RESOURCE BOUNDED SYMMETRY OF INFORMATION REVISITED

Troy Lee and Andrei Romashchenko

March 10, 2005

Abstract. The information contained in a string x about a string y is the difference between the Kolmogorov complexity of y and the conditional Kolmogorov complexity of y given x, i.e., $I(x : y) = \mathrm{C}(y) - \mathrm{C}(y \mid x)$. The Kolmogorov–Levin Theorem says that $I(x : y)$ is symmetric up to a small additive term. We investigate if this property also holds for several versions of polynomial time bounded Kolmogorov complexity.

We study symmetry of information for some variants of distinguishing complexity CD where $\mathrm{CD}(x)$ is the length of a shortest program which accepts x and only x. We show relativized worlds where symmetry of information does not hold in a strong way for deterministic and nondeterministic polynomial time distinguishing complexities $\mathrm{CD}^{\mathrm{p}oly}$ and $\mathrm{CND}^{\mathrm{p}oly}$. On the other hand, for nondeterministic polynomial time distinguishing complexity with randomness, $\mathrm{CAMD}^{\mathrm{p}oly}$, we show that symmetry of information holds for most pairs of strings in any set in NP. Our techniques extend work of Buhrman et al. (CCC 2004) on language compression by AM algorithms, and have the following application to the compression of samplable sources, introduced in Trevisan et al. (CCC 2004): any element x in the support of a polynomial time samplable source X can be given a description of size $-\log \Pr[X = x] + O(\log^3 n)$, from which x can be recovered by an AM algorithm.

Keywords. Kolmogorov complexity, Symmetry of information

Subject classification. 68Q30, 68Q15

1. Introduction

One of the most beautiful theorems in Kolmogorov Complexity is the principle of "Symmetry of Information", independently proven by Kolmogorov and Levin (ZL70). Roughly speaking, symmetry of information states that for any two strings x and y, the information contained in x about y is equal to the information contained in y about x, up to logarithmic factors. More formally, letting $\mathrm{C}(x)$ be the length of a shortest program which prints x, and $\mathrm{C}(y \,|\, x)$ be the length of a shortest program which prints y when given input x, symmetry of information can be stated as $\mathrm{C}(y) - \mathrm{C}(y \,|\, x) \approx \mathrm{C}(x) - \mathrm{C}(x \,|\, y)$. Besides its inherent attractiveness, this principle has also seen applications in diverse areas of theoretical computer science, for example in (ABK^{+}02; JSV97; VV02).

In this paper, we investigate the principal of symmetry of information when resource bounds are placed on the program to describe y given x. While the argument of Kolmogorov-Levin (ZL70) can be used without modification to show that symmetry of information holds for programs using exponential time or polynomial space, things become trickier with polynomial time bounds. Though this question has been around for some time, indeed as early as 1967 Kolmogorov suggested time-bounded versions of symmetry of information as an interesting avenue of research (Lev04), still few definite answers are known. See section 7.1 of (LV97) for a survey and open problems.

The main contributions to the problem of polynomial time symmetry of information appear in the series of works (LM93; LW95) which show, in particular, the following:

- If P=NP then polynomial time symmetry of information holds (LW95).
- If cryptographic one-way functions exist, then polynomial time symmetry of information does not hold up to a $O(\log n)$ factor (LM93; LW95).

The intuition behind the second result is, if f is a polynomial time computable one-way function, and $f(x) = y$, then y is simple given x. On the other hand, if x is simple in polynomial time given y then this would provide a way to invert the function, by cycling through all small programs.

Revisiting these works, several interesting questions arise:

- Can polynomial time symmetry of information hold up to a factor larger than $O(\log n)$? The same argument sketched above shows that if symmetry of information holds up to a factor of $\delta(n)$ then there do not exist polynomial time computable cryptographical functions which cannot be inverted in time $2^{\delta(n)}$. However, as, for example, factoring n-bit integers can be done in $2^{O(\sqrt{n})}$ time (BJP93), it is not implausible that symmetry of information could hold up to a factor of $\delta(n) = \epsilon n$ or even $\delta(n) = n^{1/2+\epsilon}$. It is the case that $2C(x, y) \geq C(x) + C(y \,|\, x)$, could we show $(2 - \epsilon)C(x, y) \geq C(x) + C(y \,|\, x)$ for some ϵ?
- Can symmetry of information hold for complexity measures other than polynomial time printing complexity? En route to showing that BPP

is in the polynomial hierarchy, Sipser (Sip83) introduced a relaxation of printing complexity called distinguishing complexity, denoted CD. For a string x, $\mathrm{CD}(x)$ is the length of a shortest program which accepts x and only x.

The arguments of (LM93; LW95) leave open the question if symmetry of information can hold for distinguishing complexity. Now if f is a polynomial time computable one-way permutation and $f(x) = y$, then $\mathrm{CD}^{poly}(x \mid y)$ is constant, as with a description of f, on input z we accept if and only if $f(z) = y$. More recently, distinguishing complexity measures using nondeterminism, denoted CND, and nondeterminism and randomness (based on the complexity class AM), denoted CAMD, have been introduced (BFL02; BLvM04). Does symmetry of information hold for these measures?

- Is there an assumption weaker than P=NP which implies polynomial time symmetry of information?

Addressing the first two questions, we show relativized worlds where symmetry of information fails in a strong way for CD^{poly} and CND^{poly} (the existence of such worlds was claimed in (BF95), though without a complete proof). On the other hand, we show that for any set $A \in \mathrm{NP}$ symmetry of information holds for most pairs of strings $\langle x, y\rangle \in A$ with respect to the measure CAMD^{poly}. We also unconditionally show that $\mathrm{C}^{poly}(x, y) \geq \mathrm{CAMD}^{poly}(x) + \mathrm{CAMD}^{poly}(y \mid x)$. This implies that symmetry of information holds under the condition $\mathrm{C}^{poly}(x \mid y) \leq \mathrm{CAMD}^{poly}(x \mid y)$. We show that this statement, however, is equivalent to P=NP.

The main tool of our positve results is an extension of the language compression technique of (BLvM04). This extension itself has an interesting implication for the compression of samplable sources, the study of which is introduced in (TVZ04). We show that for any polynomial time samplable source X, any element x in the support of X can be given a description of size $-\log \Pr[X = x] + \log^3 n$, such that x can be recovered from this description by an AM algorithm. Note that this means the source can be compressed to expected length $H(X) + O(\log^3 n)$, differing from optimal by just a $O(\log^3 n)$ additive factor.

Another interesting approach to the definition of time-bounded Kolmogorov complexity is L. Levin's Kt complexity introduced in (Lev73). Recently D. Ronneburger proved that symmetry of information does not hold for Kt complexity in a very strong sense (Ron04).

