

Count(q) does not imply Count(p)

Søren Riis*

August 1993

Revised January 1995

Abstract

It is shown that the elementary principles Count(q) and Count(p) are logically independent in the system $I\Delta_0(\alpha)$ of Bounded Arithmetic. Actually it is shown that Count(q) implies Count(p) exactly when each prime factor in p is a factor in q . This answers a question by M. Ajtai.

1 The logic of elementary counting

“She loves me, she loves me not, she loves me, . . .” The final answer does not depend on the order in which the leaves are pulled of. Every child who is familiar with the process of counting knows that. The underlying logical principle states that a set A has a well-defined cardinality modulo 2. Yet, the Count(2) principle can fail in quite strong systems of Arithmetic (Ajtai [2],[3]). Similarly for the counting principle modulo p (=Count(p)) where she can be in p states of mind.

In 1962 Cohen invented the famous technique of forcing. He used the method to show the independence of the continuum conjecture. Inspired by these ideas Ajtai showed (in [2]) that the elementary pigeon-hole principle fails in certain models of the arithmetical fragment $I\Delta_0(f)$. There is an essential equivalent way of stating this result (Ajtai). Let T be the theory which contain the basic axioms in Peanos Arithmetic, but which are modified so there exists a largest element c in the universe (with $c = c + 1, ac = c$ etc.). Then there exist a model $\mathbf{M} \models T$ in which the pigeon hole principle (stated by use of an unspecified function symbol) fails. Ajtais result came as a major break through. It became clear from Ajtais work (combined with the work of Paris and Wilkie [18]) that there is a close link between provability in Bounded Arithmetic (i.e. Arithmetical systems where the induction axiom scheme is restricted to formulas where all quantifiers appears in the context $\forall y \leq t(x) \dots$ or $\exists y \leq t(x) \dots$) and the necessary length of proofs of tautologies in systems propositional calculus. The main novelty in Ajtais work (in [2]) was the mixture of forcing and powerful probabilistic techniques.

The Count(p) versus Count(q) problem has various formulations and variants. The most famous variant is from circuit complexity theory and was first formulated by Furst, Saxe and Simpser. It asks (in the base case) whether there exist bounded depth, polynomial size circuits which counts

*This work was initiated at Oxford University England and completed at the Basic Research in Computer Science, Centre of the Danish National Research Foundation.

the number of 1's (in the input string) modulo p . This was answered (negatively) independently in [12] and [1]. Later J. Hastad [13] gave a near optimal exponential lower bound. The question becomes particular challenging if we also allow gates which can count modulo q . R. Smolensky [25] settled the case for different prime numbers q and p . The general classification is still open. It has been conjectured (by Barrington, Beigel and Rudich) that the answer is positive exactly when q contains all prime factors in p [5]. However even the simple case where $q = 6$ and $p = 5$ is still open.

One formulation of Ajtai's problem (given in [10]) concerns the question whether for different primes q and p there exist arithmetical models M , which satisfies the Count(q) principle (stated as a Δ_0 -axiom scheme), but which does not satisfies the Count(p) principle? The otherwise powerful algebraic methods by R. Smolensky [25] are not sufficient for this version of the problem. As it turns out Ajtai's version of the problem is technically more involved than the corresponding problem for circuits. Still circuit complexity (especially the method of collapsing circuits by use of random evaluations) is of major importance [15], [23].

In the first part of the paper we reduce Ajtai's question to a purely combinatorial problem. Actually (by elaborating on the ideas in [15]) it is shown that such a reduction (to a nice and purely combinatorial problem) is possible even in the case of composite numbers, and in the case where the underlying axiom system have considerable more power than that of $I\Delta_0(f)$.

In the second part of the paper we solve the combinatorial problem and thereby settle the Count(q) versus Count(p) problem.¹ The classification agree with what has been conjectured for the circuits. I.e. the answer is positive exactly when all prime factors in p belong to q .

1.1 A forest containing 16821302548060 trees

The first main result in the paper links the Count(p) versus Count(q) questions to a class of purely combinatorial problems.

Suppose T_1, T_2, \dots, T_u is a collection of specially labelled trees (i.e. a forest). Suppose that each type of branch appears 0 modulo q times. Does q divide u ? This of course depends on the underlying labelling set and the specific rules of how the trees are labelled. I consider labellings which are determined by two numbers p and n . A naive conjecture states that for each (q, p, n) (excluding trivial counter examples) there are only such forests when q divides the number ($=u$) of trees in the forest.

It turns out that there exist "exceptional" forests which violate this naive conjecture. As an example when $q = 2$ and $p = 4$, I show that for each $n \geq 9$ (not divisible by 4) there is a forest where each type of branch appears an even number of times, while the forest contain an odd number of trees. I give a concrete non-trivial example ($n = 10$) which contains 635 trees. When $q = 3$ and $p = 9$ there are also exceptional forests for each $n \geq 28$ (not divisible by 9). In these each type of branch appears 0 modulo 3 times, yet the number of trees is not divisible by 3. The non-trivial cases appear when $n = 3$ modulo 9 or $n = 6$ modulo 9. The smallest concrete (non-trivial) forest I have found for $q = 3$ appears when $p = 9$ and $n = 30$. The forest contains 16821302548060 trees when the trees are broken down to a special normal form.

¹P. Beame, R. Impagliazzo, J. Krajicek, T. Pitassi, P. Pudlak [6] solved the same combinatorial problem independently.

The first main result in the paper shows that the existence of such exceptional forests and the existence of (non-trivial) implications between $\text{Count}(q)$ and $\text{Count}(p)$ are two sides of same coin. The two examples correspond to the fact that $\text{Count}(2)$ implies $\text{Count}(4)$ and that $\text{Count}(3)$ implies $\text{Count}(9)$. I show that $\text{Count}(q)$ implies $\text{Count}(p)$ in systems of Bounded Arithmetic when all prime factors in p appears in q . According to the first main result *a priori* there must exist exceptional forest for all such q and p . In the paper it is shown how one can construct such forests. Furthermore it is shown how one can obtain proofs (in systems of Bounded Arithmetic) of $\text{Count}(p)$ from $\text{Count}(q)$ by use of these forests.

Early in this research the exceptional forests caused a major complication. At that stage all my attempts to collapse forests to particularly nice normal forms failed. I applied various probabilistic arguments which however did not quite work. Essentially the exceptional forests was the only obstacle. First when I managed to isolate these asymptotically, I was able to complete the analysis.

At present I do not have a complete picture of all exceptional forests. However it turns out that the asymptotic classification in this paper is sufficiently strong to provide a complete solution of the $\text{Count}(p)$ versus $\text{Count}(q)$ problem in the base-case (i.e. when the terms in underlying language have polynomial growth rate).

1.2 Motivation

The counting principles themselves are of course trivial. Or more specifically they hold in the category of finite sets. There are various reasons to examine these elementary counting principles.

First of all they play an important role in Bounded Arithmetic. These are systems where the induction principle is restricted to properties of a certain (well-defined) computorial complexity. Thus it is not surprising that Bounded Arithmetic provide a very natural and important interface between mathematical logic and computational complexity.

An important (but apparently very difficult) research project is to understand which parts of number theory holds in models of Bounded Arithmetic? This type of question was first studied by J. Paris, A. Wilkie. As pointed out both by A. Macintyre [16], by J. Paris, A. Wilkie and A. Woods [17] and by A. Berrarducci and B. Intrigila [7] many basic number theoretical facts are provable in system of Bounded Arithmetic. Other facts require new proofs. It seems not unreasonable to expect that the provability (in specific systems of Bounded Arithmetic) of elementary number theoretical statements often will turn out to be intimately linked to deep number theoretical problems/theorems. At present there are only sporadic suggestions of this. One such (which follows as a corollary to S.Buss' main result in [8]) is that if a certain fragment (often denoted by S_2^1) proves that the set of prime numbers is in NP (this can be proved in ordinary Arithmetic), then the prime numbers must actually be polynomial time recognisable. At present this is only known conditionally by assuming the validity of the General Riemann Hypothesis [16]. A stronger fragment (often denoted S_2) are known to show the infinitude of the set of prime numbers. This fact goes hand in hand with Sylvester's prime number theorem [17]. Besides this consider the quantifier elimination phenomenon (the strength of eliminating logic!). Clearly Bounded Arithmetic does not have quantifier elimination. However, one might still be able to eliminate many of its logical-like features. Perhaps it is possible to get our hands on the underlying unifications features arising from the induction schema. It is not unreasonable to expect Bounded Arithmetic to be tight up with the prestigious discipline of number theory (see [16] for a further discussion).

The work by [17] and later [7] show that the elementary counting principles play a central role in Bounded Arithmetic. In general the status of the elementary counting principles in models of Bounded Arithmetic seems to be a very deep problem. This problem could also be linked to deep questions and conjectures in classical number theory.

This paper consider the special case where all terms of the underlying language have polynomial growth rate, and contain at least one unspecified function or relation symbol. The presence of an unspecified function (or relation) symbol softens up the general problem. It also remove the problem from number theory and move it into a domain where methods from logic (forcing) is very powerful.

Second, systems of Bounded Arithmetic are linked to “low complexity reasoning”. One fundamental problem is to clarify the relation between automated versus intelligent reasoning. It seems natural to suggest that automatic reasoning (when this implemented in praxis) is only able to give a proper representation of objects of low complexity. The elementary process of counting introduces unpleasantly high complexity. A computation involving a counting task might (asymptotically) require exponentially many steps as a function of the length of the input. In practice this very soon becomes intractable for computers. Thus in a low complexity world we cannot assume that we are able to count. In order to verify (purely computationally) that the cardinality of a set A is unique, we would have to show that all bijections $f : A \rightarrow \{1, 2, \dots, m\}$ requires the same m . This is computationally intractable even for quite small sets A .

Finally another (related) problem is to examine the efficiency of propositional proof systems. This type of problems has already been studied intensively in the literature [2], [3], [11], [15], [18], [20], [23]. In S. Cook and A. Reckhow [11] it was shown that the efficiency of propositional proof systems is a natural way of studying the NP versus co-NP problem. Then later Paris and Wilkie [18] linked these problems to Bounded Arithmetic. And then Ajtai [2] showed that the problems also are tight up with methods and problems from circuit complexity. Recently a fascinating ‘ultra filter construction’ by Razborov [21] even suggest links to higher set-theory. In any case the study of the complexity of elementary counting provides some of the strongest known results in the field of circuit complexity.

1.3 The main results

In the following discussion let L be a countable first order language. Assume that L contains function symbols for the basic arithmetical operations ‘+’ and ‘·’. Also assume that the behaviour of terms and (the specified) relations are specified through a suitable set Ψ_L of purely universal axioms. And assume that L contains at least one unspecified relation symbol.

An axiom system ($= I\Delta_0(L)$ or just $I\Delta_0$ when L is clear from the context) of Bounded Arithmetic consists of the axioms Ψ_L together with the celebrated induction axiom schema, $(\theta(0) \wedge \forall x (\theta(x) \Rightarrow \theta(x+1))) \rightarrow \forall z \theta(z)$. However, in Bounded Arithmetic (unlike in ordinary Arithmetic), we require all quantifiers in each θ to be bounded by terms in the language L . More specifically, each quantifier is required to appear in the context $\forall x(x \leq t \rightarrow \dots$ or $\exists x(x \leq t \wedge \dots$

The elementary pigeon-hole principle ($=\text{PHP}_p$; $p \in \mathbb{N}$) states (in one of its many formulations) that for no n do there exists a bijection from $\{1, 2, \dots, n\}$ onto $\{1, 2, \dots, n+p\}$. More specifically, the $\Delta_0\text{-PHP}_p$ axiom schema states (for each bounded formula $\theta(x, y)$) that, $\forall z (\neg \forall x \leq z \exists! y \leq z+p \theta(x, y, z) \vee \neg \forall y \leq z+p \exists! x \leq z \theta(x, y, z))$. A weak form of the pigeon-hole principle is obtained by only considering monotone bijections. It is not hard to show that this form

of the pigeon hole principle is equivalent to the usual induction principle.

The $\text{Count}(p)$ principle (for a fixed number $p \in \mathbb{N}$) states that if $\{1, 2, \dots, n\}$ is divided into disjoint subsets each containing exactly p elements, then p divides n . More specifically, the $\Delta_0\text{-Count}(p)$ principle is the schema,

$\forall z ((\forall x_1 \leq z \exists! x_2, \dots, x_p \leq z (x_2 < x_3 < \dots < x_p \wedge \theta(x_1, x_2, \dots, x_p) \wedge \neg x_1 = x_2 \wedge \dots \wedge \neg x_{p-1} = x_p)) \rightarrow \exists y y \cdot p = z), \theta(x_1, \dots, x_p) \in \Delta_0$. In the first section I show,

Theorem [20] [23]

Assume that $p \geq 2$. Let L be any language where all terms have sub-exponential growth rate. Then there exists a model M^ in which*

- (1) *The $\text{Count}(p)$ principle fails.*
- (2) *All Δ_0 -pigeon-hole principles holds.*

A similar result was proved by Ajtai in [3], but only in case where all terms was assumed to have polynomial growth rate.

In section 2, the next section we construct the model M^* . And in the next two sections it is shown that M^* has the required properties. Actually in section 4 it is shown that,

Theorem *Besides (1) and (2) the model M^* satisfies the $\Delta_0\text{-Count}(q)$ principle exactly (under some weak extra assumptions) when there are no forest T_1, T_2, \dots, T_u of (p, n) -labelled trees where all branches appear 0 modulo q times, but $u \neq 0$ modulo q .*

The precise formulation of the result link the growth rate of terms in the underlying language L to an extra condition on the asymptotic height of the trees.

In section 5 we develop a general method to produce exceptional forests. It is shown that exceptional forests exist (for q and p) when all prime factors in p divides q . Furthermore the construction of such forests can be carried out inside any model of Bounded Arithmetic, so we get the following positive part of the classification.

Proposition *Let M^* be a model of Bounded Arithmetic in which the $\Delta_0\text{-Count}(q)$ principle holds. If all prime factors in p divides q , then M^* satisfies the $\Delta_0\text{-Count}(p)$ principle.*

In section 6 we return to the main problem. This is to show that $\text{Count}(p)$ not is a logical consequence of $\text{Count}(q)$ when p contains a prime factor not in q . This is shown (in the case all terms have polynomial growth rate) by showing

- (1) For each exception q -forests T_1, T_2, \dots, T_u of (p, n) trees, one can construct an exceptional q -forest T'_1, T'_2, \dots, T'_u of labelled trees related to the PHP_{q^k} -principle. No tree in this new forests has higher height than all trees in the old forest.
- (2) Suppose that T'_1, T'_2, \dots, T'_u is an exceptional q -forest of decision trees for the PHP_{q^k} -principle. Then at least one of the trees has height $\geq k$.

Combining this we get,

Theorem *Suppose that q and p are fixed. Suppose that p contains a prime factor which does not divide q . For each h there exists n_h such that for each $n \geq n_h$ there are no exceptional q -forests of (p, n) -labelled trees which all have height $\leq h$.*

Finally in section 7 I combine this result with theorem 1.3 and proposition 1.3. This gives the full classification,

Main Theorem (formulation 1) *Let \mathcal{T} be any system of Bounded Arithmetic over some countable language L . Suppose that L in addition to containing the language of arithmetic also contains at least one undefined relational symbol. Suppose that all terms t in L have polynomial growth rate. Then for all $q, p \in \mathbb{N}$ the following are equivalent:*

- (a) *There exists a model M of \mathcal{T} in which $\text{Count}(q)$ holds and $\text{Count}(p)$ fails.*
- (b) *There exists a prime factor in p which does not appear in q .*

The result has various essentially equivalent formulations.

Main Theorem (formulation 2) *Let ACA^{top} be the following modification of the celebrated system ACA . As ACA the system ACA^{top} has the full arithmetical comprehension. And it is equipped with the full induction axiom for sets. The “only” difference between this system and the normal second order Arithmetic is that the basic universal axioms are modified so that the universe contains a largest (unspecified) number c . All basic operations are modified (e.g. $c + 1 = c$). Any list of purely universal axioms might also be added. Suppose that the axiomatisation is non-trivial e.g. allows an infinite model. Then the following are equivalent:*

- (a) *$\text{Count}(p)$ holds in all structures which satisfies ACA^{top} and the $\text{Count}(q)$ principle.*
- (b) *All prime factors in p appear in q .*

Another formulation states that,

Main Theorem (formulation 3) *Let \mathcal{P} be one of the usual textbook systems in Hilbert style propositional logic. Let $\text{Count}_{\text{scheme}}(q)$ denote the substitution axiom scheme which arises from the canonical Booleanization of the $\text{Count}(q)$ principle. Let $\mathcal{P}' := \mathcal{P} + \text{Count}_{\text{scheme}}(q)$. Then there are polynomial-size bounded depth \mathcal{P}' -proofs of $\text{Count}(p)$ exactly when all prime factors in p divide q .*

In all formulations the negative part of the classification has a heuristic explanation. The analysis shows that when k becomes large, it becomes arbitrarily difficult² (but as it turns out never impossible) to show PHP_{q^k} from $\text{Count}(q)$. On the other hand if p contains a prime factor not in q it is uniformly (in k) easy to show PHP_{q^k} from $\text{Count}(p)$. So in this case $\text{Count}(p)$ is not a consequence (a bounded depth polynomial-size consequence in formulation 2) of $\text{Count}(q)$ in this case. This line of research is developed further in [24].

Finally we mention the recent and independent developments in [4] and [6].

2 Constructing the model

2.1 Translating formulas into circuits

Let M be a countable non-standard model of $\text{Th}(\mathbb{N})$ over a countable first order language L (which extends the language of arithmetic). Let $p \in \omega$, $p \geq 2$ and let $I := \{1, 2, \dots, n\} \subseteq M$, $n \in M \setminus \omega$ be fixed. Here ω denote the set of standard integer in M . As usual a set $A \subseteq M$ is said to be M -definable if there exists a formula $\psi(x, \vec{b})$ with parameters \vec{b} from M such that $A = \{a \in M : M \models \psi(a, \vec{b})\}$. For bounded sets A (i.e. sets where for some m for all $a \in A : a < m$) this definition is language independent. More specifically a set $A \subseteq M$ is M -definable if and only there exists $c \in M$ such that $a \in A$ exactly when a belongs to the sequence coded by c .

²Measured by the height of the corresponding forest.

Definition 2.1.1 For each $A \subseteq I$ with $|A| = p$ we introduce a variable p_A . The set of all such variables is denoted by $\text{VAR}_{I,p}$. ♣

Definition 2.1.2 A (Boolean) circuit π (with input variables in X) of size $s(\pi)$ and depth $d(\pi)$ is defined inductively as follows:

- (a) The constants ‘0’ and ‘1’ are circuits with $s(\text{‘1’}) = s(\text{‘0’}) = d(\text{‘1’}) = d(\text{‘0’}) = 1$.
- (b) Each $p \in X$ is a circuit with $s(p) = d(p) = 1$.
- (c) If π is a circuit, then $\neg\pi$ is a circuit with $s(\neg\pi) = s(\pi) + 1$ and $d(\neg\pi) = d(\pi) + 1$.
- (d) If $\pi_1, \pi_2, \dots, \pi_r$ are circuits, then $\bigwedge_j \pi_j$ and $\bigvee_j \pi_j$ are circuits with $s(\bigwedge_j \pi_j) = s(\bigvee_j \pi_j) = 1 + \sum_j s(\pi_j)$ and $d(\bigwedge_j \pi_j) = d(\bigvee_j \pi_j) = 1 + \max_j d(\pi_j)$. ♣

Definition 2.1.3 Let $B_d(X)$ denote the (Boolean) circuits π with input variables X of depth $d(\pi) \leq d$. Let $B_{<\omega}(X) := \cup_{d \in \omega} B_d(X)$. ♣

Definition 2.1.4 For $\psi \in B_{<\omega}(\text{VAR}_{I,p})$ and $\rho : \text{VAR}_{I,p} \rightarrow \{0, 1\}$ (neither ψ or ρ are required to be M-definable), we define the *truth-table evaluation* ψ^ρ inductively as follows:

- (a) ‘0’ $^\rho = 0$, ‘1’ $^\rho = 1$.
- (b) $p_A^\rho = 1$ iff $\rho(p_A) = 1$.
- (c) $(\neg\pi)^\rho = 1$ iff $\pi^\rho = 0$.
- (d) $(\bigwedge_j \pi_j)^\rho = 1$ iff $\pi_j^\rho = 1$ for all j .
- (e) $(\bigvee_j \pi_j)^\rho = 1$ iff $\pi_j^\rho = 1$ for some j . ♣

Let $L_{\mathbf{M}}$ be L extended by a constant c_a for each $a \in \mathbf{M}$. Let $L_{\mathbf{M}}(P)$ be $L_{\mathbf{M}}$ extended with an p -ary relation symbol. There exists a canonical translation of Bounded $L_{\mathbf{M}}(P)$ -sentences into circuits in $B_{<\omega}(\text{VAR}_{I,p})$:

Definition 2.1.5 For each sentence $\psi \in L_{\mathbf{M}}(P)$ we define $\epsilon_\psi \in B_{<\omega}(\text{VAR}_{I,p})$ inductively as follows:

- (a) For any k -ary relation symbol ($\neq P$): $\epsilon_{R(a_1, \dots, a_k)} := \text{‘1’}$ if $\mathbf{M} \models R(a_1, \dots, a_k)$, ‘0’ otherwise.
- (b) $\epsilon_{P(a_1, \dots, a_p)} := p_A$ if $A = \{a_1, \dots, a_p\} \subseteq I$ and $|A| = p$, ‘0’ otherwise.
- (c) $\epsilon_{\neg\pi} := \neg\epsilon_\pi$.
- (d) $\epsilon_{\pi \vee \pi'} := \epsilon_\pi \vee \epsilon_{\pi'}$
- (e) $\epsilon_{\pi \wedge \pi'} := \epsilon_\pi \wedge \epsilon_{\pi'}$
- (f) $\epsilon_{\exists x(x \leq u \wedge \theta(x, u))} := \bigvee_{a \leq u} \epsilon_{\theta(a, u)}$.
- (g) $\epsilon_{\forall x(x \leq u \rightarrow \theta(x, u))} := \bigwedge_{a \leq u} \epsilon_{\theta(a, u)}$. ♣

Notice that if $\psi \in L_{\mathbf{M}}(P)$ has $\leq d$ quantifiers, all bounded by $t \in \mathbf{M}$, and ψ contains k logical connectives, then $s(\epsilon_\psi) \leq kt^d$ and $d(\epsilon_\psi) \leq d + k$.

Lemma 2.1.6 Suppose that P is a partitioning of $\{1, 2, \dots, n\}$ into disjoint classes each containing exactly p elements. Let $\rho_P : \text{VAR}_{I,p} \rightarrow \{0, 1\}$ be defined by $A \in P \leftrightarrow \rho_P(p_A) = 1$. Then for $\psi \in L_{\mathbf{M}}(P)$ the following statements are equivalent:

- (a) $(\mathbf{M}, P) \models \psi$.
- (b) $(\epsilon_\psi)^{\rho_P} = 1$.

Proof: Induction on the number of logical constants in ψ . □

2.2 The forcing set up

As above let \mathbf{M} be a countable non-standard model of $\text{Th}(\mathbb{N})$ over a countable first order language L which extends the language of arithmetic. We have fixed $p \geq 2$ and $I := \{1, 2, \dots, n\} \subseteq \mathbf{M}$, $n \in \mathbf{M} \setminus \omega$. Let $L_{\mathbf{M}}$ and $L_{\mathbf{M}}(P)$ be defined as above.

Definition 2.2.1 We say that ρ is a *partial p -partitioning* if

- (a) $\forall A \in \rho \ A \subseteq I$.
- (b) $\forall A \in \rho \ |A| = p$.
- (c) $\forall A, B \in \rho \ A \neq B \rightarrow A \cap B = \emptyset$.

Let $\text{Set}(\rho) := \cup_{A \in \rho} A \subseteq I$. ♣

Definition 2.2.2 For $k \in \mathbb{N}$ let

$$\mathcal{P}_k(I) := \{\rho : \rho \text{ is a partial } p\text{-partitioning of } I \text{ and } (n - |\text{Set}(\rho)|)^k \geq n\}.$$

We define $\mathcal{P}(I) := \cup_{k \in \mathbb{N}} \mathcal{P}_k(I)$. The elements in $\mathcal{P}(I)$ are ordered under inclusion. An element $\rho \in \mathcal{P}(I)$ is called a (*forcing*) *condition*. We use letters $\mathcal{A}, \mathcal{B}, \mathcal{C}, \dots$ to denote subsets of $\mathcal{P}(I)$. When I is clear from the context we let $\mathcal{P}_k := \mathcal{P}_k(I)$ and let $\mathcal{P} := \mathcal{P}(I)$. ♣

Notice that $\mathcal{P}_1 \subseteq \mathcal{P}_2 \subseteq \dots \subseteq \mathcal{P}_r \subseteq \dots \subseteq \mathcal{P}$, for each $r \in \omega$. The idea is to use (\mathcal{P}, \subseteq) as the set of forcing conditions. As in [22]:

Definition 2.2.3 We say that $\mathcal{D} \subseteq \mathcal{P}$ is *dense* if $\forall g \in \mathcal{P} \exists h \in \mathcal{D} \ h \supseteq g$.

We say that \mathcal{D} is *quasi-definable* if there exists a formula $\theta(x) \in L_{\mathbf{M}}(R_\omega)$ such that $\mathcal{D} := \{m \in \mathbf{M} : \mathbf{M} \models \theta(m)\}$ (the relation R_ω is defined by $R_\omega(a) \leftrightarrow a \in \omega$). ♣

Example 2.2.4 \mathcal{P} is dense and quasi-definable. \mathcal{P} is not $L_{\mathbf{M}}$ -definable.

Definition 2.2.5 We say that $\rho_G \subseteq \mathcal{P}$ is a *generic filter* if

- (i) $\forall \alpha \in \rho_G \forall \beta \in \mathcal{P} \ \beta \subseteq \alpha \rightarrow \beta \in \rho_G$.
- (ii) $\forall \alpha, \beta \in \rho_G \exists \gamma \in \rho_G \ \gamma \supseteq \alpha \wedge \gamma \supseteq \beta$.
- (iii) For $\mathcal{D} \subseteq \mathcal{P}$ dense and quasi-definable $\rho_G \cap \mathcal{D} \neq \emptyset$.

We use the abbreviation $\tilde{\rho}_G := \cup_{\alpha \in \rho_G} \alpha$. ♣

2.3 Generic objects

Lemma 2.3.1 If $\rho_G \subseteq \mathcal{P}$ is a generic filter, then $\tilde{\rho}_G$ defines a partition of $\{1, 2, \dots, n\}$ into disjoint p -subsets.

Proof: The only problem is to show $\text{Set}(\tilde{\rho}_G) = I$. For an arbitrary $u \in I$ let $\mathcal{D}_u := \{\alpha \in \mathcal{P} : u \in \text{set}(\alpha)\}$. It is straightforward to show that \mathcal{D}_u is dense and quasi-definable so $\mathcal{D}_u \cap \rho_G \neq \emptyset$. Thus for each $u \in I$ there exists $\alpha_u \in \mathcal{D}_u \cap \rho_G$, and thus $u \in \text{Set}(\tilde{\rho}_G)$. □

Lemma 2.3.2 For each $\rho_0 \in \mathcal{P}$ there exists a generic filter $\rho_G \subseteq \mathcal{P}$ such that $\rho_0 \in \rho_G$.

