then define a Boolean evaluation $e_{\equiv} : X_D \to \{0, 1\}$ by:
$e_{\equiv}(x_{a,b}) = 1$ iff $(a, b) \in \sigma$.

Definition 129. (k-collection):
$K \in B$ is called a k-collection,
if there is a 2-partition p of $D(K) \subset D$ s.t. $\kappa = \bigwedge_{\{a,b\} \in p} x_{a,b}$, $|D_0(K)| = 2k$.

Definition 130.
Let $a \in D$,
then define

$$F_a' \equiv: (\bigvee_{b \in D, a \neq b} x_{a,b}) \wedge (\bigwedge_{b,b' \in D, a \neq b, a \neq b'} x_{a,b} \to \neg x_{a,b'})$$

and

$$O_D \equiv: \bigwedge_{a,b\in D, a\neq b} (x_{a,b} \leftrightarrow x_{b,a}) \wedge \bigwedge_{a\in D} F'_a$$

Fact 131.

If there is a $0,1$*-assignment for* $x_{a,b}$ *s.t* $O_D = 1$,

then we define a 2*-partition* σ *of* D *defined by* $(a,b) \in \sigma$ *iff* $x_{a,b} = 1$.

If $|D| \neq 2c$ *for* $c \in \omega$,

then the equation $O_D = 1$ *has no solution.*

Definition 132. Let $\epsilon > 0$, p a 2-partition of $D^\epsilon \subseteq D$, $Q_\epsilon : X \to \{0,1\}$,

then $Q\epsilon$ is an $\epsilon-$partial assignment (on D^ϵ),

if the following holds:

(1) $2[(n-n^\epsilon)/2] = |D^\epsilon|$

(2) $Q_\epsilon(x_{a,b}) = 0$ or $Q_\epsilon(x_{a,b}) = 1$ iff $(a \in D^\epsilon$ or $b \in D^\epsilon)$

(3) $Q_\epsilon(x_{a,b}) = 1$ iff $(a,b) \in p$.

Notation 133. $part(Q_\epsilon) =: p$, $val_p =: Q_\epsilon$ and $set(Q_\epsilon) =: D$.

Remark 134. The following two statements are essetially the same as Lemma 96 and Theorem 97 but in the context of partial 2-partitions.

Lemma 135.

For all $k,d,u \in \omega$ *there are* $\epsilon > 0, w, r \in \omega$ *s.t. for all sufficiently large* n,

if $|D| = n$, $\Phi \in B$, $|\Phi| \leq n^k$, $depth(\Phi) = d$ *and* R_ϵ *is an* ϵ*-partial assignment,*

then with probability $\geq 1 - n^{-u}$ *there is a* w*-disjunction* Δ *and a set* $V \subset D$ *s.t.* V *covers* Δ, $|V| = w$ *and* $\Phi^{R_\epsilon} L_{w,r}\Delta$.

Theorem 136.

For all $k,d,u \in \omega, \delta > 0$ *there are* $\epsilon > 0, w, r \in \omega$ *s.t. for all sufficiently large* n,

if $|D| = n$, $\Phi \in B$, $|\Phi| \leq n^k$, $depth(\Phi) = d$, $p \in \mathcal{P}^{\equiv}$ *a partial* 2*-partition of* D^ϵ,

$|p| \leq n - n^\delta$ *and* $R_\epsilon^{(p)}$ *is an* ϵ*-partial assignment,*

then with probability $\geq 1 - n^{-u}$ *there is a* w*-disjunction* Δ *and a set* $V \subset D$ *s.t.* V *covers* Δ, $|V| = w$ *and* $\Phi^{R_\epsilon^{(p)}} L_{w,r}\Delta$.

Proof. of 123

According to the definition of $\mathcal{P}^{\equiv}$ the $q \in \mathcal{P}^{\equiv}$ are (partial) 2-partitions of M_n . We

define two relations W_0 and W_1, $W_1(q, a_1, \ldots, a_j)$ will imply $q \Vdash R(a_1, \ldots, a_j)$ and $W_0(q, a_1, \ldots, a_j)$ will imply $q \Vdash \neg R(a_1, \ldots, a_j)$:

For each fixed $a \in M_n^j$ let $\Gamma_a \in B$ be the Boolean formula defining the relation $R(a_1, \ldots, a_j)$. There is such a formula Γ_a because R is definable in $< \mathcal{M}, \sigma >$ and σ can be seen as an evaluation of the variables $x_{a,b}$, $a, b \in D$. We may assume that for each Γ_a $depth(\Gamma_a) \leq d$, $|\Gamma_a| \leq n^k$, where $d, k \in \omega$ depend only on $|\Gamma_a|$ and not on a or n. We apply Theorem 136 with $u = j+1$ for each Γ_a, then $\epsilon > 0$, w, r, $R_\epsilon^{(p)}$, V_a , $|V_a| = w$ is as in the Theorem (Since $u > j$ there is such an $R_\epsilon^{(p)}$). We define $p' =: map(R_\epsilon^{(p)})$ s.t. $val_{p'}$satisfies the conclusion of 136 for all Γ_a simultaneously, W_1 iff "there is a $t \in \omega$ s.t $q \in \mathcal{P}^{\equiv}_{1/t}$ and $\Gamma^{val_q} L_{t,t} 1$" and W_0 iff "there is a $t \in \omega$ s.t. $q \in \mathcal{P}^{\equiv}_{1/t}$ and $\Gamma^{val_q} L_{t,t} 0$".

