



ulm university universität
uulm

On Toda's Theorem in structural communication complexity

Henning Wunderlich

Ulmer Informatik-Berichte

**Nr. 2008-12
September 2008**

On Toda's Theorem in structural communication complexity

Henning Wunderlich *

August 27, 2008

Abstract

We prove Toda's Theorem in the context of structural communication complexity, i.e. $\mathbf{PH}^{cc} \subseteq \mathbf{BP} \cdot \oplus \mathbf{P}^{cc} \subseteq \mathbf{P}^{cc}(\#\mathbf{P}^{cc}) = \mathbf{P}^{cc}(\mathbf{PP}^{cc})$. The class \mathbf{PSPACE}^{cc} was defined via alternating protocols with $\mathcal{O}(\log n)$ many alternations. We consider the class $\mathbf{BP} \cdot \oplus \mathbf{P}^{cc}$ of Toda's Theorem, and show that every language in this class can be decided with alternating protocols using $\mathcal{O}(\log n / \log \log n)$ many alternations. The proof is based on a new alternating protocol for the inner product function \mathbf{IP} with $\mathcal{O}(\log n / \log \log n)$ many alternations.

1 Introduction

The main contribution of this paper is to establish Toda's Theorem in the setting of communication complexity, i.e. we prove $\mathbf{PH}^{cc} \subseteq \mathbf{BP} \cdot \oplus \mathbf{P}^{cc} \subseteq \mathbf{P}^{cc}(\#\mathbf{P}^{cc}) = \mathbf{P}^{cc}(\mathbf{PP}^{cc})$. This might be useful in the search for a solution of the famous \mathbf{PH}^{cc} vs. \mathbf{PSPACE}^{cc} problem, because no communication complexity measures/lower bound methods are known for alternating classes, while for the classes \mathbf{BPP}^{cc} and $\oplus \mathbf{P}^{cc}$ lower bound methods are available. Thus, it might be easier to come up with a measure for $\mathbf{BP} \cdot \oplus \mathbf{P}^{cc}$, a class not based on the concept of alternation, than to develop a measure for alternation. Of course, it might be the case that $\mathbf{BP} \cdot \oplus \mathbf{P}^{cc} = \mathbf{PSPACE}^{cc}$, but we show that every language in $\mathbf{BP} \cdot \oplus \mathbf{P}^{cc}$ can be decided with alternating protocols using only $\mathcal{O}(\log n / \log \log n)$ many alternations, i.e. substantially less than allowed for \mathbf{PSPACE}^{cc} . The proof is based on a new alternating protocol for the inner product function \mathbf{IP} with $\mathcal{O}(\log n / \log \log n)$ many alternations.

1.1 Structural complexity

For introductions to the broad field of structural complexity see [3, 2, 6, 14, 10]. Nice surveys on a variety of topics in this field can be found in [18, 19], especially on counting complexity in [15, 7] by Schöning and Fortnow, respectively. The parity class $\oplus \mathbf{P}$ was defined by Papadimitriou and Zachos in [12], where it was shown that $\oplus \mathbf{P}(\oplus \mathbf{P}) = \oplus \mathbf{P}$. One can define operators on complexity classes, e.g. the \mathbf{BP} -operator, which was defined by Schöning [16]. Using the \mathbf{BP} -operator

*Universität Ulm, Fakultät für Ingenieurwissenschaften und Informatik, Institut für Theoretische Informatik, Oberer Eselsberg, D-89069 Ulm, e-mail: Henning.Wunderlich@uni-ulm.de

and the Valiant-Vazirani-Lemma [21] Toda [20] was able to prove his celebrated theorem

$$\mathbf{PH} \subseteq \mathbf{BP} \cdot \oplus \mathbf{P} \subseteq \mathbf{P}(\#\mathbf{P}) = \mathbf{P}(\mathbf{PP}) ,$$

which tells us that counting (mod 2 with random source) is at least as powerful as the whole polynomial-time hierarchy \mathbf{PH} . See also [17] for a simplified proof.

1.2 Communication complexity

For a thorough introduction to communication complexity we refer the reader to the book of Kushilevitz and Nisan [11].

1.2.1 Basic definitions and notation.

We only work with the *binary alphabet* $\mathbb{B} := \{0, 1\}$. The length of a string $x \in \mathbb{B}^*$ is denoted by $|x|$. A prefix-free encoding of x is $\bar{x} := 0^{|x|}1x$. In order to encode pairs of strings $x, y \in \mathbb{B}^*$ we use the pairing function $\langle x, y \rangle := \bar{x}y$. The *set of pairs of strings of equal length* is denoted by $\mathbb{B}^{**} := \{(x, y) \mid x, y \in \mathbb{B}^*, |x| = |y|\}$. A *language* L is a subset of \mathbb{B}^{**} , its *characteristic function* χ^L is defined as $\chi^L := (\chi_n^L)$, where $\chi_n^L: \mathbb{B}^n \times \mathbb{B}^n \rightarrow \mathbb{N}$, $\chi_n^L(x, y) := 1$, if $(x, y) \in L$, and 0 otherwise. We write $(x, y) \in L$ if $\chi_{|x|}^L(x, y) = 1$. The *set of all languages* is denoted by \mathcal{L} . A (*communication*) *complexity class* is a subset $\mathcal{C} \subseteq \mathcal{L}$. We define $\mathbf{poly} := \{f: \mathbb{R}^+ \rightarrow \mathbb{R}^+ \mid \exists \text{polynomial } p: f \leq p\}$, the *set of functions with polynomial growth*. With \log we denote the logarithm to the basis 2.

1.2.2 Yao's model.

We consider the basic model of communication complexity, introduced by Yao [22]. In this model, there are two players (parties) Alice and Bob, who want to cooperatively compute a function $f: \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$, where \mathcal{X} , \mathcal{Y} and \mathcal{Z} are finite sets. Both have complete information about f and unlimited computational power but receive only parts of the inputs. Alice is given $x \in \mathcal{X}$, Bob is given y , and they exchange messages in order to compute $f(x, y)$. Each message solely depends on the player's input and the messages communicated so far. The communication is carried out according to a fixed *protocol* Π (over domain $\mathcal{X} \times \mathcal{Y}$ with range \mathcal{Z}).

1.2.3 Protocols.

There are four kinds of protocols, namely *deterministic*, *randomized*, *nondeterministic* and *alternating* ones. We only describe deterministic protocols in detail: A *deterministic protocol* is a labeled binary tree, where an inner node specifies the player who sends a bit of communication next. If v is an inner node, then it is labeled either by a function $a_v: \mathcal{X} \rightarrow \{0, 1\}$ or by a function $b_v: \mathcal{Y} \rightarrow \{0, 1\}$. Each leaf l is labeled with an output value $z_l \in \mathcal{Z}$. The value of the protocol Π on input (x, y) is the label of the leaf reached by starting from the root, and walking on the tree. At each internal node v labeled by a_v Alice sends $a_v(x)$ and they walk left if $a_v(x) = 0$ and right if $a_v(x) = 1$. Analogously, if v is labeled with b_v . The cost of the protocol Π on input (x, y) is the length of the path taken on this input. In a *randomized protocol* Alice and Bob have access to a public or private source of randomness (*random string*). The functions a_v, b_v are

arbitrary functions of the inputs and the random strings. In a *nondeterministic protocol*, we have $\mathcal{Z} = \{0, 1\}$, and each player gets a *guess string* in addition to the input. Here, a_v and b_v are arbitrary functions of the inputs and the guess strings. For nondeterministic protocols there exist different *accepting modes*. For example, a nondeterministic protocol accepts a language L in the *nondeterministic accepting mode*, if for all $(x, y) \in L$ there exist guess strings g_A and g_B such that Alice on input x and guess string g_A and Bob on input y and guess string g_B reach a leaf labeled with 1, and if for all $(x, y) \notin L$ there do not exist any guess strings such that the players reach a 1-leaf. Another example is the *parity accepting mode*: Here, an input is accepted iff the number of guess strings such that the players reach a 1-leaf is odd. For a definition of *alternating protocols*, see [1, p.339]. For formal definitions concerning protocols, cost and complexity measures, and accepting modes, see [11, Def. 1.1, p.4; Chap. 3, p.28; Chap. 2, p.18] and [5]. A protocol over domain $\mathcal{X} \times \mathcal{Y}$ is an *n-bit* protocol, if $\mathcal{X} = \mathcal{Y} = \mathbb{B}^n$. A protocol family $(\Pi_n)_{n \in \mathbb{N}}$ of *n-bit* protocols Π_n *decides* a language L if each Π_n computes χ_n^L .

1.2.4 Communication complexity classes.

Each protocol type and acceptance mode leads to a complexity measure, e.g. $D(f)$ for the deterministic communication complexity of f , or $\oplus D(f)$, which is the minimum cost of a nondeterministic protocol deciding f in parity accepting mode. If a problem can be solved with communication polylogarithmically in the input size, then we consider this as *efficient*. The communication complexity classes are defined as sets of languages that can be decided efficiently according to a fixed measure. For example, \mathbf{P}^{cc} is the class of languages such that $L \in \mathbf{P}^{cc}$ iff there exists a bound $b \in \mathbf{poly}$ with $D(\chi_n^L) \leq p(\log n)$, and $\oplus \mathbf{P}^{cc}$ is the class of languages such that $L \in \oplus \mathbf{P}^{cc}$ iff there exists a bound $b \in \mathbf{poly}$ with $\oplus D(\chi_n^L) \leq p(\log n)$.

