Tools for Proving Zero Knowledge

Ingrid Biehl, Johannes Buchmann,
Bernd Meyer, Christian Thiel, Christoph Thiel

Universität des Saarlandes, Fachbereich Informatik,
Im Stadtwald 15, 6600 Saarbrücken, Germany

Abstract. We develop general techniques that can be used to prove the zero knowledge property of most of the known zero knowledge protocols. Those techniques consist in reducing the circuit indistinguishability of the output distributions of two probabilistic Turing machines to the indistinguishability of the output distributions of certain subroutines.

1 Introduction

It is an important result in the theory of zero knowledge proofs that assuming the existence of a circuit secure encryption machine every language in NP has a zero knowledge proof. This result can be obtained by constructing a zero knowledge proof system for the NP-complete language 3C of three colourable graphs (see [1, 2]). In this protocol the prover and the verifier repeat a certain subprotocol a number of times which is polynomial in the length of the input. The encryption machine is called in a subroutine used in that subprotocol. The protocol can therefore be written in the form

$$S = (MNO)^{n_x} \tag{1}$$

where MNO is the subprotocol which is repeated n_x times, where x is the input and N is the subroutine which calls the encryption machine, and where M and O are the machines that carry out the computations before and after N is used. In order to show that S has the zero knowledge property one must show that the communication carried out in S can be simulated by a probabilistic polynomial time Turing machine even if the verifier is replaced by a cheating verifier. After replacing the verifier the protocol is still of the form (1). The simulator S' is constructed by replacing N with a machine N' which has no knowledge of a three colouring of the input graph. By virtue of the circuit security of the encryption machine, the output distributions of N and N' are circuit indistinguishable. It remains to be shown that the output distributions of S and S' are circuit indistinguishable.

Protocols and simulators for other zero knowledge protocols are constructed in the same way.

The goal of this paper is to unify the proofs for the zero knowledge property. We show that replacing the subroutine N with N' in a probabilistic Turing machine S of the form (1) yields (under certain conditions) a machine S' whose output distribution is circuit indistinguishable from the output distribution of

R.A. Rueppel (Ed.): Advances in Cryptology - EUROCRYPT '92, LNCS 658, pp. 356-365, 1993.

S if the output distribution of N is circuit indistinguishable from the output distribution of N'. Another goal of this paper is to precisely define the notions used in this context.

2 Probabilistic Turing Machines

Throughout this paper we use the alphabets $\Sigma = \{0, 1, \#\}$ and $\Sigma_0 = \{0, 1\}$.

Definition 1. A *probabilistic Turing machine* is a pair $Z = (M, p)$ where

1. $M = (K, \Sigma, \Delta, s)$ is a k-tape nondeterministic Turing machine (see [3], pp. 204–211)
2. p: $\Delta \to [0, 1]$ is a function which determines the probability of each transition in Δ, i.e. for every $q \in K$ and $\mathbf{a} \in \Sigma^k$ we have

$$\sum_{d \in \Delta(q,a)} p(d) = 1 \ ,$$

where $\Delta(q, \mathbf{a}) = \Delta \cap (\{q\} \times \{\mathbf{a}\} \times (K \cup \{h\}) \times (\Sigma \cup \{L, R\})^k)$.

A probabilistic Turing machine with $p(\Delta) \subseteq \{0, \frac{1}{2}, 1\}$ is called *coin tossing machine*.

We adopt the input and output conventions of [3]. For $x, y \in \Sigma_0^*$ we denote by $\Pi_Z(x, y)$ the probability for Z to output y on input of x. It is easy to see that

$$\sum_{y \in \Sigma_0^*} \Pi_Z(x, y) \leq 1 \ .$$

For $x \in \Sigma_0^*$ we denote by $Z(x)$ the set of all elements in Σ_0^* that can with positive probability occur as an output of Z on input of x, and $Z(L) = \bigcup_{x \in L} Z(x)$. If the length of each computation of Z on input of x is bounded by $c \in \mathbb{N}$, we denote the maximal length of a computation of Z on input of x by $\text{time}(Z(x))$. We say that *the running time of Z is bounded by a function* $T : \mathbb{N} \to \mathbb{N}$ if for all $x \in \Sigma_0^*$ we have $\text{time}(Z(x)) \leq t(|x|)$.