(1) Theorem 136 implies that $D' = \{p \in \mathcal{P}^{\equiv} | \exists w, r \in \omega$ s.t $\Gamma^{val_p} L_{w,r} 1 \vee \Gamma^{val_p} L_{w,r} 0\}$ is dense in $\mathcal{P}^{\equiv}$ and $D' \in M$. Therefore there is a $q \in D' \cap G$ and $q \Vdash R(a_1, \ldots, a_j)$ or $q \Vdash \neg R(a_1, \ldots, a_j)$.

(2) Let $\delta > 0$, then by Theorem 123.1 for some $q \leq_{\mathcal{P}^{\equiv}} p'$ restricted to $q \in \mathcal{P}^{\equiv}_\delta$ we get $w, r \in \omega$ s.t. $\Gamma^{val_q} L_{w,r} 1 \vee \Gamma^{val_q} L_{w,r} 0$ and $q \Vdash R(a_1, \ldots, a_j)$ iff $q \in \mathcal{P}^{\equiv}_\epsilon$ s.t. $\Gamma^{val_q} L_{w,r} 1$. So the relation $q \Vdash R(a_1, \ldots, a_j)$ is definable in $< \mathcal{M}, \sigma >$ if $q \leq p'$ and $p \in \mathcal{P}^{\equiv}_\epsilon$.

(3) $D' = \{p \in \mathcal{P}^{\equiv} | \exists w, r \in \omega$ s.t $\forall w$-disjunctions Δ_a, $V_a \subseteq D$, $|V_a| = w$, V_a covers Δ_a and $\Gamma^{R_\epsilon^{(p)}} L_{w,r} \Delta_a\}$. If for some w, r there are Δ_a, V_a, then they are definable in $\mathcal{M}$, so D' is definable in $\mathcal{M}$. As a consequence we only have to show that D' is dense in $\mathcal{P}^{\equiv}$. Since there are only n^j different a's this is a consequence of 136.

(4) Let $Y_k(a)$ be the k-th bit of the binary code of the number $Y(a)$. Apply 3 to the relation $Y_k(a) = 1$ for $k = 1, \ldots, log(c)$. Theorem 136 implies that there is a single $p' \leq_{\mathcal{P}^{\equiv}} p$ s.t. for each k there is a function V_k. Let $V'(a_1, \ldots, a_j) = \bigcup_{k \leq log(c)} V_k(a_1, \ldots, a_j)$, then V' satisfies the needed properties for U of statement 3 of the Lemma, except $|V'(a_1, \ldots, a_j)| \leq w$. We pick $q \leq_{\mathcal{P}^{\equiv}} p'$, $q \in \mathcal{P}^{\equiv}$ s.t. for all $a_1, \ldots, a_j \in M_n$ we get $|V'(a_1, \ldots, a_j) - \bigcup q| \leq w$ simultaneously. $q \to p'$, $V' \to U$ satisfy all the requirements of statement 3.

□

4.3. $< \mathcal{M}, \sigma > \models PHP$. Suppose $< \mathcal{M}, \sigma > \models \neg PHP$, then there is a $c \in \omega$ and an one-to-one map ρ of M_n^c into $M_n^c - (\overbrace{0, \ldots, 0}^{c\times})$ s.t $< \mathcal{M}, \sigma > \models \rho$.

Remark 137. From now on ρ will serve as the function Y in Lemma 123.4.

Let $p' \in \mathcal{P}^{\equiv}$ and U^{ρ} as in the Lemma 123.4. Let ρ^{-1} be the inverse of ρ, not necessarily defined on all $a \in M_n^c$. We may suppose that $p' \Vdash \rho$ is a one-to-one map of M_n^c into $M_n^c - (0, \ldots, 0)$ and ρ^{-1} is the inverse of ρ.

Let $p^{\rho^{-1}} \in \mathcal{P}^{\equiv}$ and $U^{\rho^{-1}}$ be the function corresponding to ρ^{-1} as defined in 123.4 and $\mu(a) = U^{\rho}(a) \cup U^{\rho^{-1}}(a)$, for all $a \in M_n^c$.

Remark 138. We may suppose that $|\mu(a)| = |\mu(a')| \in \omega$ for all $a, a' \in M_n^c$ and $p' = p^{\rho^{-1}}$. Because of the Fakt 124 we may also assume that $\mu(a) \subseteq M_n - \bigcup p'$ and that $\mathcal{M} \models m = n - \bigcup p'$, as a consequence we can identify m and $n - \bigcup p'$. T will be the set of w-tuples formed from the elements of m. We'll also identify n^c and M_n^c, because $|M_n^c| = n^c$. Suppose ρ maps n^c into $n^c - \{0\}$.

Since the function μ and the relation $\Vdash$ are definable in $\mathcal{M}$ there exist functions f, g definable in $\mathcal{M}$ s.t. the following holds:
Let $a \in M_n^c$ and p any partial 2-partition supported by $\mu(a)$ compatible to p', then

(1) $p \cup p' \Vdash \rho(a) = f(a, p)$

(2) if $g(a, p)$ is defined then $p \cup p' \Vdash \rho^{-1}(a) = g(a, p)$ and
if $g(a, p)$ is not defined then $p \cup p' \Vdash$ "$\rho^{-1}$is not defined".