Proof: Recall that both M and L are assumed to be countable, so there are only countably many quasi-definable dense sets. Let these be $\mathcal{D}_1, \mathcal{D}_2, \dots$. According to the definition of denseness there exists a sequence of conditions $\rho_1 \subseteq \rho_2 \subseteq \dots \in \mathcal{P}$ with $\rho_j \in \mathcal{D}_j$, $j = 1, 2, \dots$ and $\rho_1 \supseteq \rho_0$. Clearly $\rho_0 \in \rho_G := \{\rho : \rho \subseteq \rho_k \text{ for some } k \in \omega\}$ is a generic filter. \square

Definition 2.3.3 For a sentence $\psi \in L_M(P)$ we define the *forcing relation* \Vdash by letting $\rho \Vdash \psi$ iff $(M, \tilde{\rho}_G) \models \psi$ for all generic filters $\rho_G \ni \rho$. \clubsuit

Lemma 2.3.4 If $(M, \tilde{\rho}_G) \models \psi$ for a generic filter ρ_G , then there exists $\rho_0 \in \rho_G \subseteq \mathcal{P}$ such that $\rho_0 \Vdash \psi$.

Proof: By use of induction on the logical complexity of a general formula $\psi(\vec{x})$, it is not hard to show that $\{(\vec{a}, \rho) \in M^r \times \mathcal{P} : \rho \Vdash \psi(c_{\vec{a}})\}$ is quasi-definable. Continuing this argument for each $L_M(P)$ -sentence ψ , $\mathcal{D} := \{\rho \in \mathcal{P} : \rho \Vdash \psi \vee \rho \Vdash \neg\psi\}$ is both quasi-definable and dense. For the required ρ_0 take any $\rho_0 \in \rho_G \cap \mathcal{D}$. \square

Definition 2.3.5 For $\theta, \psi \in B_{<\omega}(\text{VAR}_{I,p})$ and $\rho \in \mathcal{P}$, $\theta \equiv_\rho \psi$ if $\theta^{\tilde{\rho}_G} = \psi^{\tilde{\rho}_G}$ for each generic filter $\rho_G \ni \rho$.

For $\theta \in B_{<\omega}(\text{VAR}_{I,p})$ and $\rho \in \mathcal{P}$ we say that ρ *forces* $\theta^P = 1$ ($\theta^P = 0$) if for all generic $\rho_G \ni \rho$, $\theta^{\tilde{\rho}_G} = 1$ ($\theta^{\tilde{\rho}_G} = 0$). This is written $\rho \Vdash \theta^P = 1$ ($\rho \Vdash \theta^P = 0$). \clubsuit

The next lemma shows how each appearance of \neg can be eliminated.

Lemma 2.3.6 Suppose that $i_0 \in A$, $A \subseteq I$, $|A| = p$.

Suppose that $\pi_1 := \neg p_A$ and $\pi_2 := \bigvee_{B \subseteq I} p_B$, where B runs through all $B \subseteq I$ with $|B| = p$, $A \neq B$ and $i_0 \in B$. Then $\pi_1 \equiv_\rho \pi_2$ for all $\rho \in \mathcal{P}$.

Proof: Let $\tilde{\rho}_G \ni \rho$ be a generic partition. According to definition 2.1.4 and lemma 2.3.1, $(\pi_1)^{\tilde{\rho}_G} = 1 \Leftrightarrow (\neg p_A)^{\tilde{\rho}_G} = 1 \Leftrightarrow p_A^{\tilde{\rho}_G} = 0 \Leftrightarrow A \notin \tilde{\rho}_G \Leftrightarrow \exists B \neq A \ i_0 \in B \wedge B \in \tilde{\rho}_G \Leftrightarrow (\bigvee_{B \neq A} p_B)^{\tilde{\rho}_G} = 1 \Leftrightarrow (\pi_2)^{\tilde{\rho}_G} = 1$. \square

Lemma 2.3.7 For any Boolean circuit $\theta \in B_d(\text{VAR}_{I,p})$, there exists a negation-free circuit $\tilde{\theta} \in B_d(\text{VAR}_{I,p})$ such that $\theta \equiv_\rho \tilde{\theta}$ for any $\rho \in \mathcal{P}$. Furthermore, $s(\tilde{\theta}) \leq s(\theta) \cdot \binom{n-1}{p-1}$.

Proof: First notice that $\neg \bigvee_i \pi_i \equiv_\emptyset \bigwedge_i \neg \pi_i$, and that $\neg \bigwedge_i \pi_i \equiv_\emptyset \bigvee_i \neg \pi_i$. So without loss of generality we can assume that negations appear only in front of the input variables. For each input variable p_A pick $i_0 \in A$ and replace each appearance of $\neg p_A$ with $\bigvee_{B: i_0 \in B \wedge B \neq A} p_B$. According to lemma 2.3.6 $\theta \equiv_\emptyset \tilde{\theta}$. This new circuit $\tilde{\theta}$, still has depth d . Furthermore, $s(\tilde{\theta}) \leq s(\theta) \cdot \max_{i_0} (s(\bigvee_{B: i_0 \in B, B \neq A} p_B)) = s(\theta) \cdot \binom{n-1}{p-1}$. \square

Lemma 2.3.8 For each bounded $\psi \in L_M(P)$, $\rho \Vdash \psi$ iff $\rho \Vdash (\epsilon_\psi)^P = 1$.

Proof: Induction on the number of logical constants in ψ . \square

Definition 2.3.9 Two conditions α and β are *incompatible* ($\alpha \perp \beta$) if $\exists A \in \alpha \exists B \in \beta \ A \neq B \wedge A \cap B \neq \emptyset$.

Two conditions α and β are *compatible* ($\alpha \parallel \beta$) if $\forall A \in \alpha \forall B \in \beta \ A \neq B \rightarrow A \cap B = \emptyset$. \clubsuit

Definition 2.3.10 $\mathcal{B} \subseteq \mathcal{P}$ is *orthogonal* if $\forall \alpha, \beta \in \mathcal{B} \quad \alpha \neq \beta \rightarrow \alpha \perp \beta$ and is *complete* if $\forall \rho \in \mathcal{P} \exists \alpha \in \mathcal{B} \rho \parallel \alpha$.

A *Basis* is a collection $\mathcal{B} \subseteq \mathcal{P}$ which satisfies both these conditions (i.e. is both Orthogonal and Complete). ♣

Definition 2.3.11 $\|\mathcal{B}\| := \max_{\beta \in \mathcal{B}} (|\text{Set}(\beta)|)$. ♣

Lemma 2.3.12 Suppose that $\|\mathcal{B}\|^k < n$ for all $k \in \omega$ (or in short-hand notation $\|\mathcal{B}\| < n^{\frac{1}{\omega}}$). Then $\forall \rho \in \mathcal{P}_k, \forall \beta \in \mathcal{B} \rho \parallel \beta \rightarrow \rho \cup \beta \in \mathcal{P}_{k+1}$.

Proof: Assume that $\rho \in \mathcal{P}_k$. Thus $(n - |\text{Set}(\rho)|)^k \geq n$. Also assume that $\beta \in \mathcal{B}$, where $\|\mathcal{B}\| \leq n^{\frac{1}{\omega}}$. Clearly $|\text{Set}(\beta)|^{2k} \leq n$. If $\rho \parallel \beta$ we notice that $(n - |\text{Set}(\rho \cup \beta)|)^{k+1} \geq (n - |\text{Set}(\rho)| - |\text{Set}(\beta)|)^{k+1} \geq (n^{\frac{1}{k}} - n^{\frac{1}{2k}})^{k+1} \geq (n^{\frac{1}{k}})^{k+1} (1 - (\frac{1}{n})^{\frac{1}{2k}})^{k+1} \geq n(n^{\frac{1}{k}}(\frac{1}{2})^{k+1}) \geq n$. The last inequality follows because $n \geq 2^{(k+1)k}$ for any $k \in \omega$. Thus $\rho \cup \beta \in \mathcal{P}_{k+1}$. □

The next lemma shows an important technical point in Ajtai's choice of \mathcal{P} . In effect the lemma allows us to repeat estimates in a scaled down version. More specifically it allows us to assume that $\emptyset \Vdash \psi$ in cases where $\rho_0 \Vdash \psi$ for some $\rho_0 \in \mathcal{P}$. This is because the lemma allows us to replace $I := \{1, 2, \dots, n\}$ by $I' := \{1, 2, \dots, n'\}$ where $n' := n - |\text{Set}(\rho_0)|$ and then smoothly pass from $\mathcal{P}(I)$ to $\mathcal{P}(I')$.

Lemma 2.3.13 (Scaling down) Fix $\rho \in \mathcal{P}$, let $J := I \setminus \text{Set}(\rho)$ and let $n' := |J|$. Define $\mathcal{P}_k(J) := \{\tilde{\rho} : \tilde{\rho} \text{ is a partial } p\text{-partition of } J \text{ and } (n' - |\text{Set}(\tilde{\rho})|)^k \geq n'\}$. Let $\mathcal{P}(J) := \cup_{k \in \omega} \mathcal{P}_k(J)$. Then $\mathcal{P}(J) = \mathcal{P}^\rho$, where $\mathcal{P}^\rho := \{\tilde{\rho} : \tilde{\rho} \text{ is a partial } p\text{-partition of } J \text{ and } \tilde{\rho} \cup \rho \in \mathcal{P}\}$.

Proof: First we show $\mathcal{P}^\rho \subseteq \mathcal{P}(J)$. Suppose that $\tilde{\rho} \in \mathcal{P}^\rho$. There exists $k_0 \in \omega$ such that $n' \leq n \leq (n - |\text{Set}(\tilde{\rho} \cup \rho)|)^{k_0} = (n - |\text{Set}(\rho)| - |\text{Set}(\tilde{\rho})|)^{k_0} = (n' - |\text{Set}(\tilde{\rho})|)^{k_0}$. So $\tilde{\rho} \in \mathcal{P}_{k_0}(J) \subseteq \mathcal{P}(J)$.

Second, we show that $\mathcal{P}(J) \subseteq \mathcal{P}^\rho$. Suppose that $\tilde{\rho} \in \mathcal{P}(J)$. There exists $k \in \omega$ such that $n' \leq (n' - |\text{Set}(\tilde{\rho})|)^k$. As $\rho \in \mathcal{P}$ there exist $l \in \omega$ such that $(n - |\text{Set}(\rho)|)^l \geq n$. By combining this we get that $(n - |\text{Set}(\tilde{\rho} \cup \rho)|)^{kl} = (n - |\text{Set}(\rho)| - |\text{Set}(\tilde{\rho})|)^{kl} = (n' - |\text{Set}(\tilde{\rho})|)^{kl} \geq (n')^l = (n - |\text{Set}(\rho)|)^l \geq n$. Thus $\tilde{\rho} \cup \rho \in \mathcal{P}$ and $\tilde{\rho} \in \mathcal{P}^\rho$. □

Lemma 2.3.14 Suppose that \mathcal{B} is a basis for \mathcal{P} and $\mathcal{H} \subseteq \mathcal{B}$. Suppose also that $\|\mathcal{B}\| < n^{\frac{1}{\omega}}$. Then

- (a) $\rho \Vdash (\bigvee_{h \in \mathcal{H}} h)^P = 1$ iff ρ is incompatible with all conditions $h' \in \mathcal{B} \setminus \mathcal{H}$.
- (b) $\rho \Vdash (\bigwedge_{h \in \mathcal{H}} h)^P = 1$ iff ρ is incompatible with all conditions $h' \in \mathcal{H}$.

Proof: (a) \Rightarrow : Suppose that $\rho \Vdash (\bigvee_{h \in \mathcal{H}} h)^P = 1$, but ρ is compatible with $h' \in \mathcal{B} \setminus \mathcal{H}$. By use of lemma 2.3.12 $\rho' := \rho \cup h' \in \mathcal{P}$. By using property (a) of a basis (definition 2.3.10) h' is incompatible with all conditions in \mathcal{H} . Clearly $\rho' \supseteq h'$ so ρ' is also incompatible with all conditions in \mathcal{H} . But then $(\bigvee_{h \in \mathcal{H}} h)^{\beta_G} = 0$ for each generic filter $\rho_G \ni \rho'$ (which exists by lemma 2.3.2). This contradicts $\rho \Vdash (\bigvee_{h \in \mathcal{H}} h)^P = 1$.

(a) \Leftarrow : Assume that ρ is incompatible with all $h' \in \mathcal{B} \setminus \mathcal{H}$. Let $\rho_G \ni \rho$ be any generic filter (which exists by lemma 2.3.2). Let

$\mathcal{D} := \{\rho' \in \mathcal{P} : (\rho' \text{ is compatible with some } h' \in \mathcal{H}) \text{ or } (\rho' \text{ is incompatible with } \rho)\}$. By definition 2.3.10, $\mathcal{D} \subseteq \mathcal{P}$ is dense. Also \mathcal{D} is quasi-definable. By definition 2.2.5 (iii) there exists $\alpha \in \mathcal{D} \cap \rho_G$, so there exists $h \in \mathcal{H}$ with $h \subseteq \alpha \subseteq \tilde{\rho}_G$.

(b) \Rightarrow / (b) \Leftarrow are proved as (a) \Rightarrow / (a) \Leftarrow . □

Lemma 2.3.15 *Let $\epsilon_1, \epsilon_2, \dots, \epsilon_u$ $u \in \mathbb{M}$, be an \mathbb{M} -definable sequence of Boolean circuits, each of the form $\epsilon_j := \bigvee_{h \in \mathcal{H}_j} h$. Let $\mathcal{B}_1, \dots, \mathcal{B}_u$ be an \mathbb{M} -definable sequence and suppose that $t < n^{\frac{1}{\omega}}$ such that:*

- (a) for each $j = 1, 2, \dots, u$ $\mathcal{B}_j \subseteq \mathcal{P}$, is a basis for \mathcal{P} ,
- (b) for each $j = 1, 2, \dots, u$ $\|\mathcal{B}_j\| < t$,
- (c) for each $j = 1, 2, \dots, u$, $\mathcal{H}_j \subseteq \mathcal{B}_j$.

Then for every generic filter ρ_G either

- (a) for all $j \in \{1, 2, \dots, u\}$, $\epsilon_j^{\tilde{\rho}_G} = 0$, or
- (b) there exists $j_0 \leq u$ such that $\epsilon_{j_0}^{\tilde{\rho}_G} = 1$ and $\epsilon_j^{\tilde{\rho}_G} = 0$ for each $j < j_0$.

Proof: Let

$$\mathcal{D} := \{\rho \in \mathcal{P} : (\exists j_0 \exists \beta \in \mathcal{H}_{j_0} \beta \parallel \rho \wedge \forall \gamma \in \bigcup_{j < j_0} \mathcal{H}_j \rho \perp \gamma) \text{ or } (\forall \gamma \in \bigcup_{j \leq u} \mathcal{H}_j \rho \perp \gamma)\}.$$

Clearly \mathcal{D} is quasi-definable. For each $\rho_0 \in \mathcal{P}$, if ρ_0 is compatible with some $\beta \in \bigcup_j \mathcal{H}_j$, then there must be a smallest j_0 such that ρ_0 is compatible with some $\beta \in \mathcal{H}_{j_0}$. Here we use that the least number principle is valid in \mathbb{M} . Now $\rho := h \cup \rho_0 \in \mathcal{P}$ (by lemma 2.3.12), and thus $\rho \in \mathcal{D}$. So \mathcal{D} is dense. By definition 2.2.5 (iii) there exists $\rho \in \rho_G \cap \mathcal{D}$. This condition ρ is incompatible with all $h \in \mathcal{H}_j$, $j < j_0$. As $\tilde{\rho}_G \supseteq \rho \supseteq h \in \mathcal{H}_{j_0}$ clearly $(\bigvee_{h \in \mathcal{H}_{j_0}} h)^{\tilde{\rho}_G} = 1$. □

2.4 The key lemma

Recall that \mathbb{M} is a countable non-standard model of $\text{Th}(\mathbb{N})$ over a countable first order language L . As above we have fixed $p \in \omega \setminus \{1\}$, and $I := \{1, 2, \dots, n\} \subseteq \mathbb{M}$, $n \in \mathbb{M} \setminus \omega$. As above the set \mathcal{P} of forcing conditions consists of partial p -partitions ρ of I with $|\text{Set}(\rho)| \leq n - n^{\frac{1}{\omega}}$ for some $k \in \omega$.

Lemma 2.4.1 (key lemma) *Let $\theta_1, \theta_2, \dots, \theta_u$ be an \mathbb{M} -definable sequence of depth $\leq d \in \omega$ circuits with $\sum_{j=1}^u s(\theta_j) \leq n^t$ for some $t < n^{\frac{1}{\omega}}$ (i.e. $t^k < n$ for all $k \in \omega$).*

Let $\rho_0 \in \mathcal{P}$. There exists $\rho \supseteq \rho_0$, $\rho \in \mathcal{P}$ and an \mathbb{M} -definable sequence $\epsilon_1, \epsilon_2, \dots, \epsilon_u$ of circuits together with an \mathbb{M} -definable sequence $\mathcal{B}_1, \mathcal{B}_2, \dots, \mathcal{B}_u$ such that

- (a) for $j = 1, 2, \dots, u$ each \mathcal{B}_j , is a basis for \mathcal{P} ,
- (b) for $j = 1, 2, \dots, u$ each ϵ_j is of the form $\bigvee_{h \in \mathcal{H}_j} h$ for some $\mathcal{H}_j \subseteq \mathcal{B}_j$,
- (c) for each $j = 1, 2, \dots, u$, $\theta_j \equiv_{\rho} \epsilon_j$ (see definition 2.3.5),
- (d) for some $s \leq \omega$ for each $j = 1, 2, \dots, u$ $\|\mathcal{B}_j\| \leq s$.

If we combine the key lemma with lemma 2.3.15 we get:

Corollary 2.4.2 *If $\theta_1, \theta_2, \dots, \theta_u$ is an \mathbf{M} -definable sequence of depth $d \in \omega$ circuits with $\Sigma_{j=1}^p s(\theta_j) \leq n^t$ for some $t < n^{\frac{1}{\omega}}$, then for any generic filter $\rho_G \subseteq \mathcal{P}$ either*

- (a) *for all $j \leq u$ $\theta_j^{\rho_G} = 1$, or*
- (b) *there exists $j_0 \leq u$, such that $\theta_{j_0}^{\rho_G} = 1$ and $\tilde{\theta}_j^{\rho_G} = 0$ for all $j < j_0$.*

Before we prove the key lemma, we need to do some preparatory work.

2.5 Random conditions

My aim is to add a suitable probability distribution μ on the space \mathcal{P} of forcing conditions.

The next lemma in effect states that a randomly chosen condition $\rho \in \mathcal{P}_k$ which happens (and this is un-typical) to be compatible to some small fixed and given condition h , by far is most likely to ‘capture’ h (i.e. $\rho \supseteq h$).

Lemma 2.5.1 *For $k \geq 2p + 1$, $k \in \mathbf{N}$, and fix $m < n$ such that $(n - m)^{k+1} > n \geq (n - m)^k$. Let μ_{sym} be the symmetrical probability distribution (perceived from inside \mathbf{M}) on the set $\{\rho \in \mathcal{P} : |\text{Set}(\rho)| = m\}$. For each $h \in \mathcal{P}$ with $|h| < n^{\frac{1}{\omega}}$, $\Pr(h \subseteq \rho) > n^{\frac{1}{2}} \Pr(h \parallel \rho \wedge \neg(h \subseteq \rho))$.*

Proof: Notice that for fixed $J \subseteq I$ with $|J| = m$ the number $\eta(m, p)$ of partial p -partitions ρ with $\text{Set}(\rho) = J$ is

$$\eta(m, p) = \frac{m!}{(p!)^{\frac{m}{p}} (\frac{m}{p})!}$$

when m is divisible by p and 0 otherwise. The set $\{\rho \in \mathcal{P} : |\text{Set}(\rho)| = m\}$ contains $\binom{n}{m} \cdot \eta(m, p)$ elements. If $h' \in \mathcal{P}$, $|\text{Set}(h')| = up$ and fix $J \subseteq I \setminus \text{Set}(h')$ with $|J| = b$. Then

$$\Pr(h' \subseteq \rho \wedge J \cap \text{Set}(\rho) = \emptyset) = \frac{\binom{n-up-b}{m-up} \eta(m-up, p)}{\binom{n}{m} \eta(m, p)} = \frac{(n-up-b)!(n-m)!(p!)^u (\frac{m}{p})!}{n!(n-m-b)! (\frac{m}{p}-u)!}$$

Now suppose $n - n^{\frac{1}{k}} \leq m < n - n^{\frac{1}{k+1}}$, and $b, u < n^{\frac{1}{\omega}}$. There exists a suitable real (in the sense of \mathbf{M}) $c \in [0, 1]$ such that $\Pr(h \subseteq \rho \wedge J \cap \text{Set}(\rho) = \emptyset) = (\frac{1}{n})^{u(p-1)+b(1-\frac{1}{k+c})}$. Here we use the fact that a sufficiently strong part of real analysis can be developed inside \mathbf{M} so that we obtain a strict identity. Now

$$\begin{aligned} \Pr(h \parallel \rho \wedge \neg(h \subseteq \rho)) &= \sum_{j=0}^{u-1} \sum_{h' \subseteq h, |h'|=j} \Pr(h' \subseteq \rho \wedge (\text{Set}(h) \setminus \text{Set}(h') \cap \text{Set}(\rho) = \emptyset)) \\ &= \sum_{j=0}^{u-1} \sum_{h' \subseteq h, |h'|=j} \left(\frac{1}{n}\right)^{\binom{p}{k+c}-1} j + pu(1-\frac{1}{k+c}) = \sum_{j=0}^{u-1} \binom{u}{j} \left(\frac{1}{n}\right)^{\binom{p}{k+c}-1} j + pu(1-\frac{1}{k+c}) \end{aligned}$$

In general $\sum_{j=0}^{u-1} \binom{u}{j} a^j = (a+1)^u - a^u$. Let $a := n^{1-\frac{p}{k+c}}$, and notice that $\sum_{j=0}^{u-1} \binom{u}{j} a^j \leq 2ua^{u-1}$. Thus

$$\sum_{j=0}^{u-1} \binom{u}{j} \left(\frac{1}{n}\right)^{\binom{p}{k+c}-1} j + pu(1-\frac{1}{k+c}) = 2u \left(\frac{1}{n}\right)^{pu(1-\frac{1}{k+c})} \cdot \left(\frac{1}{n}\right)^{\binom{p}{k+c}-1} (u-1)$$

$$= 2u \cdot \left(\frac{1}{n}\right)^{(p-1)u+(1-\frac{p}{k+c})} = \Pr(h \subseteq \rho) \cdot 2u \left(\frac{1}{n}\right)^{(1-\frac{p}{k+c})} \leq \Pr(h \subseteq \rho) \cdot \left(\frac{1}{n}\right)^{\frac{1}{2}}$$

when $k \geq 2p + 1$. In all estimates c denotes an error term, which in all cases can be chosen as a suitable real number in $[0, 1]$. \square

Lemma 2.5.2 *Fix $k \in \mathbb{N}$. Also fix $t < n^{\frac{1}{\omega}}$. Then there exists a (global) probability distribution μ_{glo} on the \mathbb{M} -definable set consisting of all partial p -partitions, such that for each $h \in \mathcal{P}$ with $|h| \leq t$*

(i) *If $C(\rho)$ is a monotone property (i.e. $C(\rho) \wedge \rho \subseteq \rho' \rightarrow C(\rho')$), then*

$$\Pr(C(\rho) \mid |h| \mid \rho) \geq \frac{1}{8} \cdot \Pr(C(\rho) \mid |h| \mid \rho \wedge \neg(h \subseteq \rho)),$$

(ii) *there is $s \in \mathbb{M} \setminus \omega$ such that $\Pr(\rho \notin \mathcal{P}_{4k} \vee (\rho \notin \mathcal{P} \setminus \mathcal{P}_k)) \geq 1 - \exp(n^{-s})$.*

Proof: Notice that in general $\Pr(C \mid B_1 \vee B_2 \vee \dots \vee B_k) \leq \max_j \Pr(C \mid B_j)$, so if $h := \cup_{i \in F} \{A_i\}$, it suffices to construct a suitable μ_{glo} which besides (ii) has

$\Pr(C \mid \wedge_{i \in F} A_i \in \rho) \geq \Pr(C \mid (\wedge_{i \in G} A_i \in \rho) \wedge (\wedge_{j \in F \setminus G} \text{Set}(\rho) \cap A_j = \emptyset))$ for any $G \subseteq F$. Let $A := \wedge_{i \in F} (A_i \in \rho)$, $B := \wedge_{i \in G} (A_i \in \rho) \wedge (\wedge_{i \in F \setminus G} (A_i \cap \text{Set}(\rho) = \emptyset))$, $C \equiv C(\rho)$, and for $l = 0, 1, 2, \dots$, let $D_l := \{ \rho \mid |\rho| = l \}$. Let $p_l := \Pr(D_l)$, and let $g := |G|$. We choose μ_{glo} symmetric on each each set $\{ \rho : D_l \}$. We define μ_{glo} by choosing suitable numbers p_0, p_1, \dots, p_u with $\sum_j p_j = 1$. Notice that any μ_{glo} defined this way, for any $l = |h| - g, |h| - g + 1, \dots, u$ has $\Pr(C \mid A \wedge D_l) \geq \Pr(C \mid B \wedge D_{l-|h|+g})$. To see this notice that any monotone property C can be written as a disjunction $\vee_{\delta} (\delta \subseteq \rho)$. We have to show that $\Pr(C \mid A) \geq \frac{1}{8} \cdot \Pr(C \mid B)$ for a suitable choice of p_0, p_1, \dots . For $l < l_0$ let $p_{l+1} := 2^{\frac{1}{t}} p_l$. For $l_0 \leq l$ let $p_{l+1} := 2^{-\frac{1}{t}} p_l$. Now $\min_l (\frac{p_{l+t}}{p_l}) = \min_l (\frac{p_l}{p_{l+t}}) = \frac{1}{2}$.

