BRICS RS-04-6 Frandsen & Shparlinski: On Reducing a System of Equations to a Single Equation

BRICS

Basic Research in Computer Science

On Reducing a System of Equations to a Single Equation

Gudmund Skovbjerg Frandsen
Igor E. Shparlinski

BRICS Report Series **RS-04-6**

ISSN 0909-0878 **March 2004**

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/04/6/

On Reducing a System of Equations to a Single Equation

Gudmund S. Frandsen
BRICS, Department of Computer Science
University of Aarhus
DK-8200, Denmark
Email: gudmund@daimi.au.dk

Igor E. Shparlinski
Department of Computing
Macquarie University
NSW 2109, Australia
Email: igor@ics.mq.edu.au

Abstract

For a system of polynomial equations over $\mathbb{Q}_p$ we present an efficient construction of a single polynomial of quite small degree whose zero set over $\mathbb{Q}_p$ coincides with the zero set over $\mathbb{Q}_p$ of the original system. We also show that the polynomial has some other attractive features such as low additive and straight-line complexity.

The proof is based on a link established here between the above problem and some recent number theoretic result about zeros of p-adic forms.

1 Introduction

Let us consider a system of n polynomial equations in m variables

$$f_i(x_1, \ldots, x_m) = 0, \qquad i = 1, \ldots, n, \tag{1}$$

over a field $\mathbb{K}$,

$$f_i(X_1, \ldots, X_m) \in \mathbb{K}[X_1, \ldots, X_m], \qquad i = 1, \ldots, n.$$

It is shown in [8, Lemma 13] that if $\mathbb{K}$ is not algebraically closed then there exists a polynomial

$$f(X_1, \ldots, X_m) \in \mathbb{K}[X_1, \ldots, X_m]$$

such that the system (1) has a solution $x_1, \ldots, x_m \in \mathbb{K}$ if and only if the equation

$$f(x_1, \ldots, x_m) = 0 \tag{2}$$

has a solution $x_1, \ldots, x_m \in \mathbb{K}$. Moreover if the total degree of polynomials $f_1, \ldots, f_n$ does not exceed d, then the total degree of the polynomial f does not exceed $dn^{O(1)}$. Thus we have a polynomial blow-up of the degree. This result has been applied to studying the complexity of some linear algebra problems [8].

Here we show that over $\mathbb{Q}_p$ the same can be achieved with polylogarithmic blow-up of the degree. Moreover, the same is true for the blow-up of the additive and the straight-line complexity of the polynomials $f_1, \ldots, f_n$. In fact, for our construction

$$\mathcal{Z}_{\mathbb{K}}(f_1, \ldots, f_m) = \mathcal{Z}_{\mathbb{K}}(f)$$

where $\mathcal{Z}_{\mathbb{K}}(f_1, \ldots, f_m)$ and $\mathcal{Z}_{\mathbb{K}}(f)$ are the zero sets (over $\mathbb{K}$) of the system of equations (1) and the equation (2).

The construction is based on a link established here between the above reduction problem and some recent results on p-adic forms of low degree and exponentially many variables having only trivial p-adic solutions [2, 3, 5, 6, 18].

This type of argument seems to be new in this area and we hope that this technique may be useful for a number of other applications in complexity theory and symbolic computation.

2 Notation and Auxiliary Results

For our applications we adapt a result from [6], although other results from [2, 3, 5, 18] can be used as well.

Lemma 1 *(i) Let p be an odd prime. Given n polynomials*

$$f_0, \dots, f_{n-1} \in \mathbb{Q}_p[X_1, \dots, X_m]$$

and an integer $t > \log_p n$, we define t polynomials

$$F_j = \sum_{i=0}^{n-1} f_i^{(p-1)(2t-j)} \sum_{k=0}^{n-1} f_k^{(p-1)(2t+j)} \in \mathbb{Q}_p[X_1, \dots, X_m],$$

where $j = 0, \dots, t-1$. Then

$$\mathcal{Z}_{\mathbb{Q}_p}(f_0, \dots, f_{n-1}) = \mathcal{Z}_{\mathbb{Q}_p}(F_0, \dots, F_{t-1}).$$