Proposition 139. *some properties of* μ, f, g*:*

(1) $\mu : n^c \to T$.

(2) $dom(f) = \{(a, p) | a \in n^c \wedge p$ is a partial 2-partition of $m \wedge \mu(a)$ supports $p\}$.

(3) $dom(g) \subseteq \{(a, p) | a \in n^c \wedge p$ is a partial 2-partition of $m \wedge \mu(a)$ supports $p\}$.
The following conditions hold for all x, y, p, q where $x, y \in n^c$, p, q compatible, partial 2-partitions of m, $\mu(x)$ supports p and $\mu(y)$ support q, respectively.

(4) $f(x, p) \in n^c$, $f(x, p) \neq 0$, because $ran(\rho) = n^c - \{0\}$.

(5) If $g(x,p)$ is defined, then $g(x,p) \in n^c$, because $ran(\rho^{-1}) = n^c$.

(6) If $x \neq y \in n^c$, then $f(x,p) \neq f(y,q)$, because ρ is an one-to-one function and p, q are compatible.

(7) $y = f(x,p)$ iff ($g(y,q)$ is defined and $x = g(y,q)$), because p, q are compatible and by Lemma 123.4 we get $y \in n^c$ s.t. $p \cup q \cup p' \Vdash y = \rho(x)$.

Definition 140.

Let $w, n^c, m \in \omega$,

then $W_0(w, n^c, m)$ hold,

if there are functions μ, f, g s.t. 1-7 hold.

Definition 141.

Let $U, V \in T$ and p a partial 2-partition,

then p is a position over U, V,

iff each class of p contains at least one element from U and V.

Definition 142.

Let $U, V \in T$ and $p \subseteq p'$ partial 2-partitions,

then p' is based on p over U, V,

iff each class of p' that contains at least one element from U and V is also a class of p.

Definition 143.

Let $U \in T$, p be a 2-partition of m and U inside p,

then p_U is a minimal partial 2-partition of m that is compatible to p and covered by U.

Fact 144. *p_U is unique for U, because U has to be inside p_U and has to cover p_U.*

Lemma 145. *(M0)*

If $< \mathcal{M}, \sigma > \models \neg PHP_{n^c}$,

then there is a $w \in \omega$ *and* $n^c, m \in M$ *s.t.* $M \models W_0(w, n^c, m)$.

Lemma 146. *(M1)*

For all $w \in \omega$ *if* $m \in \omega$ *is sufficiently large and* $n^c \in \omega$,

then $PA \vdash \neg W_0(w, n^c, m)$.

Proof. *Case* 1. m is even:

Suppose that contrary to our assertion there are $w, n^c \in \omega$ s.t. $W_0(w, n^c, m)$ holds for infinitely many even m's. Let us fix such a $m > 4w$. Let p be a 2-partition of m. For all $\mu(x) \in T$ let $p_{\mu(x)}$ be the unique partial 2-partition of m that is compatible to p and supported by $\mu(x)$. Now we define a function h on n^c by $h(x) = f(x, p_{\mu(x)})$. h contradicts the Pigeonhole principle, because h is one-to-one by by Fact 139.5 but maps n^c into $n^c - \{0\}$.

□

For W_0 to hold we required that $f(x,p)$ is defined if p is just supported by $\mu(x) \in T$. Now we want $f(x,p)$ to be defined even for any p s.t. a $U \in T$ is inside p. In the same way we define $g(x,p)$.

Lemma 147.

Let $W_0(w, n^c, m)$ hold for $m > 4w$, $U, V \in T$, p is a position over U, V and p', p'' are 2-partitions of m s.t. they are based on p over U, V and U is inside p' and p'', then

(1) *for all $x, y \in n^c$ s.t. $\mu(x) = U$, $\mu(y) = V$ follows: $y = f(x, p')$ iff $y = f(x, p'')$*

(2) *for all $x, y \in n^c$ s.t. $\mu(x) = U$,$\mu(y) = V$ follows: ($g(x, p')$ is defined and $y = g(x, p')$) iff ($g(x, p'')$ is defined and $y = g(x, p'')$).*

Proof. (1)

We may suppose that V is also inside p' and p'', because else we may extend p' and p'' without changing the values of f and g. Let x, y be given as required, $y = f(x, p')$ and p'_U, p''_U the unique minimal subsets of p' and p'' respectively supported by U. p'_V, p''_V are defined alike.

Case 1. p'_U and p''_V are compatible:

Then by 139.4 $y = f(x, p'_U)$ implies $x = g(y, p''_V)$ and because p''_U and p''_V are compatible too F4 also implies that from $x = g(y, p''_V)$ follows $y = f(x, p'')$.

Case 2. p'_U and p''_V are incompatible:

We want to construct a p''' from p'_U s.t. p'''_U and p''_V are compatible and s.t for all x, y as required $y = f(x, p')$ iff $y = f(x, p''')$, so we can apply the first case.

The classes of p'_U that are incompatible to p''_V cannot be covered by V, since p' and p'' are both based on p over U, V and so these classes would already be classes of p.

These incompatible classes are also incompatible to p'_V, else they would be supported by V and as well covered by V.

We replace these classes of p'_U with new ones to get p''' s.t.:

- each new class contains exactly one element from U.
- each element of U is contained in a class of p'''.
- the set of elements not in U but contained in a new class is disjoint from $\bigcup p'_V$ and $\bigcup p''_V$.