Notice that $\Pr(D_l \mid A) = \Pr(D_l \mid |\rho| \geq |h|)$. For $l \geq |h|$ a rough estimate shows that $\frac{1}{2} \cdot p_l < \Pr(D_l \mid A) < 2 \cdot p_l$. A similar estimate shows that $\frac{1}{2} \cdot p_l < \Pr(D_l \mid B) < 2 \cdot p_l$ when $l < n - |h| + g$. Now $|h| - g \leq t$ so

$$\begin{aligned} \Pr(C \mid A) &= \sum_l [\Pr(C \mid A \wedge D_l) \cdot \Pr(D_l \mid A)] \geq \sum_l [\Pr(C \mid B \wedge D_{l-|h|+g}) \cdot \frac{1}{2} \Pr(D_l)] \\ &\geq \sum_l [\Pr(C \mid B \wedge D_{l-|h|+g}) \cdot \frac{1}{4} \Pr(D_{l-|h|+g})] \geq \sum_l [\Pr(C \mid B \wedge D_{l-|h|+g}) \cdot \frac{1}{8} \Pr(D_{l-|h|+g} \mid B)]. \end{aligned}$$

Thus $\Pr(C \mid A) \geq \frac{1}{8} \cdot \Pr(C \mid B)$ and (i) holds. Furthermore notice that if $(n - pl_0)^k \geq n > (n - pl_0)^{k-1}$ then the probabilities are sufficiently concentrated around l_0 to ensure that (ii) is satisfied. \square

The factor $\frac{1}{8}$ can be replaced by any standard rational $q < 1$. Also notice that there are many other choices of the distribution p_0, \dots, p_u . One can for instance choose the binomial distribution with a suitable mean l_0 . The point is that $\min_l (\frac{p_{l+t}}{p_l}) \cdot \min_l (\frac{p_l}{p_{l+t}})$ is not too small, while at the same time the probability distribution tails off sufficiently fast.

Notice that a phenomenon reminiscent of the complementary principle, is involved. If μ_{glo} is focussed on some \mathcal{P}_k then (i) cannot hold. On the other hand if μ_{glo} is unfocussed and global (ii) cannot hold. As an example of the first claim consider the property $C(\rho) := \exists \delta (|\delta| = l_0 - |h| + 1 \wedge \text{Set}(\delta) \cap \text{Set}(h) = \emptyset \wedge \delta \subseteq \rho)$. If $p_{l_0} = 1$ (and $p_j = 0$ for $j \neq l_0$) then $\Pr(C \mid |h| \subseteq \rho) = 0$ while $\Pr(C \mid |h| \mid \rho \wedge \neg(h \subseteq \rho)) = 1$. This is a violation of condition (i).

Corollary 2.5.3 For $k \geq 2p + 1$, $k \in \mathbb{N}$ and $t < n^{\frac{1}{\omega}}$ there exists a \mathbb{M} -definable probability distribution μ on \mathcal{P}_{4k} , such that

- (1) for each $h \in \mathcal{P}$ with $|h| < t$, $\Pr(h \subseteq \rho) > n^{\frac{1}{2}} \cdot \Pr(h \parallel \rho \wedge \neg(h \subseteq \rho))$,
- (2) for each monotone property $C(\rho)$
 $\Pr(C(\rho) \vee \rho \notin \mathcal{P}_{2k} \mid h \parallel \rho) \geq \frac{1}{8} \cdot \Pr(C(\rho) \vee \rho \notin \mathcal{P}_{2k} \mid h \parallel \rho \wedge \neg(h \subseteq \rho))$.

Proof: Let μ be the (normalised) probability distribution obtained by restricting μ_{glo} to \mathcal{P}_{4k} . By (2) in lemma 2.5.2 μ approximates μ_{glo} very well (with a factor standardly close to 1). For (1) combine this with lemma 2.5.1. For (2) combine it with lemma 2.5.2 with $C(\rho)$ replaced by the monotone property $C(\rho) \vee \rho \notin \mathcal{P}_{2k}$. \square

We need the following elementary fact:

Lemma 2.5.4 For each number w , $\Pr(A \mid B \wedge C) \geq w \cdot \Pr(A \mid B)$ if and only if $\Pr(C \mid A \wedge B) \geq w \cdot \Pr(C \mid B)$.

Proof: Both sides holds iff $\Pr(A \wedge B \wedge C)\Pr(B) \geq w \cdot \Pr(A \wedge B)\Pr(B \wedge C)$. \square

Corollary 2.5.5 If μ is chosen on \mathcal{P}_{4k} such that condition (1) and (2) in corollary 2.5.3 hold, then

$$\Pr(h^j \subseteq \rho \vee \rho \notin \mathcal{P}_{2k} \mid h^j \parallel \rho \wedge (\rho \perp h^1) \wedge \dots \wedge (\rho \perp h^{j-1})) \geq \frac{1}{8} \cdot \Pr(h^j \subseteq \rho \mid h^j \parallel \rho).$$

Proof: Let $A := (h^j \subseteq \rho)$, $B := h^j \parallel \rho$ and let $C := (\rho \perp h^1) \wedge \dots \wedge (\rho \perp h^{j-1}) \vee \rho \notin \mathcal{P}_{2k}$. The lemma now follows by applying lemma 2.5.4 to condition (2) in corollary 2.5.3. \square

2.6 Collapse of circuits

In order to prove the key lemma (lemma 2.4.1) we prove that:

Lemma 2.6.1 Suppose that $\theta := \neg(\bigvee_{h \in \mathcal{H}} h)$ where $s(\theta) \leq n^t$ for some $t < n^{\frac{1}{\omega}}$. Let $s < n^{\frac{1}{\omega}}$. Suppose that μ is a probability distribution satisfying (1) and (2) in corollary 2.5.3 on \mathcal{P}_{4k} for some $k \geq 2p + 1$, $k \in \omega$. Then there exists an \mathbb{M} -definable set $\mathcal{C} \subseteq \mathcal{P}_{4k}$ such that $\mathcal{C} \subseteq \{\rho \in \mathcal{P}_{4k} : \exists \tilde{\mathcal{H}} \subseteq \mathcal{P}, \|\tilde{\mathcal{H}}\| \leq ps \text{ such that } \theta \equiv_{\rho} \bigvee_{h \in \tilde{\mathcal{H}}} h \text{ with } s(\bigvee_{h \in \tilde{\mathcal{H}}} h) \leq n^t\}$ and such that

$$\mu(\mathcal{C}) \geq 1 - \left(\frac{1}{n}\right)^{\frac{ks-2ps}{2k}}$$

Corollary 2.6.2 Let $\epsilon_1, \epsilon_2, \dots, \epsilon_u$ be an \mathbb{M} -definable sequence of depth $\leq d$ circuits with $\Sigma_j s(\epsilon_j) \leq n^t$ for some $t < n^{\frac{1}{\omega}}$. Let $\rho_0 \in \mathcal{P}$. There exists $\rho \supseteq \rho_0$, $\rho \in P$ and an \mathbb{M} -definable sequence $\epsilon'_1, \dots, \epsilon'_u$ of depth $\leq d - 1$ (when $d \geq 3$) circuits, with $\Sigma_j s(\epsilon'_j) \leq n^t$ such that $s(\epsilon'_j) \leq s(\epsilon_j)$ $j = 0, 1, 2, \dots$. When $d = 2$ there exists an \mathbb{M} -definable sequence $\epsilon'_1, \epsilon'_2, \dots, \epsilon'_u$ of depth ≤ 2 circuits of the form $\epsilon'_j := \bigvee_{h \in \mathcal{H}_j} h$. Furthermore, each set $\mathcal{H}_j \subseteq \mathcal{P}$ contains conditions h which have all $|\text{Set}(h)| \leq ps$ for some s with $s > \omega \cdot t$, and $s < n^{\frac{1}{\omega}}$.

Proof: (lemma 2.6.1 \Rightarrow corollary 2.6.2). By use of lemma 2.3.7 we can assume $\epsilon_1, \epsilon_2, \dots, \epsilon_u$ are all negation-free. There is an M-definable sequence $\tilde{\epsilon}_1, \dots, \tilde{\epsilon}_u$ of depth $\leq d - 1$ circuits, where all ‘input nodes’ are depth ≤ 2 circuits. Let $\pi_1, \pi_2, \dots, \pi_r$ be the M-definable sequence of these. Clearly $r \leq n^t$. Without loss of generality, each π_j is either a ‘disjunction of conjunctions’ or is a ‘conjunction of disjunctions’. Notice $\sum_j s(\pi_j) < n^t$. According to the Scaling down phenomena (lemma 2.3.13) lemma 2.6.1 also holds when the underlying set I is replaced by $I' := I \setminus \text{Set}(\rho_0)$. So for some fixed $k \geq 2p + 1$, for each $j \leq r$ there exists an M-definable sequence $\mathcal{C}_1, \dots, \mathcal{C}_r \subseteq \mathcal{P}_k$ each with

$$\mu(\mathcal{C}_j) \geq 1 - \left(\frac{1}{n - |\text{Set}(\rho)|} \right)^{\frac{ks-2ps}{2k}}$$

such that for $j = 1, 2, \dots, r$ and all $\rho \in \mathcal{C}_j$ $\pi_j \equiv_\rho \bigvee_{h \in H'} h$ if π_j is a disjunction of conjunctions, and $\pi_j \equiv_\rho \neg(\bigvee_{h \in H'} h)$ if π_j is a conjunction of disjunctions.

Now $\mu(\mathcal{C}_1 \cap \mathcal{C}_2 \cap \dots \cap \mathcal{C}_r) \geq 1 - r \cdot \left(\frac{1}{n}\right)^{\frac{ks-2ps}{2k}} > 0$ (when $s \geq 2kt$). So there exists $\rho \in \mathcal{C}_1 \cap \dots \cap \mathcal{C}_r$ with $\rho \supseteq \rho_0$. Replace each depth ≤ 2 ‘input circuit’ with a suitable depth ≤ 2 circuit. \square

Repeated use of this corollary (applied at most d times) reduces problem of proving the key lemma to that of proving lemma 2.6.1.

2.7 The switching lemma

Definition 2.7.1 For $i \in I$ let

$$\mathcal{E}_i(h) := \{h' : h' \supseteq h \wedge \text{Set}(h') \supseteq \text{Set}(h) \cup \{i\} \wedge |h'| \leq |h| + 1\}. \quad \clubsuit$$

Definition 2.7.2 We say that $\mathcal{H}_2 \subseteq \mathcal{P}$ is an *atomic tree-like refinement* of $\mathcal{H}_1 \subseteq \mathcal{P}$, ($\mathcal{H}_1 \rightarrow_{\text{ATR}} \mathcal{H}_2$) if $\exists h \in \mathcal{H}_1 \exists i \in I \mathcal{H}_2 = (\mathcal{H}_1 \cup \mathcal{E}_i(h)) \setminus \{h\}$.

We say that $\tilde{\mathcal{H}}$ is a *tree-like refinement* of \mathcal{H} , ($\mathcal{H} \rightarrow_{\text{TR}} \tilde{\mathcal{H}}$) if there exists an M-definable sequence $(\mathcal{H}_0, \mathcal{H}_1, \dots, \mathcal{H}_r)$ such that $\mathcal{H}_0 = \mathcal{H}$, $\mathcal{H}_r = \tilde{\mathcal{H}}$ and such that $\mathcal{H}_j \rightarrow_{\text{ATR}} \mathcal{H}_{j+1}$ for each $j < r$. \clubsuit

Definition 2.7.3 $\mathcal{B} \subseteq \mathcal{P}$ is a *tree-like basis* if $\{\emptyset\} \rightarrow_{\text{TR}} \mathcal{B}$. \clubsuit

Lemma 2.7.4 Suppose that $\mathcal{B} \subseteq \mathcal{P}$ is M-definable and that $\|\mathcal{B}\| < n^t$ for some fixed $t < \frac{1}{\omega}$. If \mathcal{B} is a tree-like basis, then \mathcal{B} is a basis for \mathcal{P} .

Proof: First we show that $\forall \alpha, \beta \in \mathcal{B} \alpha \neq \beta \rightarrow \alpha \perp \beta$. If $\mathcal{B} = \emptyset$ there is nothing to prove. Suppose that $\mathcal{B} := (\mathcal{B}' \cup \mathcal{E}_i(h)) \setminus \{h\}$ and that $\forall \alpha, \beta \in \mathcal{B}' \alpha \neq \beta \rightarrow \alpha \perp \beta$. For $\alpha \in \mathcal{B}' \setminus \{h\}$ and $\beta \in \mathcal{E}_i(h)$ (which implies $\beta \supseteq h$) clearly $\alpha \perp \beta$. For $\alpha, \beta \in \mathcal{E}_i(h)$ we must have $\alpha \neq \beta \rightarrow \alpha \perp \beta$. Thus $\forall \alpha, \beta \in \mathcal{B} \alpha \neq \beta \rightarrow \alpha \perp \beta$.

Second we show $\forall \rho \in \mathcal{P} \exists \beta \in \mathcal{B} \rho \parallel \beta$. Suppose contrarily that $\rho_0 \in \mathcal{P}$ is incompatible with all $\beta \in \mathcal{B}$. Let $(\mathcal{B}_0, \dots, \mathcal{B}_r)$ be an M-definable sequence with $\mathcal{B}_0 := \{\emptyset\}$, $\mathcal{B}_r := \mathcal{B}$ and where $\mathcal{B}_j \rightarrow_{\text{ATR}} \mathcal{B}_{j+1}$ for $j = 0, 1, \dots, r - 1$. M satisfies the least number principle so there must be a smallest j_0 such that ρ_0 is incompatible with all $\beta \in \mathcal{B}_{j_0}$. There exists $\beta' \in \mathcal{B}_{j_0-1}$ compatible with ρ_0 . As $|\text{set}(\beta')| \leq n^{\frac{1}{\omega}}$ by lemma 2.3.12 $\rho = \rho_0 \cup \beta' \in \mathcal{P}$. Let $i_0 \in I$ such that $\mathcal{B}_{j_0} = (\mathcal{B}_{j_0-1} \cup \mathcal{E}_{i_0}(\beta'')) \setminus \{\beta''\}$.

Now $\rho \supseteq \rho_0$ (like ρ_0) must be incompatible with all conditions in \mathcal{B}_{j_0} , $\beta' \notin \mathcal{B}_{j_0}$ and thus $\beta' = \beta''$. We get the required contradiction by noticing that $\rho \in \mathcal{P}$ must be compatible with some $\beta''' \in \mathcal{E}_{i_0}(\beta') \subseteq \mathcal{B}_{j_0}$. \square

Definition 2.7.5 For $\mathcal{H} \subseteq \mathcal{P}$ and for $\rho \in \mathcal{P}$ let

$\mathcal{H}^\rho := \{h' \in \mathcal{P}(I \setminus \text{Set}(\rho)) : h' = h \setminus \rho \text{ for some } h \in \mathcal{H} \text{ with } h \parallel \rho\}$. We say that \mathcal{B} refines \mathcal{H} if for each $\beta \in \mathcal{B}$ and each $h \in \mathcal{H}$ if $\beta \parallel h$, there is $h' \in \mathcal{H}$ such that $h' \subseteq \beta$.

For $h, \rho \in \mathcal{P}$ we define the restriction $h^\rho \in \mathcal{P}(I \setminus \text{Set}(\rho))$ as $h \setminus \rho$ if $h \parallel \rho$ and let it be undefined if $h \perp \rho$. \clubsuit

Lemma 2.7.6 If \mathcal{B} is a basis which refines \mathcal{H} , and $\mathcal{H}_\mathcal{B} := \{\beta \in \mathcal{B} : \exists h \in \mathcal{H} \beta \supseteq h\}$ then $\bigvee_{h \in \mathcal{H}} h \equiv_\emptyset \bigvee_{\beta \in \mathcal{H}_\mathcal{B}} \beta$.

Proof: First notice that for any generic $\tilde{\rho}_G$ there exists $\beta_0 \in \mathcal{B}$ such that $\tilde{\rho}_G \supseteq \beta_0$. This is because $\mathcal{D} := \{\rho \in \mathcal{P} : \exists \beta \in \mathcal{B} \rho \supseteq \beta\}$ is both quasi-definable and dense. According to definition 2.7.5 \mathcal{B} refines \mathcal{H} so $\exists h \in \mathcal{H} h \parallel \beta_0$ if and only if $\exists h \in \mathcal{H} \beta_0 \supseteq h$. Thus $(\bigvee_{h \in \mathcal{H}} h)^{\tilde{\rho}_G} = 1 \Leftrightarrow \exists h \in \mathcal{H} \tilde{\rho}_G \supseteq h \Leftrightarrow \tilde{\rho}_G \supseteq \beta_0 \wedge \exists h \in \mathcal{H} \tilde{\rho}_G \supseteq h \Leftrightarrow \tilde{\rho}_G \supseteq \beta_0 \wedge (\exists h \in \mathcal{H} \tilde{\rho}_G \supseteq h \wedge h \parallel \beta_0) \Leftrightarrow \tilde{\rho}_G \supseteq \beta_0 \wedge \exists h \in \mathcal{H} \beta_0 \supseteq h \Leftrightarrow \tilde{\rho}_G \supseteq \beta_0 \wedge \beta_0 \in \mathcal{H}_\mathcal{B} \Leftrightarrow (\bigvee_{\beta \in \mathcal{H}_\mathcal{B}} \beta)^{\tilde{\rho}_G} = 1 \quad \square$

Lemma 2.7.7 Let $\mathcal{H} \subseteq \mathcal{P}$ be a M-definable collection of conditions with $\|\mathcal{H}\| \leq n^t$ for some fixed $t < n^{\frac{1}{\omega}}$. Let $\rho_0 \in \mathcal{P}_k$, $k \in \omega$, and let μ be a probability distribution on $\mathcal{P}_{4l}(I \setminus \text{Set}(\rho_0))$ (for some $l \in \omega$ with $l \geq 2p + 1$) which satisfies the conditions in corollary 2.5.3.

If $\rho \in \mathcal{P}_{4l}(I \setminus \text{Set}(\rho_0))$ is chosen randomly according to the probability distribution μ , then for each $s < n^{\frac{1}{\omega}}$, with probability $\geq 1 - \left(\frac{1}{n - |\text{Set}(\rho_0)|}\right)^{\frac{ks - 2ps}{2k}}$ there exists a tree-like basis \mathcal{B} which refines \mathcal{H}^ρ such that $\|\mathcal{B}\| \leq ps$.

This lemma immediately implies lemma 2.6.1. To see this fix $s < n^{\frac{1}{\omega}}$ and let $\mathcal{C} := \{\rho : \exists \mathcal{B} \text{ a tree-like basis which refines } \mathcal{H} \text{ and } \|\mathcal{B}\| \leq ps\}$. Notice that \mathcal{C} is M-definable. According to lemma 2.7.6, the θ in lemma 2.6.1, has $\theta \equiv_\rho \bigvee_{h \in \mathcal{H}_\mathcal{B}} h$ where $\mathcal{H}_\mathcal{B} := \{\beta \in \mathcal{B} : \exists h \in \mathcal{H} \beta \supseteq h\}$. Thus to show the key lemma (lemma 2.4.1) it suffices to show lemma 2.7.7.

2.8 Some games involving forcing

As above assume \mathbb{M} to be a countable non-standard model. Assume also that $p \in \mathbb{N} \setminus \{1\}$ and $I := \{1, 2, \dots, n\} \subseteq \mathbb{M}$, with $n \in \mathbb{M} \setminus \omega$ be fixed. Let $\mathcal{P}_1 \subseteq \mathcal{P}_2 \subseteq \dots \subseteq \mathcal{P}_r \subseteq \dots \subseteq \mathcal{P}$, $r \in \omega$, be the stratification of the set \mathcal{P} of forcing conditions defined in definition 2.2.2. Our aim is to show lemma 2.7.7.

The idea is similar to the one developed by J.Krajicek, P.Pudlak and A.Wood [15]. It also bears a resemblance to some ideas by T.Pitassi, P.Beame and R.Impagliazzo [19]. I define a two person game with full information. I then show that any winning strategy for player I are very useful in collapsing formulas (essentially the content of lemma 2.8.3). To show that player I actually have a winning strategy I show (in the spirit of [15]) that any randomly picked strategy with high probability guarantee player I a win (theorem 2.8.4). The probabilistic estimates are simplified by considering a different (but similar) game (theorem 2.8.6, lemma 2.8.7 and lemma 2.8.8). Lemma 2.7.7 follows by combining lemma 2.8.3 with theorem 2.8.4.

Definition 2.8.1 Suppose that $t \leq s$ where $s < n^{\frac{1}{\omega}}$ (e.g. t, s are small) and let $\langle h^1, h^2, \dots, h^v \rangle \in \mathbb{M}$, $v \in \mathbb{M}$ be a sequence of conditions with $|\text{Set}(h^j)| \leq t$, $j \leq v$. Suppose also that $\{h^1, h^2, \dots, h^v\}$

is complete for \mathcal{P} (i.e. $\forall \rho \in \mathcal{P} \exists j \leq v \rho \parallel h^j$). The game $G(n, k, t, s, \langle h^1, h^2, \dots, h^v \rangle)$ is played by two players I and II as follows:

Round 0: Player I selects a condition $\rho \in \mathcal{P}_k$.

Round 1: Consider the first $i \leq v$ where $h_1 := h^i$ is compatible with ρ (which exists because the collection $\{h^1, \dots, h^v\}$ is assumed to be complete for \mathcal{P}).

If $\rho \supseteq h_1$ player I wins and the *output* of the game is \emptyset .

If $\text{Set}(h_1) \setminus \text{Set}(\rho) \neq \emptyset$ let $a_1 := \min(\text{Set}(h_1) \setminus \text{Set}(\rho)) \in I$. Player II selects an p -element set $A \subseteq I$ such that:

- (1) $\{A\}$ is compatible with ρ ($\{A\} \parallel \rho$).
- (2) either (2a) or (2b),
 - (2a) $\{A\}$ is incompatible with h_1 ($\{A\} \perp h_1$),
 - (2b) $\{A\}$ is compatible with h_1 ($\{A\} \parallel h_1$).
- (3) $a_1 \in A$.

In case of (2b) the game terminates. The *output* of the game is any $\delta_1 \ni A$ where $\forall B \in \delta_1 B \cap \text{Set}(h_1) \neq \emptyset$ and $\text{Set}(h_1) \subseteq \text{Set}(\delta_1)$.

In case of (2a) let $\delta_1 := \{A\}$ and proceed to the next round.

Round $j+1$: Consider the next condition $h_{j+1} := h^{i_{j+1}}$, $i_{j+1} > i_j$ compatible with $\rho \cup \delta_j$ (according to lemma 2.3.12 such exists because $\rho \cup \delta_j \in \mathcal{P}$ when $j \leq s$, and $\{h^1, \dots, h^v\}$ is complete for \mathcal{P}).

If $\rho \cup \delta_j \supseteq h_{j+1}$ player I wins and the *output* of the game is δ_j .

If $\text{Set}(h_{j+1}) \setminus \text{Set}(\rho) \neq \emptyset$ let $a_{j+1} := \min(\text{Set}(h_{j+1}) \setminus \text{Set}(\rho)) \in I$. Player II selects a p -element set $A \subseteq I$ such that:

- (1) $A \cap \text{Set}(\rho) = \emptyset$.
- (2) either (2a) or (2b),
 - (2a) $\{A\}$ is incompatible with h_{j+1} .
 - (2b) $\{A\}$ is compatible with h_{j+1} .
- (3) $a_{j+1} \in A$.

In case of (2b) the game terminates. The *output* of the game is any $\delta_{j+1} \ni A$ where $\forall B \in \delta_{j+1} B \cap \text{Set}(h_{j+1}) \neq \emptyset$ and $\text{Set}(h_{j+1}) \subseteq \text{Set}(\delta_{j+1})$.

In case of (2a) let $\delta_{j+1} := \delta_j \cup \{A\}$, and proceed to the next round.

Round $s+1$: If this round is reached, player II wins and the game is terminated. ♣

Notice that player I does not influence the game after the choice of ρ . The strategies of player I can thus be identified with the conditions in \mathcal{P}_k .

Definition 2.8.2 We call $\rho \in \mathcal{P}_k$ a *winning strategy* for player I, if player wins irrespectively of what player II chooses. ♣

Lemma 2.8.3 Suppose that $\mathcal{H} = \mathcal{H}_0 \cup \mathcal{H}_1$ is complete for \mathcal{P} (i.e. suppose that $\forall \rho \in \mathcal{P} \exists h \in \mathcal{H} \rho \parallel h$). Suppose that $\mathcal{H}_0 := \{h^1, \dots, h^u\}$ and $\mathcal{H}_1 := \{h^{u+1}, \dots, h^v\}$, $u \leq v \in \mathbb{M}$. Consider the game $G(n, k, t, s, \langle h^1, h^2, \dots, h^v \rangle)$, and suppose that $\rho \in \mathcal{P}_k$ is a winning strategy for player I. Let \mathcal{B} be the set of possible outputs (when player II varies his/her possible plays). Then \mathcal{B} is a tree-like basis in $\mathcal{P}(I \setminus \text{Set}(\rho))$. Furthermore, \mathcal{B} refines \mathcal{H}_0^ρ and has $\|\mathcal{B}\| \leq ps$.

Proof: We are given a winning strategy ρ for player I. We have to show that \mathcal{B} is a tree-like basis. We view each δ constructed at a certain stage in an actually played game, as a (uniquely defined) ‘situation’. Let $S(\delta)$ denote the situations which can be reached from δ . We want to construct \mathcal{B} as a sequence

$$\{\emptyset\} \rightarrow_{ATR} \mathcal{B}_1 \rightarrow_{ATR} \dots \rightarrow_{ATR} \mathcal{B}_j \rightarrow_{ATR} \mathcal{B}_{j+1} \rightarrow \dots \rightarrow \mathcal{B}.$$

Suppose that \mathcal{B}_j has been constructed. Pick any situation δ' which has not been reached so far, but which can be reached from a situation corresponding to a $\delta \in \mathcal{B}_j$ which has already been considered. Let $\mathcal{B}_{j+1} := (\mathcal{B}_j \cup \mathcal{E}_a(\delta)) \setminus \{\delta\}$ where $a := \min(\text{Set}(h) \setminus \text{Set}(\rho))$. Here h denotes the next h^i compatible with ρ in the situation corresponding to δ . As ρ was assumed to be a winning strategy for player I, this procedure terminates, and all $\beta \in \mathcal{B}$ get $|\text{Set}(\beta)| \leq ps$.

Finally we show that \mathcal{B} refines \mathcal{H}_0^ρ . We have to show that if $h \parallel \beta$ for some $h \in \mathcal{H}_0^\rho$ and $\beta \in \mathcal{B}$, then there exists $h' \in \mathcal{H}_0^\rho$ such that $h' \subseteq \beta$. So suppose β is compatible with $(h^j)^\rho \in \{(h^1)^\rho, (h^2)^\rho, \dots, (h^u)^\rho\}$. If the game terminated when considering this h^j clearly $\beta \supseteq (h^j)^\rho$ and we are done. If the did terminate for another $h^{j'}$ the game which produced β , must have terminated before h^j and so $j' < j$. This is only possible if $(h^{j'})^\rho \subseteq \beta$. As the sequence $h^1, h^2, \dots, h^u, h^{u+1}, \dots, h^v$ had all the elements from \mathcal{H}_0 listed in the beginning, $(h^{j'})^\rho \in \mathcal{H}_0^\rho$. \square

The next theorem shows that almost all (in the sense of μ) strategies ρ are winning strategies for player I. More specifically:

Theorem 2.8.4 *Consider the game $G(n, k, t, s, \langle h^1, h^2, \dots, h^v \rangle)$. Let $\mathcal{W}_I \subseteq \mathcal{P}_{4k}$ be the set of winning strategies for player I (we only consider M-definable strategies). If μ is a probability distribution on \mathcal{P}_{4k} which satisfies condition (1) and (2) in corollary 2.5.3, then*

$$\mu(\mathcal{W}_I) \geq 1 - \left(\frac{1}{n}\right)^{\frac{ks-2ps}{2k}}.$$

Notice that t does not enter the estimate as long as $t < n^{\frac{1}{w}}$.