2. Preliminaries

We use the following notation:

- denote by $\mathbb{B}$ the set $\{0,1\}$; similarly, $\mathbb{B}^n$ is the set of all binary strings of length n;
- denote by $|x|$ the length of a binary string x;
- denote by $\|A\|$ the cardinality of a finite set A;
- for a set $A \subset \mathbb{B}^*$ denote by $A^{=n}$ the set $\{x \ : \ x \in A \text{ and } |x| = n\}$.
- for a set of pairs of strings $A \subset \mathbb{B}^* \times \mathbb{B}^*$ denote by $A^{=n}$ the set $\{\langle x, y\rangle \in A \ : \ |x| + |y| = n\}$.

We will make use of the complexity classes P, NP, UP, RP, and BPP. See (Aar) for definitions.

2.1. Kolmogorov Complexity Measures. We use notation for Kolmogorov complexity from (LV97):

Definition 2.1. *The Kolmogorov complexity* $\mathrm{C}(y\,|\,x)$ *is defined as*

$$\min_p\{|p| \ : \ U(p,x) = y\},$$

where U is a universal recursive function. Also we define $\mathrm{C}(z) = \mathrm{C}(z\,|\,\lambda)$, *where λ is the empty word.*

The choice of U affects the Kolmogorov complexity by at most an additive constant. We consider several flavors of time bounded Kolmogorov complexity.

Definition 2.2. *Time t printing complexity* $\mathrm{C}^t(y\,|\,x)$ *is defined as*

$$\mathrm{C}^t(y\,|\,x) = \min_p\{|p| \ : \ U(p,x) = y \text{ and } U(p,x) \text{ runs in at most } t(|x|+|y|) \text{ steps}\}$$

for a universal machine U. Also $\mathrm{C}^t(z) = \mathrm{C}^t(z\,|\,\lambda)$.

The choice of universal machine U affects $\mathrm{C}^t(x\,|\,y)$ by at most an additive constant and the time bound t by at most a $\log(t)$ multiplicative factor.

We also make use of a randomized version of printing complexity:

Definition 2.3. *Randomized printing complexity* $\mathrm{CBP}^t(x \mid y)$ *is defined as the minimal length of a program* p *such that*

(i) $\Pr[U(p, y, r) = x] \geq 2/3$ *where the probability is taken over all* $t(|x| + |y|)$ *bit strings* r*.*

(ii) $U(p, y, r)$ *runs in at most* $t(|x| + |y|)$ *steps for all* r*.*

Definition 2.4. *Distinguishing complexity* $\mathrm{CD}^t(y \mid x)$ *is defined as the minimal length of a program* p *such that*

(i) $U(p, x, y)$ *accepts,*

(ii) $U(p, x, z)$ *rejects* $\forall z \neq y$*,*

(iii) $U(p, x, z)$ *runs in at most* $t(|x| + |z|)$ *steps.*

Once again, $\mathrm{CD}^t(z) = \mathrm{CD}^t(z \mid \lambda)$*.*

There are a few other variants of distinguishing complexity. In (BFL02) a nondeterministic variant of distinguishing complexity is defined. This definition is very similar to Definition Definition 2.4 except that the universal machine is nondeterministic. This version of complexity is denoted CND^t, where t is a time bound:

Definition 2.5. *Let* U_n *be a* nondeterministic *universal machine. Nondeterministic distinguishing complexity* $\mathrm{CND}^t(y \mid x)$ *is defined as the minimal length of a program* p *such that*

(i) $U_n(p, x, y)$ *accepts,*

(ii) $U_n(p, x, z)$ *rejects* $\forall z \neq y$*,*

(iii) $U_n(p, x, z)$ *runs in at most* $t(|x| + |z|)$ *steps.*

Further, in (BLvM04) a complexity based on the class AM was defined. In this case the universal machine is nondeterministic and probabilistic. This complexity is denoted CAMD^t:

Definition 2.6. *Let U_n be a* nondeterministic *universal machine.* $\mathrm{CAMD}^t(y \mid x)$ *is defined as the minimal length of a program p such that*

(i) $\Pr_r[U_n(p, x, y, r)$ *accepts*$] > 2/3$,

(ii) $\Pr_r[U_n(p, x, z, r)$ *accepts*$] < 1/3$ *for all* $z \neq y$,

(iii) $U_n(p, x, z, r)$ *runs in at most* $t(|x| + |z|)$ *steps.*

The probabilities above are taken over all $t(|x| + |y|)$ (respectively, $t(|x| + |z|)$) bit strings r.

As usual, we let $\mathrm{CND}^t(z) = \mathrm{CND}^t(z \mid \lambda)$, and $\mathrm{CAMD}^t(z) = \mathrm{CAMD}^t(z \mid \lambda)$. We also use *relativized* version of Kolmogorov complexities, allowing the universal machine to query an oracle set.

2.2. Symmetry of Information Properties. Denote by $\mathcal{C}^{\mathrm{p}oly}$ a version of polynomial time-bounded Kolmogorov complexity, which can be $\mathrm{C}^{\mathrm{p}oly}$, $\mathrm{CD}^{\mathrm{p}oly}$, $\mathrm{CND}^{\mathrm{p}oly}$, or $\mathrm{CAMD}^{\mathrm{p}oly}$. To formulate the problem of symmetry of information more precisely, we isolate three associated properties. The first is the *Easy Direction of Symmetry of Information*:

$$\begin{array}{l}\text{For any polynomial } p \text{ there exists a}\\ \text{polynomial } q \text{ such that for all } x, y:\\ \mathcal{C}^{q(n)}(x, y) \leq \mathcal{C}^{p(n)}(x) + \mathcal{C}^{p(n)}(y|x) + O(\log(n)),\\ \text{where } n = |x| + |y|.\end{array} \tag{EDSI}$$

It is easy to verify that (EDSI) holds for any of the above complexity measures. Next is the *Hard Direction of Symmetry of Information*:

$$\begin{array}{l}\text{For any polynomial } p \text{ there exists a}\\ \text{polynomial } q \text{ such that for all } x, y:\\ \mathcal{C}^{q(n)}(x) + \mathcal{C}^{q(n)}(y \mid x) \leq \mathcal{C}^{p(n)}(x, y) + O(\log(n)),\\ \text{where } n = |x| + |y|.\end{array} \tag{HDSI}$$

Finally we also consider the property of *Symmetry of Mutual Information*:

$$\begin{array}{l}\text{For any polynomial } p \text{ there exists a}\\ \text{polynomial } q \text{ such that for all } x, y:\\ \mathcal{C}^{q}(x) + \mathcal{C}^{q}(y \mid x) \leq \mathcal{C}^{p}(y) + \mathcal{C}^{p}(x \mid y) + O(\log n)\end{array} \tag{SMI}$$

Notice that if both (EDSI) and (HDSI) hold for a complexity measure $\mathcal{C}$, then also (SMI) holds for $\mathcal{C}$. The converse is not necessarily true.

2.3. Language Compression Theorems. A fundamental theorem of Kolmogorov complexity, and one that is very useful in applications, is the following:

THEOREM 2.7 (Language Compression Theorem). *For any recursively enumerable set A, and all $x \in A^{=n}$ we have* $\mathrm{C}(x) \leq \log \|A^{=n}\| + O(\log n)$.