Remark 148. This can be done, because $m > 4k$, Fact 124 and Remark 138.

The definition of the replacement implies that p''' is supported by U and compatible to p'_V and p''_V. For all x, y as required $y = f(x, p')$ iff $y = f(x, p'_V)$ trivially holds and with p''' compatible to p'_V and 1394 also $y = f(x, p'_V)$ iff $y = f(x, p''')$ holds.

□

Definition 149.

Let p' be a partial 2-partitions and $U, V \in T$,

then $p_{U,V,p'}$ is the unique position over U, V,

if p' is based on p over U, V and U is inside p'.

Remark 150. We have shown that the truth value of the relations $y = f(x, p)$ and $x = g(y, p)$ s.t. $\mu(x) = U$, $\mu(y) = V$ is constant for all 2-partitions p' based on $p_{U,V,p'}$ over U, V where U is inside p'.

Now we define a function that gives for all $U, V \in T$ and positions p over U, V the number of pairs $< x, y >$ s.t. $y = f(x, p')$ is true for a p' based on p over U, V. In a similar way we define a counting function for the number of defined and true $x = g(y, p')$ relations.

Definition 151. Let $W_0(w, n^c, m)$ hold, $m > 4w$, $U, V \in T$ and p a position over U, V,

then

- $d(U, V, p)$ is the number of all pairs $x, y \in n^c$ s.t $\mu(x) = U$, $\mu(y) = V$ and for any 2-partition p' based on p over U, V, U inside p' follows: $y = f(x, p')$.
- $e(U, V, p)$ is the number of all pairs $x, y \in n^c$ s.t. $\mu(x) = U$, $\mu(y) = V$ and for any 2-partition p' based on p over U, V, U inside p' follows: $g(x, p')$ is defined and $y = g(x, p')$.

Definition 152.

Let $U \in T$ and p' a partial 2-partition of m supported by U,

then

$$r(U, p) = \sum_{V \in T} (d(U, V, p_{U,V,p'}) - e(U, V, p_{U,V,p'}))$$

Lemma 153.

Let $W_0(w, n^c, m)$ hold, $m > 4w$,

then the following holds:

(1) *If $U, V \in T$ and p is a position over U, V, then $d(U, V, p) = e(U, V, p)$.*

(2) *If $U \in T$ and p' is a partial 2-partition supported by U, then $r(U, p') \geq 0$.*

(3) *If there is an $U_0 \in T$, then for all partial 2-partitions p' that are supported by U_0, follows $r(U_0, p') > 0$.*

Proof. (1)

Let p', p'' be two compatible, partial 2-partitions of m, based on p over U, V and supported by U respectively V. $m > 4w$ implies that such p', p'' exists. The Lemma is a direct consequence of the definitions and 1394.

(2) Let $\mu(x) = U$, then $f(x, p')$ is defined and $y = f(x, p')$. The pair (x, y) occurs just in the $d(U, V, p_{U,V,p'})$ defined by $V = \mu(y)$. Then $\Sigma_{V \in T} d(U, V, p_{U,V,p'})$ equals to the number of $x \in n$ s.t $\mu(x) = U$. The same argument works for $e(U, V, p_{U,V,p'})$ except $g(y, p')$ may not be defined for some y, the consequence: $\Sigma_{V \in T} e(U, V, p_{U,V,p'}) \leq \Sigma_{V \in T} d(U, V, p_{U,V,p'})$.

(3) This is a special case of 2 where $U_0 = \mu(0)$ □

Definition 154.

Let $m, w \in \omega$, $m > 4w$ be fixed we define:

- Let $\Delta =: \{(U, V, p) | U, V \in T$ and p is a position over $U, V\}$.
- For all $(U, V, p) \in \Delta$ we define a variable $x_{(U,V,p)}$.
- Let $\Gamma =: \{(U, p) | U \in T$ and p is a partial 2-partition of m supported by $U\}$
- For all $(U, p') \in \Gamma$ we define the inequity $L_{(U,p')}$:

$$\Sigma_{V \in T}(x_{(U,V,p_{U,V,p'})} - x_{(V,U,p_{V,U,p'})}) \geq 0$$

- For all $w, m \in \omega, (U, p') \in \Gamma$ we define the system $L^{w,m}$ consisting of all the $L_{(U,p')}$.

Remark 155. We search for solutions to such a system of inequities over the field of real numbers s.t. at least one sum is strictly bigger than 0.

Definition 156. (*proper solution*)

Let $L^{w,m}$ be as above and $x_{(U,V,p)}$ a solution of the system,

then we call $x_{(U,V,p)}$ a solution proper,

if there is at least one $L_{(U,p')} > 0$.

Lemma 157.

If $w, n^c, m \in \omega$, $m > 4w$ and $W_0(w, n^c, m)$ holds,

then $L^{w,m}$ has the proper solution $x_{(U,V,p)} = d(U, V, p)$,

if $(U, V, p) \in \Delta$.

Proof.

This Lemma is a consequence of Lemma 153 □

Lemma 158.

If $w, m \in \omega$, m is even and p is a 2-partition of m

then the following holds:

(1) $\Sigma_{U \in T} L_{(U,p'_U)} = 0$

(2) $L^{w,m}$ has no proper solution in the field of real numbers.