If there is a function $\ell : \mathbb{N} \to \mathbb{N}$ such that, on input of strings of length u, the machine only outputs strings of length $\ell(u)$ with positive probability, then we call Z a ***homogeneous*** probabilistic Turing machine.

If there is a polynomial $f \in \mathbb{N}[X]$ such that, on input of strings of length u, the output length of the machine Z is bounded by $f(u)$, we call Z a probabilistic Turing machine with *polynomially bounded output length*.

Let Z_1 and Z_2 be probabilistic Turing machines. Then the *concatenation* $Z_1 Z_2$ of Z_1 and Z_2 is defined as the probabilistic Turing machine that first operates as Z_1. Whenever Z_1 terminates, Z_2 is called where the input of Z_2 is the output of Z_1. We also use the notation Z_1^n for $\underbrace{Z_1 Z_1 \cdots Z_1}_{n \text{ times}}$.

3 Probabilistic Circuits

A *probabilistic circuit* is a deterministic circuit (see [4], pp. 73) with a partition $\mathrm{In} = \mathrm{In}_D \cup \mathrm{In}_P$, $\mathrm{In}_D \cap \mathrm{In}_P = \emptyset$, of the input nodes. The input nodes in In_D (the deterministic input nodes) receive the input of the computation. The nodes in In_P (the probabilistic input nodes) are assigned uniformly at random 0 or 1. The number of all nodes but the input nodes of a circuit C is called $\mathrm{size}(C)$.

For a probabilistic circuit C with m input nodes and n output nodes and for $y \in \{0,1\}^m$, $z \in \{0,1\}^n$ we denote by $\Pi_C(y,z)$ the probability for C to output z on input of y.

Let C_1 be a probabilistic circuit with n output nodes and C_2 be a probabilistic circuit with n input nodes. Then the *composition* of C_1 and C_2 is the circuit which results by connecting the output nodes of C_1 with the input nodes of C_2.

Let $L \subseteq \Sigma_0^*$. A family $\{C_x\}_{x\in L}$ of probabilistic circuits is called *polynomial* if $\mathrm{size}(C_x)$ is bounded by $|x|^k$ for some $k \in \mathbb{N}$.

In order to be able to prove our main theorems we need the following results.

Lemma 2. *There is a constant $c \in \mathbb{N}$ such that for all Turing-decidable languages $L \subseteq \{0,1\}^*$ the following holds: if L is decided by a deterministic Turing machine $M = (K, \Sigma, \delta, s)$ in time $T\colon \mathbb{N} \to \mathbb{N}$, then there is a family $\{C_n\}_{n\in\mathbb{N}}$ of deterministic circuits which decides L and satisfies*

$$\mathrm{size}(C_n) = (|K|\,|\Sigma|)^c T(n) \log T(n) \ .$$

Proof. See [4], pp. 84–91.

Lemma 3. *There are $c, d \in \mathbb{N}$ such that for all homogenous polynomial coin tossing machines $M = ((K, \Sigma, \delta, s), p)$ with output length $\ell : \mathbb{N} \to \mathbb{N}$ and running time bounded by $T \in \mathbb{N}[X]$ there is a polynomial family $\{C_n\}_{n\in\mathbb{N}}$ of probabilistic circuits such that $\{\Pi_{C_{|x|}}(x,\cdot)\}_{x\in L}$ and $\{\Pi_M(x,\cdot)\}_{x\in L}$ are equal and which satisfies*

$$\mathrm{size}(C_n) = d\ell(n)(|K|\,|\Sigma|)^c T(n) \log T(n) \ .$$

Proof. Without loss of generality we assume that there is $q \in \mathbb{N}[X]$ such that on input of length n the machine M tosses the coin exactly $q(n)$ times. Moreover, we can construct a homogeneous polynomial time deterministic Turing machine $M' = (K', \Sigma, \delta', s')$ with the following property: suppose that on input of x the machine M carries out the sequence of coin tosses $\alpha = (\alpha_1, \ldots, \alpha_{q(|x|)})$ and outputs y, then, one input of (x,α), the machine M' outputs y. There is a constant $r \in \mathbb{N}$ (independent of M) such that $|K'| \le r|K|$. There is an other constant $s \in \mathbb{N}$ (independent of M') such that $T'(|(x,\alpha)|) \le sT(|x|)$ for the running time T' of M'.