This is as x can be described by its index in the enumeration of $A^{=n}$.

This theorem is essentially used in the proof of (HDSI) in the resource unbounded case given in (ZL70). Similarly, our results about resource bounded symmetry of information (both positive and negative) crucially rely on recent resource bounded language compression theorems. In (BLvM04) the following analogue of the Language Compression Theorem is shown for CND complexity.

THEOREM 2.8 (BLvM04). *There is a polynomial $p(n)$ such that for any set $A \subset \mathbb{B}^*$ and for all $x \in A^{=n}$ we have* $\mathrm{CND}^{p,A^{=n}}(x) \leq \log \|A^{=n}\| + O(\delta(n))$ *where* $\delta(n) = (\sqrt{\log \|A^{=n}\|} + \log(n)) \log(n)$.

Further (BLvM04) show that with the power of Arthur-Merlin protocols a Language Compression Theorem holds which is optimal up to an additive $\log^3 n$ term:

THEOREM 2.9 (BLvM04). *There is a polynomial $p(n)$ such that for any set $A \subset \mathbb{B}^*$ and for all $x \in A^{=n}$ we have* $\mathrm{CAMD}^{p,A^{=n}}(x) \leq \log \|A^{=n}\| + O(\log^3(n))$.

For comparison we remark that for CD complexity the situation is somewhat different. In (BFL02) it is shown that there is a polynomial $p(n)$ such that for any set A and for all $x \in A^{=n}$ it holds that $\mathrm{CD}^{p(n),A^{=n}}(x) \leq 2 \log \|A^{=n}\| + O(\log n)$. Furthermore, (BLM00) show that there is a set A where this bound is tight up to $O(\log n)$ terms. That is, the factor of 2 in general cannot be improved.

3. On CD complexity

In this section we show a relativized world where the inequalities (SMI) and, hence, (HDSI) fail in a strong way for CD^{poly} complexity. The proof of the next proposition follows the idea outlined in (BF95):

Proposition 3.1. *There exists an oracle A and a polynomial $p(n)$ satisfying the following condition. For any $\epsilon > 0$ and large enough n there exists a pair $\langle x, y\rangle \in \mathbb{B}^n \times \mathbb{B}^n$ such that*

- $\mathrm{CD}^{2^{\epsilon n}, A^{=2n}}(y) > (1-\epsilon)n - O(\log n)$,
- $\mathrm{CD}^{p(n), A^{=2n}}(x) = O(1)$,
- $\mathrm{CD}^{p(n), A^{=2n}}(y \,|\, x) = O(1)$ *and even* $\mathrm{C}^{p(n), A^{=2n}}(y \,|\, x) = O(1)$,

i.e., $\mathrm{CD}^{p(n),A^{=2n}}(x) + \mathrm{CD}^{p(n),A^{=2n}}(y \,|\, x) \ll \mathrm{CD}^{2^{\epsilon n},A^{=2n}}(y) + \mathrm{CD}^{2^{\epsilon n},A^{=2n}}(x \,|\, y)$. *Thus, (SMI) does not hold with the oracle A.*

Proof. Fix n and choose an incompressible pair $\langle x_n, y_n\rangle \in \mathbb{B}^n \times \mathbb{B}^n$. Define a mapping $f_n : \mathbb{B}^n \to \mathbb{B}^n$ as follows:

- $f_n(x_n) = y_n$,
- $f_n(z) = z$ for all $z \neq x_n$.

Now we define $A^{=2n}$. At first define two auxiliary oracles B_n and C_n: let B_n contain the graph of the function f_n (on input $\langle z, i\rangle$ the oracle B_n returns the i-th bit of $y = f_n(z)$) and C_n contain a single string x_n (on input $z \in \mathbb{B}^n$ the oracle C_n returns 1 if and only if $z = x_n$). A query to B_n consists of $(n + \log n)$ bits, and a query to C_n consists of n bits. So a query to $B_n \oplus C_n$ can be encoded as a strings of length $(n + \log n + 1)$, which is less than $2n$. Thus, we may set $A^{=2n} = B_n \oplus C_n$.

Obviously, for some polynomial $p(n)$ we have $\mathrm{CD}^{p(n),A^{=2n}}(x_n) = O(1)$ (it is enough to query C_n to distinguish x from other stings) and $\mathrm{C}^{p(n),A^{=2n}}(y_n|x_n) = O(1)$ (it is enough to query from B_n the value $f_n(x_n)$).

On the other hand, $\mathrm{CD}^{2^{\epsilon n},A^{=2n}}(y_n) \geq (1-\epsilon)n - O(\log n)$. Really, let s be a shortest $\mathrm{CD}^{2^{\epsilon n}}$ program for y, and assume

$$|s| \leq (1-\epsilon)n - D\log n$$

for a large enough constant D. If this program queries at some step $t \leq 2^{\epsilon n}$ the point x_n from the oracle C_n or any point $\langle x_n, i\rangle$ from the oracle B_n, then

$$\mathrm{C}(x_n \,|\, y_n) \leq |s| + \log t + O(\log n),$$

and

$$\mathrm{C}(x_n, y_n) \leq |y_n| + |s| + \log t + O(\log n) < 2n.$$

We get a contradiction, as the pair $\langle x_n, y_n\rangle$ is incompressible. Hence, s does not query any 'interesting' points from the oracle. Thus, it can work with a trivial oracle $B'_n \oplus C'_n$ (B'_n returns the i-th bit of z for *any* pair $\langle z, i\rangle$, and C'_n returns 0 for *any* string z). This means that

$$\mathrm{C}(y_n) \leq |s| + O(1) \ll n,$$

and we again get a contradiction. So, we have $|s| \geq (1-\epsilon)n - O(\log n)$. □

4. On CND complexity

In this section we prove that (HDSI) and (SMI) are not true for a relativized version of polynomial time bounded CND complexity. Our proof is based on the Language Compression Theorem for CND complexity, Theorem Theorem 2.8.

Theorem 4.1. *Let $m = m(n), s = s(n), t = t(n)$ be functions such that*

$$2^{s(n)} + 2^{m(n)} < 2^n$$

and

$$t(n)2^{m(n)} \leq 2^{n-3}.$$

Then there is a polynomial $p(n)$, and sets A, X such that

- ○ $X^{=n} \subset \mathbb{B}^n$, $\|X^{=n}\| = 2^{s(n)}$,
- ○ $A^{=2n} \subset \mathbb{B}^n \times \mathbb{B}^n$,
- ○ $\|\{y \ : \ (x,y) \in A^{=2n}\}\| \geq 7/8 \cdot 2^n$ *for any* $x \in X^{=n}$,
- ○ $\| \bigcup_{x \notin X} \{y \ : \ (x,y) \in A^{=2n}\}\| \leq 1/8 \cdot 2^n$,

and for large enough n, for all $x \in X^{=n}$, for at least $3/4 \cdot 2^n$ strings $y \in \mathbb{B}^n$ the following conditions hold: $\langle x, y\rangle \in A^{=2n}$,

$$\begin{array}{lcl} \mathrm{CND}^{p,A^{=2n}}(x \,|\, y) & \leq & s(n) + O(\delta(n)), \\ \mathrm{CND}^{t(n),A^{=2n}}(x) & \geq & m(n) - O(1), \\ \mathrm{CND}^{t(n),A^{=2n}}(y \,|\, x) & \geq & n - O(1), \end{array}$$

where $\delta(n) = \sqrt{n}\log(n)$.