1.2.5 Oracle protocols.

A deterministic, randomized, nondeterministic or alternating protocol Π over \mathcal{X} , \mathcal{Y} is an *oracle protocol* with oracle family $O = (O_m)_{m \in \mathbb{N}}$, if Π contains *oracle nodes* in its protocol tree. Associated with an oracle node v are two functions $a_v: \mathcal{X} \rightarrow \mathbb{B}^{m_v}$ and $b_v: \mathcal{Y} \rightarrow \mathbb{B}^{m_v}$. If Alice and Bob reach an oracle node v during a computation on input $(x, y) \in \mathcal{X} \times \mathcal{Y}$, they compute by themselves $x' := a_v(x)$ and $y' := b_v(y)$, respectively, and call O_{m_v} on (x', y') . The oracle node v has exactly $|\text{range}(O)|$ many successors. Alice and Bob continue the computation on one of them according to the returned value $O(x', y')$. The communication costs for each oracle call are $\lceil \log |\text{range}(O)| \rceil$. If a language L is used as an oracle family, we write L instead of χ^L . *Relativized communication complexity classes* are defined via efficient oracle protocol families. For example, $\mathbf{P}^{cc}(L')$ contains all languages L which can be decided by a protocol family $(\Pi_n)_{n \in \mathbb{N}}$ of deterministic *n-bit* oracle protocols with L' as the oracle.

1.3 Structural communication complexity

Research in the field of structural communication complexity started with the article of Babai, Frankl and Simon [1], where some analogies between Turing ma-

chine classes like \mathbf{P} , \mathbf{NP} , \mathbf{PP} , \mathbf{PSPACE} , the polynomial hierarchy $\mathbf{PH} = \bigcup_k \Sigma_k^p$, etc. and the corresponding communication complexity classes \mathbf{P}^{cc} , \mathbf{NP}^{cc} , \mathbf{PP}^{cc} , \mathbf{PSPACE}^{cc} , $\mathbf{PH}^{cc} = \bigcup_k \Sigma_k^{cc}$, etc. were shown. For more ground work, especially on closure properties, the boolean communication hierarchy, or counting communication complexity classes like $\text{MOD}_m \mathbf{P}$, see Halstenberg and Reischuk [8] or Damm et al. [5]. In [9] Klauck established separation results between \mathbf{MA}^{cc} and \mathbf{NP}^{cc} , \mathbf{MA}^{cc} and \mathbf{APP}^{cc} , and \mathbf{APP}^{cc} and \mathbf{PP}^{cc} , respectively. In recent research, Buhrman et al. [4] showed $\Sigma_2^{cc}, \Pi_2^{cc} \not\subseteq \mathbf{PP}^{cc}$. This was improved to $\Sigma_2^{cc}, \Pi_2^{cc} \not\subseteq \mathbf{UPP}^{cc}$ by Razborov and Sherstov [13].

1.3.1 Reductions.

We introduce different kinds of reductions between languages. The many-one reductions are also called *rectangular reductions*. The disjunctive reductions are not needed in the sequel but defined only for the sake of completeness.

Definition 1.1. (*Reductions*) *Let L and L' be languages.*

1. L is many-one reducible to L' , if there exists a bound $b \in \mathbf{poly}$ and a family of function pairs $\{(f_n, g_n)\}_{n \in \mathbb{N}}$, $f_n, g_n: \mathbb{B}^n \rightarrow \mathbb{B}^{\lceil 2^{b(\log n)} \rceil}$, such that for all $(x, y) \in (\mathbb{B}^n)^2$ it holds: $(x, y) \in L$ iff $(f_n(x), g_n(y)) \in L'$.
2. L is Turing reducible to L' , if $L \in \mathbf{P}^{cc}(L')$.
3. L is majority reducible to L' , if there exist bounds $b, t \in \mathbf{poly}$ and a family of function pairs $\{(f_n, g_n)\}_{n \in \mathbb{N}}$, $f_n, g_n: \mathbb{B}^n \rightarrow (\mathbb{B}^{\lceil 2^{b(\log n)} \rceil})^{\lceil t(\log n) \rceil}$, such that for all $(x, y) \in (\mathbb{B}^n)^2$ it holds: $(x, y) \in L$ iff $((f_n(x))_i, (g_n(y))_i) \in L'$ for the majority of the indices $i \in \llbracket t(\log n) \rrbracket$.
4. L is conjunctively reducible to L' , if there exist bounds $b, t \in \mathbf{poly}$ and a family of function pairs $\{(f_n, g_n)\}_{n \in \mathbb{N}}$, $f_n, g_n: \mathbb{B}^n \rightarrow (\mathbb{B}^{\lceil 2^{b(\log n)} \rceil})^{\lceil t(\log n) \rceil}$, such that for all $(x, y) \in (\mathbb{B}^n)^2$ it holds: $(x, y) \in L$ iff $((f_n(x))_i, (g_n(y))_i) \in L'$ for all indices $i \in \llbracket t(\log n) \rrbracket$.
5. L is disjunctively reducible to L' , if there exist bounds $b, t \in \mathbf{poly}$ and a family of function pairs $\{(f_n, g_n)\}_{n \in \mathbb{N}}$, $f_n, g_n: \mathbb{B}^n \rightarrow (\mathbb{B}^{\lceil 2^{b(\log n)} \rceil})^{\lceil t(\log n) \rceil}$, such that for all $(x, y) \in (\mathbb{B}^n)^2$ it holds: $(x, y) \in L$ iff $((f_n(x))_i, (g_n(y))_i) \in L'$ for at least one of the indices $i \in \llbracket t(\log n) \rrbracket$.

1.4 Organization of this paper

In **Section 1** we prove Toda's Theorem in the setting of communication complexity. In **Section 2** we present an alternating protocol for the inner product function IP with $\mathcal{O}(\log n / \log \log n)$ many alternations, which gives us an upper bound on the number of alternations for languages in the class $\mathbf{BP} \cdot \oplus \mathbf{P}^{cc}$ of Toda's Theorem.

2 Toda's Theorem

In order to prove Toda's Theorem we need to define different kinds of operators on communication complexity classes. Readers familiar with communication

complexity might wonder why the operators are defined in a *public coin style*, i.e. both players get the same witness/random string. Of course, one can define the operators such that each player gets his/her own witness/random string (*private coin style*). The reason is that these definitions are equivalent, if the operators are simulated by a protocol. Alice can guess Bob's witness and send it to him, or she can send him her random string, because the length of witnesses/random strings is bounded polylogarithmically in the length of the input.

Definition 2.1. (*Complexity class operators*) For a language $L \subseteq \mathbb{B}^{**}$ and bounds $p, q \in \mathbf{poly}$ we define

$$\begin{aligned} \forall^p(L) &:= \{(x, y) \in \mathbb{B}^{**} \mid \forall w \in \mathbb{B}^{\lceil p(\log |x|) \rceil} : (\langle x, w \rangle, \langle y, w \rangle) \in L\} , \\ \exists^p(L) &:= \{(x, y) \in \mathbb{B}^{**} \mid \exists w \in \mathbb{B}^{\lceil p(\log |x|) \rceil} : (\langle x, w \rangle, \langle y, w \rangle) \in L\} , \\ \text{Mod}_k^p(L) &:= \{(x, y) \in \mathbb{B}^{**} \mid |\{w \in \mathbb{B}^{\lceil p(\log |x|) \rceil} \mid (\langle x, w \rangle, \langle y, w \rangle) \in L\}| \bmod k \neq 0\} , \\ \oplus^p(L) &:= \text{Mod}_2^p(L) . \end{aligned}$$

For a communication complexity class $\mathcal{C} \subseteq \mathcal{L}$ we define

$$\begin{aligned} \text{co} \cdot \mathcal{C} &:= \{\bar{L} \mid L \in \mathcal{C}\} , \\ \forall \cdot \mathcal{C} &:= \{\forall^p(L) \mid L \in \mathcal{C}, p \in \mathbf{poly}\} , \\ \exists \cdot \mathcal{C} &:= \{\exists^p(L) \mid L \in \mathcal{C}, p \in \mathbf{poly}\} , \\ \text{Mod}_k \cdot \mathcal{C} &:= \{\text{Mod}_k^p(L) \mid L \in \mathcal{C}, p \in \mathbf{poly}\} , \\ \oplus \cdot \mathcal{C} &:= \text{Mod}_2 \cdot \mathcal{C} . \end{aligned}$$

A language L is in $\text{BP} \cdot \mathcal{C}$ if there exists a language $L' \in \mathcal{C}$ and a bound $q \in \mathbf{poly}$ such that for all $(x, y) \in (\mathbb{B}^n)^2$ it holds:

$$\begin{aligned} (x, y) \in L &\text{ implies } |\{r \in \mathbb{B}^{\lceil q(\log n) \rceil} \mid (\langle x, r \rangle, \langle y, r \rangle) \in L'\}| / 2^{\lceil q(\log n) \rceil} \geq \frac{2}{3} . \\ (x, y) \notin L &\text{ implies } |\{r \in \mathbb{B}^{\lceil q(\log n) \rceil} \mid (\langle x, r \rangle, \langle y, r \rangle) \in L'\}| / 2^{\lceil q(\log n) \rceil} \leq \frac{1}{3} . \end{aligned}$$

We give a definition of the polynomial hierarchy suitable for our purposes based on the class operators defined above. Note that this definition is equivalent to the one given in [1].