We show theorem 2.8.4 by comparing the game $G(n, k, t, s, \langle h^1, h^2, \dots, h^v \rangle)$ with another game $G'(n, k, t, s)$.

Definition 2.8.5 The game $G'(n, k, t, s)$ is played by two players I and II as follows (all sets etc. are M-definable).

Player II selects $J \subseteq I$, with $|J| \leq ps$, and selects a sequence h^1, h^2, \dots, h^l of conditions each with $\text{Set}(h^i) \subseteq I \setminus J$, and $|\text{Set}(h^i)| \leq t$.

Player I then selects a condition $\rho \in \mathcal{P}_k$. Consider the first condition $h := h^j$ compatible with ρ (if there is no such player I wins). If $h \subseteq \rho$ player I wins, otherwise player II wins. \clubsuit

In this game player II makes the choices before player I. Clearly player I always has a winning reply (just choose $\rho \supseteq h^1$). We claim almost all player I’s replies are winning:

Theorem 2.8.6 *Let $\tilde{\mathcal{W}}_I(\tau)$ be the set (M-definable) of replies ρ which ensure a win for player I after player II made a choice τ . Then if μ is a probability distribution which satisfies condition (1) and (2) in corollary 2.5.3,*

$$\mu(\tilde{\mathcal{W}}_I(\tau)) \geq 1 - \left(\frac{1}{n}\right)^{\frac{1}{2}}.$$

Proof: First notice

$$\mu(\tilde{\mathcal{W}}_I(\tau)) \geq \min_j \Pr(h^j \subseteq \rho \mid h^j \parallel \rho \wedge \rho \perp h^1 \wedge \dots \wedge \rho \perp h^{j-1}).$$

According to lemma 2.5.4 and condition (2) in corollary 2.5.3 for any j

$$\Pr(h^j \subseteq \rho \mid h^j \parallel \rho \wedge (\rho \perp h^1) \wedge \dots \wedge (\rho \perp h^{j-1})) \geq \Pr(h^j \subseteq \rho \mid h^j \parallel \rho)$$

(let $A \equiv (h^j \subseteq \rho)$, $B \equiv h^j \parallel \rho$ and $C \equiv \rho \perp h^1 \wedge \dots \wedge \rho \perp h^{j-1}$). But by condition (1) in corollary 2.5.3

$$\Pr(h^j \subseteq \rho \mid h^j \parallel \rho) = \frac{\Pr(h^j \subseteq \rho)}{\Pr(h^j \subseteq \rho) + \Pr(h^j \parallel \rho \wedge \neg(h^j \subseteq \rho))} \geq 1 - \left(\frac{1}{n}\right)^{\frac{1}{2}}. \quad \square$$

Lemma 2.8.7 *Suppose that μ satisfies condition (1) and (2) in corollary 2.5.3.*

Let $w = \max_\tau(\mu(\tilde{\mathcal{W}}_I(\tau)))$. Then for each strategy v of player II in the first game

$$\mu(\tilde{\mathcal{W}}_I(v)) \geq 1 - (1 - w)^s \geq 1 - \left(\frac{1}{n}\right)^{\frac{s}{2}}.$$

Proof: The task for player II to survive round 1 of the game $G'(n, k, t, s)$ (if player I selects the reply ρ randomly) is “easier” than the task of surviving any specific round j of the game $G(n, k, t, s, \langle h^1, h^2, \dots, h^v \rangle)$. More formally the probability $\Pr(\text{survives round } k \mid \text{history of the game})$ is

$$\geq \min_j \Pr(h^j \subseteq \rho \mid h^j \parallel \rho \wedge (\rho \perp h^1) \wedge \dots \wedge (\rho \perp h^{j-1})) \geq \min_j \Pr(h^j \subseteq \rho \mid h^j \parallel \rho). \quad \square$$

Lemma 2.8.8

$$\mu(\mathcal{W}_I) \geq 1 - (\Sigma_v(\mu(\tilde{\mathcal{W}}_I(v)))) \geq 1 - \left(\frac{1}{n}\right)^{\frac{s}{2}} \cdot n^{\frac{ps}{k}} \geq 1 - \left(\frac{1}{n}\right)^{\frac{ks-2ps}{2k}} > 0$$

when $k \geq 2p + 1$.

Proof: The number of strategies for player II in the first game is $\leq n^{\frac{ps}{k}}$. □

This completes the proof of theorem 2.8.4. Lemma 2.7.7 follows by combining lemma 2.8.3 and theorem 2.8.4.

2.9 Some consequences

Suppose that \mathbf{M} is a countable non-standard model of $\text{Th}(\mathbf{N})$ in some countable first order language L . Suppose L extends the language of Arithmetic. Let $p \geq 2$, $p \in \omega$ and let $n \in \mathbf{M} \setminus \omega$. Assume that n not is divisible by p . Let L_P be the L extended by an unspecified p -ary relation symbol P . Let

$$\mathbf{M}_n^* := \{m \in \mathbf{M} : t(n) > m \text{ for some term } t \in L\}.$$

So far we are able to prove:

Theorem 2.9.1 (weak version) *If all terms $t \in L$ have sub-exponential growth rate, then for each generic filter ρ_G $(\mathbf{M}_n^*, \tilde{\rho}_G) \models \neg \text{Count}(p)$. On the other hand $(\mathbf{M}_n^*, \tilde{\rho}_G)$ satisfies induction for bounded L_P -formulas. As above $\tilde{\rho}_G := \cup_{\alpha \in \rho_G} \alpha$.*

In the next two sections I strengthen this result. I show that the the model $(\mathbf{M}_n^*, \tilde{\rho}_G)$ satisfies the $\text{Count}(q)$ principle exactly when certain exceptional forests do not exists.

Proof: (Outline) The argument is very similar to the argument in [2] so we only outline the argument.

It suffices to show that the least number principle is valid for bounded L_P -formulas with parameters in \mathbf{M}_n^* . Now translate each instance of the least number principle into a Boolean circuit of the form $\text{LNP}_u(\pi_1, \pi_2, \dots, \pi_u) := \pi_u \vee (\bigvee_{j \leq u} (\neg \pi_j \wedge (\bigwedge_{k < j} \pi_k)))$. According to the general collapsing result from section 1, each π_j can be replaced (and this can be done simultaneously) by disjunction of small positive conjunctions (or by negations of disjunctions of small positive conjunctions). According to the key lemma (lemma 2.4.1) for any generic filter ρ_G if $(\pi_u)^{\tilde{\rho}_G} = 0$ there exists $j_0 \leq u$ with $(\pi_{j_0})^{\tilde{\rho}_G} = 0$ and with $(\pi_j)^{\tilde{\rho}_G} = 1$ for all $j < j_0$. A simple argument shows that $\text{LNP}_u(\pi_1, \dots, \pi_u)^{\tilde{\rho}_G} = 1$. But then according to lemma 2.1.6 $(\mathbf{M}_n^*, \tilde{\rho}_G)$ must satisfies induction for bounded L_P -formulas with parameters in \mathbf{M}_n^* . \square

3 Forests of decision trees

The specially labelled trees we are going to consider can also be viewed as decision trees. In our case the decisions concern a (hypothetical) partitioning of a finite set $I := \{1, 2, \dots, n\}$ into disjoint p element subsets. To avoid meaningless statements we always assume that n is larger than p times the height of the trees. All trees are rooted and finite (in later parts of the argument “finite” in the sense of a non-standard model of first order Arithmetic). When we follow a branch from the root towards the leafs we make successive decisions building up (parts of) some mathematical object. In this case (which we refer to as an (p, n) -labelling) the mathematical object is a partitioning of I into disjoint p -element subsets. At each vertex v , except at the leafs, there is assigned a “question” $i_v \in I$. At the vertex v we are asked to decide which p element subset $A \subseteq I$ the element i_v belongs to. All possible answers which concerning the partitioning at i_v have to be represented. Thus we require that there is a one to one correspondence between possible answers (at i_v) and the sons from i_v . The label α of a branch is identified with the final object (here a partial partitioning) which has been constructed.

Suppose that we are given a forest T_1, T_2, \dots, T_u of decision trees. If each object (label on branch) appears 0 modulo q times, does q divide u ? If there exists a global object (in this case when p divides n) the answer is always positive (as illustrated by theorem 3.1.3).

This type of problem has not previously been considered in the literature. For almost any mathematical structure, it is possible to define such decision trees. They specify the local diagrams. In section 6 our analysis naturally leads us to consider another type of decision trees. Now let us focus on (p, n) -labelled trees as just defined. Notice first that each (p, n) -labelled tree is a graphical representation of a tree-like basis. Because of this, the concepts from section 2 (like *conditions* and *restrictions*) will keep their obvious meaning.

Our aim is show that we have the following characterisation.

Theorem: Let $q, p \geq 2$ and $h \in \mathbb{N}$. Suppose that $h > q$. Then the following statements always hold simultaneously.

- (a) All prime factors in p divide q .
- (b) There exists n_0 such that for all $n > n_0$ which are not divisible by p there is a (p, n) -labelled forest T_1, T_2, \dots, T_u such that:
 - (i) All trees have height $\leq h$.
 - (ii) Each type of branch appears 0 modulo q times.
 - (iii) $u \neq 0$ modulo q .

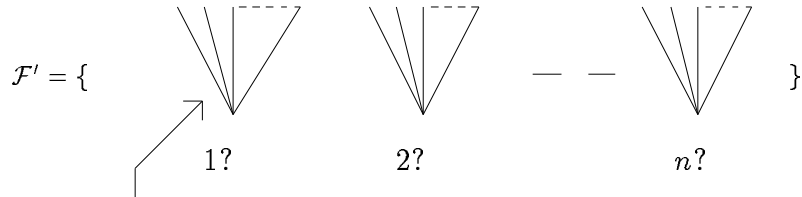
Later we also discuss the general case where there are less restrictions on the (asymptotic) height of the trees.

3.1 Some easy results

First let me illustrate the definition with a few trivial examples and observations.

A subdivision argument shows that $\text{Count}(p)$ always holds in models in which $\text{Count}(rp)$ holds. According to my analysis (section 4) this *a priori* ensures the existence of a forests T_1, \dots, T_u of (p, n) -labelled trees where each branch appears 0 modulo q times, but where $u \neq 0$ modulo q .

Example 3.1.1 Suppose that $q = rp$ and that p does not divide n . Consider the forest \mathcal{F} which contains r copies of the (p, n) -labelled trees:



An edge for each of the $\binom{n-1}{p-1}$ possible answers.

Each branch of the form $\{\{i_1, i_2, \dots, i_p\}\}$ appears in each of the r copies of the trees $i_1?, i_2?, \dots, i_p?$. Thus each such branch appears in exactly rp ($=0$ modulo q) trees. However the forest \mathcal{F} contains rn trees which $\neq 0$ modulo q (when $n \neq 0$ modulo p).

Example 3.1.2 Another trivial example arises when q divides p and $n \neq 0$ modulo q . In this case the forest $\mathcal{F} := \mathcal{F}'$ contains n (p, n) -labelled trees ($\neq 0$ modulo q) trees. Each branch appears exactly p ($=0$ modulo q) times. This example corresponds to the fact that $\text{Count}_n(uq)$ (where $n \neq 0$ modulo q) holds in the same models as $\text{Count}(q)$.

The type of forests in these two examples are so simple that we do not consider them as exceptional.

Here are two easy cases where there are no exceptional forests.

Theorem 3.1.3 Suppose that p divides n . Suppose that T_1, T_2, \dots, T_u is a (p, n) -labelled forest where each branch appears 0 modulo q times. Then $u = 0$ modulo q .

Proof: According to the assumption p divides n so there exists a partitioning ρ_{global} of $\{1, 2, \dots, n\}$ into disjoint sets $A_1, A_2, \dots, A_{\frac{n}{p}} \subseteq \{1, 2, \dots, n\}$ each containing p elements. The partition ρ_{global} extends exactly one branch from each tree. Clearly, ρ_{global} allows us to define a partitioning of the trees T_1, T_2, \dots, T_u into disjoint classes each containing exactly q trees. \square
Using a similar idea we notice

Theorem 3.1.4 *Suppose that T_1, T_2, \dots, T_u is a forest of (p, n) -labelled trees. Suppose that the sum of the heights of all trees is smaller than $\frac{n}{p}$. If all branches appear 0 modulo q times, then $u = 0$ modulo q .*

Proof: Select a branch $\beta_1 := \alpha_1$ from the tree T_1 . The branch must be compatible with at least one branch $\alpha_2 \in T_2$. Let $\beta_2 := \beta_1 \cup \alpha_2$. This branch (=condition) must be compatible to at least one branch $\alpha_3 \in T_3$. Eventually we construct a condition ρ which extends exactly one branch in each tree. \square

One can try to elaborate on this type of argument. A (very naive) strategy is to try to choose short branches from each tree. It is not hard to see that this method breaks down when $u > n$.

In [23] I presented a graph theoretical argument. I developed this argument in cooperation with P.Pudlak. It used a generalisation of a well-known theorem from graph theory. This theorem states that if in a graph G all vertex have degree at least as large as $\frac{1}{2} \cdot |G_{\text{vertex}}|$, then G contains a Hamiltonian circuit. This type of argument breaks down even when u is significantly smaller than n^2 . This illustrates that the main difficulty is to understand the cases where u is large compared to n . Early in this research it was clear that even the cases where $u < n^2$ have considerable depth.

It was also clear that results relevant for Bounded Arithmetic all would require techniques which at least would be able to deal (when n tends to infinity) with the case where $u > n^k$ for arbitrarily fixed k .

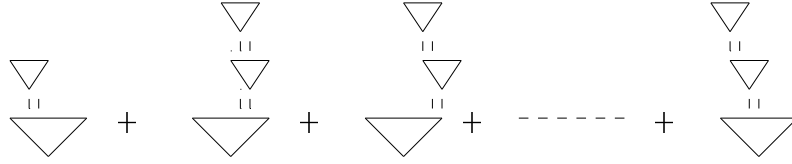
3.2 Breaking down trees

Let T be a (p, n) -labelled tree. Consider the following equation which holds modulo q .

$$\begin{array}{c} T_1 \quad T_2 \quad \dots \quad T_v \\ \parallel \quad \parallel \quad \dots \quad \parallel \\ \triangle \\ T_0 \end{array} = \begin{array}{c} T_1 \\ \parallel \\ \triangle \\ T_0 \end{array} + \begin{array}{c} T_2 \\ \parallel \\ \triangle \\ T_0 \end{array} + \dots + \begin{array}{c} T_v \\ \parallel \\ \triangle \\ T_0 \end{array} + \underbrace{\begin{array}{c} \triangle \\ T_0 \end{array} + \dots + \begin{array}{c} \triangle \\ T_0 \end{array}}_{1 - v \text{ modulo } q \text{ copies of } T_0}$$

Notice that both sides of the equation contains 1 modulo q tree. Also that each branch appears the same number of times (modulo q) on each side of the equation.

Suppose that $\mathcal{F} := \{T_1, \dots, T_u\}$ is any forest. Repeated application of the identity allows us to break down the trees in \mathcal{F} . Eventually all trees can be brought on a normal form of the following type:



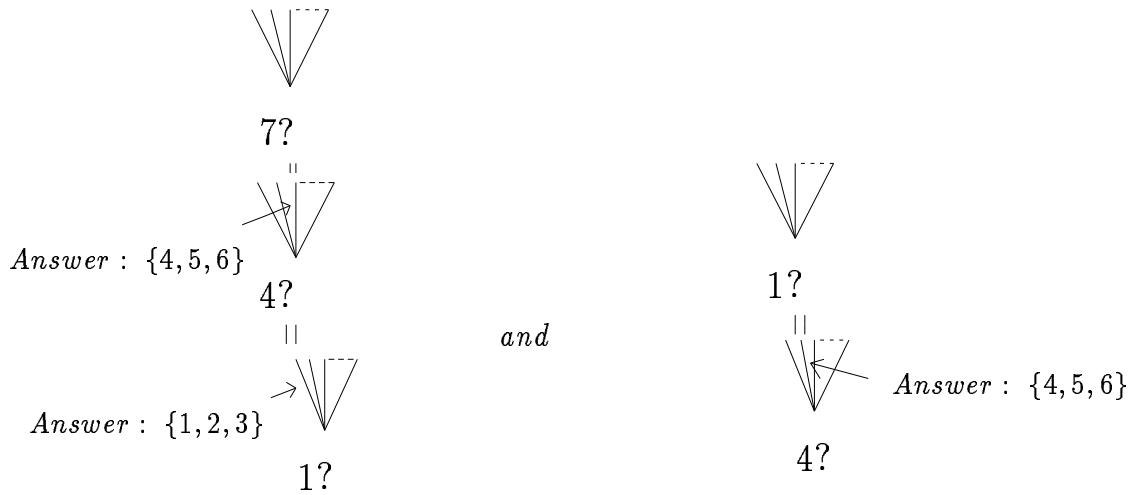
Let us call such trees *perfectly unbalanced* (=PU). Clearly we have,

Lemma 3.2.1 Fix $q \geq 2$, $q \in \mathbb{N}$. Let $\mathcal{F} := \{T_1, \dots, T_u\}$ be any forest. There exists a forest $\mathcal{F}' := \{T'_1, T'_2, \dots, T'_{u'}\}$ in which each (type of) branch counted modulo q appears the same number of times as in \mathcal{F} . Each tree in \mathcal{F}' is a PU-tree and furthermore the number u' of trees in \mathcal{F}' equals (modulo q) the number u of trees in the forest \mathcal{F} .

Notice that the PU-trees have a very simple representation. Each PU-tree can in a canonical fashion be represented by expressions of the form,

$(u_{1,1}, \{u_{1,2}, \dots, u_{1,p}\})(u_{2,1}, \{u_{2,2}, \dots, u_{2,p}\}) \dots (u_{h-1,1}, \{u_{h-1,2}, \dots, u_{h-1,p}\})(u_h)$,
 where $u_{i,j} \in I$.

Example 3.2.2 The PU-trees



have the representation

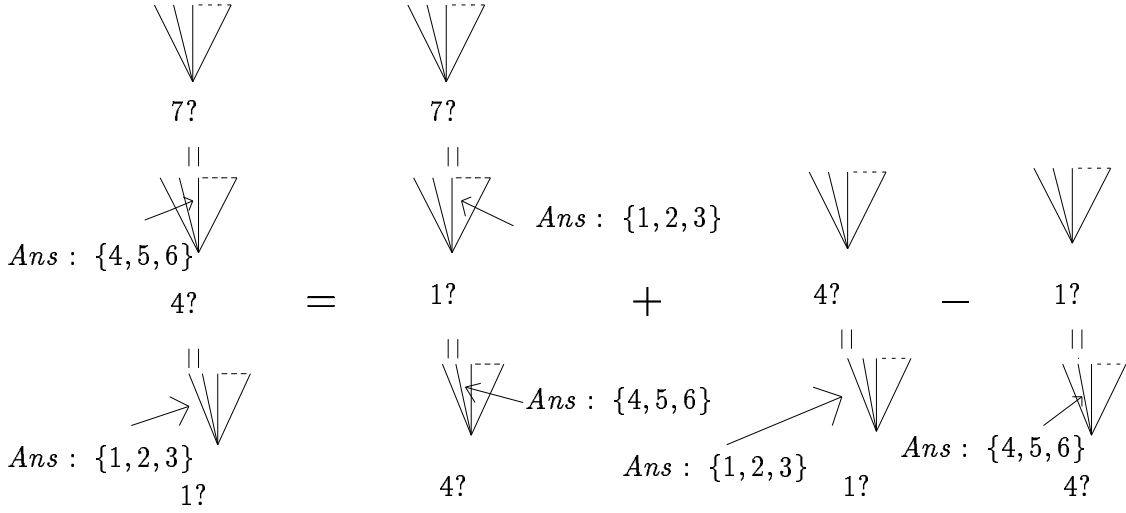
$$(1, \{2, 3\})(4, \{5, 6\})(7) \quad \text{and} \quad (4, \{5, 6\})(1)$$

3.3 Bringing the forest on normal form

It turns out that there are various useful identities between collections of PU-trees.

Example 3.3.1 Consider the PU-trees $T := (4, \{5, 6\})(1, \{2, 3\})(7)$ and $T' := (1, \{2, 3\})(4, \{5, 6\})(7)$. Notice that T and T' contain the same branches of length 3. The branch $\beta := \{\{1, 2, 3\}, \{4, 5, 6\}\}$ does not appear in T and T' . Except for the branch β the tree T contains the same branches of length ≤ 2 as the tree $(4, \{5, 6\})(1)$. Also, except for the branch β the tree T' contains the same branches of length ≤ 2 at the tree $(1, \{2, 3\})(4)$.

This can be expressed by the equation,



or equivalent in our more compact notation by the equation,

$$(1, \{2, 3\})(4, \{5, 6\})(7) = (4, \{5, 6\})(1, \{2, 3\})(7) + (1, \{2, 3\})(4) - (4, \{5, 6\})(1).$$

The equation expresses the fact that both sides of the identity contain 1 tree (counted with signs). And it expresses the fact that both sides contain exactly the same set of branches.

Here is another identity.

Example 3.3.2 $(2, \{1, 3\})(4) = (1, \{2, 3\})(4) - (1) + (2).$

The identities from the examples can be expressed generally.

Lemma 3.3.3 *We have the following identities.*

$$(1) \quad (w_1, W_1)(w_2, W_2) \dots (b, B)(a, A) \dots (w_h) = (w_1, W_1)(w_2, W_2) \dots (a, A)(b, B) \dots (w_h) - (w_1, W_1)(w_2, W_2) \dots (a) + (w_1, W_1)(w_2, W_2) \dots (b).$$

$$(2) \quad (w_1, W_1)(w_2, W_2) \dots (a_2, \{a_1, a_3, \dots, a_p\}) \dots (w_h) = (w_1, W_1) \dots (a_1, \{a_2, a_3, \dots, a_p\}) \dots (w_h) - (w_1, W_1) \dots (a_2) + (w_1, W_1) \dots (a_1).$$

The equations gives high flexibility in ordering the elements below the top-level. Repeated use of the equations gives the following lemma.

Lemma 3.3.4 *Let $\mathcal{F}' := \{T'_1, \dots, T'_u\}$ be a forest where all trees are PU-trees. Then there exist a forest $\mathcal{F}'' := \{T''_1, \dots, T''_u\}$ where all trees are of the form*

$$(u_{1,1}, \{u_{1,2}, \dots, u_{1,p}\}) \dots (u_{i,1}, \{u_{i,2}, \dots, u_{i,p}\}) \dots (u_h)$$

where $u_{1,1} < u_{2,1} < \dots < u_{h-1,1}$, and where $u_{i,1} < u_{i,2} < \dots < u_{i,p}$ for $i = 1, 2, \dots, h-1$. Furthermore,

- (i) The forests \mathcal{F}' and \mathcal{F}'' contain the same number of trees (modulo q).
- (ii) Each (type of) branch appears the same number (modulo q) of times in the forests \mathcal{F}' and \mathcal{F}'' .

We will come back to this normal form later.

4 The first main result

4.1 Reducing the count(p) versus Count(q) problem

Suppose that \mathbf{M} is a countable non-standard model of $\text{Th}(\mathbf{N})$ over a countable first order language L , which extends the language of Arithmetic. Suppose that $p \geq 2$ and $I := \{1, 2, \dots, n\} \subseteq \mathbf{M}$ for some $n \in \mathbf{M} \setminus \omega$. Assume that n is not divisible by p . As above, let $\mathbf{M}_n^* := \{m \in \mathbf{M} : t(n) > m, \text{ for some term } t \in L\}$. Let $L_{\mathbf{M}_n^*}(P)$ be L extended with a constant c_a for each $a \in \mathbf{M}_n^*$ together with an p -ary relation symbol P .

Theorem 4.1.1 (Main result) *Suppose that all terms $t \in L$ have sub-exponential growth rate. Then for each generic filter ρ_G (see definition 2.2.5),*

- (a) $(\mathbf{M}_n^*, \tilde{\rho}_G) \models \neg \text{Count}(p)$.
- (b) $(\mathbf{M}_n^*, \tilde{\rho}_G)$ satisfies induction for bounded $L_{\mathbf{M}_n^*}(P)$ -formulas.
- (c) $(\mathbf{M}_n^*, \tilde{\rho}_G)$ satisfies (all versions of) the pigeon-hole principle for bounded $L_{\mathbf{M}_n^*}(P)$ -formulas.

Furthermore, there exists a sequence $s_k(x), k \in \omega$ of (arithmetical) functions (which depend on the exact growth rate of the terms in L), such that (under the harmless extra assumption that the underlying language L might need an extension) the following are equivalent:

- (i) $(\mathbf{M}_n^*, \tilde{\rho}_G)$ satisfies the Count(q) principle.
- (ii) Each forest T_1, T_2, \dots, T_u of (p, n) -labelled trees in which all trees have height $\leq s_k(n)$ for some $k \in \omega$ and in which each branch appears 0 modulo q times, has $u = 0$ modulo q .
- (iii) As (ii) but for (p, n) -labelled PU-trees.

Suppose that all terms in L have (at most) polynomial growth rate. Then $s_k(x) := k$ gives the required characterisation.

In general $s_k(x)$ can be chosen such that $(s_k(n))^l < n$ for all $l \in \mathbf{N}$.

Our overall question is when systems of Bounded Arithmetic extended by an axiom scheme for the Count(q) principle, are able to prove Count(p). The first main result, links this to an understanding of the structure of exceptional forests. Furthermore, it shows that the asymptotic height of the trees in the minimal exceptional forests is directly linked to the strength of the underlying axiom system.

We have already proved (a) and (b). The implication (iii) \Rightarrow (ii) follows immediately from lemma 3.2.1. To show (i) \Rightarrow (iii) assume that there is a forest \mathcal{F} which violates (iii). Assume that the language contains a suitable relation symbol which allows us to define the forest and a partitioning of each type of branches into disjoint q -element subsets by a Bounded formula (this is the harmless extra assumption). I claim that the Count(q) principle fails in $(\mathbf{M}_n^*, \tilde{\rho}_G)$. To see this, notice that there is a Bounded L_P -formula with parameters in \mathbf{M}_n^* which defines (by use of $\tilde{\rho}_G$) a partitioning of the trees in the forest \mathcal{F} . And this in such a way that each class contains exactly q trees. But by assumption \mathcal{F} contains trees T_1, T_2, \dots, T_u for some u with $u \neq 0$ modulo q .

The implication (ii) \Rightarrow (i) is difficult. As it turns out our proof of (c) provides a first step in showing this implication.