Proof. (1)

Let p be a 2-partition of m. If we consider all the unequations $L_{(U,p'_U)}$ for $U \in T$, then a fixed $x_{(U_o,V_0,p_{U_o,V_o,q_o})}$ occur exactly twice:

- In the unequation $L_{(U_o,q_{U_0})} = \Sigma_{V \in T}(x_{(U_0,V,p_{U_0,V,q_{U_0}})} - x_{(V,U_0,p_{V,U_0,q_V})})$ where $V = V_0$ and
- In the unequation $L_{(V_0,q_{V_0})} = \Sigma_{U \in T}(x_{(V_0,U,p_{V_0,U,q_{v_0}})} - x_{(U,V_0,p_{U,V_0,q_U})})$ where $U = U_0$.

Therefore the sum on the left hand side is 0.

(1→2):

The first clause of the Lemma states that no $L_{(U,p'_U)}$ can be positive, hence $L^{w,m}$ can't have a proper solution. □

Definition 159. Let $Part(\omega)$ be the set of finite partial 2-partitions of ω.

Let $SP(\omega)_w =: [\omega]^w \cup Part(\omega)$.

Let $Seq(SP)_{w,i}$ be the set of sequences from $SP(\omega)_w$of length i.

Fact 160. *If λ is an one-to-one map of ω into ω, then it induces in a natural way a one-to-one map on $[\omega]^w$ for fixed w and on $Part(\omega)$ and therefore on $SP(\omega)_w$ and on $Seq(SP)_{w,i}$ for w, i fixed.*

Notation 161. If $A, B \in Seq(SP)_{w,i}$,

then we say A and B are isomorphic ($A \cong B$),

if there is an one-to-one map $\lambda : \omega$ onto ω s.t. $\lambda(A) = \lambda(B)$.

Definition 162. If $A \in Seq(SP)_{w,i}$ for some $w, i \in \omega$,

then let $type(A) =: \{B |\ B \in Seq(SP)_{w,i}$ and $A \cong B\}$. We say that $type(A)$ is the isomorphism type of A.

If $S \subseteq Seq(SP)_{w,i}$ for some $w, i \in \omega$,

then $Type(S) =: \{type(A) |\ A \in S\}$.

Definition 163. For all $(U, p') \in \Gamma$ we define an inequity $J_{(U,p')}$ from $L_{(U,p')}$ by replacing all $x_{(U,V,p)}$ for $(U, V, p) \in \Delta$ with a variable $y_{type((U,V,p))}$where $type((U, V, p)) \in Type(\Delta)$:

$$\Sigma_{V \in T} y_{type((U,V,p_{U,V,p'}))} - y_{type((V,U,p_{V,U,p'}))} \geq 0$$

.

Remark 164. If $(V,q),(V',q') \in type((U,p'))$, then the inequalities $J_{(V,q)}$ and $J_{(V',q')}$ are identical.

Notation 165. By $J_{type((U,p'))}$ we'll denote the inequity $J_{(V,q)}$ s.t. (V,q) is an arbitrary element of $type((U,p'))$.

Definition 166. For all $w,m \in \omega$ and $(U,p') \in \Gamma$, we define the system $J^{w,m}$ consisting of all the $J_{type((U,p'))}$.

Remark 167. For a fixed $w \in \omega$ $Type(\Delta)$ and $Type(\Gamma)$ do not depend on m if $m > 4w$, as a consequence the systems $J^{w,m}$ share the same set of variables and have the same number of equations. The coefficients of the variables of the equations $J_{type((U,p'))}$, however depend on the specific choice of m; namely:

The coefficient of $y_{type((U,V,p))}$ is a polynomial of m whose degree and coefficients may only depend on $w, type((U,p'))$ and $type((U,V,p))$.

Lemma 168.

(1) For each $w \in \omega, \delta =: type((U,V,p)) \in Type(\Delta)$ there is a polynomial $f_{w,\delta,\gamma}(m)$ with rational coefficients s.t. for any $m > 4w$ and $\gamma =: type((U,p')) \in Type(\Gamma)$ the inequity $J_{type((U,p'))}$ equals to:

$$\Sigma_{V \in T} f_{w,\delta,\gamma}(m) y_\delta \geq 0$$

.

(2) For each $w \in \omega, \gamma =: type((U,p')) \in Type(\Gamma)$ there is a polynomial $f_\gamma(m)$ with rational coefficients s.t for any $m > 4w$ and p a 2-partition of m, then

$$f_\gamma(m) = |\{(U,p_U)|\ U \in T\}|$$

.

Proof. (1)

Suppose w is fixed and $\gamma =: type((U_\gamma,p_\gamma)) \in Type(\Gamma)$. Let $\eta =: (U_\eta,p_\eta)$ s.t. $type(\eta) = \gamma$. We want to find the coefficient c_δ of the variable y_δ where $\delta =: type((U_\delta,V_\delta,p_\delta)) \in Type(\Delta)$ in the inequity J_γ:

c_δ itself is the sum of the coefficients of the variables $x_{(U,V,p)}$ with $type((U,V,p)) = \delta$ in the equation J_η. J_η was given in a way s.t. each $x_{(U,V,p)}$ may occur once with coefficient 1 and once with coefficient -1, so its enough to determine the number of $x_{(U,V,p)}$ with coefficient 1 and $type((U,V,p)) = \delta$ for all $\delta \in Type(\Delta)$ and the number of $x_{(U,V,p)}$ with coefficient -1, respectively.