If we define for $x, y \in \Sigma_0^*$

$$\Pi_{M'}(x,y) = \frac{1}{2^{q(|x|)}} \left| \left\{ \alpha \in \{0,1\}^{q(|x|)} | M'(x,\alpha) = y \right\} \right|$$

then we have $\Pi_{M'} = \Pi_M$.

In order to be able to apply Lemma 2 we consider the deterministic Turing machine M'_m ($m \in \mathbb{N}$) which on input of (x, α) outputs the mth bit of the output y which is defined to be 0 if $m > \ell(|x|)$.

For $x \in \{0,1\}^*, y = (y_1, \ldots, y_{\ell(|x|)}) \in \{0,1\}^*$ we have

$$\Pi_{M'}(x,y) = \frac{1}{2^{q(|x|)}} \left| \left\{ \alpha \in \{0,1\}^{q(|x|)} | M'_i(x,\alpha) = y_i, \ \forall\, 1 \leq i \leq \ell(|x|) \right\} \right| .$$

The machine M'_m works exactly as M' and deletes at the end of its computation all but the mth bit of the output. Therefore there is a constant $t \in \mathbb{N}$ (independent of M') such that $T'_m(|(x,\alpha)|) \leq tT'(|(x,\alpha)|)$ for the running time T'_m of M'_m. The number of states of M'_m is polynomial in the number of states of M.

We apply Lemma 2 to M'_m and thus obtain a polynomial family $\{C_n^{(m)}\}_{n \in \mathbb{N}}$ of deterministic circuits which simulates M'_m. The circuit $C_n^{(m)}$ has n deterministic and $q(n)$ probabilistic input vertices.

We construct the circuit C_n by connecting the $C_n^{(m)}$, $1 \leq m \leq \ell(|x|)$, in the natural order in parallel, that means all circuits have the same deterministic and probabilistic input.

Since C_n is constructed from $\ell(n)$ circuits whose size is polynomially bounded in n, the size of C_n itself is bounded by a polynomial in n, which means that $\{C_n\}_{n \in \mathbb{N}}$ is a polynomial family of circuits. Moreover, we have by construction that for every $x \in \{0,1\}^*$

$$\Pi_{C_{|x|}}(x, \cdot) = \Pi_M(x, \cdot) \ .$$

□

4 Indistinguishability

Let U and V be two probability distributions on Σ_0^*. The series

$$\delta_S(U,V) = \sum_{y \in \Sigma_0^*} |U(y) - V(y)|$$

is called the ***statistical difference*** between U and V. In general it is impossible to determine in polynomial time that two probability distributions have a non zero statistical difference. Therefore one uses tools like probabilistic circuits and probabilistic algorithms (i.e. probabilistic Turing machines) to distinguish between probability distributions.

For a probabilistic circuit with m input nodes and one output node we call

$$\delta_C(U,V) = \left| \sum_{y \in \Sigma_0^m} \Pi_C(y,1)(U(y) - V(y)) \right|$$

the *circuit difference* between U and V with respect to C.

Finally, for a probabilistic Turing machine Z we call the series

$$\delta_Z(U,V) = \Big| \sum_{y \in \Sigma_0^*} \Pi_Z(y,1)(U(y) - V(y)) \Big|$$

the *algorithmical difference* between U and V with respect to Z.

Definition 4. Let $L \subseteq \Sigma_0^*$, let $U = \{U_x\}_{x \in L}$ and $V = \{V_x\}_{x \in L}$ be two families of probability distributions on Σ_0^*.

