Basic Research in Computer Science

BRICS RS-94-26 S. Riis: Count(q) versus the Pigeon-Hole Principle

Count(q) versus the Pigeon-Hole Principle

Søren Riis

BRICS Report Series **RS-94-26**

ISSN 0909-0878 **August 1994**

See back inner page for a list of recent publications in the BRICS Report Series. Copies may be obtained by contacting:

**BRICS
Department of Computer Science
University of Aarhus
Ny Munkegade, building 540
DK - 8000 Aarhus C
Denmark**

**Telephone: +45 8942 3360
Telefax: +45 8942 3255
Internet: BRICS@daimi.aau.dk**

Count(q) versus the Pigeon-Hole Principle

Søren Riis
BRICS*

June 1994

Abstract

For each $p \leq 2$ there exist a model $\mathbb{M}^*$ of $I\Delta_0(\alpha)$ which satisfies the Count(p) principle. Furthermore if p contain all prime factors of q there exist $n, r \in \mathbb{M}^*$ and a bijective map $f \in \text{Set}(\mathbb{M}^*)$ mapping $\{1, 2, ..., n\}$ onto $\{1, 2, ..., n + q^r\}$.

A corollary is a complete classification of the Count(q) versus Count(p) problem. Another corollary solves an open question ([3]).

In this note I state and prove a Theorem which actually can be viewed as the main result of [9].

Theorem: *Suppose that $r(n)$ is an function with*

(a) $lim_{n\to\infty}\ r(n) = \infty$.

(b) *For all* $\epsilon > 0$ $lim_{n\to\infty} \frac{q^{r(n)}}{n^\epsilon} = 0$

For each $q, p \geq 2$ Count(p) $\not\vdash$ $\text{PHP}^*_{*+q^{r(*)}}(\text{bij})$ *if p divides a power of q.*

Here $\text{PHP}^*_{*+s}(\text{bij})$ is the the elementary principle stating that *there does not exists n and a bijective map from* $\{1, 2, ..., n\}$ *onto* $\{1, 2, ..., n + s\}$.And Count(p) is the elementary matching principle stating that *if* $\{1, 2, ..., n\}$ *is divided into disjoint p-element subsets, then p divides n.*

Proof: As in [9] let $\mathbb{M}$ be a countable non-standard model of first order Arithmetic. Then by a similar forcing construction (which actually avoids

*Basic Research in Computer Science, Centre of the Danish National Research Foundation.

certain technical problems) we expand $\mathbb{M}$ by a generic bijection f mapping $\{1, 2, ..., n\}$ onto $\{1, 2, ..., n + q^{r(n)}\}$. Assumption (a) allows us to assume that $q^{r(n)}$ is a non-standard number. Furthermore condition (b) ensures that the circuit collapsing argument goes through. Now it follows by the analysis in [9] that the Count(p) principle can never be forced false. If it was false, there would exists an impossible $\mathbb{M}$-definable object. In this case a forest of (D, R)-labelled trees where $\mid R \mid - \mid D \mid = q^{r(n)}$, but where all trees would have hight dominated by some standard number. This violates the main lemma (lemma 6.1.5) in [9]. Finally $\mathbb{M}^*$ is got a the initial segment $\{m \in \mathbb{M} : \; n^k > m, k \in \mathbb{N}\}$. □

Corollary 1: *Let $r(n)$ be as above. For each $q, p \geq 2$*
Count(p) $\not\vdash$ $\text{PHP}^*_{*+q^{r(*)}}$(bij) *if and only if p divides a power of q.*

Corollary 2: *For fixed $q, p \geq 2$ the following is equivalent*

(a) *p divides a power of q*

(b) Count*(q)* $\vdash$ Count*(p).*

Proof: The implication (a) $\Rightarrow$ (b) was shown in [4] or [9]. The implication (b) $\Rightarrow$ (a) follows from the Theorem. According to the Theorem Count(p) $\not\vdash$ $\text{PHP}^*_{*+q^{r(*)}}$(bij) if Count($q$) $\vdash$ Count(p). But then by the easy 'only if' in corollary 1, p must divide a power of q. □

Let PHP^{*+p}_*(inj) be the the statement that *there is no n and no injective map from* $\{1, 2, ..., n+p\}$ *into* $\{1, 2, ..., n\}$ and let PHP^*_{*+p}(sur) be the statement that *there is no n and no surjective map from* $\{1, 2, .., n\}$ *onto* $\{1, 2, ..., n+p\}$.

Corollary 3:

(a) PHP^*_{*+1}(bij) $\not\vdash$ PHP^{*+1}_*(inj).