Case 1. The coefficient of $x_{(U,V,p)}$ is 1:

Let $\delta \in Type(\Delta)$ and let $(U_0, V_0, p_{U_0,V_0,p_0}) \in \Delta$ s.t. $type((U_0, V_0, p_{U_0,V_0,p_0})) = \delta$ and $x_{(U_0,V_0,p_{U_0,V_0,p_0})}$ has coefficient 1 in J_η. By definition any $x_{(U,V,p_{U,V,p'})}$ occurs in J_η if there is a $V* \in T$ with $(U,V,p_{U,V,p'}) = (U_\eta, V*, p_{U_\eta,V*,p_\eta})$, so its enough to determine the number of $V* \in T$ s.t. $(U_\eta, V, p_{U_\eta,V,p_\eta}) \cong (U_0, V_0, p_{U_0,V_0,p_0})$:

By definition $p_{U,V,p'}$ is unique for all triples (U,V,p') with $U,V \in T$ and p' a partial 2-partition. The isomorphism types δ and γ uniquely define the numbers $i = |V - (U \cup \bigcup p)|$ and $j = |U \cup \bigcup p|$. We find a sufficient $V*$ by two steps:

(1) We choose one of the $\binom{m-i}{j}$ j-elementary subsets X of $m - (U \cup \bigcup p)$.

(2) We choose a subset H of $U \cup \bigcup p$ with $|H| = i$ s.t $< U, X \cap V, p > \cong < U, H, p >$.

The number c of such appropriate sets H depend just on the isomorphism types η and δ but not on m.

So the number $c\binom{m-i}{j}$ of appropriate $V*$'s is really a polynomial of m and its coefficients depend just on w and the isomorphism types δ and γ.

Case 2. The coefficient of $x_{(U,V,p)}$ is -1:

Similar to the case above.

The sum of these polynomials gives $f_{w,\delta,\gamma}(m)$.

Proof. (2) similar. □

□

Lemma 169.

If $m > 4w$, $\delta \in Type(\Delta)$ *then* $\Sigma_{\gamma \in Type(\Gamma)} f_\gamma(m) f_{w,\delta,\gamma}(m)$ *equals* 0.

Proof.

Let w, δ be fixed. We prove that the polynomial $\Sigma_{\gamma \in Type(\Gamma)} f_\delta(m) f_{w,\delta,\gamma}(m)$ is the 0-polynomial by proving the fact for infinitely many m's, namely the even ones: If p is

a 2-partition of m, then f_δ is the number of inequalities $L_{(U,p_U)}$ s.t. $type((U,p_U)) = \gamma$. In all $L_{(U,p_U)}$ the sum of the coefficients $c_{(U,V,p)}$ of the $x_{(U,V,p)}$ with $(U,V,p) \in \delta$ is $f_{w,\delta,\gamma}(m)$. According to 2 of the Lemma above the sum of all the lefthandsides equals 0. So the sum of the coefficients of the variables $x_{(U,V,p)}$ with $(U,V,p) \in \delta$ is 0, which implies the Lemma. □

Lemma 170.

Let $m, n^c, w \in \omega$, $m > 4w$ and $W_0(w, n^c, m)$ hold,

then the system $J^{w,m}$ has no proper solution.

Proof.

Let $\bar{J}_\gamma$ be the lefthand side of J_γ. Lemma 168 and 169 imply that $\Sigma_{\gamma \in Type(\Gamma)} f_\gamma(m) \bar{J}_\gamma = 0$: The coefficient of y_δ in J_γ is $f_{w,\delta,\gamma}$ according to Lemma 168. So the coefficient of y_δ is $\Sigma_{\gamma \in Type(\Gamma)} f_\gamma(m) f_{w,\delta,\gamma}(m)$ and this sum is equal to 0 according to Lemma 169. □

Lemma 171.

Let $m, n^c, w \in \omega$, $m > 4w$ and $W_0(w, n^c, m)$ hold,

then the system $J^{w,m}$ has a proper solution.

Proof.

Suppose that $W_0(w, n^c, m)$ holds for $m, n^c, w \in \omega$, $m > 4w$. Lemma 157 implies that $L^{w,m}$ has a proper solution $x_{(U,V,p)} = d(U,V,p)$. Let S_m be the group of permutations of ω which leaves everything outside the set m untouched. We define another evaluation of all variables $x_{(U,V,p)} \to X_{(U,V,p)} =: (1/m!) \sum_{\sigma \in S_m} x_{\sigma((U,V,p))}$. Since $x_{(U,V,p)}$ is a proper solution of $L^{w,m}$, $x_{\sigma((U,V,p))}$ s.t. $\sigma \in S_m$ is a proper solution and their average $X_{(U,V,p)}$ is a proper solution too. The definition of $X_{(U,V,p)}$ implies that its value just depends on $type((U,V,p))$. Let $\delta \in Type(\Delta)$ s.t. for all $(U,V,p) \in \delta$ follows $y_\delta = X_{(U,V,p)}$. The definition of $J^{w,m}$ implies that y_δ is a proper solution of $J^{w,m}$.

Proof. (4.3) □

Case 1. m is odd:

Suppose that contrary to our assertion there are $w, n \in \omega$ s.t. $W_0(w, n^c, m)$ holds

for infinitely many odd m's. Let us fix such a $m > 4w$. Lemma 170 implies that $J^{w,m}$ has a proper solution. This contradicts the Lemma 171 above.