Lemma 4.1.2 *Suppose that for some $a \in \mathbf{M}_n^*$, some bounded $L_{\mathbf{M}_n^*}(P)$ -formula $\theta(\cdot, \cdot)$ defines a bijection from a to b . Let $\rho_0 \in \rho_G$ be given. Then there exist \mathbf{M} -definable sequences $\mathcal{H}_{i,j}$ and $\mathcal{B}_{i,j}$, $(i, j) \in a \times b$ such that for some $\rho \supseteq \rho_0$, $\rho \in \mathcal{P}$:*

- (i) *for all $(i, j) \in a \times b$, $\mathcal{B}_{i,j}$ is a tree-like basis for $\mathcal{P}(I \setminus \text{Set}(\rho))$,*
- (ii) *for all $(i, j) \in a \times b$, $\|\mathcal{B}_{i,j}\| \leq t$ for some fixed $t < n^{\frac{1}{\omega}} = (n - |\text{Set}(\rho)|)^{\frac{1}{\omega}}$.*
- (iii) *for all $(i, j) \in a \times b$, $\mathcal{H}_{i,j} \subseteq \mathcal{B}_{i,j}$,*
- (iv) *for each $i_0 \leq a$: $\mathcal{B}_{i_0}^{\rightarrow} := \bigcup_{j \leq b} \mathcal{H}_{i_0,j}$ is a basis for $\mathcal{P}(I \setminus \text{Set}(\rho))$,*
- (v) *for each $j_0 \leq b$: $\mathcal{B}_{j_0}^{\downarrow} := \bigcup_{i \leq a} \mathcal{H}_{i,j_0}$ is a basis for $\mathcal{P}(I \setminus \text{Set}(\rho))$.*

Proof: Suppose that some Bounded $L_{\mathbf{M}_n^*}(P)$ -formula $\theta(\cdot, \cdot)$ defines a bijection from $h : \{1, 2, \dots, a\}$ onto $\{1, 2, \dots, b\}$ for $a \neq b$. According to lemma 2.1.5 there exists $d \in \omega$ and $t \in \mathbf{M}_n^*$ and a \mathbf{M} -definable sequence of circuits $\theta_{i,j} (i, j) \in a \times b$, such that each $(\theta_{i,j})^{\tilde{\rho}_G} = 1$ exactly when $(\mathbf{M}, \tilde{\rho}_G) \models \theta(i, j)$ (by lemma 2.1.6). That is exactly when $(\mathbf{M}_n^*, \tilde{\rho}_G) \models \theta(i, j)$ because θ is bounded and thus downward persistent. Now according to the key lemma (lemma 2.4.1) there exists $\rho \supseteq \rho_0$, $\rho \in \mathcal{P}$, an \mathbf{M} -definable sequence $\mathcal{B}_{i,j} (i, j) \in a \times b$ where each $\mathcal{B}_{i,j}$ is a tree-like basis, and an \mathbf{M} -definable sequence $\mathcal{H}_{i,j} \subseteq \mathcal{B}_{i,j} (i, j) \in a \times b$ such that for each $(i, j) \in a \times b$: $\theta_{i,j} \equiv_{\rho} \bigvee_{h \in \mathcal{H}_{i,j}} h$.

We claim that the sequences $\mathcal{B}_{i,j}$ and $\mathcal{H}_{i,j}$ satisfy (i)-(v). By use of the fact that h is an injective function it is straightforward to show that for each $i \leq a$ the conditions in $\mathcal{B}_i^{\rightarrow}$ must be pairwise incompatible. The fact that h is a (mono-valued) function ensures that for each $j \leq b$ the conditions in $\mathcal{B}_j^{\downarrow}$ are pairwise incompatible.

The only problem is to show that each $\mathcal{B}_i^{\rightarrow}$ and each $\mathcal{B}_j^{\downarrow}$ are complete for $\mathcal{P}(I \setminus \text{Set}(\rho))$ (see definition 2.5.3). We can simplify the notation by assuming that $\rho = \emptyset$. This simplification is possible by the scaling down lemma (lemma 2.3.13) which allows us to replace I by $I \setminus \text{Set}(\rho)$.

Suppose that $\rho' \in \mathcal{P}$ is incompatible with all conditions in $\mathcal{B}_i^{\rightarrow}$ for some fixed $i \leq a$. Let ρ_G be a generic filter (without the simplification we assume $\rho_G \ni \rho$). Now for each $j \leq b$, $\tilde{\rho}_G$ is incompatible with all conditions in $\mathcal{H}_{i,j}$, so by use of lemma 2.3.14 $\theta_{i,j}^{\tilde{\rho}_G} = 0$ for all $j \leq b$. This is in contradiction with lemma 2.3.4 which ensures that \emptyset (or ρ in the un-simplified case) forces h to be total i.e. to take a value $j \leq b$.

The completeness of the conditions in each $\mathcal{B}_j^{\downarrow}$ follows by use of the assumption that h was forced onto. \square

4.2 Using a combinatorial phenomenon

At this stage our aim is to show that (i)-(v) in lemma 4.1.2 can be only satisfied when $a = b$. First we show

Lemma 4.2.1 *Suppose that for some $a, b \in \mathbf{M}_n^*$ there exist \mathbf{M} definable sequences $\mathcal{B}_{i,j}$ and $\mathcal{H}_{i,j} (i, j) \in a \times b$. Furthermore suppose they satisfy condition (i)-(iii) in lemma 4.1.2 as well as:*

- (iv)' *For each $i_0 \leq a$: $\mathcal{B}_{i_0}^{\rightarrow} := \bigcup_{j \leq b} \mathcal{H}_{i_0,j}$ is a tree-like basis.*
- (v)' *For each $j_0 \leq b$: $\mathcal{B}_{j_0}^{\downarrow} := \bigcup_{i \leq a} \mathcal{H}_{i,j_0}$ is a tree-like basis.*

Then $a = b$.

Proof: First, notice that we can assume that all conditions $h, h' \in \mathcal{H}_{i,j}$ have $|h| = |h'|$. Otherwise make suitable tree-like refinements. Second, notice that \mathcal{P} (the set of forcing conditions), has the property that the number $N(n, p, c)$ of conditions in a tree-like basis where all conditions h have $|h| = c$, only depends on n, p and c . Now $ac = \sum_{i \leq a} |\mathcal{B}_i^\rightarrow| = \sum_{i \leq a, j \leq b} |\mathcal{H}_{i,j}| = \sum_{j \leq b} |\mathcal{B}_j^\downarrow| = bc$, so $a = b$. \square

Suppose that we could replace “is a basis for \mathcal{P} ” with “is a tree-like basis” in lemma 4.1.2. Then according to lemma 4.2.1 this would ensure that the pigeon-hole principle could never be forced false. So if a basis \mathcal{B} for \mathcal{P} in general would be tree-like, we would be done. Unfortunately, the reality is more complex.

Example 4.2.2 (By J. Krajicek)

The converse of lemma 2.7.4 does not hold in general.

The collection $\mathcal{B} := \{\{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, i\}, \{2, j\}, \{3, k\}\}_{i,j,k \geq 4 \wedge |\{i,j,k\}|=3}$ is a basis for \mathcal{P} . However \mathcal{B} is not a tree-like basis (there is no $i_0 \in I$ such that all $\beta \in \mathcal{B}$ has $i_0 \in \text{Set}(\beta)$).

Observation 4.2.3 *Consider example 4.2.2. Let $\mathcal{B}' := (\mathcal{B} \cup \mathcal{E}_1(\{\{2, 3\}\}) \setminus \{\{2, 3\}\})$, so $\mathcal{B} \rightarrow_{\text{TR}} \mathcal{B}'$. Notice that \mathcal{B}' is a tree-like basis. To see this, notice that \mathcal{B}' can be obtained from $\{\emptyset\}$ by the atomic tree-like refinements based on:*

$$\begin{aligned} & \mathcal{E}_1(\emptyset), \\ & \mathcal{E}_2(\{1, 4\}), \mathcal{E}_2(\{1, 5\}), \dots, \mathcal{E}_2(\{1, n\}), \\ & \mathcal{E}_3(\{\{1, 4\}, \{2, 5\}\}), \mathcal{E}_3(\{\{1, 4\}, \{2, 6\}\}), \dots, \mathcal{E}_3(\{\{1, 4\}, \{2, n\}\}), \\ & \mathcal{E}_3(\{\{1, 5\}, \{2, 4\}\}), \mathcal{E}_3(\{\{1, 5\}, \{2, 6\}\}), \dots, \mathcal{E}_3(\{\{1, 5\}, \{2, n\}\}), \\ & \dots \\ & \mathcal{E}_3(\{\{1, n\}, \{2, 4\}\}), \mathcal{E}_3(\{\{1, n\}, \{2, 5\}\}), \dots, \mathcal{E}_3(\{\{1, n\}, \{2, n-1\}\}). \end{aligned}$$

This observation is part of a general phenomenon. It turns out (and this was one of the combinatorial discoveries which made my general approach possible), that any basis \mathcal{B} for \mathcal{P} has a tree-like refinement to a tree-like basis.

Lemma 4.2.4 *Assume that \mathcal{B} is a basis for \mathcal{P} , and that $u \in I$. Then there exists a tree-like refinement \mathcal{B}' of \mathcal{B} such that for all $\beta' \in \mathcal{B}'$ $u \in \text{Set}(\beta')$.*

Proof: Let $\mathcal{B}' := \cup_{\beta \in \mathcal{B}} (\mathcal{E}_u(\beta) \setminus \{\beta\})$. Notice that this is actually a tree-like refinement of \mathcal{B} , and that \mathcal{B}' has the required properties. \square

Definition 4.2.5 For $U \subseteq I$, we let \mathcal{C}_U denote the tree-like basis

$\{\alpha : \forall A \in \alpha \exists u \in U u \in A \wedge \text{Set}(\alpha) \supseteq U\}$. We say \mathcal{B} is a *tree-like basis on $U \subseteq I$* if for each $\alpha \in \mathcal{C}_U$, there exists $\beta \in \mathcal{B}$ with $\beta \supseteq \alpha$. \clubsuit

Lemma 4.2.6 *Suppose that \mathcal{B} is a basis for \mathcal{P} , and $U \subseteq I$ with $|U| < n^{\frac{1}{\omega}}$. There is a tree-like refinement \mathcal{B}' of \mathcal{B} , such that \mathcal{B}' is a tree-like basis on U .*

Proof: Let $U = \{u_1, u_2, \dots, u_r\}$. According to lemma 4.2.4 there exists a sequence $\mathcal{B} = \mathcal{B}_0 \rightarrow_{\text{TR}} \mathcal{B}_1 \rightarrow_{\text{TR}} \dots \rightarrow_{\text{TR}} \mathcal{B}_r$, such that for all $\beta \in \mathcal{B}_j$ $u_j \in \text{Set}(\beta)$. Let $\mathcal{B}' := \mathcal{B}_r$. We have to show that for each $\alpha \in \mathcal{C}_U$ there exists $\beta \in \mathcal{B}'$, $\beta \supseteq \alpha$. Now by use of a calculation similar to the one in the proof of lemma 2.3.12, \mathcal{B}' is a basis for \mathcal{P} , so each $\alpha \in \mathcal{C}_U$ is compatible with some $\beta \in \mathcal{B}'$. Now as $\text{Set}(\beta) \supseteq U$ actually $\beta \supseteq \alpha$. \square

Lemma 4.2.7 *Suppose that $\|\mathcal{B}\| \leq t$ for some $t < n^{\frac{1}{w}}$. Also suppose that the conditions in \mathcal{B} are pairwise incompatible. Then \mathcal{B} is a basis for \mathcal{P} if and only if each condition $\rho \in \mathcal{P}_1$ is compatible with some $\beta \in \mathcal{B}$.*

Proof: Repeated application of lemma 4.2.6. \square

Lemma 4.2.8 *If \mathcal{B} is a basis for \mathcal{P} , and $\|\mathcal{B}\| \leq t$ for some $t < n^{\frac{1}{w}}$, then there exists a tree-like basis $\tilde{\mathcal{B}}$ such that $\|\tilde{\mathcal{B}}\| < pt(t+1)$ and such that $\mathcal{B} \rightarrow_{\text{TR}} \tilde{\mathcal{B}}$.*

Proof: First we construct $\tilde{\mathcal{B}}'$. Pick a set $V \subseteq I$ such that $V := \text{Set}(\beta)$ for some $\beta \in \mathcal{B}$. According to lemma 4.2.6 there exists a tree-like refinement \mathcal{B}_1 of \mathcal{B} such that \mathcal{B}_1 is tree-like on V . Now fix $\gamma \in \mathcal{C}_V$ and consider $\mathcal{B}_1^\gamma \subseteq \mathcal{P}(I \setminus V)$. It is not hard to show \mathcal{B}_1^γ is a basis for $\mathcal{P}(I \setminus V)$. Now by use of lemma 4.2.7 we notice that we can prove the lemma by use of induction after t inside \mathbb{M} . This is because we according to lemma 4.2.7 can replace \mathcal{P} (which not is \mathbb{M} -definable) by the \mathbb{M} -definable set \mathcal{P}_1 .

Let $\mathcal{B}_1(\gamma) := \{\beta : \beta' \cap \gamma = \beta, \beta' \in \mathcal{B}_1^\gamma\}$. Notice that $\mathcal{B}_1(\gamma)$ is a tree-like refinement of γ . Finally let $\tilde{\mathcal{B}} := \cup_\gamma \mathcal{B}_1(\gamma)$. By induction after t we have $\|\tilde{\mathcal{B}}\| \leq |\text{Set}(\gamma)| + p(t-1)t$. Now $|\text{Set}(\gamma)| \leq pt$, from which the required inequality follows. \square

In our applications lemma 4.2.8 can strictly speaking be avoided. Instead we can ‘hit’ \mathcal{B} by a randomly chosen condition ρ . Now *a priori* the claim must hold with probability exponentially close to 1. More specifically the proof of lemma 2.8.3 shows that for a randomly chosen ρ with high probability there exists a tree-like basis $\tilde{\mathcal{B}}$ (in $\mathcal{P}(I \setminus \text{Set}(\rho))$) which is a tree-like refinement of \mathcal{B}^ρ . Lemma 4.2.8 shows more than this. It shows that there exist such extensions for an arbitrary basis \mathcal{B} with absolute certainty (and not just in the probabilistic sense when \mathcal{B} is hit by a random restriction).

We actually use a two-dimensional version of lemma 4.2.8.

Lemma 4.2.9 *Suppose that there exists an \mathbb{M} -definable “generic system”. That is a sequence $\mathcal{H}_{i,j}$, $(i,j) \in a \times b$ such that:*

- (i) *For each $i \leq a$ $\mathcal{B}_i^{\rightarrow} := \cup_{j \leq b} \mathcal{H}_{i,j}$ is a basis for \mathcal{P} .*
- (ii) *For each $j \leq b$ $\mathcal{B}_j^{\downarrow} := \cup_{i \leq a} \mathcal{H}_{i,j}$ is a basis for \mathcal{P} .*
- (iii) *$\max_{(i,j) \in a \times b} \|\mathcal{H}_{i,j}\| \leq t$ for some $t < n^{\frac{1}{w}}$.*

Then there exists an \mathbb{M} -definable “tree-like generic system”. That is a sequence $\tilde{\mathcal{H}}_{i,j}$ $(i,j) \in a \times b$ such that:

- (i)' *For each $i \leq a$ $\tilde{\mathcal{B}}_i^{\rightarrow} := \cup_{j \leq b} \tilde{\mathcal{H}}_{i,j}$ is a tree-like basis.*
- (ii)' *For each $j \leq b$ $\tilde{\mathcal{B}}_j^{\downarrow} := \cup_{i \leq a} \tilde{\mathcal{H}}_{i,j}$ is a tree-like basis.*
- (iii)' *$\max_{(i,j) \in a \times b} \|\tilde{\mathcal{H}}_{i,j}\| \leq p^3(t+1)^4$.*

Proof: Fix $i \leq a$. According to lemma 4.2.8 there exists a tree-like refinement $\mathcal{B}'_i \rightarrow$ of $\mathcal{B}_i \rightarrow$, which is a tree-like basis. For each $j \leq b$ this procedure induces a tree-like refinement $\mathcal{H}'_{i,j}$ of $\mathcal{H}_{i,j}$. This way we get an M-definable sequence $\mathcal{H}'_{i,j}$, $(i,j) \in a \times b$, so (i)', (ii) and $\|\mathcal{H}'_{i,j}\| \leq pt(t+1)$.

Now fix $j \leq b$. Again according to lemma 4.2.8 there exists a tree-like refinement $\tilde{\mathcal{B}}_j^{\downarrow}$ of $\mathcal{B}_j^{\downarrow}$, which is a tree-like basis. For each $i \leq a$ this procedure induces a tree-like refinement $\tilde{\mathcal{H}}_{i,j}$ of $\mathcal{H}'_{i,j}$. Now notice that $\tilde{\mathcal{B}}_i \rightarrow$ remains tree-like basis, and thus the M-definable sequence $\tilde{\mathcal{H}}_{i,j}$, $(i,j) \in a \times b$ satisfies (i)', (ii)'. Clearly also (iii)' holds because $\|\tilde{\mathcal{H}}_{i,j}\| \leq p(pt(t+1)+1)(pt(t+1)) \leq p^3(t+1)^4$. \square

This immediately shows (c) in theorem 4.1.1, in the case of the bijective pigeon-hole principle. The other versions of the pigeon-hole principle are treated with minor changes.

4.3 The hard implication

The implication (ii) \Rightarrow (i) in theorem 4.1.1 follows by the same type of argument.

Lemma 4.3.1 *Suppose that $\theta(x_1, x_2, \dots, x_q)$ is a bounded $L(P)$ -formula with q free variables, and all its parameters in $(\mathbf{M}_n^*, \tilde{\rho}_G)$. Suppose that θ defines a partition of $I_a := \{1, 2, \dots, a\}$, $a \in \mathbf{M}_n^*$ into disjoint q -element subsets ($a \neq 0$ modulo q). Then there exists an M-definable map $A \rightarrow \mathcal{H}_A$, which to each q -subset A of I_a assigns a collection of conditions $\mathcal{H}_A \subseteq \mathcal{P}$ such that for some $t < n^{\frac{1}{q}}$, $\max_A(\|\mathcal{H}_A\|) \leq t$. Furthermore, for each $v \in I_a$, $\mathcal{B}_v := \cup_{A \subseteq I_a, |A|=q, v \in A} \mathcal{H}_A$ is a basis for \mathcal{P} .*

Proof: Suppose that some bounded $L(P)$ -formula $\theta(x_1, x_2, \dots, x_q)$ defines a partition of $\{1, 2, \dots, a\}$ into disjoint q -subsets, and q does not divide a . According to definition 2.1.5 and lemma 2.1.6 there exists $d \in \omega$, $t < n^{\frac{1}{q}}$ and an M-definable sequence of circuits θ_{v_1, \dots, v_q} , $v_1, \dots, v_q \in I_a$, such that $\theta_{i_1, \dots, i_q}^{\tilde{\rho}_G} = 1$ exactly when $(\mathbf{M}_n^*, \tilde{\rho}_G) \models \theta(i_1, \dots, i_q)$. Now according to the key lemma (lemma 2.4.1) there exists $\rho \supseteq \rho_0$ (for any given ρ_0), and an M-definable sequence $\mathcal{B}_{v_1, \dots, v_q}$, $v_1, \dots, v_q \in I_a$ where each $\mathcal{B}_{v_1, \dots, v_q} \subseteq \mathcal{P}$ is a (tree-like) basis with $\|\mathcal{B}_{v_1, \dots, v_q}\| \leq t$. Furthermore, there exists a M-definable sequence $\mathcal{H}_{v_1, v_2, \dots, v_q} \subseteq \mathcal{B}_{v_1, \dots, v_q}$ such that for each $v_1, \dots, v_q \in I_a$, $\theta_{v_1, v_2, \dots, v_q} \equiv_{\rho} \bigvee_{h \in \mathcal{H}_{v_1, v_2, \dots, v_q}} h$. Fix $v \in I_a$ and consider $\mathcal{B}_v := \cup_{A \subseteq I_a, v \in A} \mathcal{H}_A$. For $\alpha, \beta \in \mathcal{B}_v$, $\alpha \neq \beta$ we claim $\alpha \perp \beta$. To see this notice that otherwise there would exist $\rho \supseteq \alpha \cup \beta$, and $\rho \in \mathcal{P}$ would force both θ_{v_1, \dots, v_q} and $\theta_{v'_1, \dots, v'_q}$ true. Now $v \in \{v_1, \dots, v_q\} \cap \{v'_1, \dots, v'_q\}$ so this is only possible when $\{v_1, \dots, v_q\} = \{v'_1, \dots, v'_q\}$. Thus both α and β belong to $\mathcal{H}_{v_1, \dots, v_q} \subseteq \mathcal{B}_{v_1, \dots, v_q}$. As $\mathcal{B}_{v_1, \dots, v_q}$ is a (tree-like) basis it is orthogonal and $\alpha \perp \beta$.

It remains to show that \mathcal{B}_v , $v \in I_a$ is complete for $\mathcal{P}(\{1, 2, \dots, n\} \setminus \text{Set}(\rho_0))$. Assume for the simplicity of the notation that $\rho_0 = \emptyset$. According to the scaling down lemma (lemma 2.3.13) this assumption is harmless. We have to show that no $\rho \in \mathcal{P}$ is incompatible with all the conditions $h \in \mathcal{B}_v$. Now using lemma 2.3.14 each generic filter ρ_G contains some $h \in \mathcal{B}_{v_1, \dots, v_q}$ for each $v_1, v_2, \dots, v_q \in I_a$. But this contradicts the assumption that ρ_0 (in our case \emptyset) forces θ to define a total partition of I_a into disjoint q subsets. \square

We want to that $\text{Count}(q)$ is never forced false when p contains a prime factor which does not appear in q . To show this it suffices to show that if \mathcal{H}_A is an M-definable assignment as in lemma 4.3.1, then q must divide a . The following example shows that this trivially holds when $a \ll n$.

Example 4.3.2 *Suppose that $a \ll n$. Consider $I_a := \{1, 2, \dots, a\}$. Pick $\rho_1 \subseteq \rho_2 \subseteq \dots \subseteq \rho_a$ such that for each $v \leq a$ there is $\alpha_v \in \mathcal{B}_v$ such that $\alpha_v \subseteq \rho_v$. This is possible whenever $\rho_v \in \mathcal{P}$, $v =$*

$1, 2, \dots, a$ (which is the case when $a \ll n$). Notice that ρ_a induces an \mathbf{M} -definable partition of I_a into disjoint q -subsets. As \mathbf{M} shares its first order properties with \mathbf{N} this is only possible when q divides a .

A major step in solving the $\text{Count}(p)$ versus $\text{Count}(q)$ problem is to show that the conclusion in lemma 4.3.1 can be strengthened by replacing ‘each \mathcal{B}_v is a basis for \mathcal{P} ’, with ‘each \mathcal{B}_v to be a tree-like basis’.

Lemma 4.3.3 *Let $t < n^{\frac{1}{q}}, a \in \mathbf{M}$. Let \mathcal{P} be the set of forcing conditions (definition 2.2.2). Suppose that $A \rightarrow \mathcal{H}_A$ is an \mathbf{M} -definable map which assigns a collection of conditions $\mathcal{H}_A \subseteq \mathcal{P}$, to each q -subset A of $I_a = \{1, 2, \dots, a\}$ such that*

- (i) $\max_A(\|\mathcal{H}_A\|) \leq t$
- (ii) $\mathcal{B}_v := \cup_{A \subseteq I_a, |A|=q, v \in A} \mathcal{H}_A$ is a basis for \mathcal{P} ($v = 1, 2, \dots, a$).

Then there exists a \mathbf{M} -definable map $A \rightarrow \tilde{\mathcal{H}}_A$ which assigns a tree-like refinement $\tilde{\mathcal{H}}_A$ of \mathcal{H}_A , to each q -subset A of $I_a := \{1, 2, \dots, a\}$ such that

- (i)' $\max_A(\|\mathcal{H}_A\|) \leq qpt(t + 1)$.
- (ii)' $\tilde{\mathcal{B}}_v := \cup_{A \subseteq I_a, |A|=q, v \in A} \tilde{\mathcal{H}}_A$ is a tree-like basis ($v = 1, 2, \dots, a$).

As a first attempt of a proof consider the following argument. According to lemma 4.2.8 there exists a tree-like basis $\mathcal{B}_1^{(1)}$ which is a tree-like refinement of $\mathcal{B}_1 := \cup_{1 \in A} \mathcal{H}_A$. This refinement induces tree-like refinements $\mathcal{H}_A \rightarrow_{\text{TR}} \mathcal{H}_A^{(1)}$ for each $A \subseteq I_a, |A|=q$ (when $1 \notin A$, $\mathcal{H}_A^{(1)} = \mathcal{H}_A$). For each $v \in I_a$ let $\mathcal{B}_v^{(1)} := \cup_{v \in A} \mathcal{H}_A^{(1)}$.

Again by lemma 4.2.8 there exists a tree-like basis $\mathcal{B}_2^{(2)}$ which is a tree-like refinement of $\mathcal{B}_2^{(1)}$. This refinement induce a tree-like refinement $\mathcal{H}_A^{(1)} \rightarrow_{\text{TR}} \mathcal{H}_A^{(2)}$ for each $A \subseteq I_a, |A|=q$ (when $2 \notin A$, $\mathcal{H}_A^{(2)} = \mathcal{H}_A^{(1)}$). For each $v \in I_a$ let $\mathcal{B}_v^{(2)} := \cup_{v \in A} \mathcal{H}_A^{(2)}$.

Eventually (again using lemma 4.2.8) there exists a tree-like basis $\mathcal{B}_a^{(a)}$ which is a tree-like refinement of $\mathcal{B}_a^{(a-1)}$. This refinement induces a tree-like refinement $\mathcal{H}_A^{(a-1)} \rightarrow_{\text{TR}} \mathcal{H}_A^{(a)}$ for each $A \subseteq I_a, |A|=q$ (when $a \notin A$, $\mathcal{H}_A^{(a)} = \mathcal{H}_A^{(a-1)}$). For each $v \in I_a$ let $\mathcal{B}_v^{(a)} := \cup_{v \in A} \mathcal{H}_A^{(a)}$.

Let $\tilde{\mathcal{H}}_A := \mathcal{H}_A^{(a)}$. We claim that each $\tilde{\mathcal{B}}_v := \cup_{v \in A} \tilde{\mathcal{H}}_A$ is a tree-like basis. To see this notice $\tilde{\mathcal{B}}_v = \mathcal{B}_v^{(a)}$. By construction each $\mathcal{B}_v^{(v)}$ is a tree-like basis. Now

$$\mathcal{B}_v^{(v)} \rightarrow_{\text{TR}} \mathcal{B}_v^{(v+1)} \rightarrow_{\text{TR}} \dots \rightarrow_{\text{TR}} \mathcal{B}_v^{(a)}$$

so $\mathcal{B}_v^{(a)}$ is a tree-like basis.

This argument has to be adjusted. We have to ensure that all conditions h are small throughout the construction. To this end we need some more lemmas.

Definition 4.3.4 For $\mathcal{H}, \mathcal{H}' \subseteq \mathcal{P}$ let $\mathcal{H} \times \mathcal{H}' := \{h \cup h' : h \in \mathcal{H}, h' \in \mathcal{H}'\}$. ♣

Lemma 4.3.5 *Let $A \rightarrow \mathcal{H}_A$ and $A \rightarrow \mathcal{H}'_A$ be two \mathbf{M} -definable maps. Suppose that*

- (i) *for each condition in \mathcal{H}_A is compatible with some condition in \mathcal{H}'_A and vice versa.*

(ii) for A, B with $A \neq B$ and $A \cap B \neq \emptyset$, all conditions in \mathcal{H}_A are incompatible with all conditions in \mathcal{H}'_B and vice versa.