(ii) Let $p = 2$. Given n polynomials

$$f_0, \dots, f_{n-1} \in \mathbb{Q}_2[X_1, \dots, X_m]$$

and an integer $t > \log_8 n$, we define t polynomials

$$F_j = \sum_{i=0}^{n-1} f_i^{2(4t-j)} \sum_{k=0}^{n-1} f_k^{2(4t+j)} \in \mathbb{Q}_2[X_1, \dots, X_m],$$

where $j = 0, \dots, t-1$. Then

$$\mathcal{Z}_{\mathbb{Q}_2}(f_0, \dots, f_{n-1}) = \mathcal{Z}_{\mathbb{Q}_2}(F_0, \dots, F_{t-1}).$$

Proof. Let be be an odd prime. Clearly

$$\mathcal{Z}_{\mathbb{Q}_p}(f_0, \dots, f_{n-1}) \subseteqq \mathcal{Z}_{\mathbb{Q}_p}(F_0, \dots, F_{t-1}).$$

It is now enough to show that for $t > \log_p n$ the following system of homogeneous equations

$$\sum_{i=0}^{n-1} x_i^{(p-1)(2t-j)} \sum_{k=0}^{n-1} x_k^{(p-1)(2t+j)} = 0, \qquad j = 0, \dots, t-1,$$

does not have a nontrivial solution over $\mathbb{Q}_p$. Indeed, let $(x_1, \dots, x_n)$ be such a nontrivial solution. We can also assume that all $x_1, \dots, x_n$ are nonzero p-adic integers, not all divisible by p. We remark that the above system of equations leads to t equations of the form

$$\sum_{i=0}^{n-1} x_i^{(p-1)j_\nu} = 0, \qquad \nu = 1, \dots, t,$$

with some integers $t < j_1 < \ldots < j_t < 3t$. By *Basic Odd Lemma* of [6, Section 2] we see that this system does not have nonzero modulo p solutions which contradicts our assumption on $x_1, \ldots, x_n$, which finishes the proof in the case $p \geq 3$.

For $p = 2$ the proof is completely analogous except that we use *Basic Even Lemma* of [6, Section 2]. $\square$

We also need a more trivial construction of higher degree:

Lemma 2 *Let p be a prime. Given n polynomials*

$$f_0, \ldots, f_{n-1} \in \mathbb{Q}_p[X_1, \ldots, X_m]$$

and an integer $k > \log_p n$, we define a polynomial $F \in \mathbb{Q}_p[X_1, \ldots, X_m]$ by

$$F = \sum_{i=0}^{n-1} f_i^{(p-1)p^{k-1}}$$

Then $\mathcal{Z}_{\mathbb{Q}_p}(f_0, \ldots, f_{n-1}) = \mathcal{Z}_{\mathbb{Q}_p}(F)$.

Proof. We observe that if $p \not| \, y$ then $y^{(p-1)p^{k-1}} \equiv 1 \pmod{p^k}$, and if $p \,|\, y$ then $y^{(p-1)p^{k-1}} \equiv 0 \pmod{p^k}$. Hence for the polynomial

$$\Phi(Y_1, \ldots, Y_{p^k-1}) = \sum_{i=1}^{p^k-1} Y_i^{(p-1)p^{k-1}} \in \mathbb{Q}_p[Y_1, \ldots, Y_{p^k-1}]$$

we have

$$\mathcal{Z}_{\mathbb{Q}_p}(\Phi) = \{(0, \ldots, 0)\}$$

and the result follows, when using that $p^k - 1 \geq n$. $\square$

Now we recall several notions from algebraic complexity theory.

For a polynomial $f(X_1, \ldots, X_m) \in \mathbb{K}[X_1, \ldots, X_m]$ we define its *additive complexity* $A(f)$ as the least number of signs $+$ and $-$ which are necessary to represent f as an algebraic formula over $\mathbb{K}$ (thus we do not count $\times$ and $/$).

We also define its *straight-line complexity* $L(f)$ as the length of the shortest *straight-line* arithmetic program which computes the values of f at any point $(x_1, \ldots, x_m) \in \mathbb{K}^m$. That is the length L of the shortest chain of the relations $u_i = x_i$, $i = 1, \ldots, m$, and either $u_i = u_{j_i} \circ u_{k_i}$ or $u_i = c_i$ where $c_i \in \mathbb{K}$ is a constant, $i = m+1, \ldots, L$, with $u_L = f(x_1, \ldots, x_m)$ for all $(x_1, \ldots, x_m) \in \mathbb{K}^m$, where $\circ$ stands for one of the arithmetic operations and $1 \leq j_i, k_i \leq i - 1$.

