BRICS

Basic Research in Computer Science

BRICS RS-00-12 U. Kohlenbach: Intuitionistic Choice and Restricted Classical Logic

Intuitionistic Choice and Restricted Classical Logic

Ulrich Kohlenbach

BRICS Report Series RS-00-12

ISSN 0909-0878 May 2000

See back inner page for a list of recent BRICS Report Series publications. 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@brics.dk

BRICS publications are in general accessible through the World Wide Web and anonymous FTP through these URLs:

http://www.brics.dk
ftp://ftp.brics.dk
This document in subdirectory RS/00/12/

Intuitionistic choice and restricted classical logic

Ulrich Kohlenbach

BRICS[*]
Department of Computer Science
University of Aarhus
Ny Munkegade
DK-8000 Aarhus C, Denmark
kohlenb@brics.dk

May 2000

Abstract

Recently, Coquand and Palmgren considered systems of intuitionistic arithmetic in all finite types together with various forms of the axiom of choice and a numerical omniscience schema (**NOS**) which implies classical logic for arithmetical formulas. Feferman subsequently observed that the proof theoretic strength of such systems can be determined by functional interpretation based on a non-constructive μ-operator and his well-known results on the strength of this operator from the 70's.

In this note we consider a weaker form **LNOS** (lesser numerical omniscience schema) of **NOS** which suffices to derive the strong form of binary König's lemma studied by Coquand/Palmgren and gives rise to a new and mathematically strong semi-classical system which, nevertheless, can proof theoretically be reduced to primitive recursive arithmetic **PRA**. The proof of this fact relies on functional interpretation and a majorization technique developed in a previous paper.

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

In [6], systems of intuitionistic arithmetic in all finite types extended by various kinds of the axiom of choice and the schema of numerical omnisience

$$\textbf{NOS:}\ \forall n(A(n) \vee \neg A(n)) \to \forall n\, A(n) \vee \exists n \neg A(n),$$

where n ranges over the natural numbers and A is any formula[1], are studied.

In [5], Feferman noticed that the proof theoretic strength of such systems can be determined by functional interpretation based using his non-constructive μ-operator and his classical results on the strength of systems based on this operator (see [1] for a survey of those results).

In this note we show that a similar use of functional interpretation combined with the majorization arguments which we developed in [8] can be used to determine the strength of systems which instead of **NOS** are based on the weaker schema of lesser numerical omnisience

$$\textbf{LNOS} :\equiv \begin{cases} \forall n^0((A(n) \vee \neg A(n)) \wedge (B(n) \vee \neg B(n)))\wedge \\ \neg(\exists n A(n) \wedge \exists n B(n)) \to \forall n \neg A(n) \vee \forall n \neg B(n), \end{cases}$$

which generalizes the well-known 'lesser limited principle of omniscience' (see [2] for various equivalent formulations of this principle)

$$\textbf{LLOP} :\equiv \forall f^0, g^0(\neg(\exists n(fn = 0) \wedge \exists n(gn = 0)) \to \forall n(fn \neq 0) \vee \forall n(gn \neq 0))$$

in the same way as **NOS** generalizes **LPO**.
We will define a system based on **LNOS** and the full axiom schema of choice **AC** which allows to prove the version of König's lemma studied in [6] and is Π^0_2-conservative over **PRA**.

In the following $\mathbf{HA}^\omega$ and $\widehat{\mathbf{HA}}^\omega$ are the systems of arithmetic in all finite types denoted by WE-HA$^\omega$ and WE-$\widehat{\mathrm{HA}}^\omega$ in [1], where, however, the quantifier-free rule of extensionality is defined as

$$\frac{\vdash A_0 \to s =_\rho t}{\vdash A_0 \to r[s] =_\tau r[t],}$$

where A_0 is quantifier-free.[2] $\widehat{\mathbf{HA}}^\omega$ contains only recursion on type 0 and induction restricted to Σ^0_1-formulas. $\widehat{\mathbf{HA}}^\omega\!\upharpoonright$ is the still weaker system with quantifier-free induction only.

[1] A may contain arbitrary parameters.

[2] '$\vdash$' indicates that further non-logical axioms are not allowed to be used in the proof of a premise of that rule. This restriction is necessary for the deduction theorem to hold true which we will use below.

$\mathbf{E\text{-}HA}^\omega$ and $\mathbf{E\text{-}}\widehat{\mathbf{HA}}^\omega$ are the corresponding systems with full extensionality.