1. The families U and V are called *perfectly indistinguishable* (p-indistinguishable) if $U = V$.
2. The families U and V are called *statistically indistinguishable* (s-indistinguishable) if for every $k \in \mathbb{N}$

$$\lim_{\substack{x \in L \\ |x| \to \infty}} |x|^k \delta_S(U_x, V_x) = 0 \ .$$

3. The families U and V are called *circuit indistinguishable* (c-indistinguishable) if for every polynomial family $\{C_x\}_{x \in L}$ of probabilistic circuits C_x and for every $k \in \mathbb{N}$ we have

$$\lim_{\substack{x \in L \\ |x| \to \infty}} |x|^k \delta_{C_x}(U_x, V_x) = 0 \ .$$

4. The families U and V are called *algorithmically indistinguishable* (a-indistinguishable) if for every polynomial time probabilistic Turing machine Z and for every $k \in \mathbb{N}$ we have

$$\lim_{\substack{x \in L \\ |x| \to \infty}} |x|^k \delta_Z(U_x, V_x) = 0 \ .$$

Lemma 5. *Let $L \subseteq \Sigma_0^*$. Let Z and Z' be homogeneous probabilistic Turing machines. Assume that Z has polynomial output length. If $\{\Pi_Z(x,\cdot)\}_{x \in L}$ and $\{\Pi_{Z'}(x,\cdot)\}_{x \in L}$ are circuit indistinguishable then for all $x \in L$ but a finite set the elements of $Z(x)$ and $Z'(x)$ are of the same length.*

Proof. The case $|L| < \infty$ is trivial. So assume $|L| = \infty$. Assume that there is an infinite subset $L' \subseteq L$ such that for every $x \in L'$ the elements of $Z(x)$ and $Z'(x)$ are of different length. For $x \in L$ let C_x be the circuit with m_x input nodes, m_x being the length of the elements in $Z(x)$, which always outputs 1. Then we have

$$\delta_{C_x}(\Pi_Z(x,\cdot), \Pi_{Z'}(x,\cdot)) = 1$$

for all $x \in L'$, hence

$$\lim_{\substack{|x| \to \infty \\ x \in L}} |x| \delta_{C_x}(U_x, V_x) \neq 0 \ .$$

□

5 The Main Theorems

Let $L \subseteq \Sigma_0^*$. A family $\{Z_x = ((K_x, \Sigma_x, \delta_x, s_x), p_x)\}_{x \in L}$ of probabilistic Turing machines is called *polynomial* if there are $p, q, r \in \mathbb{N}[X]$ such that for all $x \in L$ and $y \in \Sigma_0^*$ $\text{time}(Z_x(y)) \leq p(|x|)q(|y|)$ and $|K_x|\,|\Sigma_x| \leq r(|x|)$.

Theorem 6. *Let $L \subseteq \Sigma_0^*$. Let $\{M_x\}_{x \in L}$ be a family of probabilistic Turing machines. Let N and N' be homogeneous probabilistic Turing machines, N' having polynomial output length. We define $\Gamma = \bigcup_{x \in L} M_x(x)$. Let $\{O_x\}_{x \in L}$ be a polynomial family of homogenous coin tossing machines. Assume that the following conditions hold:*

1. *$|z| \geq |x|$ for all $x \in L$ and $z \in M_x(x)$.*
2. *For $x \in L$ all elements of $M_x(x)$ are of the same length.*
3. *$\{\Pi_N(u, \cdot)\}_{u \in \Gamma}$ and $\{\Pi_{N'}(u, \cdot)\}_{u \in \Gamma}$ are c-indistinguishable.*

Then $\{\Pi_{M_x N O_x}(x, \cdot)\}_{x \in L}$ and $\{\Pi_{M_x N' O_x}(x, \cdot)\}_{x \in L}$ are c-indistinguishable.

Proof. For $x \in L$ we set $A_x = M_x N O_x$ and $B_x = M_x N' O_x$. Let $x \in L$ and let $\{O_{x,n}\}_{n \in \mathbb{N}}$ be a polynomial family of circuits simulating the probabilistic Turing machine O_x (see Lemma 3). Let $\overline{N}(u) = N(u) \cup N'(u)$.

Let $I \in \mathbb{N}$ such that for every $u \in \Gamma$, $|u| > I$ the elements of $N(u)$ and $N'(u)$ are of the same length. According to Lemma 5 such an I exists. Let $x \in L$, $|x| > I$, the elements of $A_x(x)$ and $B_x(x)$ are of the same length, say m_x. To measure a non zero circuit difference between $\Pi_{A_x}(x, \cdot)$ and $\Pi_{B_x}(x, \cdot)$ a circuit C must have m_x input nodes. Let $\{C_x\}_{x \in L}$ be a polynomial family of circuits. We assume that C_x has exactly m_x input nodes.