Note that the term $\delta(n) = \sqrt{n}\log(n)$ comes from Theorem Theorem 2.8.

Corollary 4.2. *There exists an oracle A such that a* $\mathrm{CND}^{\mathrm{poly}}$ *version of (HDSI) and (SMI) do not hold. Moreover, for any $\varepsilon \in (0,1)$ there exists a polynomial p such that for any polynomial q for large enough n*

$$(2-\varepsilon)\mathrm{CND}^{p,A^{=2n}}(x,y) < \mathrm{CND}^{q,A^{=2n}}(x) + \mathrm{CND}^{q,A^{=2n}}(y\,|\,x)$$

and

$$\mathrm{CND}^{p,A^{=2n}}(y) + \mathrm{CND}^{p,A^{=2n}}(x\,|\,y) \ll \mathrm{CND}^{q,A^{=2n}}(x) + \mathrm{CND}^{q,A^{=2n}}(y\,|\,x)$$

for most $\langle x,y\rangle \in A^{=2n}$.

Proof. It follows from Theorem Theorem 4.1 for $s(n) = \varepsilon n/3$, $m(n) = (1-\varepsilon/3)n$, $t(n) = 2^{\varepsilon n/6}$. □

The bound $(2-\varepsilon)$ in the first inequality of Corollary Corollary 4.2 is tight. This can be easily seen as,

$$\mathrm{CND}^{\mathrm{poly},A^{=2n}}(x,y) \geq \mathrm{CND}^{\mathrm{poly},A^{=2n}}(x) - O(1)$$

and

$$\mathrm{CND}^{\mathrm{poly},A^{=2n}}(x,y) \geq \mathrm{CND}^{\mathrm{poly},A^{=2n}}(y\,|\,x) - O(1).$$

Hence for any oracle A

$$2\mathrm{CND}^{p,A^{=2n}}(x,y) \geq \mathrm{CND}^{q,A^{=2n}}(x) + \mathrm{CND}^{q,A^{=2n}}(y\,|\,x) - O(1).$$

Proof. (Theorem Theorem 4.1) Fix an integer $n > 0$. We denote by F the characteristic function of $A^{=2n}$, i.e., $F(\langle x,y\rangle) = 1$ if $\langle x,y\rangle \in A^{=2n}$ and $F(x,y) = 0$ otherwise. We define this function in a few stages: construct a sequence of functions $F_0, F_1, \dots, F_{2^{m(n)}-1}$,

$$F_i : \mathbb{B}^n \times \mathbb{B}^n \to \{0, 1, \mathrm{undef}\}.$$

For $i < j$ the function F_j should be an extension of F_i, i.e.,

$$\forall \langle a,b\rangle \text{ if } F_i(a,b) \neq \mathrm{undef} \text{ then } F_j(a,b) = F_i(a,b).$$

The initial function is trivial: $F_0(a,b) = \mathrm{undef}$ for all $\langle a,b\rangle$. In the sequel we shall define F as an extension of $F_{2^{m(n)}-1}$.

Let us introduce some notation. We say that a set $B \subset \mathbb{B}^n \times \mathbb{B}^n$ *respects* a function F_i if

$$\begin{cases} F_i(a,b) = 1 & \Rightarrow \quad \langle a,b\rangle \in B, \\ F_i(a,b) = 0 & \Rightarrow \quad \langle a,b\rangle \notin B. \end{cases}$$

Let $s_1, \dots, s_{2^{m(n)}-1}$ be the list of all CND-programs of length less than $m(n)$. We suppose each program s_j can access an oracle O (the oracle is not fixed in advance). Also we suppose that each s_j is clocked and runs at most $t(n)$ steps. We say that s_j is a *well defined* CND program for an oracle O if s_j^O accepts exactly one string x.

Further define F_i by induction. Let the functions $F_0, \dots, F_{k-1}$ be already defined. We must construct a function F_k which is an extension of F_{k-1}. Consider the program s_k. There are two possibilities:

1. for any $B \subset \mathbb{B}^n \times \mathbb{B}^n$ that respects F_{k-1}, the program s_k is not well defined for the oracle B;

2. there exists at least one set $B \subset \mathbb{B}^n \times \mathbb{B}^n$ that respects F_{k-1}, and the program s_k is well defined for the oracle B.

The first case is trivial: we set $F_k(x, y) = F_{k-1}(x, y)$ for all $\langle x, y\rangle$. In the second case there exists a set B and a string x such that s_k^B accepts x in time $T(B, x)$, which is at most $t(n)$, and rejects all other strings. If there is more than one such set, we choose a set B with the minimal possible $T(B, x)$. Denote by x_k the fixed string x. Let the list of all queries of the program $s_k^B(x_k)$ to the oracle (for one of the shortest path, i.e., for an accepting path of length $T(B, x)$) be

$$\langle a_0, b_0\rangle, \langle a_1, b_1\rangle, \dots, \langle a_r, b_r\rangle,$$

$r < t(n)$. We include all these pairs in the oracle. More precisely, define F_k as follows:

$$\begin{array}{lcll} F_k(a,b) & = & F_{k-1}(a,b) & \text{if } F_{k-1}(a,b) \neq \text{undef}, \\ F_k(a_j,b_j) & = & 1 & \text{if } \langle a_j, b_j\rangle \in B,\ j = 0, \dots, r, \\ F_k(a_j,b_j) & = & 0 & \text{if } \langle a_j, b_j\rangle \notin B,\ j = 0, \dots, r, \\ F_k(a,b) & = & \text{undef} & \text{if } F_{k-1}(a,b) = \text{undef and } \langle a, b\rangle \neq \langle a_j, b_j\rangle,\ \forall j. \end{array}$$

For any set R that respects F_k, the program s_k^R accepts the string x_k in time $T(B, x)$. Note that for a time bound $t_0 \geq T(B, x)$ the CND program s_k^R may accept also a few other strings except x_k. But for any $t_0 < T(B, x)$ the program s_k^R does not accept in time t_0 any string, because we chose x_k that provides minimum to the value $T(B, x)$. Thus, if for a time bound $t_0 \leq t(n)$ the program s_k^R accepts at least one string, it must accept also x_k. In other words, it cannot *distinguish* any string except x_k.

We have described an inductive procedure, which defines the functions $F_0, \dots, F_{2^{m(n)}-1}$. At each step i we set $F_i(a, b) \neq F_{i-1}(a, b)$ for at most $t(n)$

values $\langle a, b\rangle$. Hence the function $F_{2^{m(n)}-1}$ is equal to undef for all values in $\mathbb{B}^n \times \mathbb{B}^n$ except for at most $t(n)2^{m(n)}$ values.