The axiom schema of choice is given by

$$\mathbf{AC}^{\rho,\tau} : \forall x^\rho \exists y^\tau A(x,y) \to \exists Y^{\rho\to\tau} \forall x^\rho A(x, Yx), \quad \mathbf{AC} := \bigcup_{\rho,\tau} \{\mathbf{AC}^{\rho,\tau}\}.$$

The axiom schema of unique choice is given by

$$\mathbf{AC!}^{\rho,\tau} : \forall x^\rho \exists ! y^\tau A(x,y) \to \exists Y^{\rho\to\tau} \forall x^\rho A(x, Yx).$$

Lemma 1 $\mathbf{HA}^\omega$**+**$\mathbf{AC}^{0,0}$**+LLOP** $\vdash$ **LNOS.** *Similarly for* $\widehat{\mathbf{HA}}^\omega\restriction$ *instead of* $\mathbf{HA}^\omega$.

Proof: By intuitionistic logic and $0 \neq 1$ one proves that

$$\forall n^0 (A(n) \vee \neg A(n)) \to \forall n^0 \exists k^0 ([k = 0 \to A(n)] \wedge [k \neq 0 \to \neg A(n)]).$$

By $\mathbf{AC}^{0,0}$ and the stability of $=_0$ this yields

$$\exists f \forall n (f(n) = 0 \leftrightarrow A(n)).$$

Likewise, we get a characteristic function for $B(n)$. So by applying **LLOP** to f, g we obtain **LNOS**. $\square$

In the following, $\mathbf{M}^\omega$**,** $\mathbf{IP}_0^\omega$ denote the Markov principle resp. the independence-of-premise principle from [11](3.5.10).

Theorem 2 *1)* $\mathbf{HA}^\omega$**+AC+**$\mathbf{M}^\omega$**+**$\mathbf{IP}_0^\omega$**+LNOS** *is* Π_2^0*-conservative over* **HA**.

2) $\widehat{\mathbf{HA}}^\omega$**+AC+**$\mathbf{M}^\omega$**+**$\mathbf{IP}_0^\omega$**+LNOS** *is* Π_2^0*-conservative over* **PRA**.

If **AC** *is replaced by* $\mathbf{AC}^{0,\tau}$ *plus* $\mathbf{AC!}^{1,\tau}$ *(with arbitrary* τ*) and* $\mathbf{M}^\omega$ *and* $\mathbf{IP}_0^\omega$ *are restricted to instances containing only quantified variables of types* ≤ 1*, then the above conservation results also hold for the fully extensional systems* $\mathbf{E\text{-}HA}^\omega$ *and* $\mathbf{E\text{-}}\widehat{\mathbf{HA}}^\omega$.

Proof: 1) By the lemma above it is sufficient to consider **LLOP**. So let

$$\mathbf{HA}^\omega\mathbf{+AC+M}^\omega\mathbf{+IP}_0^\omega \vdash \mathbf{LLOP} \to \forall x \exists y\, R(x,y),$$

where $\forall x \exists y\, R(x,y)$ is a Π_2^0-sentence in $\mathcal{L}(\mathbf{HA})$.
Relative to $\mathbf{HA}^\omega$ we can write **LLOP** equivalently as

$$\forall n, \tilde{n} (fn \neq 0 \vee g\tilde{n} \neq 0) \to \exists k \leq 1 ([k = 0 \to \forall n (fn \neq 0)] \wedge [k \neq 0 \to \forall n (gn \neq 0)]).$$

The latter is implied by

$$\exists k \leq 1 \forall z (\underbrace{\forall n, \tilde{n} \leq z (fn \neq 0 \vee g\tilde{n} \neq 0) \to ([k=0 \to fz \neq 0] \wedge [k \neq 0 \to gz \neq 0])}_{A_0(f,g,k,z):\equiv}),$$

where A_0 can be written as a quantifier-free formula.
Hence

$$(*)\ \mathbf{HA}^\omega + \mathbf{AC} + \mathbf{M}^\omega + \mathbf{IP}_0^\omega \vdash \forall f, g \exists k \leq 1 \forall z\, A_0(f,g,k,z) \to \forall x \exists y\, R(x,y).$$

By a combination of functional interpretation and majorization as used in [8] one can reduce the use of

$$\forall f, g \exists k \leq 1 \forall z\, A_0(f,g,k,z)$$

to

$$\forall f, g, z \exists k \leq 1 \forall \tilde{z} \leq z\, A_0(f,g,k,\tilde{z}).$$