For example, for the polynomial

$$\begin{aligned} f(x_1,x_2,x_3) &= \left(\left((2x_1+x_2)^k + 3x_1^{k^2+1}x_3^{k^3}\right)^{2k+1}+1\right) \\ &\qquad \times \left((x_1+3x_2x_3)^k-2\right)+1. \end{aligned}$$

we have

$$A(f)=6, \qquad L(f)=O(\log k).$$

These two notions play a central role in many parts of complexity theory [7, 10, 17, 19, 21, 22, 23, 24]. In particular, polynomials of low additive complexity admit a short encoding but exhibit quite complicated behaviour.

Also, for a polynomial $f(X_1,\ldots,X_m) \in \mathbb{K}[X_1,\ldots,X_m]$ we define its *sparsity* $S(f)$ as the number of non-zero coefficients in the representation of f of the form

$$f(X_1,\ldots,X_m) = \sum_{i_1,\ldots,i_m} a_{i_1\ldots i_m} X_1^{i_1}\ldots X_m^{i_m}.$$

That is $S(f)$ is the number of distinct monomials in such a representation.

Obviously $A(f) \le S(f)$ but as the above example shows $S(f)$ cannot be estimated in terms of $A(f)$.

There is a constantly growing interest to various features of sparse polynomials over various algebraic domains, see [4, 9, 11, 12, 13, 14, 15, 16, 20, 25, 27, 28, 29] and references therein.

One can easily verify the following statement.

Lemma 3 *For given n polynomials*

$$f_0,\ldots,f_{n-1} \in \mathbb{Q}_p[X_1,\ldots,X_m],$$

we put

$$F = \sum_{i=0}^{n-1} f_i^{D_1} \sum_{k=0}^{n-1} f_k^{D_2},$$

where D_1, D_2 are non-negative integers with $D_1+D_2 = O(\log n)$. Let

$$\begin{aligned} d &= \max\nolimits_{1\le i\le n} \deg f_i, & a &= \max_{1\le i\le n} A(f_i), \\ l &= \max\nolimits_{1\le i\le n} L(f_i), & s &= \max_{1\le i\le n} S(f_i). \end{aligned}$$

Then

$$\begin{array}{rclcrcl} \deg F & = & O(d \log n), & \qquad & A(F) & = & O(an), \\ L(F) & = & O(ln + n \log\log n), & \qquad & S(F) & = & s^{O(\log n)}, \end{array}$$

provided $s \geq 2$.

In connection with the iterated use of Lemma 1 we need the following notation. Let $\log^{(i)} n$ denote i iterations of the function $x \mapsto \lceil \log_3(x+1) \rceil$ taken on n, and let $\log^* n$ denote the minimal i for which $\log^{(i)} n \leq 1$. Finally, we denote

$$\lambda(n) = \prod_{i=1}^{\log^* n} \log^{(i)} n.$$

Throughout this paper p is assumed to be fixed; thus implicit constants in 'O'-symbols may depend on p.

3 Main Results

Theorem 4 *Let polynomials*

$$f_i(X_1, \ldots, X_m) \in \mathbb{Q}_p[X_1, \ldots, X_m],$$

where $i = 1, \ldots, n$, *be of total degree at most* d, *of additive complexity at most* a, *of straight-line complexity at most* l *and of sparsity at most* $s \geq 2$.

Then there exists a polynomial

$$G(X_1, \ldots, X_m) \in \mathbb{Q}_p[X_1, \ldots, X_m]$$

- *of total degree* $\deg G = d\lambda(n) 2^{O(\log^* n)}$;
- *of additive complexity* $A(G) = an\lambda(n)2^{O(\log^* n)}$;
- *of straight-line complexity* $L(G) = O(ln + n \log n)$;
- *of sparsity* $S(G) = s^{\lambda(n)2^{O(\log^* n)}}$;

and such that $\mathcal{Z}_{\mathbb{Q}_p}(f_1, \ldots, f_m) = \mathcal{Z}_{\mathbb{Q}_p}(G)$.