Besides we get the list L of strings x_i which can be possibly accepted by distinguishing programs s_i^R if a set R respects $F_{2^{m(n)}-1}$. This set is rather small: $\|L\| < 2^{m(n)}$.

Further we choose an arbitrary set

$$X^{=n} \subset \mathbb{B}^n \setminus L$$

of size $2^{s(n)}$. Now define the function F as follows:

$$\begin{array}{lcll} F(x,y) & = & F_{2^{m(n)}-1}(x,y) & \text{if } F_{2^{m(n)}-1}(x,y) \neq \text{undef}, \\ F(x,y) & = & 1 & \text{if } F_{2^{m(n)}-1}(x,y) = \text{undef and } x \in X, \\ F(x,y) & = & 0 & \text{if } F_{2^{m(n)}-1}(x,y) = \text{undef and } x \notin X. \end{array}$$

The characteristic function F defines the oracle $A^{=2n}$ and the construction is finished. Note that for any $x \in X^{=n}$

$$\|\{y \ : \ (x,y) \in A^{=2n}\}\| \geq 7/8 \cdot 2^n,$$

and

$$\| \bigcup_{x \notin X^{=n}} \{y \ : \ (x,y) \in A^{=2n}\}\| < 1/8 \cdot 2^n.$$

Now fix any string $x_0 \in X$. Obviously, $\mathrm{CND}^{t(n),A^{=2n}}(x_0) \geq m(n)$ because $x_0 \notin L$. Further, there are at least

$$2^n - 2^{m(n)}t(n) - 2^{n-3} > 3/4 \cdot 2^n$$

strings y such that

- ○ $(x_0, y) \in A^{=2n}$,
- ○ $(x, y) \notin A^{=2n}$ for any $x \notin X^{=n}$, and
- ○ $\mathrm{C}^{A^{=2n}}(y \,|\, x_0) \geq n - 3$.

Denote by y_0 any of these strings. From the conditions above it follows that

- ○ $\mathrm{CND}^{t(n),A^{=2n}}(y_0 \,|\, x_0) > n - O(1)$ since resource bounded complexity is not less than plain complexity;
- ○ $\mathrm{CND}^{p(n),A^{=2n}}(x_0 \,|\, y_0) \leq \log \|\{x \ : (x, y_0) \in A^{=2n}\}\| + O(\delta(n)) \leq s(n) + O(\delta(n))$ from Theorem Theorem 2.8.

□

5. On CAMD complexity

In this section we study symmetry of information under the CAMD complexity measure. In contrast to the case of CD and CND complexity, with the power of nondeterminism and randomness we can prove some positive results, showing that some weaker versions of (HDSI) hold for CAMD.

Our proof will follow the proof in the resource unbounded case as given in (ZL70). We first review this proof to see how it can be used in our case. Let α, β be two strings such that $|\alpha| + |\beta| = n$, and suppose that $\mathrm{C}(\alpha, \beta) = m$. We define the set $A_{x,m} = \{y : \mathrm{C}(x, y) \leq m\}$. Notice that $\|A_{x,m}\| \leq 2^{m+1}$ and that given x and m the set $A_{x,m}$ is recursively enumerable. Thus as $\beta \in A_{\alpha,m}$ by the Language Compression Theorem (Theorem Theorem 2.7), $\mathrm{C}(\beta \,|\, \alpha) \leq \log \|A_{\alpha,m}\| + O(\log n)$. Let k^* be such that $2^{k^*} \leq \|A_{\alpha,m}\| < 2^{k^*+1}$. Then the above says that $\mathrm{C}(\beta \,|\, \alpha) \leq k^* + O(\log n)$.

Now consider the set $B_{m,k} = \{x : \|A_{x,m}\| \geq 2^k\}$. Notice that the size of $B_{m,k}$ is less than 2^{m-k+1}, and that $\alpha \in B_{m,k^*}$. The set $B_{m,k}$ is recursively enumerable given m, k, thus by the Language Compression Theorem, $\mathrm{C}(\alpha) \leq m - k^* + O(\log n)$. And so

$$\begin{aligned} \mathrm{C}(\alpha) + \mathrm{C}(\beta \,|\, \alpha) &\leq m - k^* + k^* + O(\log n) \\ &\leq \mathrm{C}(\alpha, \beta) + O(\log n) \end{aligned}$$

If we substitute polynomial time printing complexity in the above argument, then the set $A_{x,m}$ is in NP. Further, by the approximate lower bound counting property of AM (Bab85) there is an AM algorithm which accepts with high probability for $x \in B_{m,k}$ and rejects with high probability for $x \notin B_{m,k-1}$. We have, however, no guarantee on the algorithm's behavior for $x \in B_{m,k-1}$. In the next theorem, we extend the language compression results of (BLvM04) to work for AM 'gap' sets of this type, allowing the above argument to go through. This result also implies near optimal AM compression of polynomial time samplable sources, recently studied in (TVZ04).

5.1. AM compression of AM gap sets.

LEMMA 5.1. *Let $A \subseteq \mathbb{B}^*$. Suppose there is a polynomial time bound $q(n)$, and predicate Q such that*

- *for all $u \in A^{=n}, \Pr_{r \in \mathbb{B}^{q(n)}}[\exists v\; Q(u, v, r) = 1] \geq 2/3$*
- $\|\{u \in \mathbb{B}^n : \Pr_{r \in \mathbb{B}^{q(n)}}[\exists v\; Q(u, v, r) = 1] > 1/3\}\| \leq 2^k$,

and for all u, v, r the predicate $Q(u, v, r)$ can be computed in polynomial time. Then there is a polynomial time bound $p(n)$ such that for all $u \in A^{=n}$, we have $\mathrm{CAMD}^p(u) \le k + O(\log^3 n)$.

Before going into the proof of Lemma Lemma 5.1, we briefly recall the technique of (BLvM04). Let $\mathrm{TR} : \mathbb{B}^n \times \mathbb{B}^d \to \mathbb{B}^m$ be the function underlying Trevisan's extractor (Tre01), that is the composition of a good error correcting code with the Nisan-Wigderson generator (NW94). The output of $\mathrm{TR}(u, e)$ is the evaluation of the Nisan-Wigderson generator on seed e when using $\hat{u}$ as the 'hard' function supplied to the generator, where $\hat{u}$ is the image of u under an error correcting code. The key property of this function, what makes it a good extractor and compressor, is that if $\mathrm{TR}(u, e)$ is not close to uniform over choice of $e \in \mathbb{B}^d$ on some set $B \subset \mathbb{B}^m$, then u has a short description given oracle access to B. In (BLvM04) it is shown that u can be printed in polynomial time from this description and oracle access to B. This construction works for $d = O(\log^3 n)$, where this term arises from the *weak design* construction of (RRV02).