Definition 2.2. (*Polynomial hierarchy*) $\mathbf{PH}^{cc} := \bigcup_{k \geq 0} \Sigma_k^{cc}$, where $\Sigma_0^{cc} := \mathbf{P}^{cc}$ and $\Sigma_{k+1}^{cc} := \exists \cdot \text{co} \cdot \Sigma_k^{cc}$.

We observe the following properties of the communication complexity class operators. The proofs are easy, so we omit most of them for space reasons.

Observation 2.3. (*Probability amplification*) Let $\mathcal{C} \subseteq \mathcal{L}$ be a communication complexity class closed under majority reductions, and let $b \in \mathbf{poly}$. If a language L is in $\text{BP} \cdot \mathcal{C}$, then there exists a language $L' \in \mathcal{C}$ and a bound $q \in \mathbf{poly}$ such that for all $(x, y) \in (\mathbb{B}^n)^2$ it holds:

$$\begin{aligned} (x, y) \in L &\Rightarrow |\{r \in \mathbb{B}^{\lceil q(\log n) \rceil} \mid (\langle x, r \rangle, \langle y, r \rangle) \in L'\}| / 2^{\lceil q(\log n) \rceil} \geq 1 - 2^{-b(\log n)} . \\ (x, y) \notin L &\Rightarrow |\{r \in \mathbb{B}^{\lceil q(\log n) \rceil} \mid (\langle x, r \rangle, \langle y, r \rangle) \in L'\}| / 2^{\lceil q(\log n) \rceil} \leq 2^{-b(\log n)} . \end{aligned}$$

Observation 2.4. (*Inclusion*) Let $\mathcal{C} \subseteq \mathcal{L}$ be a communication complexity class closed under many-one reductions. Then $\mathcal{C} \subseteq \text{Op} \cdot \mathcal{C}$ for every operator $\text{Op} \in \{\forall, \exists, \text{Mod}_k, \oplus, \text{BP}\}$.

Observation 2.5. (*Monotonicity*) Let $\mathcal{C}, \mathcal{D} \subseteq \mathcal{L}$ be communication complexity classes such that $\mathcal{C} \subseteq \mathcal{D}$. Then $\text{Op} \cdot \mathcal{C} \subseteq \text{Op} \cdot \mathcal{D}$ for every operator $\text{Op} \in \{\text{co}, \forall, \exists, \text{Mod}_k, \oplus, \text{BP}\}$.

Observation 2.6. (*Idempotency*) Let $\mathcal{C} \subseteq \mathcal{L}$ be a communication complexity class closed under many-one reductions. Then $\text{Op} \cdot \text{Op} \cdot \mathcal{C} = \text{Op} \cdot \mathcal{C}$ for every operator $\text{Op} \in \{\forall, \exists, \oplus\}$.

The idempotency of the BP-operator follows from its probability amplification property (Observation 2.3).

Observation 2.7. (*Idempotency of BP*) Let $\mathcal{C} \subseteq \mathcal{L}$ be a communication complexity class closed under majority reductions. Then $\text{BP} \cdot \text{BP} \cdot \mathcal{C} = \text{BP} \cdot \mathcal{C}$.

Observation 2.8. (*co vs. ...*) Let $\mathcal{C} \subseteq \mathcal{L}$ be a communication complexity class. Then $\text{co} \cdot \exists \cdot \mathcal{C} = \forall \cdot \text{co} \cdot \mathcal{C}$, $\text{co} \cdot \forall \cdot \mathcal{C} = \exists \cdot \text{co} \cdot \mathcal{C}$, and $\text{co} \cdot \text{BP} \cdot \mathcal{C} = \text{BP} \cdot \text{co} \cdot \mathcal{C}$.

Definition 2.9. (*Intersection and Union*) Let \mathcal{C} and \mathcal{C}' be communication complexity classes. \mathcal{C} is closed under \mathcal{C}' -intersection iff for all $L \in \mathcal{C}$ and $L' \in \mathcal{C}'$ we have $L \cap L' \in \mathcal{C}$. \mathcal{C} is closed under \mathcal{C}' -union iff for all $L \in \mathcal{C}$ and $L' \in \mathcal{C}'$ we have $L \cup L' \in \mathcal{C}$.

Observation 2.10. (*co vs. \oplus*) Let $\mathcal{C} \subseteq \mathcal{L}$ be a communication complexity class that contains \mathbf{P}^{cc} , is closed under \mathbf{P}^{cc} -intersection, \mathbf{P}^{cc} -union, and many-one reductions. Then $\text{co} \cdot \oplus \cdot \mathcal{C} = \oplus \cdot \mathcal{C}$.

Proof. Let $L \in \oplus \cdot \mathcal{C}$. There exist a bound $p \in \mathbf{poly}$ and a language $L_1 \in \mathcal{C}$ such that $L = \oplus^p(L_1)$. Define

$$\begin{aligned} L_2 &:= \{(\langle x, b_1 w_1 \rangle, \langle y, b_2 w_2 \rangle) \mid b_1, b_2 \in \mathbb{B}, (\langle x, w_1 \rangle, \langle y, w_2 \rangle) \in L_1\} , \\ L_3 &:= \{(\langle x, 1 w_1 \rangle, \langle y, 1 w_2 \rangle) \mid |x| = |y| = n, |w_1| = |w_2| = \lceil p(\log n) \rceil\} , \\ L_4 &:= \{(\langle x, 0 w_1 \rangle, \langle y, 0 w_2 \rangle) \mid |x| = |y| = n, w_1 = w_2 = 0^{\lceil p(\log n) \rceil}\} . \end{aligned}$$

Then L_2 is in \mathcal{C} , because \mathcal{C} is closed under many-one reductions, and $L_3, L_4 \in \mathbf{P}^{\text{cc}}$. The language $L_5 := (L_2 \cap L_3) \cup L_4$ is in \mathcal{C} , because \mathcal{C} is closed under \mathbf{P}^{cc} -intersection and \mathbf{P}^{cc} -union. Define $L' := \oplus^{p+1}(L_5)$. Clearly, $\bar{L} = L' \in \oplus \cdot \mathcal{C}$. \square

Observation 2.11. If $\mathcal{C} \subseteq \mathcal{L}$ is a communication complexity class closed under conjunctive reductions, then $\oplus \cdot \mathcal{C}$ is closed under conjunctive reductions.

Using Observations 2.10 and 2.11 one can prove the result of Papadimitriou and Zachos [12] in the setting of communication complexity as in time complexity (see also [10, Prop. 4.8, p.125]).

Fact 2.12. (*Papadimitriou & Zachos*) Let $\mathcal{C} \subseteq \mathcal{L}$ be a communication complexity class, which contains \mathbf{P}^{cc} , is closed under \mathbf{P}^{cc} -intersection, \mathbf{P}^{cc} -union, and conjunctive reductions. Then $\oplus \mathbf{P}^{\text{cc}}(\oplus \cdot \mathcal{C}) = \oplus \cdot \mathcal{C}$.

The following observation shows that the names used for the operators are compatible with the names of classical communication complexity classes, if the operators are applied to \mathbf{P}^{cc} .

Observation 2.13. (*Compatibility*)

$$\begin{aligned} \mathbf{NP}^{\text{cc}} &= \exists \cdot \mathbf{P}^{\text{cc}} , & \oplus \mathbf{P}^{\text{cc}} &= \oplus \cdot \mathbf{P}^{\text{cc}} , \\ \text{co-NP}^{\text{cc}} &= \forall \cdot \mathbf{P}^{\text{cc}} , & \mathbf{BPP}^{\text{cc}} &= \text{BP} \cdot \mathbf{P}^{\text{cc}} . \end{aligned}$$

Swapping lemmata are well known in the field of structural complexity theory. Below, we give a proof of a lemma of this type for the sake of completeness. The main ingredient is the probability amplification property of the BP-operator (Observation 2.3).

Lemma 2.14. (*Swapping*) *Let $\mathcal{C} \subseteq \mathcal{L}$ be a communication complexity class closed under majority reductions. Then $\oplus \cdot \text{BP} \cdot \mathcal{C} \subseteq \text{BP} \cdot \oplus \cdot \mathcal{C}$.*

Proof. Let L be a language in $\oplus \cdot \text{BP} \cdot \mathcal{C}$. Then there exists a language L' in $\text{BP} \cdot \mathcal{C}$ and a bound $p' \in \mathbf{poly}$ such that $L = \oplus^{p'}(L')$. As $L' \in \text{BP} \cdot \mathcal{C}$ and \mathcal{C} is closed under majority reductions we use probability amplification to obtain a language L'' in \mathcal{C} and a bound $p'' \in \mathbf{poly}$ such that

$$\begin{aligned} \langle \langle x, w \rangle, \langle y, w \rangle \rangle \in L' &\Rightarrow \Pr_r[\langle \langle x, w \rangle, r \rangle, \langle \langle y, w \rangle, r \rangle \rangle \in L''] \geq 1 - 2^{-l'_n - 2}, \text{ and} \\ \langle \langle x, w \rangle, \langle y, w \rangle \rangle \notin L' &\Rightarrow \Pr_r[\langle \langle x, w \rangle, r \rangle, \langle \langle y, w \rangle, r \rangle \rangle \in L''] \leq 2^{-l'_n - 2}. \end{aligned}$$

for every input $(x, y) \in (\mathbb{B}^n)^2$ and witness w . Here, $l'_n := \lceil p'(\log n) \rceil$, and the random string r is uniformly drawn from $\mathbb{B}^{l'_n}$, where $l''_n := \lceil p''(\log n) \rceil$. We define $W_{(x,y)} := \{w \in \mathbb{B}^{l'_n} \mid \langle \langle x, w \rangle, \langle y, w \rangle \rangle \in L'\}$ and $\text{Good}_n := \bigcap_{w \in \mathbb{B}^{l'_n}} \text{Good}_{n,w}$, where $\text{Good}_{n,w} := \{r \in \mathbb{B}^{l''_n} \mid \forall (x, y) \in (\mathbb{B}^n)^2: \langle \langle x, w \rangle, r \rangle, \langle \langle y, w \rangle, r \rangle \rangle \in L'' \Leftrightarrow w \in W_{(x,y)}\}$. For a fixed w_0 we get

$$\Pr_r[r \notin \text{Good}_n] \leq 2^{l'_n} \cdot \Pr_r[r \notin \text{Good}_{n,w_0}] \leq 2^{l'_n} \cdot 2^{l'_n - 2} \leq \frac{1}{4}.$$