(b) PHP^{*+1}_*(inj) $\dashv\vdash$ PHP^*_{*+1}(sur).

(c) Count*(q)* $\not\vdash$ PHP^{*+1}_*(inj).

Proof: (b) is a simple exercise, and (a) clearly follows from (c). To show (c) notice that PHP^{*+1}_*(inj) $\vdash$ $\text{PHP}^*_{*+q^{r(*)}}$(bij) for any r. □

This solves an open question concerning the strength of the pigeon hole principle for injective maps [3]. Actually it shows that:

Corollary 4: *There exists a model $\mathbb{M}^*$ of $I\Delta_0(\alpha)$ in which* Count*(p) holds for each $p \in \mathbb{N} \setminus \{1\}$. Yet, there exists $n \in \mathbb{M}^*$ and an injective map $f \in$* Set($\mathbb{M}^*$) *mapping $\{1, 2, ..., n+1\}$ into $\{1, 2, ..., n\}$.*

Proof: By the completeness theorem it suffice to show that for each finite set $p_1, p_2, .., p_l$ of integers, the conjunction Count(p_1) $\wedge$ ....$\wedge$ Count(p_l) does not imply PHP_*^{*+1}(inj). This follows by an argument similar to the one given for (c) in corollary 3. □

References

[1] M.Ajtai; On the complexity of the pigeonhole principle. 29^{th} Annual symp. on Found. Comp.Sci.(1988),pp 340-355.

[2] M.Ajtai; Parity and the pigeon-hole principle, in Feasible Mathematics Birkhauser, (1990), pp 1-24.

[3] M.Ajtai; The independence of the modulo p counting principles, Proceedings 9^{th}-annual IEEE symposium on computer science (1994).

[4] P.Beame, R. Impagliazzo, J. Krajicek, T. Pitassi, P. Pudlak; Lower bounds on Hilbert's Nullstellensatz and propositional proofs, preliminary version.

[5] J.Krajicek, P.Pudlak, and A.Wood, Exponential lower bound to the size of bounded depth Frege proofs of the pigeonhole principle, submitted (1991).

[6] T.Pitassi, P.Beame, and R.Impagliazzo; Exponential lower bounds for the pigeonhole principle, preprint (1991).

[7] T.Pitassi, P.Beame; An Exponential separation between the Matching Principle and the pigeonhole principle. Proceedings 8^{th}-annual IEEE symposium on computer science (1993), pp 308-319

[8] S.M.Riis; Independence in Bounded Arithmetic; DPhil dissertation, Oxford University (1993)

[9] S.M.Riis; Count(q) does not imply Count(p); Submitted to APAL. Report Series, BRICS RS-94-21.

Recent Publications in the BRICS Report Series

RS-94-26 Søren Riis. ***Count(q) versus the Pigeon-Hole Principle*****. August 1994, 3 pp.**

RS-94-25 Søren Riis. ***Bootstrapping the Primitive Recursive Functions by 47 Colors*****. August 1994, 5 pp.**

RS-94-24 Søren Riis. ***A Fractal which violates the Axiom of Determinacy*****. August 1994, 3 pp.**

RS-94-23 Søren Riis. ***Finitisation in Bounded Arithmetic*****. August 1994, 31 pp.**

RS-94-22 Torben Braüner. ***A General Adequacy Result for a Linear Functional Language*****. August 1994, 39 pp. Presented at MFPS '94.**

RS-94-21 Søren Riis. ***Count(q) does not imply Count(p)*****. July 1994, 55 pp.**

RS-94-20 Peter D. Mosses and Martín Musicante. ***An Action Semantics for ML Concurrency Primitives*****. July 1994, 21 pp. To appear in Proc. FME '94 (Formal Methods Europe, Symposium on Industrial Benefit of Formal Methods), LNCS, 1994.**

RS-94-19 Jens Chr. Godskesen, Kim G. Larsen, and Arne Skou. ***Automatic Verification of Real–Timed Systems Using*** EPSILON**. June 1994, 8 pp. Appears in: Protocols, Specification, Testing and Verification PSTV '94.**

RS-94-18 Sten Agerholm. ***LCF Examples in HOL*****. June 1994, 16 pp. To appear in:** ***Proceedings of the 7th International Workshop on Higher Order Logic Theorem Proving and its Applications*****, LNCS, 1994.**

RS-94-17 Allan Cheng. ***Local Model Checking and Traces*****. June 1994, 30 pp.**

RS-94-16 Lars Arge. ***External-Storage Data Structures for Plane-Sweep Algorithms*****. June 1994, 37 pp.**