□

Abstract

Here I review some articles of Paris, Wilkie [PW] and Ajtai [AJ2, AJ3] concerning connections between complexity and proof theory.

J. Paris and A. Wilkie [PW] were interested in the question whether every Δ_0 subset A of $\mathbb{N}$ has a Δ_0 definable counting function: $\{< n, m > | m = |A \cap n|\}$. A closely related question is whether the Pigeonhole Principle PHP can be proved in the weak fragment of Peano Arithmetic called $I\Delta_0$. $I\Delta_0$ consists of the axioms of Peano arithmetic with the induction scheme restricted to bounded formulas. They showed the consistency of $I\exists_1(F) + \exists x F : x \mapsto x - 1$, by an application of forcing. They also showed the consistency of $I\Delta_0(F) + \exists x F : x \mapsto x - 1$ under the assumption of the Cook-Reckhov Conjecture, that is, the assumption that it is "hard to prove" the propositional form PHP_n of PHP. This proof establishes a connection between $I\Delta_0$ and Frege systems.

Ajtai [AJ2] combined the application of forcing and this connection to prove the consistency of $I\Delta_0(F)+\exists x F : x \mapsto x-1$ (if we only consider Frege proofs of constant size and polynomial depth) without assuming the Cook-Reckhov Conjecture. His main idea was the following: Take a non-standard model $\mathcal{M}$ of $I\Delta_0$. Assume there is a "simple" proof of PHP_n for some n. Take the substructure $M_n = \mathcal{M} \restriction n$, extend it by forcing to some $M[G]$ where PHP cannot hold. By a combinatorial argument $M[G]$ is also a model of complete induction up to n, so we can step-wise check our "simple" proof of PHP_n and get a contradiction to the soundness of its construction.

Later [AJ3] Ajtai generalized this technique and showed that $PHP\Delta_0 \nvdash PAR$, where $PHP\Delta_0 = I\Delta_0 \cup PHP$ and PAR is the assertion that no odd set has a partition into subsets with two elements. PAR can be generalized further [AJ3] to "the modulo p Counting Principles" CP_p , where $PAR = CP_2$. He also showed that for all primes $p \neq q$, CP_p and CP_q are pairwise independent.

As a consequence of these observations we get a hierarchy of stronger and stronger weak theories of Peano Arithmetic:

$$I\exists_1 \subset I\Delta_0 \subset PHP\Delta_0 \subset CP_p\Delta_0 \text{ for every prime } p$$

Abstract Deutsch

In dieser Arbeit betrachte ich einige Arbeiten von Paris, Wilky [PW] und Ajati [AJ2, AJ3] welche einen Zusammenhang zwischen Komplexitäts- und Beweistheorie herstellen.

J. Paris und A. Wilkie [PW] betrachteten die Fragen ob jede Δ_0-Teilmenge A von $\mathbb{N}$ auch eine Δ_0 definierbare Zählfunktion $\{< n, m > | m = |A \cap n|\}$ besitzt. Eine damit eng verwanndte Fragestellung ist, ob das Schubfachprinzip PHP in einer schwachen Teiltheorie $I\Delta_0$ der Peano Arithmetik bewiesen werden kann. $I\Delta_0$ umfasst die selben Axiome wie die Peano Arithmetik. Das Axiomenschema der Induktion ist jedoch nur für beschränkte Formeln gegeben. Paris und Wilky konnten mithilfe der Forcing-Technik die Konsistenz von $I\exists_1(F) + \exists x F : x \mapsto x - 1$ zeigen. Weiters konnten sie unter Verwendung der Cook-Reckhov Vermutung, die Konsistenz von $I\Delta_0(F) + \exists x F : x \mapsto x - 1$ zeigen. Die Cook-Reckhov Vermutung besagt, dass ein Beweis der aussagenlogischen Form PHP_n von PHP "schwer" ist. Dieser zweite Beweis benutzt einen Zusammenhang zwischen $I\Delta_0$ und Frege Systemen.

Ajtai [AJ2] verband die Verwendung der Forcing-Technik und dieses Zusammenhangs um die Konsistenz von $I\Delta_0(F) + \exists x F : x \mapsto x - 1$, ohne der Verwendung der Cook-Reckhov Vermutung, zu zeigen. Dazu nahm er an, dass in einem nichtstandard Modell $\mathcal{M}$ von $I\Delta_0$ ein "einfacher" Beweis von PHP_n für ein n existiert. Dieses $\mathcal{M}$ beschränkte er auf die Substruktur $M_n = \mathcal{M} \restriction n$, welche er dann durch Forcing zu einem $M[G]$ erweiterte in welchem PHP auf natürliche Weise nicht wahr sein kann. Eine kombinatorische Überlegung zeigt, dass in $M[G]$ aber das Axiomenschema der vollständigen Induktion bis n wahr ist. Damit kann man nun den "einfachen" Beweis von PHP_n Schritt für Schritt prüfen, was zu einem Widerspruch führt.

Später [AJ3] verallgemeinerte Ajtai diese Art der Beweisführung, um zu zeigen, dass $PHP\Delta_0 \nvdash PAR$, wobei $PHP\Delta_0 = I\Delta_0 \cup PHP$ und PAR folgende Aussage ist: Keine Menge mit einer ungeraden Anzahl von Elementen kann in Teilmengen mit genau zwei Elementen partitioniert werden. PAR kann weiter zum "module p Counting Principle" CP_p verallgemeinert werden [AJ3]. Schlussendlich zeigte Ajtai für alle Primzahlen $p \neq q$, dass die CP_p paarweise unabhängig sind.