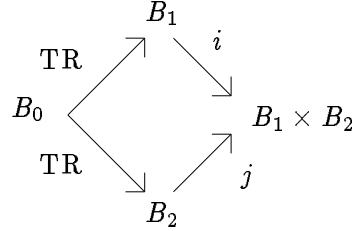
Suppose that both the maps $A \rightarrow \mathcal{H}_A$ and $A \rightarrow \mathcal{H}'_A$ satisfy conditions (i) and (ii) in lemma 4.3.3. Then the M-definable map $A \rightarrow \mathcal{H}_A \times \mathcal{H}'_A$ ensures that (i) and (ii) remain valid with t replaced by $2t$.

Proof: Direct verification. □

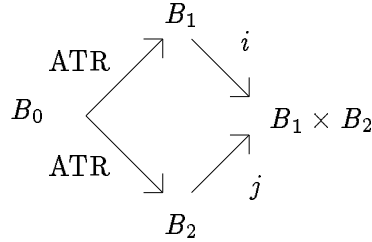
Lemma 4.3.6 Suppose that \mathcal{B}_0 is a basis for \mathcal{P} . If both B_1 and B_2 are tree-like refinements of \mathcal{B}_0 , then $B_1 \times B_2$ is a tree-like refinement of both B_1 and B_2 .

Proof: Proved by induction on the number of atomic tree-like refinements needed to get from \mathcal{B}_0 to B_1 added to the number of atomic tree-like refinements needed to get from \mathcal{B}_0 to B_2 .

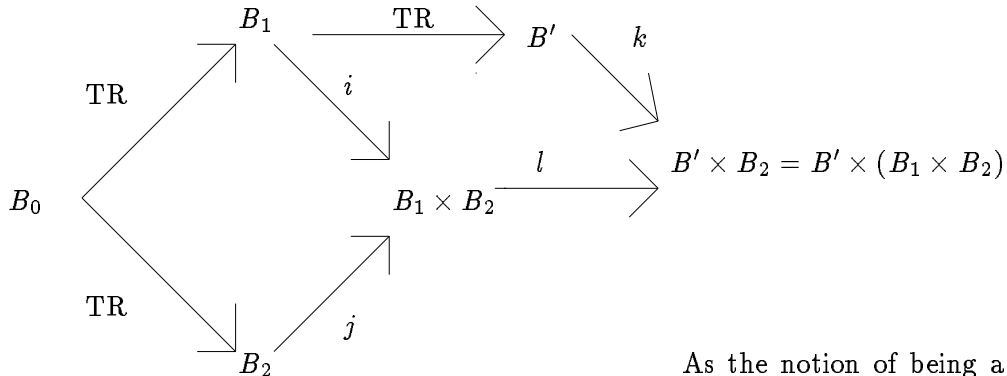
It suffices to show that i and j are tree-like refinements in the following diagram:



As the first step in the induction argument notice that i and j are tree-like refinements in the diagram:



Now each next step in the induction argument is shown by noticing (by use of the induction assumption) that i and j are tree-like refinements, and by noticing (again by use of the induction assumption) that k and l are tree-like refinements:

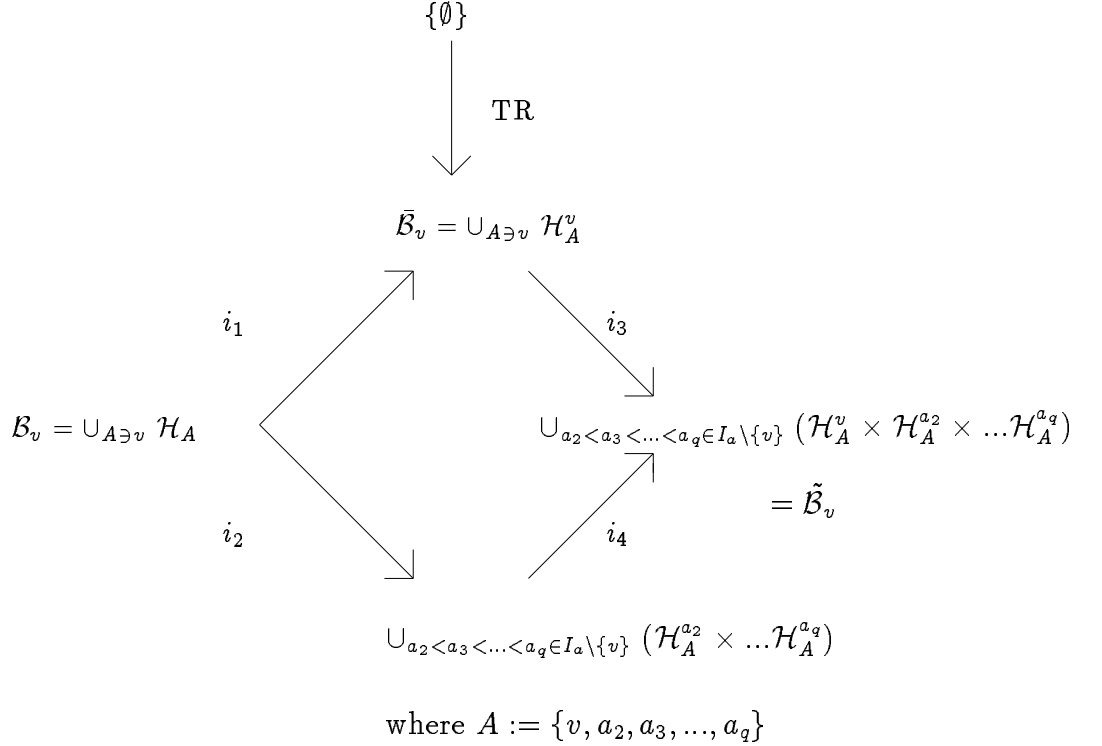


As the notion of being a tree-like refinement is transitive we are done. □

The following proof simplifies an argument in an earlier and preliminary version of this paper.

Proof of lemma 4.3.3: Let $A \rightarrow \mathcal{H}_A$ be an M-definable map which satisfies (i) and (ii). For each $v \in I_a$ consider $\mathcal{B}_v := \cup_{A \ni v} \mathcal{H}_A$. According to lemma 4.2.8 there exists a tree-like refinement $\mathcal{B}_v \rightarrow_{i(v)} \mathcal{B}_v(i(v))$ for some tree-like basis $\mathcal{B}_v(i(v))$ with $\|\mathcal{B}_v(i(v))\| \leq pt(t+1)$. This induce tree-like refinements $\mathcal{H}_A \rightarrow_{i(v)} \mathcal{H}_A(i(v))$ where $\mathcal{B}_v(i(v)) = \cup_{A \ni v} \mathcal{H}_A(i(v))$.

I claim that the M-definable map $A \rightarrow \tilde{\mathcal{H}} := \mathcal{H}_A(i(a_1)) \times \mathcal{H}_A(i(a_2)) \times \dots \times \mathcal{H}_A(i(a_q))$ satisfies (i)' and (ii)' ($A = \{a_1, \dots, a_q\}$). The first claim follows because $\|\tilde{\mathcal{H}}_A\| \leq q \max_a \|\mathcal{H}_A^a\| \leq qpt(t+1)$. To show the second claim we need to show that $\tilde{\mathcal{B}}_v := \cup_{A \ni v} \tilde{\mathcal{H}}_A$ is a tree-like basis. To see this notice that for each $A \subseteq I_a$ where $A = \{v, a_2, a_3, \dots, a_q\}$ we have $\mathcal{B}_v \rightarrow_{\text{TR}} \mathcal{B}_v(i(a_2)) \times \dots \times \mathcal{B}_v(i(a_q))$ (by lemma 4.3.6). This refinement induces a tree-like refinement $\mathcal{H}_A \rightarrow_{\text{TR}} \mathcal{H}_A(i(a_2)) \times \dots \times \mathcal{H}_A(i(a_q))$. This tree-like refinement extend to a tree-like refinement $\mathcal{B}_v = \cup_{A \ni v} \mathcal{H}_A \rightarrow \cup_{A \ni v} (\mathcal{H}_A(i(a_2)) \times \mathcal{H}_A(i(a_3)) \dots \mathcal{H}_A(i(a_q)))$ (where $A := \{v, a_2, a_3, \dots, a_q\}$). Thus i_2 in the following diagram is a tree-like refinement.



By assumption (i) \mathcal{B}_v is a basis. We used lemma 4.2.8 to construct the tree-like refinement $i_1 := i(v)$. And this could be done such that $\{\emptyset\} \rightarrow_{\text{TR}} \bar{\mathcal{B}}_v$. Now $\mathcal{B}_v(i(v)) \times \cup_{a_2 < a_3 < \dots < a_q \in I_a \setminus \{v\}} (\mathcal{H}_A(i(a_2)) \times \dots \mathcal{H}_A(i(a_q)))$

$= \cup_{a_2 < a_3 < \dots < a_q} (\mathcal{H}_A(i(v)) \times \mathcal{H}_A(i(a_2)) \times \dots \mathcal{H}_A(i(a_q))) = \tilde{\mathcal{B}}_v$, so by lemma 4.3.6 both i_3 and i_4 are tree-like refinements. So $\{\emptyset\} \rightarrow_{\text{TR}} \bar{\mathcal{B}}_v \rightarrow_{\text{TR}} \tilde{\mathcal{B}}_v$ and thus $\tilde{\mathcal{B}}_v$ is a tree-like basis. \square

Combining lemma 4.3.1 and lemma 4.3.3 it is not hard to show (ii) \Rightarrow (i) in theorem 4.1.1.

5 The positive part

5.1 Count(2) imply Count(4)

Assume that the Δ_0 -Count(2) principle is valid in \mathbf{M} . What is the status of the Δ_0 -Count(4) principle? Is it possible that there exists $n' \in \mathbf{M}$ such that the ordered set $\{1, 2, \dots, 4n' + r\} \subseteq \mathbf{M}$ of “numbers” can be divided (in a Δ_0 -definable way) into disjoint 4-element subsets, and $r \in \{1, 2, 3\}$?

Consider the following informal argument: We want to show (reasoning inside \mathbf{M}) that a set of numbers of the form $\{1, 2, \dots, n\}$ can be divided into a collection of disjoint 4 element subsets only when n is divisible by 4. Suppose that on the contrary some interval $\{1, 2, \dots, 4n' + r\}$, $r \in \{1, 2, 3\}$ can be divided into a collection \mathcal{P} of disjoint 4 element subsets. The case where $r = 1$ or $r = 3$ can be excluded for trivial reasons. To see this sub-divide each 4-element subset into two 2-element subsets. This induces a partitioning of $\{1, 2, \dots, 4n' + r\}$ into disjoint 2-element subsets violating the Count(2) principle.

The case where $r = 2$ require a more involved argument. Consider all pairs of $\{1, 2, \dots, 4n' + 2\}$. It only requires a quite weak part of arithmetic to prove that these pairs are in 1-1 correspondence with $\{1, 2, \dots, \binom{4n'+2}{2}\}$. And even less Arithmetical assumptions to show that $\binom{4n'+2}{2}$ is an odd number. To get a contradiction (by violating the Count(2) principle) it suffices to show that the partitioning \mathcal{P} induces a partitioning \mathcal{R} of all pairs of $\{1, 2, \dots, 4n' + 2\}$ into disjoint 2 element sets. Consider the pair $\{v_1, v_2\}$. If both v_1 and v_2 belongs to the same 4-element subset $\{v_1, v_2, v_3, v_4\} \in \mathcal{P}$ let $\{\{v_1, v_2\}, \{v_3, v_4\}\} \in \mathcal{R}$. Otherwise suppose $v_1 \in \{w_1, w_2, w_3, w_4\} \in \mathcal{P}$ and $v_2 \in \{\tilde{w}_1, \tilde{w}_2, \tilde{w}_3, \tilde{w}_4\} \in \mathcal{P}$. All elements are listed after size. So there are unique $i, j \leq 4$ such that $v_1 = w_i$ and $v_2 = \tilde{w}_j$. If $i \neq j$ let $\{\{v_1, v_2\}, \{\tilde{w}_i, w_j\}\} \in \mathcal{R}$. If $i = j$ let $\{\{v_1, v_2\}, \{w_{i'}, \tilde{w}_{i'}\}\} \in \mathcal{R}$ where $1' = 2, 2' = 1, 3' = 4$ and $4' = 3$. This completes the argument.

To summarise: We considered a structure S_I constructed from $I := \{1, 2, \dots, n\}$. In this concrete case the structure consisted of all pairs of $\{1, 2, \dots, 4n' + 2\}$. This structure S_I had the property that partial partitions of $\{1, 2, \dots, 4n' + 2\}$ into 4 element subsets induced (in a flexible way) pairings of the elements in S_I . And crucially the structure S_I contained an odd number of elements. One could try to modify the type of argument to the case where for example $q = 2$ and $p = 3$. At an early stage in this research J.Krajicek showed me some ingenious constructions attempting show that Count(3) was a consequence of Count(2). However as J.Krajicek pointed out careful calculations always seems to give the wrong parities. Irrespectively of the ingenuity however clever the structures S was constructed, it always seemed to end up containing an even number of elements. So it seemed that strong and unknown forces wanted Count(2) and Count(3) to be independent.

In retrospect this is of course a simple consequence of the negative part of the classification which is developed in the next section. The first Main result (Theorem 4.1.1) shows that only forests of specially labelled trees are relevant as structures S .

5.2 Count($q \cdot s$) imply Count($q^2 \cdot s$)

In this subsection we show how a reminiscence of the ‘Count(2) implies Count(4)’ argument above can be used to construct exceptional forests for various general q, p and n . More specifically we will show:

Lemma 5.2.1 *Suppose that $q \geq 2, s, v$ and n are given numbers with $n \neq 0$ modulo $q^v \cdot s$, $n \geq q^{2v+1}$.*

Then there exists a(n exceptional) forest T_1, T_2, \dots, T_u of $(q^{v+1} \cdot s, n)$ -labelled trees, where each branch appears 0 modulo $q^v \cdot s$ times, and where $u \neq 0$ modulo $q^v \cdot s$.

By use of the first Main result (Theorem 4.1.1) the existence of these forests gives us the main ingredient in the positive part of the classification.

Corollary 5.2.2 *Suppose that $q \geq 2, s, v$ are given numbers.*

Then the Δ_0 -Count($q^{v+1} \cdot s$) axiom scheme follows from the Δ_0 -Count($q^v \cdot s$) axiom scheme.

Definition 5.2.3 By $[i_1, \dots, i_l]_p$ we denote the (p, n) -labelled trees which contain all the branches α of the form $\alpha = \{A_1, \dots, A_r\}$ where $A_j \subseteq I$, $|A_j| = p$, $j = 1, 2, \dots, r$ and where $A_j \cap A_k = \emptyset$ for $j \neq k$. Besides that we require that,

(a) $A_j \cap \{i_1, i_2, \dots, i_l\} \neq \emptyset$ for $j = 1, 2, \dots, r$,

(b) $\forall k \leq l \exists j \leq r \ i_k \in A_j$. ♣.

Definition 5.2.4 Let $p, q \geq 2$. The forest $\mathcal{F}_{p,r,n}^*$ consists of all the trees $[i_1, i_2, \dots, i_r]_p$ where $i_1 < i_2 < \dots < i_r \leq n$. ♣

Definition 5.2.5 By $A_{p,l,r}$ we denote the number of ways it is possible to select r elements from the sets $\{1, 2, \dots, p\}, \{p+1, p+2, \dots, 2p\}, \dots, \{pl-p+1, pl-p+2, \dots, pl\}$, such that at least one element is chosen from each of the p elements sets. ♣

Lemma 5.2.6 *The forest $\mathcal{F}_{p,r,n}^*$ of (p, n) -labelled trees, contains $\binom{n}{r}$ trees. Each branch α with $|\alpha| = l$ appears in $A_{p,l,r}$ trees.*

Proof: Clearly $|\mathcal{F}_{p,r,n}^*| = \binom{n}{r}$. Suppose that

$\alpha = \{\{i_1^1, i_2^1, \dots, i_p^1\}, \{i_1^2, \dots, i_p^2\}, \dots, \{i_1^l, i_2^l, \dots, i_p^l\}\}$ where $i_1^1 < i_2^1 < \dots < i_p^1$ and where $i_1^j < i_2^j < \dots < i_p^j$ for $j = 1, 2, \dots, l$. Now there is a one to one correspondence between the r element subsets of $\text{Set}(\alpha)$, which contains at least one element from each member in α , and the trees in $\mathcal{F}_{p,r,n}^*$ which contain α . □

Proof of lemma 5.2.1: Let $q \geq 2, s, v$ and $n \geq q^{2v+1}$ be given. Let \mathcal{F} be the forest which contains which contains q^{v-1} copies of the forest $\mathcal{F}_{p,r,n}^*$ where $p := q^{v+1} \cdot s$, $r := q^v$. The critical cases (the only non-trivial cases) are when $n = q^{v+1}n' + u \cdot q^v$, $u = 1, 2, \dots, q-1$. The forest \mathcal{F} contains $q^{v-1} \binom{n}{q^v}$ trees. Now $\binom{n}{q^v} = \frac{(q^{v+1}n' + uq^v) \dots (q^{v+1}n' + uq^v - q^v + 1)}{q^{v!}}$. The factor q appears exactly $q \binom{q^v-1}{q-1}$ times in both nominator and denominator. Thus $\binom{n}{q^v} = k$ modulo $s \cdot q^v$ and thus \mathcal{F} contains $k \cdot q^{v-1}$ modulo $s \cdot q^v$ trees for some k which not is divisible by q .

Each branch of length 1 appears exactly $q^{v-1} \cdot A_{q^{v+1}s, 1, q^v} = q^{v-1} \cdot \binom{q^{v+1}s}{q^v} = 0$ modulo $s \cdot q^v$ times. In general $\binom{p}{i} = 0$ modulo $s \cdot q^v$ (when $i < q^v$) so longer branches appears $q^{v-1} \cdot A_{q^{v+1}s, l, q^v} = \frac{1}{l!} \sum_{i_1, i_2, \dots, i_l} \binom{p}{i_1} \binom{p}{i_2} \dots \binom{p}{i_l} = 0$ modulo $s \cdot q^v$. □

This gives the positive part of the classification:

Corollary 5.2.7 *If $p, q \geq$ and all prime factors in p appears in q then the Δ_0 -Count(p) axiom scheme follows from the Δ_0 -Count(q) axiom scheme.*

Proof: Assume that $q := p_1 \cdot p_2 \cdot \dots \cdot p_k \cdot s$ and assume that $p := p_1^{i_1} \cdot p_1^{i_2} \cdot \dots \cdot p_k^{i_k}$. According to corollary 5.2.2 the claim holds when $q := q^v \cdot s$ and $p := q^{v+1} \cdot s$. Repeated application of this show that the Δ_0 -Count($p_1^{i_1} \cdot p_2^{i_2} \cdot \dots \cdot p_k^{i_k}$) axiom scheme follows from the Δ_0 -Count($p_1 \cdot p_2 \cdot \dots \cdot p_k$) axiom scheme. This scheme in turn follows from the Δ_0 -Count($p_1 \cdot p_2 \cdot \dots \cdot p_k \cdot s$) axiom scheme. □

5.3 Some examples

Before we turn our attention on the negative part of the classification it is instructive to examine the structure of the exceptional forests when these are on the **PU**-form. Each (irreducible) exceptional forest \mathcal{F} of **PU**-trees I have found can be derived from the forests given in definition 5.2.4.

Example 5.3.1 Let $q = 2$, $p = 4$ and $n = 4n' + 2$, $n' \geq 2$. Consider the forest $\mathcal{F}_{2,4,n}$ of $(4, n)$ -labelled **PU**-trees which contains:

All **PU**-trees of the form $(i_1, W_1)(i_2)$ where $i_1 < i_2 \leq n$ and where $W_1 \subseteq \{1, 2, \dots, n\}$ has 3 elements. The **PU**-trees $(1), (3), (5), \dots, (4n' + 1)$.

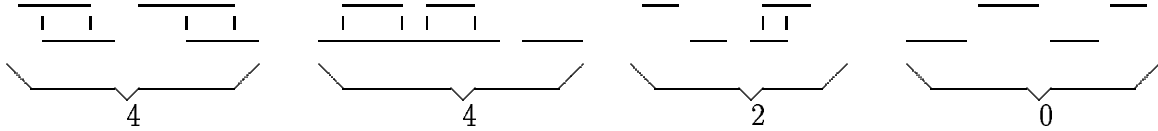
Each branch of length 2 appears 16 times. A branch $\{j_1, j_2, j_3, j_4\}$ of length 1, appears in $\text{mod}(j_1, 2) + \text{mod}(j_2, 2) + \text{mod}(j_3, 2) + \text{mod}(j_4, 2)$ trees of height 1. And the branch appears in $\binom{n-2}{3} - 4n + 6 + j_1 + j_2 + j_3 + j_4$ trees of height 2.

The forests $\mathcal{F}_{2,4,n}$ contain $\binom{n}{2} \binom{n-2}{3} + \frac{n}{2}$ trees. This is always an odd number. When $n' = 2$ the forests contain 2525 trees.

Example 5.3.2 Let $n = 4n' + 2$. For each $n' \geq 2$ there exists a 2-exceptional forest of $(4, n)$ -labelled trees. The forest contains all trees:

$(j_1, \{j_2, j_3, j_4\})(j_5)$ where $j_1 < j_2 < j_3 < j_4$ and where $j_1 < j_5 < j_2$ or $j_3 < j_5 < j_4$.
 $(1), (3), \dots, (4n' + 1)$.

Each branch of length 2 appears an even number of times. The branch $\{\{i_1, i_2, i_3, i_4\}, \{i_5, i_6, i_7, i_8\}\}$ appears a number of times depending on the number of vertical lines in the following kind of figure:



The branch $\{\{i_1, i_2, i_3, i_4\}\}$ appears in all trees (of height 2) except $(i_2 - i_1) + (i_4 - i_3)$ which counted modulo 2 is $i_1 + i_2 + i_3 + i_4$. This is the same number (modulo 2) it appears in trees of height 1.

When $n' = 2$ this is a forest of 635 trees. I conjecture that for $q = 2$ this is the smallest exceptional forest of **PU**-trees.

Both examples resembles the fact that $\text{Count}(2)$ implies $\text{Count}(4)$ in models of $I\Delta_0$. The next example is derived from lemma 5.2.6

Example 5.3.3 Let $q = 3$, $p = 9$ and $n = 9n' + 3$, $n' \geq 3$. Consider the forests $\mathcal{F}_{3,9,n}$ which contain the $(9, n)$ -labelled **PU**-trees:

- (1) The trees of the form $(i_1, W_1)(i_2, W_2)(i_3)$ where $i_1 < i_2 < i_3 \leq n$ and where W_1, W_2 are two disjoint 8-element subsets of $\{1, 2, \dots, n\} \setminus \{i_1, i_2, i_3\}$.
- (2) Two copies of each tree of the form $(i_1, W_1)(i_2)$ where $i_2 = 1$ modulo 3 and $i_1 < i_2 \leq n$.
- (3) Each tree of the form $(i_1, W_1)(i_2)$ where $i_2 = 2$ modulo 3 and $i_1 < i_2$.
- (4) Each tree of the form (i_1) where $\binom{n-i_1}{2} = 1$ modulo 3.

(5) Two copies of each tree of the form (i_1) where $\binom{n-i_1}{2} = 2$ modulo 3.

A careful checking shows that each branch appears 0 modulo 3 times. The forests contains 1 modulo 3 trees. In the smallest case (i.e. when $n'=3$) the forest contains

$$\binom{30}{3} \binom{27}{8} \binom{19}{8} + \sum_i \sum_{j > i, j \equiv 1 \pmod 3} 1 + \sum_i \sum_{j > i, j \equiv 2 \pmod 3} 1 + \sum_i \pmod{\binom{n-i}{2}, 3}$$

trees. This is a forest of 681259986982585 trees. This is not the smallest exceptional forest for $q = 3$.

Example 5.3.4 Consider the forest \mathcal{F} which contains:

t copies of each tree $(i_1, \{i_2, i_3, \dots, i_9\})(j_1, \{j_2, \dots, j_9\})(k)$ where $i_1 < i_2 < \dots < i_9$, $i_1 < j_1$, $j_1 < j_2 < \dots < j_9$ and if $i_r < k < i_{r+1}$ and $j_s < k < j_{s+1}$ then $r + s = t$ modulo 3.

t copies of each tree $(i_1, \{i_2, \dots, i_9\})(j)$ where $i_1 < i_2 < \dots < i_9$ and if $i_r < j < i_{r+1}$ then $t = r$ modulo 3.

t copies of each tree (i) where $t = i$ modulo 3.

I claim (without proof) that each branch appears 0 modulo 3 times. However for each $n = 9n' + 3$ $n' \geq 3$ $|\mathcal{F}| \neq 0$ modulo 3. More specifically

$|\mathcal{F}| = \frac{1}{3} \cdot \binom{n}{9} \binom{n-9}{9} \cdot (n-18)$. In the case when $n' = 3$, \mathcal{F} only contains 16821302548060 PU-trees. I conjecture that this is the smallest exceptional forest for $q = 3$.

Example 5.3.3 and example 5.3.4 resembles the fact that Count(3) implies Count(9) in models of $I\Delta_0$. From the examples we notice a general feature. The trees of maximal height h are very homogeneously organised and easy to describe. The trees of height $h - 1$ are still quite regular but each such tree's frequency $0 \leq v < q$ is slightly more complicated to describe. The collection of trees of height 1 have the frequencies which are the most complicated to calculate.

In the next section it is shown that all exceptional forests asymptotically (when $n \rightarrow \infty$ and the height of all trees is bound by a constant) can be assumed to have the same feature.

6 The negative part

6.1 Forests of (D, R) -labelled trees

The negative part of the classification states that Count(q) does not imply Count(p) when p contains a prime factor which is not in q . We consider the case where all terms in the underlying language L have (at most) polynomial growth-rate. By the first main result theorem 4.1.1 it suffice to show that for each $h \in \mathbb{N}$ asymptotically (when $n \rightarrow \infty$, and $h(\mathcal{F}) \leq h$) there are no q -exceptional forests T_1, T_2, \dots, T_u of (p, n) -labelled trees.

This is shown by considering forests T'_1, T'_2, \dots, T'_u of specially labelled trees corresponding to the PHP_{q^k} versus Count(q) problem.

Definition 6.1.1 A (D, R) -labelled tree T is a decision tree for constructing a partial bijection $f : D \rightarrow R$. We always assume that $D \cap R = \emptyset$. Each vertex $v \in T$ corresponds to a certain stage f_v in the construction of f . At the root v_{root} we have $f_{v_{\text{root}}} = \emptyset$.