To give the elements of a set $A \subset \mathbb{B}^n$ short descriptions, we let the set B be the image of $A \times \mathbb{B}^d$ under the function TR. That is, $B = \cup_{x \in A} \cup_{e \in \mathbb{B}^d} \mathrm{TR}(x, e)$. Notice that for any $x \in A$, $\Pr_e[\mathrm{TR}(x, e) \in B] = 1$. On the other hand if we take m to be $\log \|A\| + d + 1$ then the probability that a uniformly chosen $y \in \mathbb{B}^m$ is in B is less than $1/2$. Thus all the elements of A have a short description relative to B. Now notice that with nondeterminism and an oracle for A, we can decide membership in B, thus all the elements of A have a short CND^A description. The elements of A can be given an even more succinct CAMD^A description by using the randomness in the AM protocol to simulate part of the probabilistic argument in (NW94; Tre01).

Proof. (Lemma Lemma 5.1) By amplification and the results of (FGM$^+$89), we can transform the predicate Q into a predicate Q' taking random strings of length a polynomial $q'(n)$ and with the property

- if $u \in A^{=n}$ then $\Pr_r[\exists v\ Q'(u, v, r) = 1] = 1$
- $\|\{u : \Pr_r[\exists v\ Q'(u, v, r) = 1] \ge 2^{-n-2}\}\| \le 2^k$

for r chosen uniformly over $\mathbb{B}^{q'(n)}$. Let $L = \{u : \Pr_r[\exists v\ Q'(u, v, r) = 1] \ge 2^{-n-2}\}$.

For each $r \in \mathbb{B}^{q'(n)}$ we define a set

$$B_r = \{w\ :\ \exists u \in \mathbb{B}^n, \exists v, e\ \mathrm{TR}(u, e) = w \wedge Q'(u, v, r) = 1\}$$

In the sequel we denote by $B_r(w)$ the property $w \in B_r$.

Clearly if $u \in A^{=n}$, then $\Pr_e[B_r(\mathrm{TR}(u,e))] = 1$, for any $r \in \mathbb{B}^{q'(n)}$. Now for a randomly chosen $w \in \mathbb{B}^m$ and randomly chosen $r \in \mathbb{B}^{q'(n)}$, we calculate the probability that $w \in B_r$. As for a 0/1 variable the probability of being 1 is equal to the expectation of the variable, we have

$$\Pr_{r,w}[w \in B_r] = E_{r,w}[B_r(w)].$$

By linearity of expectation, we can divide the latter into two contributions, that from elements w for which $\exists u \in L$ and seed e such that $\mathrm{TR}(u,e) = w$, and those w for which this is not the case.

$$E_{r,w}[B_r(w)] = \sum_{\substack{w=\mathrm{TR}(u,e)\\ u \in L'}} E[B_r(w)] + \sum_{\substack{w \neq \mathrm{TR}(u,e)\\ u \in L'}} E[B_r(w)]$$

By taking $m = k + d + 2$ the first term can be bounded by $1/4$. The second term is bounded by $2^m 2^{-n-2} \leq 1/4$. Going back to probability notation, we have for any $u \in A^{=n}$

$$\Pr_{r,e}[B_r(\mathrm{TR}(u,e))] - \Pr_{r,w}[B_r(w)] \geq 1/2.$$

The value of Trevisan's function $\mathrm{TR}(u,e)$ can be viewed as a sequence of bits

$$\hat{u}_1(e) \ldots \hat{u}_m(e),$$

where $\hat{u}_i = \hat{u}(e|_{S_i})$, i.e., the result of application of the boolean function $\hat{u}$ to the i-th set of the *weak design set system* (for details see (RRV02) or (BLvM04)). Thus, $\hat{u}_i$ depends on $\|S_i\|$ variables. By definition of a weak design the cardinalities of S_i for all i are equal to each other. Denote $\bar{n} = 2^{\|S_i\|}$. We choose a weak design system as in the proof of AM language compression in (BLvM04, Theorem 3). For this weak design $\bar{n}$ is polynomial in n.

It follows by the hybrid argument that there is an $i \in [m]$ and a setting of the bits of e outside of the set S_i such that

(5.2)
$$\Pr_{x,r,r'}[B_r(\hat{u}_1(x) \ldots \hat{u}_{i-1}(x)\hat{u}_i(x)r'] - \Pr_{x,r,r',b}[B_r(\hat{u}_1(x) \ldots \hat{u}_{i-1}(x)br')] \geq 1/2m.$$

When the bits of e outside of S_i are fixed, all the functions $\hat{u}_i$ only depend on the bits inside of S_i, thus the variable x in the above ranges uniformly over $\|S_i\|$ bit strings.

Let $F(x,b,r') = \hat{u}_1(x) \ldots \hat{u}_{i-1}(x)br'$. Our algorithm to approximate $\hat{u}_i$ will do the following: on input x, choose uniformly at random b, r, r' and evaluate

$B_r(F(x,b,r'))$; if this evaluates to 1, then output b, otherwise output $1-b$. Call the output of this algorithm $g_b(e,r,r')$. We now estimate the probability that $g_b(e,r,r')$ agrees with $u_i(x)$.

$$\begin{aligned}
\Pr_{x,r,r',b}[g_b(x,r,r') = \hat{u}(x)] &= \Pr_{x,r,r',b}[g_b(x,r,r') = \hat{u}(x) | b = \hat{u}(x)] \Pr_{x,b}[b = \hat{u}(x)] \\
&+ \Pr_{x,r,r',b}[g_b(x,r,r') = \hat{u}(x) | b \neq \hat{u}(x)] \Pr_{x,b}[b \neq \hat{u}(x)] \\
&= \frac{1}{2} \Pr_{x,r,r',b}[B_r(F(x,b,r')) = 1 | b = \hat{u}(x)] \\
&+ \frac{1}{2} \Pr_{x,r,r',b}[B_r(F(x,b,r')) = 0 | b \neq \hat{u}(x)] \\
&= \frac{1}{2} + \frac{1}{2}\Bigg(\Pr_{x,r,r',b}[B_r(F(x,b,r')) = 1 | b = \hat{u}(x)] \\
&- \Pr_{x,r,r',b}[B_r(F(x,b,r')) = 1 | b \neq \hat{u}(x)] \Bigg) \\
&= \frac{1}{2} + \frac{1}{2}\Bigg(\Pr_{x,r,r'}[B_r(F(x,\hat{u}(x),r')) = 1] \\
&- \Pr_{x,r,r'}[B_r(F(x,1-\hat{u}(x),r')) = 1] \Bigg) \\
&= \frac{1}{2} + \Pr_{x,r,r',b}[B_r(F(x,\hat{u}(x),r')) = 1] \\
&- \Pr_{x,r,r',b}[B_r(F(x,b,r')) = 1] \\
&\geq \frac{1}{2} + \frac{1}{2m}
\end{aligned}$$

The last line follows from Equation ((5.2)). We fix the bit b to a value b_1 which preserves this prediction advantage. Notice that $g_{b_1}(x,r,r')$ cannot be computed by Arthur himself, as he needs Merlin to demonstrate witnesses for acceptance in B_r. We now show how the computation of $g_{b_1}(x,r,r')$ can be simulated by an Arthur-Merlin protocol.