Thus, $\Pr_r[r \in \text{Good}_n] \geq \frac{3}{4}$. The language

$$L''' := \{(\langle \langle x, r \rangle, w \rangle, \langle \langle y, r' \rangle, w' \rangle) \mid (\langle \langle x, w \rangle, r \rangle, \langle \langle y, w' \rangle, r' \rangle) \in L''\}$$

is in \mathcal{C} (closure under many-one reductions).

In case $(x, y) \in L$ we have

$$\begin{aligned} &\Pr_r[\langle \langle x, r \rangle, \langle y, r \rangle \rangle \in \oplus^{p'}(L''')] \\ &= \Pr_r[|\{w \mid (\langle \langle x, w \rangle, r \rangle, \langle \langle y, w \rangle, r \rangle) \in L''\}| \text{ odd}] \\ &\geq \Pr_r[\forall w: w \in W_{(x,y)} \Leftrightarrow (\langle \langle x, w \rangle, r \rangle, \langle \langle y, w \rangle, r \rangle) \in L''] \quad (1) \\ &\geq \Pr_r[\forall (x, y): \forall w: w \in W_{(x,y)} \Leftrightarrow (\langle \langle x, w \rangle, r \rangle, \langle \langle y, w \rangle, r \rangle) \in L''] \\ &= \Pr_r[r \in \text{Good}_n] \geq \frac{3}{4}, \end{aligned}$$

where (1) follows from $(x, y) \in L \Leftrightarrow |W_{(x,y)}| \text{ odd}$.

The case $(x, y) \notin L$ is treated similarly. We conclude $L \in \text{BP} \cdot \oplus \cdot \mathcal{C}$. \square

The Valiant-Vazirani-Lemma is well known in structural complexity theory, and there exist many proof ideas for this important result. The solution we propose is an adaptation of an algebraic proof due to Fortnow in [7, p.88, Lemma 3.12].

Lemma 2.15. (*Valiant-Vazirani*) *Let $\mathcal{C} \subseteq \mathcal{L}$ be a communication complexity class containing \mathbf{P}^{cc} and closed under \mathbf{P}^{cc} -intersection, \mathbf{P}^{cc} -union and conjunctive reductions. Then $\exists \cdot \mathcal{C} \subseteq \text{BP} \cdot \oplus \cdot \mathcal{C}$.*

Proof. Let L be a language in $\exists \cdot \mathcal{C}$. There exists a language $L' \in \mathcal{C}$ and a bound $p \in \mathbf{poly}$ such that $L = \exists^p(L')$. Define $l_n := \lceil p(\log n) \rceil$. We fix an input

$(x, y) \in L$, $|x| = |y| = n$. Let $S := \{w \in \mathbb{B}^{l_n} \mid (\langle x, w \rangle, \langle y, w \rangle) \in L'\}$ be the set of witnesses of (x, y) and $d := |S|$ its size. We pick a natural number m such that $2l_n d < m \leq 4l_n d$ and encode the witnesses as polynomials over $F := \text{GF}(2^m)$, the finite field with 2^m elements. We then consider pairs $(a, b) \in F^2$ and show that for a sizable fraction of them there will be exactly one polynomial p representing a witness such that $p(a) = b$. The statement follows by choosing m , a and b at random. For a string $s = s_1 \cdots s_l$ we define the polynomial $p_s(X) := \sum_{i=1}^l s_i X^i$. We fix a witness w in S . An element a of F is called w -good, if for all witnesses $w' \neq w$ in S we have $p_w(a) \neq p_{w'}(a)$. Since p_w and $p_{w'}$ can agree on at most l_n elements, there are at least $|F| - l_n d$ many w -good elements in F . Consider the set A_w containing all pairs $(a, p_w(a))$ for w -good elements a . The sets A_w and $A_{w'}$ are disjoint for different strings w and w' . Define $A := \bigcup_{w \in S} A_w$. Then $|A| \geq d(|F| - l_n d)$. We define the language L'' in \mathcal{C} by

$$L'' := \{(\langle x, r \rangle, w), (\langle y, r \rangle, w) \mid n := |x| = |y|, r = \langle m^*, a, b \rangle, m^* \in [2l_n], \\ a, b \in \text{GF}(2^{m^*}), |w| = l_n, p_w(a) = b, (\langle x, w \rangle, \langle y, w \rangle) \in L'\},$$

where $r = \langle m^*, a, b \rangle$ means that we use r as an encoding of a natural number m^* and field elements a and b . Furthermore, define $L''' := \bigoplus^p(L'') \in \bigoplus \cdot \mathcal{C}$. If $(x, y) \notin L$ then for all w and r the pair $(\langle x, r \rangle, w), (\langle y, r \rangle, w)$ is not in L'' , and thus $(x, y) \notin L'''$.

If $(x, y) \in L$ then with probability $1/2l_n$ we have $m = m^*$ as $m \leq \log 4l_n d \leq 2l_n$. In case $m = m^*$ there is exactly one witness w for $(\langle x, r \rangle, \langle y, r \rangle)$ showing $(x, y) \in L'''$. The size of A is at least $l_n d^2$, the size of F^2 is at most $16l_n^2 d^2$. If we choose (a, b) at random in F^2 we have a $1/16l_n$ chance of being in A . Thus, for fixed input (x, y) the probability of choosing r at random such that $m = m^*$ and $(a, b) \in A$ is at least $1/32l_n^2$.

The class $\bigoplus \cdot \mathcal{C}$ is closed under majority reductions by Fact 2.12. Thus, probability amplification is possible, and we get $L \in \text{BP} \cdot \bigoplus \cdot \mathcal{C}$. \square

Theorem 2.16. (Toda) $\text{PH}^{cc} \subseteq \text{BP} \cdot \bigoplus \cdot \text{P}^{cc}$.

Proof. We prove $\Sigma_k^{cc} \subseteq \text{BP} \cdot \bigoplus \cdot \text{P}^{cc}$ by induction on k :

Case $k = 0$: The class P^{cc} is closed under many-one reductions. The class $\bigoplus \cdot \text{P}^{cc}$ is also closed under many-one reductions by Fact 2.12, because P^{cc} is closed under P^{cc} -intersection, P^{cc} -union, and conjunctive reductions. Thus, $\Sigma_0^{cc} = \text{P}^{cc} \subseteq \bigoplus \cdot \text{P}^{cc} \subseteq \text{BP} \cdot \bigoplus \cdot \text{P}^{cc}$ by the inclusion property of the \bigoplus - and BP-operator (Observation 2.4).

Case $k \rightarrow k + 1$: It holds

$$\Sigma_{k+1}^{cc} = \exists \cdot \text{co} \cdot \Sigma_k^{cc} \tag{2}$$

$$\subseteq \exists \cdot \text{co} \cdot \text{BP} \cdot \bigoplus \cdot \text{P}^{cc} \tag{3}$$

$$= \exists \cdot \text{BP} \cdot \text{co} \cdot \bigoplus \cdot \text{P}^{cc} \tag{4}$$

$$= \exists \cdot \text{BP} \cdot \bigoplus \cdot \text{P}^{cc} \tag{5}$$

$$\subseteq \text{BP} \cdot \bigoplus \cdot \text{BP} \cdot \bigoplus \cdot \text{P}^{cc} \tag{6}$$

$$\subseteq \text{BP} \cdot \text{BP} \cdot \bigoplus \cdot \bigoplus \cdot \text{P}^{cc} \tag{7}$$

$$= \text{BP} \cdot \text{BP} \cdot \bigoplus \cdot \text{P}^{cc} \tag{8}$$

$$= \text{BP} \cdot \bigoplus \cdot \text{P}^{cc} \tag{9}$$

- (2) By Definition 2.2.
- (3) By the induction hypothesis for Σ_k^{cc} and monotonicity (Observation 2.5) of the operators $\text{co}\cdot$ and \exists .
- (4) By Observation 2.8.
- (5) By closure under complement of $\oplus \cdot \mathbf{P}^{cc}$ (Observation 2.10).
- (6) By the Valiant-Vazirani-Lemma (Lemma 2.15). Its application is possible, because $\text{BP} \cdot \oplus \cdot \mathbf{P}^{cc}$ is closed under conjunctive reductions and \mathbf{P}^{cc} -intersection.
- (7) By the Swapping-Lemma (Lemma 2.14) and monotonicity of the BP-operator (Observation 2.5). The Swapping-Lemma can be applied, because $\oplus \cdot \mathbf{P}^{cc}$ is closed under majority reductions.
- (8) By idempotency of the \oplus -operator (Observation 2.6).
- (9) By idempotency of the BP-operator (Observation 2.7). This holds because $\oplus \cdot \mathbf{P}^{cc}$ is closed under majority reductions.