For $u \in M_x(x)$ all elements in $\overline{N}(u)$ have the same length $\ell(u)$, $\ell \in \mathbb{N}[X]$. Let $O'_{x,u} = O_{x,\ell(u)} C_x$ be the composition of $O_{x,\ell(u)}$ and C_x. Now we have:

$$
\begin{aligned}
&\delta_{C_x}\left(\Pi_{A_x}(x, \cdot), \Pi_{B_x}(x, \cdot)\right) \\
&= \left| \sum_{y \in \Sigma_0^{m_x}} \Pi_{C_x}(y, 1) \left(\Pi_{M_x N O_x}(x, y) - \Pi_{M_x N' O_x}(x, y)\right) \right| \\
&= \left| \sum_{y \in \Sigma_0^{m_x}} \Pi_{C_x}(y, 1) \sum_{u \in M_x(x)} \sum_{v \in \overline{N}(u)} \Pi_{M_x}(x, u) \left(\Pi_N(u, v) - \Pi_{N'}(u, v)\right) \Pi_{O_x}(v, y) \right| \\
&= \left| \sum_{u \in M_x(x)} \Pi_{M_x}(x, u) \sum_{v \in \overline{N}(u)} \sum_{y \in \Sigma_0^{m_x}} \Pi_{O_x}(v, y)\, \Pi_{C_x}(y, 1) \left(\Pi_N(u, v) - \Pi_{N'}(u, v)\right) \right| \\
&= \left| \sum_{u \in M_x(x)} \Pi_{M_x}(x, u) \sum_{v \in \overline{N}(u)} \Pi_{O'_{x,u}}(v, 1) \left(\Pi_N(u, v) - \Pi_{N'}(u, v)\right) \right| \\
&\leq \sum_{u \in M_x(x)} \Pi_{M_x}(x, u)\, \delta_{O'_{x,u}}\left(\Pi_N(u, \cdot), \Pi_{N'}(u, \cdot)\right) \ .
\end{aligned}
$$

Let $u \in \Sigma_0^*$ and let $x' \in L$ such that $u \in M_{x'}(x')$ then $|x'| \leq |u|$. Hence there are only finitely many $x' \in L$ with $u \in M_{x'}(x')$. Among the finitely many circuits $O'_{x',u}$, $u \in M_{x'}(x')$, we denote by O'_u the circuit which maximizes $\delta_{O'_{x',u}}(\Pi_N(u,\cdot), \Pi_{N'}(u,\cdot))$. Then we have

$$\delta_{C_x}(\Pi_{A_x}(x,\cdot), \Pi_{B_x}(x,\cdot)) \leq \max_{u \in M_x(x)} \delta_{O'_u}(\Pi_N(u,\cdot), \Pi_{N'}(u,\cdot)) \ . \qquad (2)$$

Now we consider $\mathrm{size}(O'_u)$:

$$\begin{aligned} \mathrm{size}(O'_u) &\leq \max_{\substack{x \in L \\ |x| < |u|}} \mathrm{size}(O'_{x,u}) = \max_{\substack{x \in L \\ |x| \leq |u|}} \mathrm{size}(O_{x,\ell(u)} C_x) \\ &\leq \max_{\substack{x \in L \\ |x| \leq |u|}} (\mathrm{size}(O_{x,\ell(u)}) + \mathrm{size}(C_x)) \ . \end{aligned}$$

Since $\{O_x\}_{x \in L}$ is a polynomial family of coin tossing machines and $|x| \leq |u|$ there is (according to Lemma 3) a $p \in \mathbb{N}[X]$ such that for all $u \in M_x(x)$ $\mathrm{size}(O'_u) \leq p(|u|)$. This implies with (2) that

$$\begin{aligned} &\lim_{\substack{x \in L \\ |x| \to \infty}} |x|^k \delta_{C_x}(\Pi_{A_x}(x,\cdot), \Pi_{B_x}(x,\cdot)) \\ &\leq \lim_{\substack{x \in L \\ |x| \to \infty}} \max_{u \in M_x(x)} |u|^k \delta_{O'_u}(\Pi_N(u,\cdot), \Pi_{N'}(u,\cdot)) \\ &= 0 \ . \end{aligned}$$

□

Let $L \subseteq \Sigma_0^*$ be a language and let $\{n_x\}_{x \in L}$ be a sequence in $\mathbb{N}$. That sequence is called *polynomially bounded* if there is $d > 0$ such that for every $x \in L$ we have $n_x \leq |x|^d$.