For the sake of completeness we sketch the proof here: $(*)$ implies

$$\mathbf{HA}^\omega + \mathbf{AC} + \mathbf{M}^\omega + \mathbf{IP}_0^\omega \vdash \forall x \forall F \leq_\rho 1^\rho \exists f, g, z, y (A_0(f,g,Ffg,z) \to R(x,y)),$$

where $\rho := 1 \to (1 \to 0)$, $\leq_\rho$ is defined pointwise and $1^\rho := \lambda f, g.1$.
By functional interpretation (see [11](3.5.10)) one extracts a closed term Φ of $\mathbf{HA}^\omega$ such that

$$\mathbf{HA}^\omega \vdash \forall x \forall F \leq 1 (\forall f, g\, A_0(f,g,Ffg,\Phi F x) \to \exists y\, R(x,y)).$$

By [7], Φ has a majorizing functional Φ^* and hence (using basic properties of majorization in Howard's sense)

$$\mathbf{HA}^\omega \vdash \forall x \forall F \leq 1 (tx := \Phi^* 1^\rho x \geq \Phi F x).$$

Put together we get

$$\mathbf{HA}^\omega \vdash \forall x \forall F \leq 1 (\forall f, g \forall z \leq tx A_0(f,g,Ffg,z) \to \exists y\, R(x,y))$$

and hence

$$\mathbf{HA}^\omega \vdash \forall z \exists F \leq 1 \forall f, g \forall \tilde{z} \leq z\, A_0(f,g,Ffg,\tilde{z}) \to \forall x \exists y\, R(x,y).$$

Since F can be obtained by primitive recursive definition by cases this yields

$$\mathbf{HA}^\omega \vdash \forall f, g, z \exists k \leq 1 \forall \tilde{z} \leq z\, A_0(f,g,k,\tilde{z}) \to \forall x \exists y\, R(x,y).$$

However, $\forall f, g, z \exists k \leq 1 \forall \tilde{z} \leq z\, A_0(f, g, k, \tilde{z})$ can easily be verified in $\mathbf{PA}^\omega$ and hence (using negative translation and the fact that this statement can be written as a purely universal sentence) in $\mathbf{HA}^\omega$. Thus $\mathbf{HA}^\omega \vdash \forall x \exists y\, R(x, y)$. The theorem now follows by the well-known conservation of $\mathbf{HA}^\omega$ over $\mathbf{HA}$.

2) The proof is analogous to 1) using that $\widehat{\mathbf{PA}}^\omega$ has a negative translation into $\widehat{\mathbf{HA}}^\omega + \mathbf{M}^\omega$ and the latter has a functional interpretation in $\widehat{\mathbf{HA}}^\omega\!\restriction$ which is Π^0_2-conservative over $\mathbf{PRA}$.

The claim for the fully extensional systems follows by the well-known elimination of extensionality technique (see [10] for details). $\square$

In [6] an extension of the usual weak König's lemma WKL to binary trees given by arbitrary formulas $\Phi(\underline{x}, m)$ which are decidable in the variable m which defines the tree, i.e. $\forall m(\Phi(\underline{x}, m) \vee \neg\Phi(\underline{x}, m))$. Let's call that schema **DWKL** (see [6] p.57 for details).

Theorem 3 *Both* $\mathbf{HA}^\omega + \mathbf{AC}^{0,0} + \mathbf{LNOS}$ *and* $\widehat{\mathbf{HA}}^\omega\!\restriction + \mathbf{AC}^{0,0} + \mathbf{LNOS}$ *prove* $\mathbf{DWKL}$.

Proof: We show the theorem for $\widehat{\mathbf{HA}}^\omega\!\restriction + \mathbf{AC}^{0,0} + \mathbf{LNOS}$. Analogously to the proof of the lemma above one verifies that $\widehat{\mathbf{HA}}^\omega\!\restriction + \mathbf{AC}^{0,0}$ allows to reduce **DWKL** to the usual weak König's lemma WKL as defined in [12]:

WKL:$\equiv \forall f^1(T(f) \wedge \forall x^0 \exists n^0(lth(n) = x \wedge fn = 0) \to \exists b^1 \forall x^0(f(\overline{b}x) = 0))$, where

$Tf :\equiv \forall n^0, m^0(f(n * m) =_0 0 \to fn =_0 0) \wedge \forall n^0, x^0(f(n * \langle x \rangle) =_0 0 \to x \leq_0 1)$.