We say that (r,r') gives an α-approximation to $\hat{u}$ if $\Pr_x[g_{b_1}(x,r,r') = \hat{u}(x)] \geq \alpha$. For fixed (r,r'), we identify $g_{b_1}(x,r,r')$ with the string $z_{b_1,r,r'}$ where $z_{b_1,r,r'}$ has bit b_1 in position x if and only if $g_{b_1}(x,r,r') = 1$. For convenience we assume without loss of generality that $b_1 = 1$ and drop the subscript. Note that with this choice the number of ones in z_r is the number of strings x for which B accepts $\hat{u}_1(x)\cdots\hat{u}_{i-1}(x)b_1r$. With $w(z)$ we denote the number of ones in a string z.

Arthur randomly selects strings $r_1,\ldots,r_s \in \{0,1\}^{q'(n)}$ and $r'_1,\ldots,r'_s \in$

$\{0,1\}^{m-i}$, and asks Merlin to provide witnesses for $B_{r_i}(F(x, b_1, r'_i))$. Included as part of our description will be the average number of acceptances over all choices of r, r': $\bar{a} = 2^{-q'(n)} 2^{i-m} \sum_{x,r,r'} g_{b_1}(x, r, r')$. To limit Merlin's freedom in choosing which acceptances to demonstrate in an adverse way, we want that the total number of acceptances of the choice of $r_1, \ldots, r_s$ and $r'_1, \ldots, r'_s$ is close to the expected $s \cdot \bar{a}$. This is insured by an easy Chernoff bound argument:

Claim 5.3. *For any $\gamma = \gamma(m, \bar{n}) > 0$, there exists $s = O(\bar{n}^2/\gamma^2)$ such that with probability at least $3/4$ over Arthur's choice of $(r_1, r'_1), \ldots, (r_s, r'_s)$ the following two things will simultaneously happen:*

(i) A $1/8m$ fraction of $(r_1, r'_1), \ldots, (r_s, r'_s)$ will give $\frac{1}{2} + \frac{1}{4m}$ approximations to $\hat{u}$.

(ii) The total number of acceptances by B over the strings $(r_1, r'_1), \ldots, (r_s, r'_s)$ will be within γs of the expected. That is,

$$|\sum_{j=1}^{s} w(z_j) - s\bar{a}| \leq \gamma s.$$

Proof. To lower bound the probability that both of these events happen, we upper bound the probability that each event individually does not happen and use a union bound.
Item (1): Notice that for a given (r, r'), if

$$\Pr_x[B_r(\hat{u}_1(x) \cdots \hat{u}_{i-1}(x)\hat{u}(x)r')] - \Pr_x[B_r(\hat{u}_1(x) \cdots \hat{u}_{i-1}(x)b_1 r')] \geq 1/4m$$

then (r, r') gives a $(\frac{1}{2} + \frac{1}{4m})$-approximation of $\hat{u}$. We will say that the pair (r, r') is bad if it does not yield a $\frac{1}{2} + \frac{1}{4m}$ approximation to $\hat{u}$. By Equation ((5.2)) and Markov's inequality,

$$\Pr_{r,r'}[(r, r') \in \text{bad}] \leq \frac{1 - 1/2m}{1 - 1/4m} < 1 - 1/4m.$$

By a Chernoff bound, for some constant $c_1 > 0$,

$$\Pr_{(r_1,r'_1),\ldots,(r_s,r'_s)}[\|\text{bad}\| \geq (1 - 1/8m)s] \leq \exp(-c_1 s/m^2).$$

Item (2): By a Chernoff bound, for some constant $c_2 > 0$,

$$\Pr[|1/s \sum_{j=1}^{s} w(z_j) - \bar{a}| \geq \gamma] \leq 2\exp(-c_2 \gamma^2 s/\bar{n}^2).$$

By taking $s = c_3\bar{n}^2/\gamma^2$ for a sufficiently large constant c_3, the probability of each item will be less than 1/8, and the claim follows. □

From this point the proof follows verbatim as in the proof of AM language compression (BLvM04, Theorem 3). □

One application of this lemma is for the AM compression of samplable sources. The study of the compression of samplable sources is introduced in (TVZ04). They give evidence that it is unlikely that all polynomial time samplable sources can be (near) optimally compressed by probabilistic polynomial time algorithms. We show, by contrast, that with AM algorithms, and when we only consider decompression efficiency, we can achieve nearly optimal compression.

Definition 5.4. *Let X_n be a probability distribution on strings of length n. We say that X_n is polynomial time samplable if there is a polynomial $p(n)$ and algorithm S such that*

$$\Pr_{r\in\{0,1\}^{p(n)}}[S(1^n, r) = x] = \Pr[X_n = x]$$

for every $x \in \{0,1\}^n$, and where the running time of $S(1^n, r)$ is bounded by $p(n)$.

Theorem 5.5. *Let X_n be a polynomial time sampable source. There is a polynomial $p(n)$ such that for every x in the support of X_n,*

$$\mathrm{CAMD}^{p(n)}(x) \leq -\log \Pr[X_n = x] + O(\log^3 n).$$

Proof. Consider the set $L_k = \{x : \Pr[X_n = x] \geq 2^{-k}\}$. As the source X_n is samplable, say by an algorithm S, the set $\{r : S(1^n, r) = x\}$ is in P. Thus by the approximate lower bound counting property of AM (Bab85), there is an AM algorithm which accepts any $x \in L_k$ with probability greater than 2/3, and rejects any element x not in L_{k-1} with probability greater than 2/3. Thus the total number of strings x which will be accepted by the AM lower bound counting algorithm will be less than the number of strings which receive probability more than 2^{-k-1} which is less than 2^{k+1}. Now applying Lemma Lemma 5.1 we obtain that there exists a polynomial p such that $\mathrm{CAMD}^p(x) \leq k + O(\log^3 n)$ for all $x \in L_k$. □

Finally, we remark that these results relativize.

5.2. Application to symmetry of information.

THEOREM 5.6. *There is a polynomial $p(n)$ such that for any set $A \subset \mathbb{B}^* \times \mathbb{B}^*$ and all $\langle x, y\rangle \in A^{=n}$*

$$\log \|A^{=n}\| \geq \mathrm{CAMD}^{p,A^{=n}}(x) + \mathrm{CAMD}^{p,A^{=n}}(y \mid x) - O(\log^3 n).$$

Furthermore, if $A \in \mathrm{NP}$ then there is a polynomial $q(n)$ such that

$$\log \|A^{=n}\| \geq \mathrm{CAMD}^{q}(x) + \mathrm{CAMD}^{q}(y \mid x) - O(\log^3 n).$$

PROOF. Fix n and $\langle \alpha, \beta\rangle \in A^{=n}$. Denote $m = \log \|A^{=n}\|$ and $A_x = \{y : (x, y) \in A^{=n}\}$. Membership in the set A_x can be decided in polynomial time given x and the oracle $A^{=n}$. As $\beta \in A_\alpha$ it follows from Theorem Theorem 2.9 that $\mathrm{CAMD}^{q,A^{=n}}(\beta \mid \alpha) \leq \log \|A_\alpha\| + O(\log^3 n)$.