Theorem 7. *Let $L \subseteq \Sigma_0^*$. Let $\{n_x\}_{x \in L}$ be a polynomially bounded sequence in $\mathbb{N}$. Let S and T be homogeneous probabilistic Turing machines. Assume that the following conditions hold:*

1. *$|y| \geq |x|$ for all $x \in L$ and $y \in S(x)$.*
2. *$S(L) \subseteq L$.*
3. *T is a coin tossing machine such that for $q \in \mathbb{N}[X]$ and for all $i \in \mathbb{N}$ we have $\mathrm{time}(T^i(z)) \leq iq(|z|)$.*
4. *$\{\Pi_S(x,\cdot)\}_{x \in L}$ and $\{\Pi_T(x,\cdot)\}_{x \in L}$ are c-indistinguishable.*

Then $\{\Pi_{S^{n_x}}(x,\cdot)\}_{x \in L}$ and $\{\Pi_{T^{n_x}}(x,\cdot)\}_{x \in L}$ are c-indistinguishable.

Proof. We have

$$\delta_{C_x}(\Pi_{S^{n_x}}(x,\cdot), \Pi_{T^{n_x}}(x,\cdot)) = \left| \sum_{y \in \Sigma_0^{m_x}} \Pi_{C_x}(y,1) (\Pi_{S^{n_x}}(x,y) - \Pi_{T^{n_x}}(x,y)) \right| \ .$$

We can write

$$\Pi_{S^{n_x}}(x,y) - \Pi_{T^{n_x}}(x,y) = \sum_{i=0}^{n_x-1} \Pi_{S^{n_x-i}T^i}(x,y) - \Pi_{S^{n_x-i-1}T^{i+1}}(x,y)$$

and therefore

$$\begin{aligned}
&\delta_{C_x}\left(\Pi_{S^{n_x}}(x,\cdot), \Pi_{T^{n_x}}(x,\cdot)\right) \\
&= \left| \sum_{y \in \Sigma_0^{m_x}} \Pi_{C_x}(y,1) \left(\sum_{i=0}^{n_x-1} \Pi_{S^{n_x-i}T^i}(x,y) - \Pi_{S^{n_x-i-1}T^{i+1}}(x,y) \right) \right| \\
&= \left| \sum_{i=0}^{n_x-1} \sum_{y \in \Sigma_0^{m_x}} \Pi_{C_x}(y,1) \left(\Pi_{S^{n_x-i}T^i}(x,y) - \Pi_{S^{n_x-i-1}T^{i+1}}(x,y) \right) \right| \\
&\leq \sum_{i=0}^{n_x-1} \left| \sum_{y \in \Sigma_0^{m_x}} \Pi_{C_x}(y,1) \left(\Pi_{S^{n_x-i}T^i}(x,y) - \Pi_{S^{n_x-i-1}T^{i+1}}(x,y) \right) \right| \\
&\leq n_x \max_{0 \leq i \leq n_x-1} \delta_{C_x}\left(\Pi_{S^{n_x-i-1}ST^i}(x,\cdot), \Pi_{S^{n_x-i-1}TT^i}(x,\cdot)\right) \ ,
\end{aligned}$$

i.e. for $x \in L$ there is $0 \leq i_x \leq n_x - 1$ with

$$\begin{aligned}
&\delta_{C_x}\left(\Pi_{S^{n_x}}(x,\cdot), \Pi_{T^{n_x}}(x,\cdot)\right) \\
&\qquad \leq n_x \delta_{C_x}\left(\Pi_{S^{n_x-i_x-1}ST^{i_x}}(x,\cdot), \Pi_{S^{n_x-i_x-1}TT^{i_x}}(x,\cdot)\right) \ . \qquad (3)
\end{aligned}$$