□

Fact 2.17. $\mathbf{P}^{cc}(\mathbf{PP}^{cc}) = \mathbf{P}^{cc}(\#\mathbf{P}^{cc})$.

Proof. Alice and Bob can compute every $\#\mathbf{P}^{cc}$ -function f by binary search with polylog communication asking oracle queries to $\text{Graph}_{\leq}(f) := \{(\langle x, v \rangle, \langle y, v \rangle) \mid (v)_2 \leq f(x, y)\} \in \mathbf{PP}^{cc}$. □

Theorem 2.18. (Toda) $\mathbf{PH}^{cc} \subseteq \text{BP} \cdot \oplus \mathbf{P}^{cc} \subseteq \mathbf{P}^{cc}(\#\mathbf{P}^{cc}) = \mathbf{P}^{cc}(\mathbf{PP}^{cc})$.

Proof. Let $\text{acc}_{\Pi}(x, y)$ denote the number of accepting paths of a nondeterministic protocol Π on input (x, y) . The class $\#\mathbf{P}^{cc}$ contains all constant functions and is closed under addition and multiplication. If $(\Pi_n)_{n \in \mathbb{N}}$ is an efficient nondeterministic protocol family with $\text{acc}_{\Pi} := (\text{acc}_{\Pi_n})_{n \in \mathbb{N}}$ in $\#\mathbf{P}^{cc}$, and if we choose $p \in \mathbf{poly}$, then there exists an efficient nondeterministic protocol family $(\Pi'_n)_{n \in \mathbb{N}}$ such that $\text{acc}_{\Pi'_n}(x, y) = (1 + \text{acc}_{\Pi_n}(x, y))^{[p(\log n)]^{[p(\log n)]}}$. This proves $\text{BP} \cdot \oplus \mathbf{P}^{cc} \subseteq \mathbf{P}^{cc}(\#\mathbf{P}^{cc})$ as in the time complexity setting. □

Let IP denote the *inner product* function (see [11, Ex. 1.25, p.12]), and let MAJ denote the *majority function* (see e.g. [9]). The corollary below considers the consequences of the unlikely case that the inner product or majority function can be computed with a constant number of alternations.

Corollary 2.19. *It holds:*

1. $\text{IP} \in \mathbf{PH}^{cc}$ iff $\mathbf{PH}^{cc} = \text{BP} \cdot \oplus \mathbf{P}^{cc}$.
2. If $\mathbf{PH}^{cc} = \mathbf{PSPACE}^{cc}$ then $\mathbf{PH}^{cc} = \text{BP} \cdot \oplus \mathbf{P}^{cc}$.
3. $\text{MAJ} \in \mathbf{PH}^{cc}$ iff $\mathbf{PH}^{cc} = \text{BP} \cdot \oplus \mathbf{P}^{cc} = \mathbf{BP}^{cc}(\mathbf{PP}^{cc})$.
4. $\text{IP} \in \mathbf{PH}^{cc}$ iff $\text{MAJ} \in \mathbf{PH}^{cc}$.

Proof. 1. \Rightarrow : $\text{IP} \in \mathbf{PH}^{cc}$ implies $\oplus\mathbf{P}^{cc} \subseteq \mathbf{PH}^{cc}$ because IP is complete for $\oplus\mathbf{P}^{cc}$ under many-one reductions. Applying the BP-operator yields $\text{BP} \cdot \oplus\mathbf{P}^{cc} \subseteq \text{BP} \cdot \mathbf{PH}^{cc} = \mathbf{PH}^{cc}$. \Leftarrow : $\text{IP} \in \oplus\mathbf{P}^{cc} \subseteq \text{BP} \cdot \oplus\mathbf{P}^{cc} = \mathbf{PH}^{cc}$.

2. Follows from $\oplus\mathbf{P}^{cc} \subseteq \mathbf{PSPACE}^{cc}$ and (1.).

3. \Rightarrow : $\text{MAJ} \in \mathbf{PH}^{cc}$ implies $\mathbf{PP}^{cc} \subseteq \mathbf{PH}^{cc}$ because MAJ is complete for \mathbf{PP}^{cc} under many-one reductions. We obtain $\mathbf{BPP}^{cc}(\mathbf{PP}^{cc}) \subseteq \mathbf{BPP}^{cc}(\mathbf{PH}^{cc}) = \mathbf{PH}^{cc} \subseteq \text{BP} \cdot \oplus\mathbf{P}^{cc} \subseteq \mathbf{P}^{cc}(\mathbf{PP}^{cc}) \subseteq \mathbf{BPP}^{cc}(\mathbf{PP}^{cc})$. \Leftarrow : $\text{MAJ} \in \mathbf{PP}^{cc} \subseteq \mathbf{BPP}(\mathbf{PP}^{cc}) = \mathbf{PH}^{cc}$.

4. Follows from (1.) and (3.). \square

3 An alternating protocol for IP

The class \mathbf{PSPACE}^{cc} was defined as the class of languages which can be recognized with protocols using $(\log n)^{\mathcal{O}(1)}$ communication and $\mathcal{O}(\log n)$ alternations. In this section we show that languages in the class $\text{BP} \cdot \oplus\mathbf{P}^{cc}$ can be recognized by alternating protocols using only $\mathcal{O}(\log n / \log \log n)$ many alternations. It is enough to give such a protocol for the inner product function, because IP is complete for $\oplus\mathbf{P}^{cc}$, and Schöning's generalization $\text{BP} \cdot \mathcal{C} \subseteq \exists \cdot \forall \cdot \mathcal{C} \cap \forall \cdot \exists \cdot \mathcal{C}$ of the well known result of Lautemann, which is easily transferred into the communication complexity context. For a proof, see [10, Prop. 2.24, p.76]. Fix an odd natural number k . Alice has input $x = x_0 \dots x_{n-1}$ and Bob has input $y = y_0 \dots y_{n-1}$. They execute the following alternating protocol $I_k(s, t, b)$ on their inputs:

if ($k \geq t - s + 1$) **then** Alice and Bob determine if $\text{IP}_{t-s+1}(x_s \dots x_t, y_s \dots y_t) = b$ using the trivial protocol (Alice sends her input; both compute the value by themselves). They return the value of the trivial protocol.

else Alice guesses the following strings and sends them to Bob:

1. $\exists S \subseteq \{0, \dots, k-1\}, |S|$ odd: (branch disjunctively)
2. $\exists \tilde{b} \in \{0, 1\}$: (branch disjunctively)
3. $\forall i \in S$: (branch conjunctively)
4. $\forall j \in \bar{S}$: (branch conjunctively)
5. $\forall h \in \{i, j\}$: (branch conjunctively)

return $I_k(s_1, t_1, b_1)$, where $d := t - s + 1$, $B := \lceil \frac{d}{k} \rceil$, $s_1 := h \cdot B$, $t_1 := \min\{n-1, (h+1) \cdot B - 1\}$, and if $(h = i)$ then $b_1 := b$ else $b_1 := \tilde{b}$.

Correctness. Divide each input x and y in an odd number k of blocks of approximately equal sizes, i.e. $x = x^{(1)} \dots x^{(k)}$, $y = y^{(1)} \dots y^{(k)}$. It holds $\text{IP}(x, y) = \sum_{i \in [k]} \text{IP}(x^{(i)}, y^{(i)}) \bmod 2$. If $\text{IP}(x, y)$ evaluates to 1, there exists an odd number of blocks $S' \subseteq [k]$ where IP evaluates to 1 and the values of IP cancel on \bar{S}' . There are three cases:

1. $\text{IP}(x^{(j)}, y^{(j)}) = 0$ for all $j \in \bar{S}'$. We set $S := S'$ and $\tilde{b} := 0$.
2. $\text{IP}(x^{(j)}, y^{(j)}) = 1$ for all $j \in \bar{S}'$. We set $S := S'$ and $\tilde{b} := 1$.
3. There exist $j_0, j_1 \in \bar{S}'$ such that $\text{IP}(x^{(j_0)}, y^{(j_0)}) = 0$ and $\text{IP}(x^{(j_1)}, y^{(j_1)}) = 1$. The number of $j \in \bar{S}'$ with $\text{IP}(x^{(j)}, y^{(j)}) = 1$ has to be even. We set $S := S' \cup \{j \in \bar{S}' \mid \text{IP}(x^{(j)}, y^{(j)}) = 1\}$ and $\tilde{b} := 0$. Note that $|S|$ is odd.

In all three cases we have obtained a set $S \subseteq [k]$ of odd cardinality and a \tilde{b} such that $\text{IP}(x^{(i)}, y^{(i)}) = 1$ for all $i \in S$ and $\text{IP}(x^{(j)}, y^{(j)}) = \tilde{b}$ for all $j \in \bar{S}$. The case when $\text{IP}(x, y)$ evaluates to 0 is analogous. Thus, the protocol $I_k(s, t, b)$ accepts iff $\text{IP}_{t-s+1}(x_s \dots x_t, y_s \dots y_t) = b$. The protocol $I_k(0, n-1, 1)$ computes $\text{IP}_n(x, y)$.