At each vertex v (except the top node) there is assigned a question, i.e. an element $u \in D \cup R \setminus (\text{dom}(f_v) \cup \text{ran}(f_v))$. The possible answers correspond to the sons of v . If $u \in D$, there is an edge to a son, for each $r \in R \setminus \text{ran}(f_v)$. Each of these edges lead to a vertex v' in which $f_{v'} \supseteq f_v$, and $f_{v'}(u) = r$ (and $|f_{v'}| = |f_v| + 1$). Similarly if $u \in R$. In this case there is an edge for each $d \in D \setminus \text{dom}(f_v)$. Each of these edges lead to a vertex v' in which $f_{v'} \supseteq f_v$, and $f_{v'}(d) = u$ (and $|f_{v'}| = |f_v| + 1$).

The type of a branch through T is identified with the partial map f_v constructed at the leaf v . ♣

Definition 6.1.2 The height $h(\mathcal{F})$ of the forest \mathcal{F} denotes the maximal height of a tree $T \in \mathcal{F}$. ♣

Definition 6.1.3 A (D, R) -labelled tree T is a PU-labelled tree (= on PU-form) if at each level all but possible one vertex is a top node. □

Observation 6.1.4 A (D, R) -labelled tree T on PU-form can be written of the form:

$$(u_1^1, u_2^1)(u_1^2, u_2^2) \dots (u_1^{l-1}, u_2^{l-1})(u^l)$$

If $u_1^i \in D$ then $u_2^i \in R$ and if $u_1^i \in R$ then $u_2^i \in D$ ($i = 1, 2, \dots, l-1$). The element u^l belongs to either D or R . In the first case we say T is of D -type, while we say that T is on R -type.

As an example consider the following (obvious) proposition:

Proposition 6.1.5 Suppose that \mathcal{F} is a forest which solely consists of (D, R) -labelled trees of D -type. Suppose also (as usual) that $|D| \leq |R|$. Suppose that each branch α in \mathcal{F} appears 0 modulo q times. Then the forest \mathcal{F} contains 0 modulo q trees.

Proof: Let $\rho : D \rightarrow R$ be an (total) injection. Each tree $T \in \mathcal{F}$ contains exactly one branch α with $\alpha \subseteq \rho$. Thus ρ induces a partitioning of the trees in \mathcal{F} into disjoint classes which each contains 0 modulo q trees. □

If the forest \mathcal{F} contains trees of both D -type and R -type the situation becomes more complicated.

Example 6.1.6 Let $q \in \mathbb{N}$. Consider the following forests \mathcal{F} of (D, R) -labelled trees. For each $d \in D$ it contain $(q-1)$ copies of (d) , and for each $r \in R$ it contain the tree (r) .

This forests \mathcal{F} contains $|R| - |D|$ modulo q trees. Each type of branch appears 0 modulo q times. So trivially if $|R| \neq |D|$ modulo q , there exists a forest \mathcal{F} in which all branches appears 0 modulo q times, but $|\mathcal{F}| \neq 0$ modulo q .

This type of forest is trivial. It corresponds to the obvious fact that $\text{Count}(q)$ implies PHP_p when $p \neq 0$ modulo q .

Definition 6.1.7 A forest \mathcal{F} of (D, R) -labelled trees is called (q, l) -exceptional if

- (i) Each type branch appears 0 modulo q times.
- (ii) $|R| = |D| + q^l$.
- (iii) The number of trees in \mathcal{F} is not divisible by q . ♣

Example 6.1.8 Suppose $|R| - |D| = 4p' + 2$ for some $p' \in \mathbb{N}$. Assume that $|R|$ is an odd number. Let \mathcal{F} denote the (D, R) -labelled forest which contains the following PU-trees:

- (1) All trees of the form $(d, r_1)(r_2)$ where $d \in D$ and $r_1 > r_2$ when $|r_1 - r_2|$ is odd, and $r_1 < r_2$ when $|r_1 - r_2|$ is even.
- (2) All trees of the form $(d_1, r)(d_2)$ where $r \in R$ and $d_1 < d_2$.

Each branch appears an even number in \mathcal{F} . However, the forest \mathcal{F} contains

$$|D| \binom{|R|}{2} + |R| \binom{|D|}{2}$$

trees which is always an odd number. The smallest example of this form is when $|D| = 5$ and $|R| = 7$. In this case \mathcal{F} contains 175 trees. I claim without proof that this is the smallest $(2, 1)$ -exceptional forest. The forest resemble the fact that $\text{Count}(2)$ implies PHP_2 .

Our general machinery allow us to prove that there exists exceptional forest (without explicit constructing them!). More specifically there are (q, l) -exceptional forests for each $q, l \in \mathbb{N}$, $q \neq 1$ (we do not need this fact). This follows by combining:

- (1) A version of theorem 4.1.1 for the PHP_{q^l} versus $\text{Count}(q)$ problem.
- (2) That PHP_1 follows from $\text{Count}(q)$
- (3) That PHP_{q^l} follows from PHP_1 (according to [23]).

This argument is non-constructive (in so far the forcing construction is non-constructive). However it turn out that the existence of (q, l) -exceptional forests can be proved by constructing them explicitly along the same lines as the constructions in section 5.

6.2 Projecting forests

Let T be a (p, n) -labelled tree. Suppose $n = pn' + q^l$ for $q \in \mathbb{N} \setminus \{1\}$ and $l \in \mathbb{N}$. Then we can transform it to a (D, R) -labelled tree by the following procedure.

First divide $I := \{1, 2, \dots, n\}$ into p disjoint sets D_1, D_2, \dots, D_{p-1} and R such that $|D_1| = |D_2| = \dots = |D_{p-1}| = n'$ and $|R| = n' + q^l$. Let $D := D_1$. For $j = 1, 2, \dots, p-1$ chose bijections $y_j : D_j \rightarrow D$. Let us call a subset $\{i_1, i_2, \dots, i_p\} \subseteq I$ for *regular* if $i_p \in R$, $i_j \in D_j$, $j = 1, 2, \dots, p-1$ and $y_1(i_1) = y_2(i_2) = \dots = y_{p-1}(i_{p-1})$. A branch $\{A_1, \dots, A_r\}$ is *regular* if each A_j , $j = 1, 2, \dots, r$ is regular. By use of this definition it is straight forward to show that:

Lemma 6.2.1 *Let T be a (p, n) -labelled tree. Suppose that $n = pn' + q^l$ and let D_1, \dots, D_{p-1} and R be given as above. Then the set of regular branches in T form a new tree T' which is (D, R) -labelled. Furthermore $h(T') \leq h(T)$.*

If T is on PU-form, then T' will also be on PU-form.

Instead of projecting a single tree we can project forests. The important point is that the projection of an q -exceptional forest of (p, n) -labelled trees produces an (q, l) -exceptional forest of (D, R) -labelled trees.

Corollary 6.2.2 *Let $\mathcal{F} := \{T_1, T_2, \dots, T_u\}$ be a forest of (p, n) -labelled trees. Suppose \mathcal{F} is an q -exceptional forest. Or more specifically suppose that each branch in \mathcal{F} appears 0 modulo q times, but $u \neq 0$ modulo q . Suppose also that $n = pn' + q^l$. The projection of the trees T_1, \dots, T_u gives an (q, l) -exceptional (D, R) -labelled forest \mathcal{F}' (with $|D| = n'$ and $|R| = n' + q^l$). Furthermore $h(\mathcal{F}') \leq h(\mathcal{F})$.*

The condition that $n = pn' + q^l$ might not in general be satisfied for a given n . However, usually we do not lose any generality by assuming n is of this form. To see this consider the following procedure:

Definition 6.2.3 Suppose that ρ is a partial partition of $I := \{1, 2, \dots, n\}$ into disjoint p -element subsets. Consider a (p, n) -labelled tree T . For each branch (=condition) α through T consider the following procedure. If α is incompatible with ρ remove it. Otherwise replace it by $\beta := \alpha \setminus \rho$.

Suppose that ρ' is a partial bijection from D to R . Consider a (D, R) -labelled tree T . For each branch (=condition) α' through T consider the following procedure. If α' is incompatible with ρ' remove it. Otherwise replace it by $\beta' := \alpha' \setminus \rho'$. ♣

Lemma 6.2.4 (Stability) *Suppose that T is a (p, n) -labelled tree. Let ρ be a partial partition of $I = \{1, 2, \dots, n\}$ into disjoint p -element subsets. Suppose that $p \cdot (h(T) + |\rho|) < n$. Then the collection of all branches β which are produced from some $\alpha \in T$ (as described in the first part of definition 6.2.3) can be organised into a (p, n') -labelled tree T^ρ where $n' = n - p|\rho|$.*

Suppose that T' is a (D, R) -labelled tree. Let ρ' be a partial bijection from D to R . Suppose that $h(T') + |\rho'| < n$. Then the collection of all branches β' which are produced from some $\alpha' \in T'$ (as described in the second part of definition 6.2.3) can be organised into a (D', R') -labelled tree $T'^{\rho'}$ where $D' := D \setminus \text{dom}(\rho')$ and $R' := R \setminus \text{ran}(\rho')$.

If T (T') is a PU-tree then T^ρ ($T'^{\rho'}$) is a PU-tree.

Proof: It suffice to show the lemma when $|\rho| = 1$. Suppose that $\rho := \{\{i_1, i_2, \dots, i_p\}\}$. Let V be the set of vertex in T which have assigned $v \in \{i_1, \dots, i_p\}$. Let E_\perp denote the set of edges in T which has assigned p -subset $A \subseteq I$ with non-trivial intersection with $\{i_1, \dots, i_p\}$ (i.e. $\neq \emptyset$ and $\neq A$). Let E_\parallel be the set of edges which have assigned $A = \{i_1, i_2, \dots, i_p\}$.

For each vertex (=question) in V all edges (but exactly one) edge (=answer) belongs to E_\perp . Remove all these edges (and the sub-tree above this). Then contract the edge in E_\parallel . Finally, after having exhausted this procedure, remove all edges in E_\perp (and the sub-tree above this). The condition that $p(h(T) + |\rho|) < n$ is exactly what in general is required to ensure that T^ρ actually becomes a properly labelled tree. The second part of the lemma is showed similarly. The last claim is also straight forward to check. □

The lemma is one of many stability results which are important for the overall argument. In short it shows that trees (PU-trees) remains on this form when they are “hit” by a restriction ρ .

The following main lemma gives us an understanding of the asymptotic behaviour of exceptional (D, R) -labelled trees.

Lemma 6.2.5 (Main lemma) *Let q be a prime number. Let $k, l \in \mathbb{N}$. There exists $d_0 \in \mathbb{N}$ such that for any (q^k, l) -exceptional forest of (D, R) -labelled trees, where $d_0 \leq |D| \leq |R|$, we have $h(\mathcal{F}') \geq q^{l-k}$.*

Corollary 6.2.6 *Let p be any prime number which does not appear in $q = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_r^{\alpha_r}$. Fix $h \in \mathbb{N}$. There exists n_0 such that for each $n \geq n_0$ each forest $\mathcal{F} := \{T_1, T_2, \dots, T_u\}$ of (p, n) -labelled trees never simultaneously satisfies:*

- (1) *All branches appears 0 modulo q times.*
- (2) *$h(\mathcal{F}) \leq h$.*
- (3) *$u \neq 0$ modulo q .*

Proof: Suppose that (1) and (3) hold. Choose $j \in \{1, 2, \dots, r\}$ such that $u \neq 0$ modulo $q_j^{\alpha_j}$. According to the assumptions \mathcal{F} is an $q_j^{\alpha_j}$ -exceptional forest of (p, n) -labelled trees. By lemma 6.2.4 we can assume that $n = pn' + q_j^l$ for any l given in advance (of course l has to be reasonable i.e. $q^l \ll n$ etc). Choose l such that $q_j^{l-\alpha_j} > h$. By corollary 6.2.2 the projected forest \mathcal{F}' is $(q_j^{\alpha_j}, l)$ -exceptional and $h(\mathcal{F}') \leq h(\mathcal{F})$. According to lemma 6.2.5 $h(\mathcal{F}') \geq q^{l-\alpha_j} > h$. Now $h(\mathcal{F}') \leq h(\mathcal{F})$ so this contradicts (2). \square

6.3 Creating order among trees of maximal height h

Lemma 6.3.1 *Fix $q \in \mathbb{N} \setminus \{1\}$, and fix $l, h \in \mathbb{N}$. For each $d_0 \in \mathbb{N}$ with $d_0 \geq h$, there exists (a very large) $d_1 \in \mathbb{N}$ such that for each forest $\mathcal{F} = \{T_1, T_2, \dots, T_u\}$ of (D, R) -labelled trees with $|R| = |D| + q^l$, $h(\mathcal{F}) \leq h$ and $|D| \geq d_1$ the following is true:*

There exists a partial bijection $\rho : D \rightarrow R$, such that the forest $\mathcal{F}^\rho := \{T_1^\rho, T_2^\rho, \dots, T_u^\rho\}$ of (D', R') -labelled trees, with $D' = D \setminus \text{dom}(\rho)$ and $R' = R \setminus \text{ran}(\rho)$, satisfies:

- (1) *For each $h-1$ element subset $\{d_1, d_2, \dots, d_{h-1}\} \subseteq D'$ with $d_1 < d_2 < \dots < d_{h-1}$ and for each permutation $\pi : \{1, 2, \dots, h\} \rightarrow \{1, 2, \dots, h\}$ the number (modulo q) of trees (in the forest \mathcal{F}^ρ) of the form*

$$(d_1, r_{\pi(1)})(d_2, r_{\pi(2)}) \dots (d_{h-1}, r_{\pi(h-1)})(r_{\pi(h)})$$

does not depend on the elements $r_1 < r_2 < \dots < r_h$ in R' .

- (2) *For each $(h-1)$ -element subset $\{d_1, d_2, \dots, d_{h-1}\} \subseteq D'$ (where $d_1 < d_2 < \dots < d_{h-1}$), for each element $d_h \in D' \setminus \{d_1, d_2, \dots, d_{h-1}\}$, and for each permutation $\pi : \{1, 2, \dots, h-1\} \rightarrow \{1, 2, \dots, h-1\}$ the number (modulo q) of trees of the form*

$$(d_1, r_{\pi(1)})(d_2, r_{\pi(2)}) \dots (d_{h-1}, r_{\pi(h-1)})(d_h)$$

does not depend on the elements $r_1 < r_2 < \dots < r_{h-1}$ in R' .

- (3) *$|D'| \geq d_0$.*

Proof: Let $D_1 \subseteq D$ be a subset with $|D_1| \geq d'_0$ for some d'_0 much larger than d_0 . The size of d'_0 can be expressed in terms of the estimates arising from the second part of the argument (where we ensure the validity of property (3)). For each $h-1$ element subset $\{d_1, d_2, \dots, d_{h-1}\} \subseteq D_1$ with $d_1 < d_2 < \dots < d_{h-1}$ and for each permutation $\pi : \{1, 2, \dots, h\} \rightarrow \{1, 2, \dots, h\}$ we define a map

$F(d_1, d_2, \dots, d_{h-1}; \pi)$ which maps h -element subsets of R to the set $\{0, 1, 2, \dots, q-1\}$. It is defined by letting $F(d_1, d_2, \dots, d_{h-1}; \pi)(\{r_1, r_2, \dots, r_h\})$ (where $r_1 < r_2 < \dots < r_h$) denote the number (modulo q) of the **PU**-trees

$$(*) \quad (d_1, r_{\pi(1)})(d_2, r_{\pi(2)}) \dots (d_{h-1}, r_{\pi(h-1)})(r_{\pi(h)})$$

These maps induce as a map \tilde{F} which to each h element subset $\{r_1, r_2, \dots, r_h\} \subseteq R$ takes one of $q^{\binom{|d_0|}{h-1} h!}$ -values. This value expresses uniquely for each $h-1$ element subset of D_1 and each permutation $\pi : \{1, 2, \dots, h\} \rightarrow \{1, 2, \dots, h\}$, the number (modulo q) of **PU**-trees of the form $(*)$.

Now by Ramsey's theorem if d_1 is sufficiently large (not depending on \mathcal{F}) there must be a set $R_1 \subseteq R$ with $|R_1| \geq |D_1| + q^l$ and which is homogeneous for the "colouring" \tilde{F} . By possible making R_1 slightly smaller we can ensure that $|D \setminus D_1| = |R \setminus R_1|$. Choose a partial bijection $\rho : D \rightarrow R$ such that $\text{dom}(\rho) = D \setminus D_1$ and $\text{ran}(\rho) = R \setminus R_1$. This ensure that the new restricted forest satisfies property (1).

This procedure is now repeated (with d'_0 replaced by d_0 so (3) becomes satisfied) such that property (2) becomes satisfied. Notice that application of a new ρ' does not destroy property (1) (see lemma 6.3.3 if necessary). \square

Definition 6.3.2 Two tuples $\langle r_1, r_2, \dots, r_h \rangle$ and $\langle r'_1, r'_2, \dots, r'_h \rangle$ have the same *order structure* if for the same permutation π we have that $r_{\pi(1)} < r_{\pi(2)} < \dots < r_{\pi(h)}$ and $r'_{\pi(1)} < r'_{\pi(2)} < \dots < r'_{\pi(h)}$.

♣

Lemma 6.3.3 (Stability) *Suppose that $\mathcal{F} := \{T_1, T_2, \dots, T_u\}$ is a forest of (D, R) -labelled **PU**-trees. Suppose all trees of maximal height h satisfies (1) and (2) in lemma 6.3.1. For any partial bijection $\rho : D \rightarrow R$, with $h + |\rho| < |D|$, the forest $\mathcal{F}' := \{T_1^\rho, T_2^\rho, \dots, T_u^\rho\}$ of (D', R') -labelled trees ($D' := D \setminus \text{dom}(\rho)$, $R' := R \setminus \text{ran}(\rho)$) also satisfies (1) and (2).*

Proof: By the second part of lemma 6.2.4, we only have to check that (1) and (2) in lemma 6.3.1 will be satisfied. To show (1) we have to prove that the **PU**-trees

$$(d_1, r_1)(d_2, r_2) \dots (d_{h-1}, r_{h-1})(r_h)$$

and

$$(d'_1, r'_1)(d'_2, r'_2) \dots (d'_{h-1}, r'_{h-1})(r'_h)$$

appears the same number of times (modulo q) when $d_1 < d_2 < \dots < d_{h-1}$, when $d'_1 < d'_2 < \dots < d'_{h-1}$, and when the order type of $\langle r_1, r_2, \dots, r_h \rangle$ and $\langle r'_1, r'_2, \dots, r'_h \rangle$ are the same. This follows from the fact that none of the representations can have been altered by ρ . \square

6.4 Creating order among trees of height $h' < h$

Let \mathcal{F} be a forest of (D, R) -labelled trees of **PU**-form. Write \mathcal{F} as the union $\mathcal{F}_1 \cup \mathcal{F}_2 \cup \dots \cup \mathcal{F}_h$, where the sub-forest $\mathcal{F}_{h'}$, $1 \leq h' \leq h$ contains all trees of height h' . Suppose that we have already achieved that all trees in $\mathcal{F}_{h''}$ ($h' < h'' \leq h$) satisfies condition (1) and (2) in lemma 6.3.1. By the same Ramsey type of argument as in lemma 6.3.1 there exists a restriction ρ (i.e. a partial bijection) such that all trees in $\mathcal{F}_{h'}^\rho$ satisfies (1) and (2) in lemma 6.3.1 with h replaced by h' .

Consider the trees in \mathcal{F}^ρ of height \tilde{h} ; $h' \leq \tilde{h} \leq h$. In general there will be a flux of restricted trees T^ρ which originate from some $T \in \mathcal{F}_{h''}$ with $\tilde{h} < h'' \leq h$. It is possible to construct restrictions ρ such that the flux actually ruin what has already been achieved (but I believe only if \mathcal{F} not is exceptional). However it turn out that if we choose ρ in a suitable way (there are various choices) the number (modulo q) of productions of a tree $(d^1, r^1)(d^2, r^2) \dots (d^{h'-1}, r^{h'-1})(r^{h'})$ (or $(d^1, r^1)(d^2, r^2) \dots (d^{h'-1}, r^{h'-1})(d^{h'})$) can be expressed as a polynomial in $d^1, d^2, \dots, d^{h'-1}$ and $r^1, r^2, \dots, r^{h'}$ modulo $q^{h-h'}$ (when these elements are enumerated according to their size in $D' := D \setminus \text{Dom}(\rho)$ and $R' := R \setminus \text{Ran}(\rho)$). In other words suppose that we have already achieved that all trees in $\mathcal{F}_{h''}$ ($h' < h'' \leq h$) satisfies condition (1) and (2) in lemma 6.3.1. Then without loss of generality we can assume that all trees in $\mathcal{F}_{h''}$ ($h' \leq h'' \leq h$) satisfies condition (1) and (2) in lemma 6.3.1.

Definition 6.4.1 (Strong normal form) A forest $\mathcal{F} := \{T_1, T_2, \dots, T_u\}$ of PU-trees is on *strong normal form* if for each $h' \leq h$:

(1) For arbitrary $d_1 < d_2 < \dots < d_{h'-1}$ and for each permutation $\pi : \{1, 2, \dots, h\} \rightarrow \{1, 2, \dots, h\}$ the number (modulo q) of trees of the form

$$(d_1, r_{\pi(1)})(d_2, r_{\pi(2)}) \dots (d_{h-1}, r_{\pi(h-1)})(r_{\pi(h)})$$

only depends on residue classes modulo $q^{h-h'}$ of the elements $r_1 < r_2 < \dots < r_h$ and $d_1 < d_2 < \dots < d_{h'-1}$.

(2) For arbitrary $d_1 < d_2 < \dots < d_{h'-1}$, for each $d_{h'} \in D \setminus \{d_1, d_2, \dots, d_{h'-1}\}$ and for each permutation $\pi : \{1, 2, \dots, h' - 1\} \rightarrow \{1, 2, \dots, h' - 1\}$ the number (modulo q) of trees of the form

$$(d_1, r_{\pi(1)})(d_2, r_{\pi(2)}) \dots (d_{h'-1}, r_{\pi(h'-1)})(d_{h'})$$

only depends on residue classes modulo $q^{h-h'}$ of the elements $r_1 < r_2 < \dots < r_{h-1}$ and $d_1 < d_2 < \dots < d_{h'-1}$ and $d_{h'}$. ♣

Definition 6.4.2 For each permutation π of $\{1, 2, \dots, h'\}$ let $\mathcal{F}_{h'}^R(\pi; c_1, c_2, \dots, c_{h'}; s)$ denote the *block* of trees of the form $(d_1, r_{\pi(1)})(d_2, r_{\pi(2)}) \dots (d_{h'-1}, r_{\pi(h'-1)})(r_{\pi(h)})$ where $d_1 < d_2 < \dots < d_{h'-1}$, $r_1 < r_2 < \dots < r_{h'}$ and $r_1 = c_1$ modulo s , $r_2 = c_2$ modulo s , \dots , $r_{h'} = c_{h'}$ modulo s .

Similarly for each $k \in \{0, 1, \dots, h' - 1\}$ and for each permutation π of $\{1, 2, \dots, h' - 1\}$ we let $\mathcal{F}_{h'}^D(\pi, k; c_1, c_2, \dots, c_{h'-1}; s)$ denote the *block* of trees of the form

$$(d_1, r_{\pi(1)})(d_2, r_{\pi(2)}) \dots (d_{h'-1}, r_{\pi(h'-1)})(d_{\pi(h')})$$

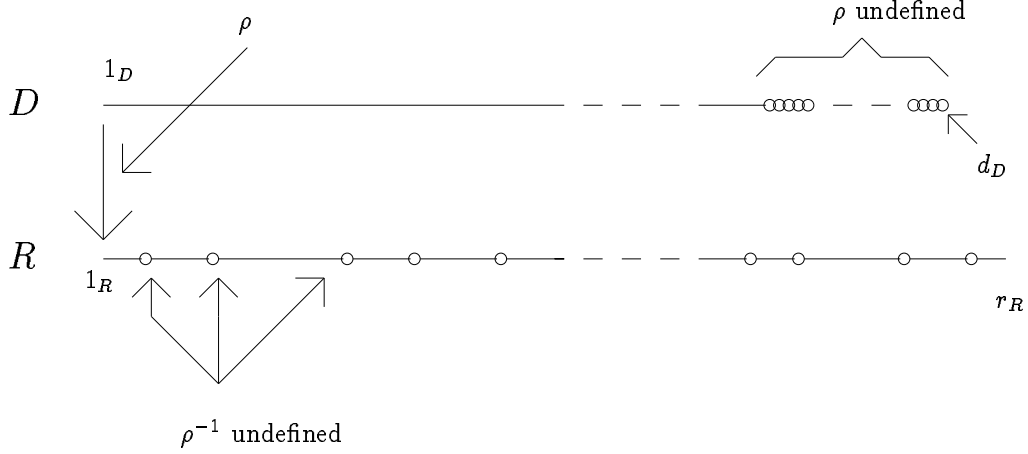
where $d_1 < d_2 < \dots < d_{h'-1}$, $d_k < d_{h'} < d_{k+1}$, $r_1 < r_2 < \dots < r_{h'}$ and $r_1 = c_1$ modulo s , $r_2 = c_2$ modulo s , \dots , $r_{h'-1} = c_{h'-1}$ modulo s . ♣

Notice that a forest on strong normal form can be got as a union (repetitions might appear) of blocks $\mathcal{F}_j^R(\pi; c_1, c_2, \dots, c_j; q^{h-j})$ and $\mathcal{F}_j^D(\pi, k; c_1, c_2, \dots, c_{j-1}; q^{h-j})$.

We are now ready to show that the regularity among the trees of height l (for suitable restrictions ρ) get inherited by the collection of trees of smaller height.

Lemma 6.4.3 (Stability) *Suppose d', d and h are given numbers such that $d' < d - h$. Let ρ be a restriction where $\text{dom}(\rho) = \{1, 2, \dots, d'\} \subseteq D$, where $d = |D|$ and where $\forall r, r' \in \text{Ran}(\rho) : |r - r'| = 0 \text{ modulo } q^h$. Assume ρ is monotone i.e. that for all $i, j \in \text{Dom}(\rho)$ with $i < j$ we have $\rho(i) < \rho(j)$. Suppose that \mathcal{F} is a forest on strong normal form and suppose that each tree in \mathcal{F} have height $\leq h$. Then \mathcal{F}^ρ remain on strong normal form.*

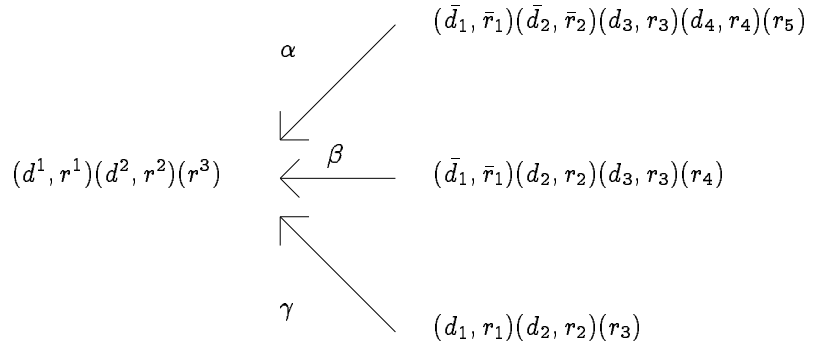
Proof: The restriction ρ is of the following form:



This choice of ρ is somewhat arbitrary. The main point of the choice is that the number of productions of a tree $(d^1, r^1)(d^2, r^2) \dots (d^{j-1}, r^{j-1})(r^j)$ (or $(d^1, r^1)(d^2, r^2) \dots (d^{j-1}, r^{j-1})(d^j)$) can be expressed as a (low-degree) polynomial (modulo q^h) in the elements $d^1, d^2, \dots, d^j, r^1, r^2, \dots, r^j$ (when these elements are enumerated according to their size in $D' := D \setminus \text{Dom}(\rho)$ and $R' := R \setminus \text{Ran}(\rho)$).