Consider the formula[3]

$$(+) \begin{cases} \forall x^0 \exists n \leq_0 1 \forall k > 0(\exists m \leq \overline{1}k(lth(m) = k \wedge f(x * m) = 0) \\ \to \exists m \leq \overline{1}(k \dot{-} 1)(lth(m) = k \dot{-} 1 \wedge f(x * \langle n \rangle * m) = 0)). \end{cases}$$

We first show that $\widehat{\mathbf{PA}}^\omega\!\restriction \vdash T(f) \to (+)$, where $\widehat{\mathbf{PA}}^\omega\!\restriction$ is the classical counterpart of $\widehat{\mathbf{HA}}^\omega\!\restriction$: Let x be arbitrary but fixed.

Case 1: $\forall k > 0 \exists m \leq \overline{1}k(lth(m) = k \wedge f(x * m) = 0)$.

Then classical logic yields

$$\forall k > 0 \exists m \leq \overline{1}k(lth(m) = k \wedge f(x * \langle 0 \rangle * m) = 0) \vee$$
$$\forall k > 0 \exists m \leq \overline{1}k(lth(m) = k \wedge f(x * \langle 1 \rangle * m) = 0).$$

[3]Here we use that our coding of finite sequences has the property that $\forall n, m, f, g(n \geq m \wedge \forall x(fx \geq gx) \to \overline{f}n \geq \overline{g}m)$, which can be arranged.

In the case the first disjunct is true, choose $n = 0$ and $n = 1$ otherwise.
Case 2: $\exists k > 0 \neg \exists m \leq \overline{1}k(lth(m) = k \wedge f(x * m) = 0)$. By the quantifier-free least-number-principle (hence by the schema QF-IA of quantifier-free induction) we find the least such k. Call it k_0.
2.1: $k_0 = 1$: Choose $n \leq 1$ arbitrarily.
2.2: $k_0 > 1$: Then

$$\exists m \leq \overline{1}(k_0 \dot{-} 1)(lth(m) = k_0 \dot{-} 1 \wedge f(x * m) = 0).$$

choose $n := (m)_0$ for such an m. This finishes the proof of $\widehat{\mathbf{PA}}^\omega\!\upharpoonright \vdash T(f) \to (+)$. By negative translation we get

$$\widehat{\mathbf{HA}}^\omega\!\upharpoonright \vdash T(f) \to (+)',$$

where

$$(+)' :\equiv \begin{cases} \forall x^0 \neg\neg \exists n \leq_0 1 \forall k > 0 (\exists m \leq \overline{1}k(lth(m) = k \wedge f(x * m) = 0) \\ \to \exists m \leq \overline{1}(k \dot{-} 1)(lth(m) = k \dot{-} 1 \wedge f(x * \langle n \rangle * m) = 0)). \end{cases}$$

But $\widehat{\mathbf{HA}}^\omega\!\upharpoonright + \mathbf{LLOP} \vdash (+)' \to (+)$. Hence

$$\widehat{\mathbf{HA}}^\omega\!\upharpoonright + \ \mathbf{LLOP} \ \vdash T(f) \to (+).$$

Assume $T(f) \wedge \forall x \exists n(lth(n) = x \wedge fn = 0)$.
By applying $\mathbf{AC}^{0,0}$ to $(+)$ we get a function g such that

$$\begin{cases} \forall x^0 (gx \leq_0 1 \wedge \forall k > 0 (\exists m \leq \overline{1}k(lth(m) = k \wedge f(x * m) = 0) \\ \to \exists m \leq \overline{1}(k \dot{-} 1)(lth(m) = k \dot{-} 1 \wedge f(x * \langle gx \rangle * m) = 0))). \end{cases}$$

Define $\tilde{h}(0) := \langle \rangle, \ \tilde{h}(n+1) := \tilde{h}(n) * \langle g(\tilde{h}(n)) \rangle$.
Now take $h(n) := (\tilde{h}(n+1))_n$. By quantifier-free induction we show that
$(++)$ $\forall n(\tilde{h}(n) = \overline{h}(n))$:
$n = 0 :\quad \tilde{h}(0) = \langle \rangle = \overline{h}(0)$.
$n \to n+1 : \tilde{h}(n+1) = \tilde{h}(n) * \langle g(\tilde{h}n) \rangle \overset{\text{I.H.}}{=} \overline{h}n * \langle g(\tilde{h}n) \rangle \overset{lth(\tilde{h}n)=n}{=} \overline{h}(n) * \langle (\tilde{h}(n+1))_n \rangle =$
$\overline{h}(n) * \langle hn \rangle = \overline{h}(n+1)$.