Proof. Let t be the minimal integer such that $t > \log_3 n$ and use the construction of Lemma 1 to find polynomials $F_1, \ldots, F_t$ such that $\mathcal{Z}_{\mathbb{Q}_p}(f_1, \ldots, f_m) = \mathcal{Z}_{\mathbb{Q}_p}(F_1, \ldots, F_t)$. While $t > 1$ the construction of Lemma 1 is repeated and after a total of $\log^* n$ iterations the result is a single polynomial G such that $\mathcal{Z}_{\mathbb{Q}_p}(f_1, \ldots, f_m) = \mathcal{Z}_{\mathbb{Q}_p}(G)$.

For each application of Lemma 1, the degree of the constructed polynomial grows by a factor $O(\log n)$. When the construction is repeated $\log^* n$ times the constant factor hidden in the O-notation may grow to a factor $2^{O(\log^* n)}$. Bearing this in mind, the stated bounds on the degree and the sparsity follows from Lemma 3.

The bound on the additive complexity similarly follows from repeated applications of Lemma 3.

For the straight line complexity, one must in addition compute the intermediate results only once in order to obtain the stated bound $O(ln + n \log n)$ □

It is an open question, whether our result is nearly optimal. Over the field of real numbers, one may encode an arbitrary number of polynomials into a single polynomial while only doubling the degree when using the form $x_1^2 + x_2^2 + \cdots + x_n^2$. It is known, see [26], that any form in n variables having only trivial zeros over $\mathbb{Q}_p$ must have degree at least $\Omega(\log \log n)$. The construction of Theorem 4 implicitly uses such a form of degree $\lambda(n) 2^{O(\log^* n)}$. An improved result may, however, not be based on such forms, in which case no lower bound is known.

There seems to be a trade-off between additive complexity and degree in the result of Theorem 4 in that a modified construction leads to a better additive complexity with the cost of a slightly higher degree (and sparsity):

Theorem 5 *Under the same assumptions as in Theorem 4 there exists a polynomial*

$$H(X_1, \ldots, X_m) \in \mathbb{Q}_p[X_1, \ldots, X_m]$$

- *of total degree* $\deg H = O(d \log^2 n)$;
- *of additive complexity* $A(H) = O(an \log n)$;
- *of straight-line complexity* $L(H) = O(ln + n \log n)$;
- *of sparsity* $S(H) = s^{O(\log^2 n)}$;

and such that $\mathcal{Z}_{\mathbb{Q}_p}(f_1, \ldots, f_m) = \mathcal{Z}_{\mathbb{Q}_p}(H)$.

Proof. Let integer t be the minimal such that $t > \log_3 n$ and use the construction of Lemma 1 to find polynomials $F_1, \dots, F_t$. Apply the construction of Lemma 2 on these t polynomials (with integer k chosen minimal such that $k > \log_2 t$) to get the single polynomial H with the same zero set as the original n polynomials.

The complexity bounds for H are proved similarly to those for G in theorem 4. $\square$

Finally we show how to reduce studying zero sets of p-adic polynomials of low additive complexity to studying zero sets of sparse polynomials which admit a number of algorithmic approaches [4, 9, 11, 12, 13, 14, 15, 16, 19, 25, 28, 29].

Theorem 6 *For any polynomial*

$$F(X_1, \dots, X_m) \in \mathbb{Q}_p[X_1, \dots, X_m]$$

of additive complexity at most $A(F)$ there exists a polynomial

$$f(X_1, \dots, X_{m+n}) \in \mathbb{Q}_p[X_1, \dots, X_{m+n}]$$

of sparsity

$$S(f) \le A(F)^{\lambda(\log n) 2^{O(\log^* n)}}$$

and such that

$$\mathcal{Z}_{\mathbb{Q}_p}(F) = \pi_m \mathcal{Z}_{\mathbb{Q}_p}(f).$$

where $\pi_m : \mathbb{Q}_p^{m+n} \to \mathbb{Q}_p^m$ is the projection map along the first m coordinates.