Communication costs. There are two alternations in each round and the number of rounds is bounded by $t = \log_2 n / \log_2 k$. If we choose an odd k of size $(\log n)^c$ then the communication costs in each round are $\mathcal{O}(k)$ bits and the number of alternations is $\mathcal{O}(\log n / \log \log n)$. If $\mathbf{AComm}_{\mathcal{A}}(\mathcal{F})$ denotes the class of languages which can be recognized by alternating protocols using communication bounded by a function in \mathcal{F} and a number of alternations bounded by a function in \mathcal{A} , we have obtained

Theorem 3.1. $\text{BP} \cdot \oplus \mathbf{P}^{cc} \subseteq \mathbf{AComm}_{\mathcal{O}(\log n / \log \log n)}((\log n)^{\mathcal{O}(1)})$.

Acknowledgement

I would like to express my deep gratitude to Martin Dietzfelbinger, Uwe Schöning and Jacobo Torán for careful reading, fruitful discussions, and their support.

References

- [1] L. Babai, P. Frankl, and J. Simon. Complexity classes in communication complexity theory (preliminary version). In *27th Annual Symposium on Foundations of Computer Science, 27-29 October 1986, Toronto, Ontario, Canada*, pages 337–347, 1986.
- [2] J. L. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity II*. Texts in Theoretical Computer Science, An EATCS Series. Springer-Verlag, 1st edition, 1990.
- [3] J. L. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity I*. Texts in Theoretical Computer Science, An EATCS Series. Springer-Verlag, 2nd edition, 1995.
- [4] H. Buhrman, N. K. Vereshchagin, and R. de Wolf. On computation and communication with small bias. In *22nd Annual IEEE Conference on Computational Complexity (CCC 2007), 13-16 June 2007, San Diego, California, USA*, pages 24–32. IEEE Computer Society, 2007.
- [5] C. Damm, M. Krause, C. Meinel, and S. Waack. On relations between counting communication complexity classes. *J. Comput. Syst. Sci.*, 69(2):259–280, 2004.
- [6] D.-Z. Du and K.-I. Ko. *Theory of Computational Complexity*. Series in Discrete Mathematics and Optimization. Wiley-Interscience, 1st edition, 2000.
- [7] L. Fortnow. Counting complexity. In Selman and Hemaspaandra [19], pages 81–107.
- [8] B. Halstenberg and R. Reischuk. Relations between communication complexity classes. *J. Comput. Syst. Sci.*, 41(3):402–429, 1990.

- [9] H. Klauck. Rectangle size bounds and threshold covers in communication complexity. In *18th Annual IEEE Conference on Computational Complexity, 7-10 July 2003, Aarhus, Denmark*, pages 118–134. IEEE Computer Society.
- [10] J. Köbler, U. Schöning, and J. Torán. *The Graph Isomorphism Problem – Its Structural Complexity*. Birkhäuser Boston, 1993.
- [11] E. Kushilevitz and N. Nisan. *Communication Complexity*. Cambridge University Press, 1997.
- [12] C. H. Papadimitriou and S. Zachos. Two remarks on the power of counting. In A. B. Cremers and H.-P. Kriegel, editors, *Theoretical Computer Science, 6th GI-Conference, Dortmund, Germany, January 5-7, 1983, Proceedings*, volume 145 of *Lecture Notes in Computer Science*, pages 269–276. Springer-Verlag, 1983.
- [13] A. Razborov and A. Sherstov. The sign-rank of \mathbf{AC}^0 . *FOCS'08, to appear*.
- [14] U. Schöning. *Complexity and Structure*, volume 211 of *Lecture Notes in Computer Science*. Springer-Verlag, 1986.
- [15] U. Schöning. The power of counting. In Selman [18], pages 204–223.
- [16] U. Schöning. Probabilistic complexity classes and lowness. *J. Comput. Syst. Sci.*, 39(1):84–100, 1989.
- [17] U. Schöning. Recent highlights in structural complexity theory (invited talk). In *SOFSEM'91, Nizké Tratry (CSFR)*, Conference Proceedings, pages 205–216. Springer-Verlag, December 1991.
- [18] A. L. Selman, editor. *Complexity Theory Retrospective*, Foundations of Computing. Springer-Verlag, 1988.
- [19] A. L. Selman and L. A. Hemaspaandra, editors. *Complexity Theory Retrospective II*, Foundations of Computing. Springer-Verlag, 1997.
- [20] S. Toda. PP is as hard as the polynomial-time hierarchy. *SIAM J. Comput.*, 20(5):865–877, 1991.
- [21] L. G. Valiant and V. V. Vazirani. NP is as easy as detecting unique solutions. *Theor. Comput. Sci.*, 47(3):85–93, 1986.
- [22] A. C.-C. Yao. Some complexity questions related to distributive computing (preliminary report). In *Conference Record of the Eleventh Annual ACM Symposium on Theory of Computing, 30 April-2 May, 1979, Atlanta, Georgia, USA*, pages 209–213. ACM, 1979.

Liste der bisher erschienenen Ulmer Informatik-Berichte
Einige davon sind per FTP von `ftp.informatik.uni-ulm.de` erhältlich
Die mit * markierten Berichte sind vergriffen

List of technical reports published by the University of Ulm
Some of them are available by FTP from `ftp.informatik.uni-ulm.de`
Reports marked with * are out of print

- 91-01 *Ker-I Ko, P. Orponen, U. Schöning, O. Watanabe*
Instance Complexity
- 91-02* *K. Gladitz, H. Fassbender, H. Vogler*
Compiler-Based Implementation of Syntax-Directed Functional Programming
- 91-03* *Alfons Geser*
Relative Termination
- 91-04* *J. Köbler, U. Schöning, J. Toran*
Graph Isomorphism is low for PP
- 91-05 *Johannes Köbler, Thomas Thierauf*
Complexity Restricted Advice Functions
- 91-06* *Uwe Schöning*
Recent Highlights in Structural Complexity Theory
- 91-07* *F. Green, J. Köbler, J. Toran*
The Power of Middle Bit
- 91-08* *V.Arvind, Y. Han, L. Hamachandra, J. Köbler, A. Lozano, M. Mundhenk, A. Ogiwara,*
U. Schöning, R. Silvestri, T. Thierauf
Reductions for Sets of Low Information Content
- 92-01* *Vikraman Arvind, Johannes Köbler, Martin Mundhenk*
On Bounded Truth-Table and Conjunctive Reductions to Sparse and Tally Sets
- 92-02* *Thomas Noll, Heiko Vogler*
Top-down Parsing with Simultaneous Evaluation of Noncircular Attribute Grammars
- 92-03 *Fakultät für Informatik*
17. Workshop über Komplexitätstheorie, effiziente Algorithmen und Datenstrukturen
- 92-04* *V. Arvind, J. Köbler, M. Mundhenk*
Lowness and the Complexity of Sparse and Tally Descriptions
- 92-05* *Johannes Köbler*
Locating P/poly Optimally in the Extended Low Hierarchy
- 92-06* *Armin Kühnemann, Heiko Vogler*
Synthesized and inherited functions -a new computational model for syntax-directed semantics
- 92-07* *Heinz Fassbender, Heiko Vogler*
A Universal Unification Algorithm Based on Unification-Driven Leftmost Outermost Narrowing

- 92-08* *Uwe Schöning*
On Random Reductions from Sparse Sets to Tally Sets
- 92-09* *Hermann von Hasseln, Laura Martignon*
Consistency in Stochastic Network
- 92-10 *Michael Schmitt*
A Slightly Improved Upper Bound on the Size of Weights Sufficient to Represent Any Linearly Separable Boolean Function
- 92-11 *Johannes Köbler, Seinosuke Toda*
On the Power of Generalized MOD-Classes
- 92-12 *V. Arvind, J. Köbler, M. Mundhenk*
Reliable Reductions, High Sets and Low Sets
- 92-13 *Alfons Geser*
On a monotonic semantic path ordering
- 92-14* *Joost Engelfriet, Heiko Vogler*
The Translation Power of Top-Down Tree-To-Graph Transducers
- 93-01 *Alfred Lupper, Konrad Froitzheim*
AppleTalk Link Access Protocol basierend auf dem Abstract Personal Communications Manager
- 93-02 *M.H. Scholl, C. Laasch, C. Rich, H.-J. Schek, M. Tresch*
The COCOON Object Model
- 93-03 *Thomas Thierauf, Seinosuke Toda, Osamu Watanabe*
On Sets Bounded Truth-Table Reducible to P-selective Sets
- 93-04 *Jin-Yi Cai, Frederic Green, Thomas Thierauf*
On the Correlation of Symmetric Functions
- 93-05 *K.Kuhn, M.Reichert, M. Nathe, T. Beuter, C. Heinlein, P. Dadam*
A Conceptual Approach to an Open Hospital Information System
- 93-06 *Klaus Gaßner*
Rechnerunterstützung für die konzeptuelle Modellierung
- 93-07 *Ullrich Keßler, Peter Dadam*
Towards Customizable, Flexible Storage Structures for Complex Objects
- 94-01 *Michael Schmitt*
On the Complexity of Consistency Problems for Neurons with Binary Weights
- 94-02 *Armin Kühnemann, Heiko Vogler*
A Pumping Lemma for Output Languages of Attributed Tree Transducers
- 94-03 *Harry Buhrman, Jim Kadin, Thomas Thierauf*
On Functions Computable with Nonadaptive Queries to NP
- 94-04 *Heinz Faßbender, Heiko Vogler, Andrea Wedel*
Implementation of a Deterministic Partial E-Unification Algorithm for Macro Tree Transducers