Let k be arbitrary but fixed. We now show – again by quantifier-free induction on n – that

$$\forall n < k \exists m \leq \overline{1}(k \dot{-} n)(lth(m) = k \dot{-} n \wedge f(\overline{h}(n) * m) = 0):$$

$n = 0 : \overline{h}(0) * m = m$, hence the claim follows from $T(f) \wedge \forall x \exists n(lth(n) = x \wedge fn = 0)$.
$n \to n+1 :$ We may assume that $n + 1 < k$: By I.H.

$$\exists \tilde{m} \leq \overline{1}(k \dot{-} n)(lth(\tilde{m}) = k \dot{-} n \wedge f(\overline{h}(n) * \tilde{m}) = 0).$$

Hence by g-definition

$$\exists m \leq \overline{1}(k \dot{-}(n+1))(lth(m) = k \dot{-}(n+1) \wedge f(\underbrace{\overline{h}n * \langle g(\overline{h}n)\rangle}_{=\overline{h}(n+1)\ (++)} * m) = 0),$$

which is the claim for $n + 1$.
So in total we have shown that $T(f) \wedge \forall x \exists n(lth(n) = x \wedge fn = 0)$ implies

$$\forall k \forall n < k \exists m \leq \overline{1}(k \dot{-} n)(lth(m) = k \dot{-} n \wedge f(\overline{h}(n) * m) = 0)$$

and hence

$$\forall n(f(\overline{h}n) = 0),$$

i.e. h satisfies WKL. $\square$.

Corollary to the proof of the theorem: In the proof of the theorem above we have only used elementary recursive functionals from $\widehat{\mathbf{HA}}^{\omega}\!\restriction$. So the argument also applies to even weaker systems having the strength of Kalmar elementary arithmetic **EA.**

Remark 4 *By combining theorems 2 and 3 proved above, one concludes that the strong version of (weak) König's lemma from* [6] **DWKL** *may be added to the systems in question without destroying the conservation results. Instead of the rather tedious proof of weak König's lemma from* **LLOP** *and* $\mathbf{AC}^{0,0}$ *one could also more easily directly apply the proof of theorem 2 to the situation where weak König's lemma is added and use the WKL-elimination from* [8]. *However, we preferred the first route as an application of* **LLOP**.

Remark 5 *If one is not interested in proof theoretic reductions to systems of low proof theoretic strength but in the more applied aspect of extracting algorithms or bounds from proofs of semi-classical systems, then (at least in the absence of* $\mathbf{M}^{\omega}$*)*[4]

[4]For a strong result in this direction in the presence of $\mathbf{M}^{\omega}$ see [9](thm.3.18).

the much stronger results can be obtained as we have shown in [9]. *E.g. consider the comprehension principle for negated formulas in all types*

$$\mathbf{CA}_\neg : \exists \Phi^{\rho \to 0} \forall x^\rho (\Phi(x) = 0 \leftrightarrow \neg A(x))$$

(where A is an arbitrary formula) and the full double negation shift schema

$$\mathbf{DNS} : \ \forall x^\rho \neg\neg A \to \neg\neg \forall x^\rho A$$

and define $\mathcal{T} := \widehat{\mathbf{HA}}^\omega + \mathbf{AC} + \mathbf{DNS} + \mathbf{CA}_\neg$. Then the provable[5] *functions of $\mathcal{T}$ are bounded by primitive recursive functions although $\mathcal{T}$ allows to interpret full classical type theory via negative translation. For weak subsystems instead of $\widehat{\mathbf{HA}}^\omega$, even polynomial bounds are guaranteed.*

Remark 6 *Intuitionistically one can allow certain induction principles which classically would go beyond the strength of* **PRA** *and still obtain conservation over* **PRA**. *E.g.* [13] *considered function parameter free forms of induction rules for fomulas like $\exists f^1 \forall x^0 A_0$ (with quantifier-free A_0). It seems likely that also in this context one may add* **LNOS** *and still preserve* **PRA***-reducibility.*

References

[1] Avigad, J., Feferman, S., Gödel's functional ('Dialectica') interpretation. In: [3], pp. 337-405 (1998).