Proof. It is easy to show by induction, see also [10, 21, 22], that the equation

$$F(x_1, \dots, x_m) = 0$$

can be written down as an equivalent system of $n+1 \le A(F)+1$ equations in $m+n$ variables of the following shape

$$\begin{aligned} x_i &= \alpha_i \prod_{j \in J_i} x_j^{e_{ij}} + \beta_i \prod_{k \in K_i} x_k^{h_{ik}}, \\ &\qquad i = m+1, \dots, m+n, \\ \prod_{j \in J_{m+n+1}} x_j &= 0, \end{aligned}$$

where $J_i, K_i \subseteq \{1, \dots, i-1\}$, $\alpha_i, \beta_i \in \mathbb{K}$, with some integer non-negative exponents e_{ij}, h_{ik}. Applying Theorem 4 (with $s = 3$) and using that

$$3^{\lambda(n)} = (n+1)^{\lambda(\log n)} \leq (A(F)+1)^{\lambda(\log n)}$$

we obtain the desired statement. $\square$

We remark that an analogue of Lemma 1 is known for finite algebraic extensions of $\mathbb{Q}_p$ as well [1], thus our results can be transferred to such fields, too.

4 Acknowledgments

This work was essentially done during a visit by I. S. to the University of Aarhus, whose hospitality is gratefully acknowledged. This visit as well as the work of the first author was supported by BRICS, Basic Research in Computer Science (`www.brics.dk`), Centre of the Danish National Research Foundation.

References

[1] Y. Alemu, 'On zeros of forms over local fields', *Acta Arithm.*, **45** (1985), 163–171.

[2] G. I. Arkhipov and A. A. Karatsuba, 'On a problem in the theory of congruences', *Uspechi Mat. Nauk*, **37** (1981), 161–162 (in Russian).

[3] G. I. Arkhipov and A. A. Karatsuba, 'On the local representation of zero by a form', *Izv. Akad Nauk USSR*, **19** (1982), 231–240 (in Russian).

[4] M. Ben-Or and M. Tiwari, 'A deterministic algorithm for sparse multivariate polynomial interpolation', *Proc. 20th ACM Symp. on Theor. Comp. Sci.*, 1988, 301–309.

[5] J. Browkin, 'On systems of congruences', *Bull. of the Polish Acad. Sci.*, **31** (1983), 219–226.

[6] J. Brownawell, 'On p-adic zeros of forms', *J. Number Theory*, **18** (1984), 342–349.

[7] P. Bürgisser, M. Clausen and M. A. Shokrollahi, *Algebraic complexity theory*, Springer-Verlag, Berlin, 1996.

[8] J. F. Buss, G. S. Frandsen and J. O. Shallit, 'The computational complexity of some problems of linear algebra', *J. Comp. and Syst. Sci.*, **58** (1999), 572–596.

[9] M. Clausen, A. Dress, J. Grabmeier and M. Karpinski, 'On zero testing and interpolation of k-sparse multivariate polynomials over finite field', *Theor. Comp. Sci.*, **84** (1991), 151–164.

[10] D. Grigoriev, 'Lower bounds in the algebraic computational complexity', *Zapiski Nauchn. Semin. Leningr. Otdel. Matem. Inst. Acad. Sci. USSR*, **118** (1982), 25–82 (in Russian).

[11] D. Grigoriev and M. Karpinski, 'Algorithms for sparse rational interpolation', *Proc. Intern. Symp. on Symbolic and Algebraic Comp.*, 1991, 7–13.

[12] D. Grigoriev and M. Karpinski, 'A zero-test and an interpolation algorithm for the shifted sparse polynomials', *Lect. Notes in Comp. Sci.*, **673** (1993), 162–169.

[13] D. Grigoriev, M. Karpinski and M. Singer, 'Fast parallel algorithm for sparse multivariate polynomials over finite fields', *SIAM J. Comput.*, **19** (1990), 1059–1063.

[14] D. Grigoriev, M. Karpinski and M. Singer, 'Computational complexity of sparse rational interpolation', *SIAM J. Comput.*, **23** (1994), 1–11.

[15] M. Karpinski, A. van der Poorten and I. E. Shparlinski, 'Zero testing of p-adic and modular polynomials', *Theor. Comput. Sci.*, **233** (2000), 309–317.

[16] M. Karpinski and I. E. Shparlinski, 'On some approximation problems concerning sparse polynomials over finite fields', *Theor. Comp. Sci.*, **157** (1996), 259–266.

[17] A. G. Khovanski, *Fewnomials*, Amer. Math. Soc., Providence, 1991.