That this can be obtained is not surprising because the number of elements between any neighbours r and r' (in $R' := R \setminus \text{Dom}(\rho)$) is -1 modulo q^v for some $v = v(r, r') \geq h$.

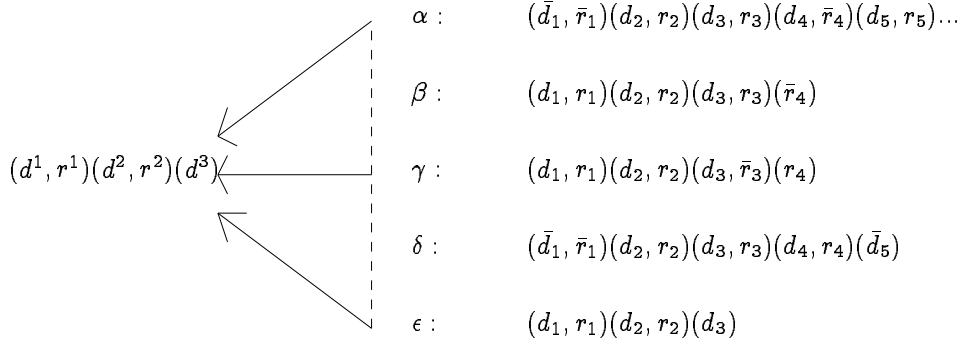
In order to avoid unreasonable heavy notation we illustrate the point by considering a few typical examples. The first diagram shows how the PU-trees of the form $(d^1, r^1)(d^2, r^2)(r^3)$ can arrive.



In the first case $d_3 := d^1, r_3 := r^1, d_4 := d^2, r_4 := r^2$ and $r_5 := r^3$. The bar indicates that ρ is defined for this element. There is one such tree for each \bar{r}_1, \bar{r}_2 (with $\langle \bar{d}_1, \bar{r}_1 \rangle \in \rho$ and

$\langle \bar{d}_2, \bar{r}_2 \rangle \in \rho$), which stand in the relation to r^1, r^2 and r^3 which is specified by π . This relation could for instance require that $\bar{r}_1 < \bar{r}_2$ and that $r^1 < \bar{r}_1, \bar{r}_2 < r^3$. Now this number α depends on $s := r^3 - r^1 - 1 - |R' \cap \{r^1 + 1, r^1 + 2, \dots, r^3 - 1\}|$ the number of possible choices of \bar{r}_1 and \bar{r}_2 . Let \hat{r}^3 and \hat{r}^1 denote the values of r^3 and r^1 in the enumeration of R' when these elements are listed according to size. Then clearly $s = r^3 - r^1 - (\hat{r}^3 - \hat{r}^1)$. In the example $\alpha = \binom{s}{2} = \binom{r^3 - r^1 - (\hat{r}^3 - \hat{r}^1)}{2}$. Now we assumed that $r^3 = r^1$ modulo q^h so α (modulo q) only depends on the values of \hat{r}^3 and \hat{r}^1 modulo q^2 (actually modulo q except when $q = 2$). In other words (in general) if the elements in R' are enumerated according to size, the flux α modulo q only depends on the values of r^1, r^2 and r^3 modulo $q^{h'}$ in the new enumeration. In the second case (where we consider the flux β) $d_2 := d^1, r_2 := r^1, d_3 := d^2, r_3 := r^2$ and $r_4 := r^3$. There is one such tree for each \bar{r}_1 which stand in the relation to r^1, r^2 and r^3 which is specified by π . The numbers β (modulo q) of such trees only depends (after having re-enumerated the elements in $R \setminus \text{Ran}(\rho)$ according to their size) on the values of r^1, r^2 and r^3 modulo $q^{h'}$ ($h' = 3$) in the new enumeration. The third case (where we consider the flux γ) $d_1 := d^1, r_1 := r^1, d_2 := d^2, r_2 := r^2$ and $r_3 := r^3$. There is exactly one such tree for each such three in the original block.

The next diagram show how the PU-trees of the form $(d^1, r^1)(d^2, r^2)(d^3)$ can arrive.



In the first case $d_2 := d^1, r_2 := r^1, d_3 := d^2, r_3 := r^2$ and $d_4 := d^3$. The bar indicate that the element either belong the domane or range of ρ . Furthermore $\langle \bar{d}_1, \bar{r}_1 \rangle \in \rho$. Again the number α (modulo q) of such threes are purely determined by r^1 and r^2 modulo $q^{h'}$ in the reenumeration. (where $h' = 3$ in this example). In the second case $d_1 := d^1, r_1 := r^1, d_2 := d^2, r_2 := r^2$ and $d_3 := d^3$. The bar on \bar{r}_4 (and lack of bar on r_3) indicates that \bar{r}_4 belongs to $\text{Ran}(\rho)$. The number β (modulo q) of such trees is purely determined by r^1 and r^2 modulo $q^{h'}$ in the reenumeration. The third case is treated simimilarly.

The case of δ is very interesting. Here $d_2 := d^1, r_2 := r^1, d_3 := d^2, r_3 := r^2$ and $d_4 := d^3$. The element \bar{d}_5 belongs to $\text{Dom}(\rho)$ and $\langle \bar{d}_1, \bar{r}_1 \rangle \in \rho$. The number of values by \bar{d}_5 depends on \bar{d}_1 . It is either $\bar{d}_1 - 1, d_2 - \bar{d}_1, d_3 - d_2, d_4 - d_3$ or $|\text{Dom}(\rho)| - d_4$. For each $\bar{d}_1 < d^1$ there is such a contribution. Thus the number δ is either $\frac{1}{2}(d^1 - 1)(d^1 - 2)$ or $d^1 \cdot d_2 - \frac{1}{2}d^1(d^1 - 1)$ or just $d^2 - d^1, d^3 - d^2$ or $|\text{Dom}(\rho)| - d^3$. So in all cases the number δ (modulo q) only depends on d^1, d^2 and d^3 (modulo q^2).

From these examples it should now be clear that the number of productions of a tree $(d^1, r^1)(d^2, r^2) \dots (d^{j-1}, r^{j-1})(r^j)$ (or $(d^1, r^1)(d^2, r^2) \dots (d^{j-1}, r^{j-1})(d^j)$) in general can be expressed as a polynomial (modulo q^h) of degree $\leq h - j$ in the elements $d^1, d^2, \dots, d^j, r^1, r^2, \dots, r^j$ (when these elements are enumerated according to there size in $D' := D \setminus \text{Dom}(\rho)$ and $R' := R \setminus \text{Ran}(\rho)$).

In the general argument it is worth noticing that $\binom{s}{j} = \binom{s'}{j}$ modulo q whenever $s = s'$ modulo q^j (whether q is a composite number or is a prime number). Thus \mathcal{F} remain on strong normal form when it is “hit” by ρ . \square

If we combine this lemma with lemma 6.2.4, 6.3.3 and lemma 6.3.3 we get:

Lemma 6.4.4 (Strong normal form) *Fix $q \in \mathbb{N} \setminus \{1\}$. For all $h, l \in \mathbb{N}$ there exists $d \in \mathbb{N}$ such that the following hold:*

*Suppose that $\mathcal{F} := \{T_1, T_2, \dots, T_u\}$ is a (D, R) -labelled forest of **PU**-trees where all trees have height $\leq h$ and where $|R| = |D| + q^l$. Then there exists a partial bijection $\rho : D \rightarrow R$ such that $\mathcal{F}^\rho := \{T_1^\rho, T_2^\rho, \dots, T_u^\rho\}$ is a forest of (D', R') -labelled trees (where $D' := D \setminus \text{dom}(\rho)$ and $R' := R \setminus \text{ran}(\rho)$) on the strong normal form.*

Furthermore if \mathcal{F} is (q, l) -exceptional, then \mathcal{F}^ρ is (q, l) -exceptional.

Now we are ready to show the main lemma (lemma 6.2.5)

Proof: By a similar reducing procedure as the one behind lemma 3.2.1 we can assume that all trees in \mathcal{F} are **PU**-trees. According to lemma 6.4.4 we lose no generality by assuming that \mathcal{F} is on strong normal form. Also we can assume that $|D| = 0$ modulo q^{k+1} . For each $d \in D$ and $r \in R$ we can consider the branch $\{< d, r >\}$ of length 1. It appears 0 modulo q^k times so we have the identity:

$$(1) \quad |(d, *) \rightsquigarrow| - |(d, r) \rightsquigarrow| + |(d)| + |(r)| = 0 \text{ modulo } q^k.$$

Here $(d, *) \rightsquigarrow$ is the collection of **PU**-trees (counted with multiplicity) of the form

$$(d, r_1)(u_1^2, u_2^2) \dots (u_1^{l-1}, u_2^{l-1})(u^l)$$

Similarly $(d, r) \rightsquigarrow$ is the collection of **PU**-trees of the form

$$(d, r)(u_1^2, u_2^2) \dots (u_1^{l-1}, u_2^{l-1})(u^l),$$

(d) the collection of copies of the tree (d) , and (r) is the collection of copies of the tree (r) . The forest \mathcal{F} is on strong normal form so $\sum_d |(d)| = 0$ modulo q^k and $\sum_r |(r)| = 0$ modulo $q^{\min(k, l)}$ where $|R| - |D| = q^l$. Later we assume $l \geq k$ so the number u of trees in \mathcal{F} is given by:

$$(2) \quad u = \sum_{d \in D} |(d, *) \rightsquigarrow| + \sum_{d \in D} |(d)| + \sum_{r \in R} |(r)| \\ = \sum_{d \in D} |(d, *) \rightsquigarrow|.$$

Now for each $d \in D$ consider $d_2, d_3, \dots, d_{l-1}, d_l$. Consider the set of trees of the form

$(d, r_1)(d_2, r_2) \dots (d_{l-1}, r_{l-1})(r_l)$ or $(d, r_1)(d_2, r_2) \dots (d_{l-1}, r_{l-1})(d_l)$ where r_1, r_2, \dots, r_l belongs to a certain type (expressed by the relative size of r_1, \dots, r_l , but also taking their residue classes modulo q^{l-h} into account). The number of such trees is 0 modulo q^{l-h} provided $|R| = |D| + q^l$. But then:

$$(3) \quad |(d, *) \rightsquigarrow| = 0 \text{ modulo } q^k \text{ for each } d \in D.$$

Thus $u = \sum_{d \in D} |(d, *) \rightsquigarrow| = 0$ modulo q^k . \square

6.5 Brief discussion of the general problem

The method provided in this paper only give an asymptotic classification of exceptional forest. This is good enough for a complete classification of the $\text{Count}(p)$ versus $\text{Count}(q)$ problem in the case of polynomial growth rate.

The fact that forests on the strong normal form remains on this form when ‘hit’ by a (randomly chosen?) restriction is very important. And it is very promising for the full classification (when n is large). The critical question is whether we can create order fast enough? Is it possible to create sufficiently much regularity before we have used the elements in $I = \{1, 2, \dots, n\}$?

In the first version of this paper I applied a different strategy to transform a hypothetically given exceptional forests \mathcal{F} into an exceptional forest on a normal form. This was done by selecting a suitable collection G of group actions on \mathcal{F} . For each $g \in G$ I defined a forest \mathcal{F}^g containing the same number of trees as \mathcal{F} . Now by a suitable choice of G (so $u \cdot |G| \not\equiv 0 \pmod{q}$) the forest $\bigcup_{g \in G} \mathcal{F}^g$ remains exceptional. By a proper choice of G it was argued that the resulting forest would get efficiently closer to the normal form. This idea did not *a priori* require any strong assumptions on the height of the forest. However the argument was incomplete and the revised version settled for a weaker (but sufficiently strong) version of this claim.

7 Some applications

There are various alternative formulations of the classification. It is well known that complexity theory can be viewed as recursion theory done within a finite set of unspecified size. The levels in Arithmetical Hierarchy correspond to the levels in Polynomial Hierarchy [8]. It can be argued that low complexity reasoning is reasoning which can be formalised within (arbitrarily large) finite structures. Suppose that the universe is such an unspecified finite set. Although this is almost impossible to picture it is consistent. Such an ‘axiomatic finite’ universe can be axiomatised in various ways. Its models (which are highly non-recursive) are of course not really finite.

As an example consider the following axiomatisation over second order logic. Suppose that we have the full Arithmetical comprehension axiom schema,

$$\forall z \exists \mathbf{X} \psi(x, z) \leftrightarrow x \in \mathbf{X}.$$

Here ψ is any first order formula. We allow ψ to contain set-variables. And assume that we have the usual induction axiom

$$0 \in \mathbf{X} \wedge \forall n (n \in \mathbf{X} \rightarrow n + 1 \in \mathbf{X}) \rightarrow \forall n n \in \mathbf{X}.$$

If the underlying universe was not assumed to be finite this would be the celebrated and powerful system \mathbf{ACA} of analysis. If the underlying universe is axiomatic finite (e.g. satisfies the pigeon-hole principle) we denote the axiom system by $\mathbf{ACA}^{\text{top}}$. For this system

Theorem 7.0.1 *$\text{Count}(p)$ holds in all structures of $\mathbf{ACA}^{\text{top}} + \text{Count}(q)$ exactly when all prime divisors in p appear in q .*

Proof: (Outline) Combine the conservation results in [22],[23] with results for Bounded Arithmetic. By these results $\mathbf{ACA}^{\text{top}}$ has the same deductive strength as $I\Delta_0(\alpha)$. By use of the usual

coding methods the system is able to handle terms of polynomial growth rate. Thus the positive part of the classification must remain valid if $I\Delta_0(\alpha)$ is replaced by ACA^{top} . \square

It is also possible to link the result to length of proofs in propositional logic. This type of link was first pointed out by J. Paris and A. Wilkie in [18].

Definition 7.0.2 A *Boolean formula* is a Boolean circuit where for each disjunction $\vee_j \pi_j$ and for each conjunction $\wedge_j \pi_j$ a particular bracketing is specified. The size and the depth of a Boolean formula is defined in the obvious way. In the calculation of the depth, disjunctions $\vee_j \pi_j$ and conjunctions $\wedge_j \pi_j$ are chosen maximally. \clubsuit

Definition 7.0.3 A *general propositional proof system* \mathbf{P} consists of:

(1) A finite number of substitution schemes.

A *substitution scheme* is a Boolean formula θ which only contains *special variables* (substitution variables). A *substitution instance* of θ is obtained by substituting the substitution variables y_1, \dots, y_k by Boolean formulas η_1, \dots, η_k .

(2) A finite number of deduction rules.

A *deduction rule* $\frac{\theta_1, \theta_2, \dots, \theta_k}{\theta}$ where $\theta_1, \dots, \theta_k$ and θ are substitution schemes. A substitution instance is obtained by substituting the substitution variables y_1, \dots, y_k by Boolean formulas η_1, \dots, η_k .

A \mathbf{P} -*proof* (in Hilbert style) of η is a sequence $\eta_1, \dots, \eta_u = \eta$ of Boolean formulas, such that each η_j , $j = 1, 2, \dots, u$ is either a substitution instance of a substitution scheme, or there are $i_1, \dots, i_k < j$ such that $\frac{\eta_{i_1}, \dots, \eta_{i_k}}{\eta_j}$ is a substitution instance of a deduction rule.

We only consider general propositional proof systems which are consistent and prove the usual tautologies.

The *size* s of a propositional proof is $s := \sum_j s(\eta_j)$, and the *depth* d is $d := \max_j d(\eta_j)$. \clubsuit

Definition 7.0.4 A *Frege proof system* (or a textbook proof system) is a general propositional proof system, where modus ponens $\frac{y_1, \neg y_1 \vee y_2}{y_2}$ is the only deduction rule. \clubsuit

Definition 7.0.5 Let $\text{Count}_n(p)$ denote the tautology:

$$(\vee_{i \leq n} \vee_{\{A: i \in A\}} \vee_{\{B: i \in B \wedge A \neq B\}} (p_A \wedge p_B)) \vee (\vee_{i \leq n} \wedge_{\{i \in A\}} \neg p_A)$$

where the sets A and B run through the p subsets of $\{1, 2, \dots, n\}$. \clubsuit

Theorem 7.0.6 Fix $p \in \mathbb{N}$. Let \mathcal{A}_p be the collection of all substitution schemes of the $\text{Count}(q)$ principle for $q \in \mathbb{N}$ which contain all prime factors of p . Let \mathbf{P} be any general proof system to which all the schemes in \mathcal{A}_p are added. Then the tautologies $\text{Count}_n(p)$, do not have bounded depth polynomial size \mathbf{P} -proofs.

Proof: Suppose that for arbitrarily large $n \in \mathbb{N}$, there exists a **P**-proof of depth $\leq d$ and size $\leq \exp(n^{\epsilon(n)})$. Let R be a suitable relation with domain \mathbb{N}^r , $r \in \omega$, which codes these proofs. Let \mathbf{M} be a countable non-standard model of $\text{Th}(\mathbb{N})$ over some countable language L which extends the language of Arithmetic and contains R . By overspill there exists a non-standard number $n \in \mathbf{M}$ which is not divisible by p , and there exists an \mathbf{M} -definable sequence $\theta_1, \theta_2, \dots, \theta_u$ of formulas, which (within \mathbf{M}) is a general propositional **P**-proof of $\text{Count}_n(p)$. Furthermore, we can assume that the depth of the proof is $\leq d$, and that the size of the proof is $\leq \exp(n^t)$ for some $t < \frac{1}{\omega}$ (the map $\epsilon : \mathbb{N} \rightarrow \mathbf{Q}_+$ can without loss of generality be assumed to be L -definable, because otherwise L can be extended with a relation which defines ϵ).

Now choose a generic truth-table evaluation $\tilde{\rho}_G$. Such an evaluation exists according to lemma 2.3.2. Consider the sequence $\theta_1, \dots, \theta_u$ (considered as circuits) and notice that $(\theta_u)^{\tilde{\rho}_G} = (\text{Count}_n(p))^{\tilde{\rho}_G} = 0$. According to corollary 2.4.2 there exists $j_0 \leq u$ such that $(\theta_{j_0})^{\tilde{\rho}_G} = 0$ but $(\theta_j)^{\tilde{\rho}_G} = 1$ for all $j < j_0$. Now each substitution instance θ_j of a substitution scheme has $(\theta_j)^\rho = 1$ for each general truth-table evaluation ρ . If θ_j is obtained from a deduction rule then $(\theta_j)^\rho = 1$ provided that all the premises also have truth-value 1.

Finally we claim that all substitution instances of the $\text{Count}(q)$ principle also get truth-value 1. Now if it got the truth value 0, then by the work in section 4 there would be a \mathbf{M} -definable generic system. By our refinement technique this would imply the existence of a specially labelled (I, p) -forest in which all branches appear 0 modulo q times. And the forest would contain a number of trees not divisible by q . According to the combinatorial results in section 6 this (first order) statement fails in the standard universe. We chose \mathbf{M} to be a model of first order arithmetic, so this is a contradiction. \square

Theorem 7.0.7 *Let \mathbf{M} be a countable non-standard model of $\text{Th}(\mathbb{N})$ over a countable first order language L which extend the language of arithmetic. Suppose that $p \in \mathbb{N}$, $p \geq 2$ and $I := \{1, 2, \dots, n\} \subseteq \mathbf{M}$ for some $n \in \mathbf{M} \setminus \omega$ not divisible by p . Let*

$$\mathbf{M}_n^* := \{m \in \mathbf{M} : t(n) > m \text{ for some term } t \in L\}.$$

For any generic filter ρ_G the partition $\tilde{\rho}_G$ (see definition 2.2.5) partitions I into disjoint classes, each containing exactly p elements. If the terms $t \in L$ all have polynomial growth rate

- (a) $(\mathbf{M}_n^*, \rho_G) \models \neg \text{Count}(p)$.
- (b) (\mathbf{M}_n^*, ρ_G) satisfies induction for bounded $L(P)$ -formulas.
- (c) $(\mathbf{M}_n^*, \rho_G) \models \text{Count}(q)$ for all q which contains all prime factors in p .

Proof: It suffices to show that the least number principle is valid for bounded $L(P)$ -formulas with parameters in \mathbf{M}_n^* . Now each instance of the least number principle gets translated into a Boolean circuit (or Boolean formula if we specify the bracketing) of the form $\text{LNP}_n(\pi_1, \dots, \pi_u) := \pi_u \vee (\vee_{j \leq u} (\neg \pi_j \wedge (\wedge_{k < j} \pi_k)))$. Furthermore, according to earlier observation, each translated instance gets depth ≤ 4 and size $\leq \exp(n^t)$ for some $t < n^{\frac{1}{\omega}}$. According to the key lemma (lemma 2.4.1) for any generic filter ρ_G if $(\pi_u)^{\tilde{\rho}_G} = 1$, there exists $j_0 \leq u$ with $(\pi_{j_0})^\rho = 1$ and $(\pi_j)^\rho = 0$ for $j < j_0$. A simple argument shows that $\text{LPN}_n(\pi_1, \dots, \pi_u)^{\tilde{\rho}_G} = 1$. Using lemma 2.1.6 $(\mathbf{M}, \tilde{\rho}_G)$ satisfies induction for bounded $L(P)$ -formulas with parameters in \mathbf{M}_n^* .

Again all $\text{Count}(q)$ much be forced true when p contains a prime factor not in q . If not there would exist an \mathbf{M} -definable generic system. And thus by the refinement argument there would be

a (I, p) forest with $\neq 0$ modulo q trees, in which each (type of) branch appears 0 modulo q times. This is a contradiction when p does not divide q . \square

Theorem 7.0.8 *Suppose that all terms in L have polynomial growth rate, and contains at least one unspecified relation symbol. Then $I\Delta_0(L) + \text{Count}(q)$ prove $\text{Count}(p)$ exactly when all prime factors in p divides q .*

Proof: $(M_n^*, \tilde{\rho}_G) \models I\Delta_0(L) + \neg \text{Count}(p) + \text{Count}(q)$. \square

8 Final remarks

The first version of this paper contained the complete reduction of the $\text{Count}(p)$ versus $\text{Count}(q)$ problem. This reduced the problem to a purely combinatorial problem. The revised version of the paper solves this problem explicitly (in the case of polynomial growth-rate). In addition the revised paper develops the underlying theory in more details.

To end I would like to thank P. Beame, J. Krajicek, A. Macintyre, P. Pudlak, A. Razborov, M. Thorup and A. Wilkie for many helpful remarks and comments. Independent of this paper it has been shown that the topic is related to Hilbert's Nullstellensatz (P. Beame, R. Impagliazzo, J. Krajicek, T. Pitassi, P. Pudlak [6]), as well as related to the representation theory of the symmetrical groups (M. Ajtai [4]). I hope these links will be further clarified and developed in the future.

References

- [1] M. Ajtai; Definability in first order structures; Annals of Pure and Applied Logic 24, (1983) pp 1-48.
- [2] M. Ajtai; On the complexity of the pigeonhole principle. 29th Annual symp. on Found. Comp.Sci.(1988),pp 340-355.
- [3] M. Ajtai; Parity and the pigeon-hole principle, in Feasible Mathematics Birkhauser, (1990), pp 1-24.
- [4] M. Ajtai; The independence of the modulo p counting principles, preprint.
- [5] Barrington, Beigel, Rudich; Representing Boolean functions as Polynomials Modulo composite numbers, 24th ACM STOC (1992) pp 455-461.
- [6] P. Beame, R. Impagliazzo, J. Krajicek, T. Pitassi, P. Pudlak; Lower bounds on Hilberts Nullstellensatz and propositional proofs, preliminary version.
- [7] A. Berrarducci, B. Intrigila; Combinatorial principles in elementary number theory, Annals of Pure and Applied Logic 55 (1991) pp 35-50.
- [8] S. Buss; Bounded Arithmetic. Ph.D. dissertation, Princeton University, (1985). As book, Bibliopolis, Napoli (1986).

- [9] S. Buss; The propositional pigeonhole principle has polynomial size Frege proofs, *Journal of Symbolic logic* 52 (1987) pp 916-927
- [10] P. Clote, J. Krajicek, ; Open problems in: *Arithmetic, Proof theory and computorial complexity*, Oxford university press (1993) pp 289-319.
- [11] S. Cook, A. Recknow; The relative efficiency of Propositional proof systems, *Journal of Symbolic logic* 44 (1977) pp 36-50
- [12] Furst, Saxe, Simpser; Parity circuits and the polynomial time hierarchy, *Proc 22nd IEEE FOCS* (1981) pp 260-270.
- [13] J. Haastad; Almost optimal lower bounds for small depth circuits, *Proc 18th ACM STOC* (1986) pp 6-20. J. Haastad; *Computorial limitations for small depth circuits*, Ph.D thesis M.I.T. (1986)
- [14] J. Krajicek; *On Frege and Extended Frege Proof Systems*. To appear.
- [15] J. Krajicek, P. Pudlak, and A. Wood, Exponential lower bound to the size of bounded depth Frege proofs of the pigeonhole principle, submitted (1991).
- [16] A. Macintyre; The strength of weak systems, in: *Schriftenreihe der Wittgenstein Gessellschaft* 13, *Logic, Philosophy of Science and Epistemology*, Wien (1987) pp43-50.
- [17] J. Paris, A. Wilkie, A. Woods; Provability of the pigeonhole principle and the existence of infinitely many primes. *Journal of Symbolic Logic* 53, (1988), pp 1231-1244.
- [18] J. Paris, A. Wilkie; Counting problems in Bounded Arithmetic, in: *Methods in Mathematical Logic*, LNM 1130, Springer (1985), pp 317-340.
- [19] T. Pitassi, P. Beame, and R. Impagliazzo; Exponential lower bounds for the pigeonhole principle, preprint (1991).
- [20] T. Pitassi, P. Beame; An Exponential separation between the Matching Principle and the pigeonhole principle. *Proceedings 8th-annual IEEE symposium on computer science* (1993), pp 308-319
- [21] A. Razborov; On the method of approximation, in: *Proc. 21th ACM STOC* (1989) pp 168-176.
- [22] S. Riis; Making infinite structures finite in models of Second Order Bounded Arithmetic, in: *Arithmetic, Proof theory and computorial complexity*, Oxford university press (1993) pp 289-319.
- [23] S. Riis; *Independence in Bounded Arithmetic*; DPhil dissertation, Oxford University (1993)
- [24] S. Riis; *Count(p) versus the pigeon-hole principle*; Forthcomming in *The Arkive of Logic*.
- [25] R. Smolensky; Algebraic methods in the theory of lower bounds for boolean circuit complexity; *Proc. 19th ACM STOC* (1987) pp 77-82.