[2] Bridges, D., Richman, F., Varieties of Constructive Mathematics. London Mathematical Society LNS **97**, Cambridge University Press, pp. x+149 (1987).

[3] Buss, S.R. (editor), Handbook of Proof Theory. Studies in Logic and the Foundations of Mathematics Vol 137, Elsevier, vii+811 pp. (1998).

[4] Feferman, S., Theories of finite type related to mathematical practice. In: Barwise, J. (ed.), Handbook of Mathematical Logic, pp. 913-972, North-Holland, Amsterdam (1977).

[5] Feferman, S., On the proof theoretical strength of some systems with the numerical omniscience scheme (abstract). Submitted to ASL Summer Meeting, Paris 2000.

[5] Not only provably **recursive** functions!

[6] Coquand, T., Palmgren, E., Intuitionistic choice and classical logic. Arch. Math. Logic **39**, pp. 53-74 (2000).

[7] Howard, W.A., Hereditarily majorizable functionals of finite type. In [11], pp. 454-461.

[8] Kohlenbach, U., Effective bounds from ineffective proofs in analysis: an application of functional interpretation and majorization. J. Symbolic Logic **57**, pp. 1239–1273 (1992).

[9] Kohlenbach, U., Relative constructivity. J. Symbolic Logic **63**, pp. 1218-1238 (1998).

[10] Luckhardt, H., Extensional Gödel functional interpretation. A consistency proof of classical analysis. Springer Lecture Notes in Mathematics **306** (1973).

[11] Troelstra, A.S. (ed.) Metamathematical investigation of intuitionistic arithmetic and analysis. Springer Lecture Notes in Mathematics **344** (1973).

[12] Troelstra, A.S., Note on the fan theorem. J. Symbolic Logic **39**, pp. 584–596 (1974).

[13] Ye, F., Strict Constructivism and the Philosophy of Mathematics. Ph.D. Thesis, Princeton University 1999.

Recent BRICS Report Series Publications

RS-00-12 **Ulrich Kohlenbach.** ***Intuitionistic Choice and Restricted Classical Logic*****. May 2000. 9 pp.**

RS-00-11 **Jakob Pagter.** ***On Ajtai's Lower Bound Technique for R-way Branching Programs and the Hamming Distance Problem*****. May 2000. 18 pp.**

RS-00-10 **Stefan Dantchev and Søren Riis.** ***A Tough Nut for Tree Resolution*****. May 2000. 13 pp.**

RS-00-9 **Ulrich Kohlenbach.** ***Effective Uniform Bounds on the Krasnoselski-Mann Iteration*****. May 2000. 34 pp.**

RS-00-8 **Nabil H. Mustafa and Aleksandar Pekeč.** ***Democratic Consensus and the Local Majority Rule*****. May 2000. 38 pp.**

RS-00-7 **Lars Arge and Jakob Pagter.** ***I/O-Space Trade-Offs*****. April 2000. To appear in** ***7th Scandinavian Workshop on Algorithm Theory*****, SWAT '98 Proceedings, LNCS, 2000.**

RS-00-6 **Ivan B. Damgård and Jesper Buus Nielsen.** ***Improved Non-Committing Encryption Schemes based on a General Complexity Assumption*****. March 2000. 24 pp.**

RS-00-5 **Ivan B. Damgård and Mads J. Jurik.** ***Efficient Protocols based on Probabilistic Encryption using Composite Degree Residue Classes*****. March 2000. 19 pp.**

RS-00-4 **Rasmus Pagh.** ***A New Trade-off for Deterministic Dictionaries*****. February 2000.**

RS-00-3 **Fredrik Larsson, Paul Pettersson, and Wang Yi.** ***On Memory-Block Traversal Problems in Model Checking Timed Systems*****. January 2000. 15 pp. Appears in Graf and Schwartzbach, editors,** ***Tools and Algorithms for The Construction and Analysis of Systems: 6th International Conference*****, TACAS '00 Proceedings, LNCS 1785, 2000, pages 127–141.**

RS-00-2 **Igor Walukiewicz.** ***Local Logics for Traces*****. January 2000. 30 pp.**

RS-00-1 **Rune B. Lyngsø and Christian N. S. Pedersen.** ***Pseudoknots in RNA Secondary Structures*****. January 2000. 15 pp. To appear in** ***Fourth Annual International Conference on Computational Molecular Biology*****, RECOMB '00 Proceedings, 2000.**