[18] D. J. Lewis and H. L. Montgomery, 'On zeros of p-adic forms', *Michigan Math. J.*, **30** (1983), 83–87.

[19] L. Lipshitz, '*P*-adic zeros of polynomials', *J. Reine Angew. Math.*, **390** (1988), 208–214.

[20] R. Lipton and N. Vishnoi, 'Deterministic identity testing for multivariate polynomials', *Proc. 14th ACM-SIAM Symp. on Discr. Algorithms*, ACM, 2003, 756–760.

[21] J.-J. Risler, 'Khovansky's theorem and complexity theory', *Rocky Mountain J. Math.*, **14** (1984), 851–853.

[22] J.-J. Risler, 'Additive complexity of real polynomials', *SIAM J. Comp.*, **14** (1985), 178–183.

[23] J. M. Rojas, 'Additive complexity and p-adic roots of polynomials', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2369** (2002), 506–516.

[24] J. M. Rojas, 'Arithmetic multivariate Descartes' rule', *Amer. J. Math.*, **126** (2004) 1–30.

[25] R. M. Roth and G. M. Benedek, 'Interpolation and approximation of sparse multivariate polynomials over $GF(2)$', *SIAM J. Comp.* **20** (1991), 291–314.

[26] W. M. Schmidt, 'The solubility of certain p-adic equations', *J. Number Theory*, **19** (1984), 63–80.

[27] I. E. Shparlinski, 'Sparse polynomial approximation in finite fields', *Proc. 33rd ACM Symp. on Theory of Comput.*, ACM, 2001, 209–215.

[28] K. Werther, 'The complexity of sparse polynomials interpolation over finite fields', *Appl. Algebra in Engin., Commun. and Comp.*, **5**(1994), 91–103.

[29] R. Zippel, *Effective polynomial computation*, Kluwer Acad. Publ., Dordrecht, 1993.

Recent BRICS Report Series Publications

RS-04-6 Gudmund Skovbjerg Frandsen and Igor E. Shparlinski. *On Reducing a System of Equations to a Single Equation*. March 2004. 11 pp. To appear in Schicho and Singer, editors, *ACM SIGSAM International Symposium on Symbolic and Algebraic Computation*, ISSAC '04 Proceedings, 2004.

RS-04-5 Biernacki Dariusz and Danvy Olivier. *From Interpreter to Logic Engine by Defunctionalization*. March 2004. 20 pp. To appear in Bruynooghe, editor, *International Symposium on Logic Based Program Development and Transformation, LOPSTR '03 Proceedings*, Revised Selected Papers, LNCS, 2003. This report supersedes the earlier BRICS report RS-03-25.

RS-04-4 Patricia Bouyer, Franck Cassez, Emmanuel Fleury, and Kim G. Larsen. *Optimal Strategies in Priced Timed Game Automata*. February 2004. 32 pp.

RS-04-3 Mads Sig Ager, Olivier Danvy, and Jan Midtgaard. *A Functional Correspondence between Call-by-Need Evaluators and Lazy Abstract Machines*. February 2004. 17 pp. This report supersedes the earlier BRICS report RS-03-24. Extended version of an article to appear in *Information Processing Letters*.

RS-04-2 Gerth Stølting Brodal, Rolf Fagerberg, Ulrich Meyer, and Norbert Zeh. *Cache-Oblivious Data Structures and Algorithms for Undirected Breadth-First Search and Shortest Paths*. February 2004. 19 pp.

RS-04-1 Luca Aceto, Willem Jan Fokkink, Anna Ingólfsdóttir, and Bas Luttik. *Split-2 Bisimilarity has a Finite Axiomatization over CCS with Hennessy's Merge*. January 2004. 16 pp.

RS-03-53 Kyung-Goo Doh and Peter D. Mosses. *Composing Programming Languages by Combining Action-Semantics Modules*. December 2003. 39 pp. Appears in *Science of Computer Programming*, 47(1):2–36, 2003.

RS-03-52 Peter D. Mosses. *Pragmatics of Modular SOS*. December 2003. 22 pp. Invited paper, published in Kirchner and Ringeissen, editors, *Algebraic Methodology and Software Technology: 9th International Conference*, AMAST '02 Proceedings, LNCS 2422, 2002, pages 21–40.