Let $M_x = S^{n_x-i_x-1}$, $N = S$, $N' = T$ and $O_x = T^{i_x}$. We know:

1. M_x being a concatenation of homogeneous Turing machines is also homogeneous. Since we have $|y| \geq |x|$ for $y \in S(x)$, we find $|y| \geq |x|$ for all $y \in M_x(x)$.
2. N' has polynomial output length.
3. The families $\{\Pi_N(x,\cdot)\}_{x \in L}$ and $\{\Pi_{N'}(x,\cdot)\}_{x \in L}$ are c-indistinguishable. The set $\Gamma = \bigcup_{x \in L} M_x(x)$ is a subset of L and therefore $\{\Pi_N(x,\cdot)\}_{x \in \Gamma}$ and $\{\Pi_{N'}(x,\cdot)\}_{x \in \Gamma}$ are c-indistinguishable, too.
4. O_x has the same alphabet as T. The set of states of O_x is at most n_x-times the size of the set of states of T. Being a concatenation of homogeneous Turing machines, O_x itself is a homogeneous Turing machine. Therefore $\{O_x\}_{x \in L}$ is a polynomial family of homogeneous coin tossing machines.

Therefore we can apply Theorem 6. Using (3) we have for every $k \in \mathbb{N}$

$$\begin{aligned}
&\lim_{\substack{|x| \to \infty \\ x \in L}} |x|^k \delta_{C_x}\left(\Pi_{S^{n_x}}(x,\cdot), \Pi_{T^{n_x}}(x,\cdot)\right) \\
&\leq \lim_{\substack{|x| \to \infty \\ x \in L}} n_x |x|^k \delta_{C_x}\left(\Pi_{M_x N O_x}(x,\cdot), \Pi_{M_x N' O_x}(x,\cdot)\right) \\
&\quad \left(\{n_x\}_{x \in L} \text{ is polynomially bounded. Therefore there is } d \in \mathbb{N} \text{ with } n_x \leq |x|^d\right) \\
&\leq \lim_{\substack{|x| \to \infty \\ x \in L}} |x|^{d+k} \delta_{C_x}\left(\Pi_{M_x N O_x}(x,\cdot), \Pi_{M_x N' O_x}(x,\cdot)\right) \\
&= 0 \ .
\end{aligned}$$

Thus $\{\Pi_{S^{n_x}}(x,\cdot)\}_{x\in L}$ and $\{\Pi_{T^{n_x}}(x,\cdot)\}_{x\in L}$ are c-indistinguishable. □

Theorem 8. *Let $L \subseteq \Sigma_0^*$. Let $\{n_x\}_{x\in L}$ be a sequence in $\mathbb{N}$. Let S and T be coin tossing machines. Assume that $S(L) \subseteq L$. If $\{\Pi_S(x,\cdot)\}_{x\in L}$ and $\{\Pi_T(x,\cdot)\}_{x\in L}$ are p-indistinguishable, then also $\{\Pi_{S^{n_x}}(x,\cdot)\}_{x\in L}$ and $\{\Pi_{T^{n_x}}(x,\cdot)\}_{x\in L}$.*

Proof.

$$
\begin{aligned}
&\Pi_{S^{n_x}}(x,y) - \Pi_{T^{n_x}}(x,y) \\
&= \sum_{i=0}^{n_x-1} \Pi_{S^{n_x-i}T^i}(x,y) - \Pi_{S^{n_x-i-1}T^{i+1}}(x,y) \\
&= \sum_{i=0}^{n_x-1} \sum_{u\in\Sigma_0^*} \sum_{v\in\Sigma_0^*} \Pi_{S^{n_x-i-1}}(x,u) \underbrace{(\Pi_S(u,v) - \Pi_T(u,v))}_{=0} \Pi_{T^i}(v,y) \\
&= 0 \ .
\end{aligned}
$$

□

Theorem 9. *Let $L \subseteq \Sigma_0^*$. Let $\{n_x\}_{x\in L}$ be a polynomially bounded sequence in $\mathbb{N}$. Let S and T be coin tossing machines. Assume that the following conditions hold:*

1. *$|y| \geq |x|$ for all $x \in L$ and all $y \in S(x)$.*
2. *$S(L) \subseteq L$.*
3. *$\{\Pi_S(x,\cdot)\}_{x\in L}$ and $\{\Pi_T(x,\cdot)\}_{x\in L}$ are s-indistinguishable.*

Then $\{\Pi_{S^{n_x}}(x,\cdot)\}_{x\in L}$ and $\{\Pi_{T^{n_x}}(x,\cdot)\}_{x\in L}$ are s-indistinguishable.