- 94-05 *V. Arvind, J. Köbler, R. Schuler*
On Helping and Interactive Proof Systems
- 94-06 *Christian Kalus, Peter Dadam*
Incorporating record subtyping into a relational data model
- 94-07 *Markus Tresch, Marc H. Scholl*
A Classification of Multi-Database Languages
- 94-08 *Friedrich von Henke, Harald Rueß*
Arbeitstreffen Typtheorie: Zusammenfassung der Beiträge
- 94-09 *F.W. von Henke, A. Dold, H. Rueß, D. Schwier, M. Strecker*
Construction and Deduction Methods for the Formal Development of Software
- 94-10 *Axel Dold*
Formalisierung schematischer Algorithmen
- 94-11 *Johannes Köbler, Osamu Watanabe*
New Collapse Consequences of NP Having Small Circuits
- 94-12 *Rainer Schuler*
On Average Polynomial Time
- 94-13 *Rainer Schuler, Osamu Watanabe*
Towards Average-Case Complexity Analysis of NP Optimization Problems
- 94-14 *Wolfram Schulte, Ton Vullingsh*
Linking Reactive Software to the X-Window System
- 94-15 *Alfred Lupper*
Namensverwaltung und Adressierung in Distributed Shared Memory-Systemen
- 94-16 *Robert Regn*
Verteilte Unix-Betriebssysteme
- 94-17 *Helmuth Partsch*
Again on Recognition and Parsing of Context-Free Grammars:
Two Exercises in Transformational Programming
- 94-18 *Helmuth Partsch*
Transformational Development of Data-Parallel Algorithms: an Example
- 95-01 *Oleg Verbitsky*
On the Largest Common Subgraph Problem
- 95-02 *Uwe Schöning*
Complexity of Presburger Arithmetic with Fixed Quantifier Dimension
- 95-03 *Harry Buhrman, Thomas Thierauf*
The Complexity of Generating and Checking Proofs of Membership
- 95-04 *Rainer Schuler, Tomoyuki Yamakami*
Structural Average Case Complexity
- 95-05 *Klaus Achatz, Wolfram Schulte*
Architecture Independent Massive Parallelization of Divide-And-Conquer Algorithms

- 95-06 *Christoph Karg, Rainer Schuler*
Structure in Average Case Complexity
- 95-07 *P. Dadam, K. Kuhn, M. Reichert, T. Beuter, M. Nathe*
ADEPT: Ein integrierender Ansatz zur Entwicklung flexibler, zuverlässiger kooperierender Assistenzsysteme in klinischen Anwendungsumgebungen
- 95-08 *Jürgen Kehrer, Peter Schulthess*
Aufbereitung von gescannten Röntgenbildern zur filmlosen Diagnostik
- 95-09 *Hans-Jörg Burtschick, Wolfgang Lindner*
On Sets Turing Reducible to P-Selective Sets
- 95-10 *Boris Hartmann*
Berücksichtigung lokaler Randbedingung bei globaler Zielloptimierung mit neuronalen Netzen am Beispiel Truck Backer-Upper
- 95-12 *Klaus Achatz, Wolfram Schulte*
Massive Parallelization of Divide-and-Conquer Algorithms over Powerlists
- 95-13 *Andrea Mößle, Heiko Vogler*
Efficient Call-by-value Evaluation Strategy of Primitive Recursive Program Schemes
- 95-14 *Axel Dold, Friedrich W. von Henke, Holger Pfeifer, Harald Rueß*
A Generic Specification for Verifying Peephole Optimizations
- 96-01 *Ercüment Canver, Jan-Tecker Gayen, Adam Moik*
Formale Entwicklung der Steuerungssoftware für eine elektrisch ortsbediente Weiche mit VSE
- 96-02 *Bernhard Nebel*
Solving Hard Qualitative Temporal Reasoning Problems: Evaluating the Efficiency of Using the ORD-Horn Class
- 96-03 *Ton Vullingsh, Wolfram Schulte, Thilo Schwinn*
An Introduction to TkGofer
- 96-04 *Thomas Beuter, Peter Dadam*
Anwendungsspezifische Anforderungen an Workflow-Management-Systeme am Beispiel der Domäne Concurrent-Engineering
- 96-05 *Gerhard Schellhorn, Wolfgang Ahrendt*
Verification of a Prolog Compiler - First Steps with KIV
- 96-06 *Manindra Agrawal, Thomas Thierauf*
Satisfiability Problems
- 96-07 *Vikraman Arvind, Jacobo Torán*
A nonadaptive NC Checker for Permutation Group Intersection
- 96-08 *David Cyrluk, Oliver Möller, Harald Rueß*
An Efficient Decision Procedure for a Theory of Fix-Sized Bitvectors with Composition and Extraction
- 96-09 *Bernd Biechele, Dietmar Ernst, Frank Houdek, Joachim Schmid, Wolfram Schulte*
Erfahrungen bei der Modellierung eingebetteter Systeme mit verschiedenen SA/RT-Ansätzen

- 96-10 *Falk Bartels, Axel Dold, Friedrich W. von Henke, Holger Pfeifer, Harald Rueß*
Formalizing Fixed-Point Theory in PVS
- 96-11 *Axel Dold, Friedrich W. von Henke, Holger Pfeifer, Harald Rueß*
Mechanized Semantics of Simple Imperative Programming Constructs
- 96-12 *Axel Dold, Friedrich W. von Henke, Holger Pfeifer, Harald Rueß*
Generic Compilation Schemes for Simple Programming Constructs
- 96-13 *Klaus Achatz, Helmuth Partsch*
From Descriptive Specifications to Operational ones: A Powerful Transformation Rule, its Applications and Variants
- 97-01 *Jochen Messner*
Pattern Matching in Trace Monoids
- 97-02 *Wolfgang Lindner, Rainer Schuler*
A Small Span Theorem within P
- 97-03 *Thomas Bauer, Peter Dadam*
A Distributed Execution Environment for Large-Scale Workflow Management Systems with Subnets and Server Migration
- 97-04 *Christian Heinlein, Peter Dadam*
Interaction Expressions - A Powerful Formalism for Describing Inter-Workflow Dependencies
- 97-05 *Vikraman Arvind, Johannes Köbler*
On Pseudorandomness and Resource-Bounded Measure
- 97-06 *Gerhard Partsch*
Punkt-zu-Punkt- und Mehrpunkt-basierende LAN-Integrationsstrategien für den digitalen Mobilfunkstandard DECT
- 97-07 *Manfred Reichert, Peter Dadam*
ADEPT_{flex} - Supporting Dynamic Changes of Workflows Without Loosing Control
- 97-08 *Hans Braxmeier, Dietmar Ernst, Andrea Mößle, Heiko Vogler*
The Project NoName - A functional programming language with its development environment
- 97-09 *Christian Heinlein*
Grundlagen von Interaktionsausdrücken
- 97-10 *Christian Heinlein*
Graphische Repräsentation von Interaktionsausdrücken
- 97-11 *Christian Heinlein*
Sprachtheoretische Semantik von Interaktionsausdrücken
- 97-12 *Gerhard Schellhorn, Wolfgang Reif*
Proving Properties of Finite Enumerations: A Problem Set for Automated Theorem Provers

- 97-13 *Dietmar Ernst, Frank Houdek, Wolfram Schulte, Thilo Schwinn*
Experimenteller Vergleich statischer und dynamischer Softwareprüfung für eingebettete Systeme
- 97-14 *Wolfgang Reif, Gerhard Schellhorn*
Theorem Proving in Large Theories
- 97-15 *Thomas Wennekers*
Asymptotik rekurrenter neuronaler Netze mit zufälligen Kopplungen
- 97-16 *Peter Dadam, Klaus Kuhn, Manfred Reichert*
Clinical Workflows - The Killer Application for Process-oriented Information Systems?
- 97-17 *Mohammad Ali Livani, Jörg Kaiser*
EDF Consensus on CAN Bus Access in Dynamic Real-Time Applications
- 97-18 *Johannes Köbler, Rainer Schuler*
Using Efficient Average-Case Algorithms to Collapse Worst-Case Complexity Classes
- 98-01 *Daniela Damm, Lutz Claes, Friedrich W. von Henke, Alexander Seitz, Adelinde Uhrmacher, Steffen Wolf*
Ein fallbasiertes System für die Interpretation von Literatur zur Knochenheilung
- 98-02 *Thomas Bauer, Peter Dadam*
Architekturen für skalierbare Workflow-Management-Systeme - Klassifikation und Analyse
- 98-03 *Marko Luther, Martin Strecker*
A guided tour through *Typelab*
- 98-04 *Heiko Neumann, Luiz Pessoa*
Visual Filling-in and Surface Property Reconstruction
- 98-05 *Ercüment Canver*
Formal Verification of a Coordinated Atomic Action Based Design
- 98-06 *Andreas Küchler*
On the Correspondence between Neural Folding Architectures and Tree Automata
- 98-07 *Heiko Neumann, Thorsten Hansen, Luiz Pessoa*
Interaction of ON and OFF Pathways for Visual Contrast Measurement
- 98-08 *Thomas Wennekers*
Synfire Graphs: From Spike Patterns to Automata of Spiking Neurons
- 98-09 *Thomas Bauer, Peter Dadam*
Variable Migration von Workflows in *ADEPT*
- 98-10 *Heiko Neumann, Wolfgang Sepp*
Recurrent V1 – V2 Interaction in Early Visual Boundary Processing
- 98-11 *Frank Houdek, Dietmar Ernst, Thilo Schwinn*
Prüfen von C-Code und Statmate/Matlab-Spezifikationen: Ein Experiment