Als Konsequenz dieser Erkenntnisse bekommen wir eine Hierarchie von schwachen Theorien der Peano Arithmetik:

$$I\exists_1 \subset I\Delta_0 \subset PHP\Delta_0 \subset CP_p\Delta_0 \text{ für alle Primzahlen } p$$

Index

References

[PW] Paris, J. and Wilkie, A. - Counting Problems in Bounded Arithmetic. In: Methods in Mathematical Logic, LNM 1130.- Springer-Verlag 1985, pp. 317-340. 48, 49

[AJ1] Ajtai, M. - First-Order Definability on Finite Structures. In: Annals of Pure and Applied Logic. Vol. 25.- 1989, pp. 211-225. 23

[AJ2] Ajtai, M. - The Complexity of the Pigeonhole Principle. In: 29th FOCS.- 1988, pp. 346-355. 13, 48, 49

[AJ3] Ajtai, M. - Parity and the Pigeonhole Principle. In Buss, S.R. and Scott, P.J. editors, Feasible Mathematics.- Birkhauser 1990, pp. pages 1-24. 48, 49

[AJ4] Ajtai, M. - The Independence of the modulo p Counting Principles. In: Proceedings of the 26th Annual ACM Symposium on the Theory of Computing.- New York: ACM Press 1994, pp. 402-411.

[BIKPPW] Beame, P., Impaliazzo, R., Krajicek, J., Pitassi, T., Pudlak, P., Woods, A. - Exponential Lower Bounds for the Pigeonhole Principle. In: Proceedings of the 24th Annual ACM Syposium on the Theory of Computing.- New York: ACM Press 1992, pp. 200-221. 2

[BPU] Bellantoni, S., Pitassi, T., Urquhart, A. - Approximation and Small-Depth Frege Proofs. In: SIAM Journal of Computing Vol.21.- Dec. 1992, pp. 1161-1179. 2

[KPW] Krajicek, J., Pudlak, P., Woods, A. - An Exponential Lower Bound to the Size of Bounded Depth Frege Proofs of the Pigeonhole Principle. In: Preprint.- 1991. 2

[BP] Beame, P., Pitassi, T. - An Exponential Seperation between the Matching Principle and the Pigeonhole Principle. In: Annals of Pure and Applied Logic. Vol. 80.- 1996, pp. 195-228. 2

[K] Krejicek, J. - Bounded Arithmetic, Propositional Logic, and Complexity Theory.- Cambridge University Press 1995. 3

[U] Urquhart, A. - The Complexity of Propositional Proofs. In: The Bulletin of Symbolic Logic. Vol. 1/3.- 1995. 10

Lebenslauf

Persönliche Daten:

Name: Schöller, Christoph

Adresse: Gentzgasse 10/4/4/13, 1180 Wien

Telefon: +43-680-2163390

e-mail-Adresse: lord_vader@gmx.net

Familienstand: ledig

Staatsangehörigkeit: Österreich

Geburtsdaten: 04 09 1978 in Braunau a. Inn

Schulische Ausbildung/Studium:

09/1985 – 07/1989 Volksschule / Mattighofen Abschluss: Volksschulabschluß

09/1989 - 07/1998 Werkschulheim Felbertal / Ebenau bei Salzburg Abschluss:

09/1997: Schlosserlehre 1998: Matura

09/1999 - Universität / Wien / Mathematik

Berufliche Erfahrungen:

07/1994 – 09/1999 Ka-Ma Metallbau Gmbh / Mattighofen jeden Sommer mehrwöchige Praktika als Schlosserlehrling/- geselle

07/2000 – 09/2000 S&T / Wien Tätigkeit als Systemintegrator einer firmenspezifischen Linuxdistribution

08/2001 Plativio / Wien Tätigkeit als Schulungsleiter für Systembetreuer

11/09/2001 Beginn meiner Zusammenarbeit mit Exacon-IT/ Wien mein Tätigkeitsschwerpunkt lag auf der Systembetreuung von Kunden aus der Grafik/Werbebranche, d.h. vorallem Mac OS X Server und Client aber auch Entwicklung und Betreuung von entsprechenden Backuplösungen

07/02/2002 Erlangung der Gewerbeberechtigung für Dienstleistungen in der automatischen Datenverarbeitung und Informationstechnik

07/2005 – 09/2007 3united mobile solutions AG / Wien Tätigkeit als Systemadministrator auf Werkvertragsbasis

10/2005 – 02/2007 Anstellung bei 3united als Teilzeitkraft

03/2007 – 06/2007 Wechsel zur Eurojobs GmbH / Wien aber Fortsetzung meiner Tätigkeit für 3united

10/07/2007 Ruhendmeldung meiner Gewerbeberechtigung

01/03/2008 Anstellung bei i5invest

01/11/2009 Wechsel zu 123people

Sprachkenntnisse: Deutsch in Wort und Schrift

Englisch in Wort und Schrift

Spezielle Kenntnisse:

Führerschein: Klasse B

EDV: Fundierte Linux- Mac OS X-, Windows-, Netz- und Hardwarekenntnisse