Proof. As in the proof of Theorem 7 we obtain

$$
\delta_S(\Pi_{S^{n_x}}(x,\cdot), \Pi_{T^{n_x}}(x,\cdot)) \leq n_x \delta_S(\Pi_{M_x N O_x}(x,\cdot), \Pi_{M_x N' O_x}(x,\cdot)) \ ,
$$

where $M_x = S^{n_x-i_x-1}$, $N = S$, $N' = T$ and $O_x = T^{i_x}$. According to the conditions the families $\{\Pi_N(x,\cdot)\}_{x\in L}$ and $\{\Pi_{N'}(x,\cdot)\}_{x\in L}$ are s-indistinguishable.

$$
\begin{aligned}
&\delta_S\left(\Pi_{M_x N O_x}(x,\cdot), \Pi_{M_x N' O_x}(x,\cdot)\right) \\
&= \sum_{y\in\Sigma_0^*} |\Pi_{M_x N O_x}(x,y) - \Pi_{M_x N' O_x}(x,y)| \\
&\leq \sum_{y\in\Sigma_0^*} \sum_{u\in\Sigma_0^*} \sum_{v\in\Sigma_0^*} |\Pi_{M_x}(x,u)\,(\Pi_N(u,v) - \Pi_{N'}(u,v))\,\Pi_{O_x}(v,y)| \\
&\leq \sum_{u\in\Sigma_0^*} \Pi_{M_x}(x,u) \sum_{v\in\Sigma_0^*} |(\Pi_N(u,v) - \Pi_{N'}(u,v))| \underbrace{\sum_{y\in\Sigma_0^*} \Pi_{O_x}(v,y)}_{\leq 1} \\
&\leq \underbrace{\sum_{u\in\Sigma_0^*} \Pi_{M_x}(x,u)}_{\leq 1} \sup_{u\in M_x(x)} \sum_{v\in\Sigma_0^*} |\Pi_N(u,v) - \Pi_{N'}(u,v)| \ .
\end{aligned}
$$

Then we have for all $k \in \mathbb{N}$

$$\lim_{\substack{x \in L \\ |x| \to \infty}} |x|^k \delta_S(\Pi_{S^{n_x}}(x,\cdot), \Pi_{T^{n_x}}(x,\cdot))$$

$$\leq \lim_{\substack{x \in L \\ |x| \to \infty}} n_x |x|^k \sup_{u \in M_x(x)} \delta_S(\Pi_N(u,\cdot), \Pi_{N'}(u,\cdot))$$

$$\leq \lim_{\substack{x \in L \\ |x| \to \infty}} n |x|^{k+d} \sup_{u \in M_x(x)} \delta_S(\Pi_N(u,\cdot), \Pi_{N'}(u,\cdot))$$

($\{n_x\}_{x \in L}$ is polynomially bounded. Therefore there is $d \in \mathbb{N}$ with $n_x \leq |x|^d$)

$$\leq \limsup_{\substack{u \in L \\ |u| \to \infty}} |u|^{k+d} \delta_S(\Pi_N(u,\cdot), \Pi_{N'}(u,\cdot))$$

$$= 0 \ .$$

□

References

1. M. Garey and D. S. Johnson. *Computers and Intractability, A Guide to the Theory of NP-Completeness.* Freeman, 1979.
2. O. Goldreich, S. Micali, and A. Widgerson. *Proofs that Yield Nothing But Their Validity or All Languages in NP Have Zero-Knowledge Proof Systems.* J. ACM Vol. 38, pp. 691–729, 1991.
3. Harry R. Lewis and Christos H. Papadimitriou. *Elements of the theory of Computation.* Prentice-Hall, 1981.
4. K. R. Reischuk. *Einführung in die Komplexitätstheorie.* Teubner, 1990.