- 98-12 *Gerhard Schellhorn*
Proving Properties of Directed Graphs: A Problem Set for Automated Theorem Provers
- 98-13 *Gerhard Schellhorn, Wolfgang Reif*
Theorems from Compiler Verification: A Problem Set for Automated Theorem Provers
- 98-14 *Mohammad Ali Livani*
SHARE: A Transparent Mechanism for Reliable Broadcast Delivery in CAN
- 98-15 *Mohammad Ali Livani, Jörg Kaiser*
Predictable Atomic Multicast in the Controller Area Network (CAN)
- 99-01 *Susanne Boll, Wolfgang Klas, Utz Westermann*
A Comparison of Multimedia Document Models Concerning Advanced Requirements
- 99-02 *Thomas Bauer, Peter Dadam*
Verteilungsmodelle für Workflow-Management-Systeme - Klassifikation und Simulation
- 99-03 *Uwe Schöning*
On the Complexity of Constraint Satisfaction
- 99-04 *Ercument Canver*
Model-Checking zur Analyse von Message Sequence Charts über Statecharts
- 99-05 *Johannes Köbler, Wolfgang Lindner, Rainer Schuler*
Derandomizing RP if Boolean Circuits are not Learnable
- 99-06 *Utz Westermann, Wolfgang Klas*
Architecture of a DataBlade Module for the Integrated Management of Multimedia Assets
- 99-07 *Peter Dadam, Manfred Reichert*
Enterprise-wide and Cross-enterprise Workflow Management: Concepts, Systems, Applications. Paderborn, Germany, October 6, 1999, GI-Workshop Proceedings, Informatik '99
- 99-08 *Vikraman Arvind, Johannes Köbler*
Graph Isomorphism is Low for ZPP^{NP} and other Lowness results
- 99-09 *Thomas Bauer, Peter Dadam*
Efficient Distributed Workflow Management Based on Variable Server Assignments
- 2000-02 *Thomas Bauer, Peter Dadam*
Variable Serverzuordnungen und komplexe Bearbeiterzuordnungen im Workflow-Management-System ADEPT
- 2000-03 *Gregory Baratoff, Christian Toepfer, Heiko Neumann*
Combined space-variant maps for optical flow based navigation
- 2000-04 *Wolfgang Gehring*
Ein Rahmenwerk zur Einführung von Leistungspunktsystemen

- 2000-05 *Susanne Boll, Christian Heinlein, Wolfgang Klas, Jochen Wandel*
Intelligent Prefetching and Buffering for Interactive Streaming of MPEG Videos
- 2000-06 *Wolfgang Reif, Gerhard Schellhorn, Andreas Thums*
Fehlersuche in Formalen Spezifikationen
- 2000-07 *Gerhard Schellhorn, Wolfgang Reif (eds.)*
FM-Tools 2000: The 4th Workshop on Tools for System Design and Verification
- 2000-08 *Thomas Bauer, Manfred Reichert, Peter Dadam*
Effiziente Durchführung von Prozessmigrationen in verteilten Workflow-
Management-Systemen
- 2000-09 *Thomas Bauer, Peter Dadam*
Vermeidung von Überlastsituationen durch Replikation von Workflow-Servern in
ADEPT
- 2000-10 *Thomas Bauer, Manfred Reichert, Peter Dadam*
Adaptives und verteiltes Workflow-Management
- 2000-11 *Christian Heinlein*
Workflow and Process Synchronization with Interaction Expressions and Graphs
- 2001-01 *Hubert Hug, Rainer Schuler*
DNA-based parallel computation of simple arithmetic
- 2001-02 *Friedhelm Schwenker, Hans A. Kestler, Günther Palm*
3-D Visual Object Classification with Hierarchical Radial Basis Function Networks
- 2001-03 *Hans A. Kestler, Friedhelm Schwenker, Günther Palm*
RBF network classification of ECGs as a potential marker for sudden cardiac death
- 2001-04 *Christian Dietrich, Friedhelm Schwenker, Klaus Riede, Günther Palm*
Classification of Bioacoustic Time Series Utilizing Pulse Detection, Time and
Frequency Features and Data Fusion
- 2002-01 *Stefanie Rinderle, Manfred Reichert, Peter Dadam*
Effiziente Verträglichkeitsprüfung und automatische Migration von Workflow-
Instanzen bei der Evolution von Workflow-Schemata
- 2002-02 *Walter Guttmann*
Deriving an Applicative Heapsort Algorithm
- 2002-03 *Axel Dold, Friedrich W. von Henke, Vincent Vialard, Wolfgang Goerigk*
A Mechanically Verified Compiling Specification for a Realistic Compiler
- 2003-01 *Manfred Reichert, Stefanie Rinderle, Peter Dadam*
A Formal Framework for Workflow Type and Instance Changes Under Correctness
Checks
- 2003-02 *Stefanie Rinderle, Manfred Reichert, Peter Dadam*
Supporting Workflow Schema Evolution By Efficient Compliance Checks
- 2003-03 *Christian Heinlein*
Safely Extending Procedure Types to Allow Nested Procedures as Values

- 2003-04 *Stefanie Rinderle, Manfred Reichert, Peter Dadam*
On Dealing With Semantically Conflicting Business Process Changes.
- 2003-05 *Christian Heinlein*
Dynamic Class Methods in Java
- 2003-06 *Christian Heinlein*
Vertical, Horizontal, and Behavioural Extensibility of Software Systems
- 2003-07 *Christian Heinlein*
Safely Extending Procedure Types to Allow Nested Procedures as Values
(Corrected Version)
- 2003-08 *Changling Liu, Jörg Kaiser*
Survey of Mobile Ad Hoc Network Routing Protocols)
- 2004-01 *Thom Frühwirth, Marc Meister (eds.)*
First Workshop on Constraint Handling Rules
- 2004-02 *Christian Heinlein*
Concept and Implementation of C+++, an Extension of C++ to Support User-Defined
Operator Symbols and Control Structures
- 2004-03 *Susanne Biundo, Thom Frühwirth, Günther Palm(eds.)*
Poster Proceedings of the 27th Annual German Conference on Artificial Intelligence
- 2005-01 *Armin Wolf, Thom Frühwirth, Marc Meister (eds.)*
19th Workshop on (Constraint) Logic Programming
- 2005-02 *Wolfgang Lindner (Hg.), Universität Ulm , Christopher Wolf (Hg.) KU Leuven*
2. Krypto-Tag – Workshop über Kryptographie, Universität Ulm
- 2005-03 *Walter Guttmann, Markus Maucher*
Constrained Ordering
- 2006-01 *Stefan Sarstedt*
Model-Driven Development with ACTIVECHARTS, Tutorial
- 2006-02 *Alexander Raschke, Ramin Tavakoli Kolagari*
Ein experimenteller Vergleich zwischen einer plan-getriebenen und einer
leichtgewichtigen Entwicklungsmethode zur Spezifikation von eingebetteten
Systemen
- 2006-03 *Jens Kohlmeyer, Alexander Raschke, Ramin Tavakoli Kolagari*
Eine qualitative Untersuchung zur Produktlinien-Integration über
Organisationsgrenzen hinweg
- 2006-04 *Thorsten Liebig*
Reasoning with OWL - System Support and Insights –
- 2008-01 *H.A. Kestler, J. Messner, A. Müller, R. Schuler*
On the complexity of intersecting multiple circles for graphical display

- 2008-02 *Manfred Reichert, Peter Dadam, Martin Jurisch, Ulrich Kreher, Kevin Göser, Markus Lauer*
Architectural Design of Flexible Process Management Technology
- 2008-03 *Frank Raiser*
Semi-Automatic Generation of CHR Solvers from Global Constraint Automata
- 2008-04 *Ramin Tavakoli Kolagari, Alexander Raschke, Matthias Schneiderhan, Ian Alexander*
Entscheidungsdokumentation bei der Entwicklung innovativer Systeme für produktlinien-basierte Entwicklungsprozesse
- 2008-05 *Markus Kalb, Claudia Dittrich, Peter Dadam*
Support of Relationships Among Moving Objects on Networks
- 2008-06 *Matthias Frank, Frank Kargl, Burkhard Stiller (Hg.)*
WMAN 2008 – KuVS Fachgespräch über Mobile Ad-hoc Netzwerke
- 2008-07 *M. Maucher, U. Schöning, H.A. Kestler*
An empirical assessment of local and population based search methods with different degrees of pseudorandomness
- 2008-08 *Henning Wunderlich*
Covers have structure
- 2008-09 *Karl-Heinz Niggl, Henning Wunderlich*
Implicit characterization of FPTIME and NC revisited
- 2008-10 *Henning Wunderlich*
On span- P^{cc} and related classes in structural communication complexity
- 2008-11 *M. Maucher, U. Schöning, H.A. Kestler*
On the different notions of pseudorandomness
- 2008-12 *Henning Wunderlich*
On Toda's Theorem in structural communication complexity

Ulmer Informatik-Berichte
ISSN 0939-5091

Herausgeber:
Universität Ulm
Fakultät für Ingenieurwissenschaften und Informatik
89069 Ulm