Now consider the set $B_k = \{x : \|A_x\| \geq 2^k\}$. Let k^* be such that $2^{k^*} \leq \|A_\alpha\| < 2^{k^*+1}$. Then $\alpha \in B_{k^*}$. By the approximate lower bound counting property of AM (Bab85), there is a predicate Q (computable in polynomial time given the oracle $A^{=n}$) such that

- ◦ If $x \in B_k$ then $\Pr_r[\exists y Q(x, y, r) = 1] \geq 2/3$
- ◦ If $x \notin B_{k-1}$ then $\Pr_r[\exists y Q(x, y, r) = 1] \leq 1/3$

Thus if $\Pr_r[\exists y\ Q(x, y, r) = 1] > 1/3$ then $x \in B_{k-1}$. However $\|A^{=n}\| = 2^m$ implies that $\|B_{k-1}\| \leq 2^{m-k+1}$. Now by Theorem Theorem 2.9 we obtain $\mathrm{CAMD}^{q,A^{=n}}(\alpha) \leq m - k^* + O(\log^3 n)$.

Putting the above together we have

$$\mathrm{CAMD}^{q,A^{=n}}(\alpha) + \mathrm{CAMD}^{q,A^{=n}}(\beta|\alpha) \leq m - k^* + k^* + O(\log^3 n) \leq m + O(\log^3 n)$$

which gives the first statement of the theorem.

To prove the "furthermore", note that approximate lower bound counting of NP sets can be done in AM (Bab85), and apply Lemma Lemma 5.1 to give the bound on (unrelativized) CAMD complexity of NP sets. □

COROLLARY 5.7. *For any set $A \subset \mathbb{B}^* \times \mathbb{B}^*$ and any polynomial $p(n)$ there is a polynomial q such that for all but at most a $1/n$ fraction of $\langle x, y\rangle \in A^{=n}$,*

$$\mathrm{CAMD}^{p(n),A^{=n}}(x,y) \geq \mathrm{CAMD}^{q(n),A^{=n}}(x) + \mathrm{CAMD}^{q(n),A^{=n}}(y \,|\, x) - O(\log^3 n).$$

Furthermore, if $A \in \mathrm{NP}$ then

$$\mathrm{CAMD}^{p(n)}(x,y) \geq \mathrm{CAMD}^{q(n)}(x) + \mathrm{CAMD}^{q(n)}(y \,|\, x) - O(\log^3 n).$$

PROOF. For all but at most a $1/n$ fraction of $\langle x, y\rangle \in A^{=n}$ we have

$$\mathrm{CAMD}^{p(n),A^{=n}}(x,y) \geq \log \|A^{=n}\| - O(\log n).$$

Applying Theorem Theorem 5.6 we get the first statement of the corollary. Applying the "furthermore" of Theorem Theorem 5.6 gives the furthermore here. □

THEOREM 5.8. *For any strings $x, y \in \mathbb{B}^n$, and polynomial $p(n)$ there is a polynomial $q(n)$ such that $\mathrm{C}^p(x,y) \geq \mathrm{CAMD}^q(x) + \mathrm{CAMD}^q(y \,|\, x) - O(\log^3 n)$.*

PROOF. Fix a pair of strings $\langle \alpha, \beta\rangle$. Let $n = |\alpha| + |\beta|$, and suppose that $\mathrm{C}^p(\alpha, \beta) = m$. Consider the set $A = \{\langle x, y\rangle : C^p(x,y) \leq m\}$. As membership in A can be decided in nondeterministic polynomial time, we may invoke the "furthermore" of Theorem Theorem 5.6 to give $\log \|A\| \geq \mathrm{CAMD}^q(\alpha) + \mathrm{CAMD}^q(\beta \,|\, \alpha) - O(\log^3 n)$ for some polynomial q. On the other hand, $\|A\| \leq 2^{m+1}$, and the theorem is proven. □

From Theorem Theorem 5.8 we obtain as a corollary a result of (LW95), up to an additive $O(\log^3(n))$ factor: if $\mathrm{P} = \mathrm{NP}$ then

$$\mathrm{C}^p(x,y) \geq \mathrm{C}^q(x) + \mathrm{C}^q(y \,|\, x) - O(\log^3 n).$$

More generally, the following corollary holds.

COROLLARY 5.9. *Suppose that for any polynomial $p = p(n)$ there is a polynomial $q = q(n)$ such that for any x, y, $\mathrm{C}^q(x \,|\, y) \leq \mathrm{CAMD}^p(x \,|\, y) + O(\log^3 n)$. Then (HDSI) holds for polynomial time printing complexity, up to an $O(\log^3 n)$ additive factor.*

6. What Implies Symmetry of Information?

Is there an assumption weaker than P=NP which would imply symmetry of information? Corollary Corollary 5.9 shows that symmetry of information (up to a $\log^3 n$ factor) follows from the assumption:

$$\begin{array}{l}\text{For any polynomial } p \text{ there exists a}\\ \text{polynomial } q \text{ such that for all } x, y:\\ \mathrm{C}^q(x \mid y) \leq \mathrm{CAMD}^p(x \mid y) + O(\log(n)),\\ \text{where } n = |x| + |y|.\end{array} \qquad (*)$$

It is easily seen that this property follows from P = NP. We now see that it is in fact equivalent to P = NP.

Theorem 6.1. *Property* $(*)$ *implies* P = NP.

We first prove the following lemma.

Lemma 6.2. *Suppose the following hold:*

- ○ NP $\subseteq$ BPP
- ○ *For every polynomial* q *there exists a polynomial* p *such that for all* x, $\mathrm{C}^p(x) \leq \mathrm{CBP}^q(x) + O(\log |x|)$.

Then P = NP.

Proof. By the results of Ko (Ko82), the first item implies PH $\subseteq$ BPP and NP = RP. Thus to show P=NP it suffices to derandomize RP. Let $L \in$ RP witnessed by a machine M running in polynimial time and using $m = m(n)$ random bits on an input x of length n. We shall assume that $m > n$.

By standard amplification we transform M into a polynomial machine M', which uses $m(n)^3$ random bits and for which the probability that $M'(x, r)$ rejects when $x \in L$ is less than 2^{-m^2}. As the set of random strings $r \in \mathbb{B}^{m^3}$ which give the 'wrong' answer is in P given x, we can apply the Language Compression Theorem for nondeterministic complexity to give that for a polynomial time bound q', $\mathrm{CND}^{q'}(r \mid x) \leq |r| - m^2 + O(\delta(m))$, for any such 'bad' r, where $\delta(m) = \sqrt{m} \log m$ as in Theorem Theorem 2.8. In particular, this means that if $\mathrm{CND}^{q'}(r) = |r| = m^3$ then $M'(x, r)$ must accept.

We now claim that for a given length n we can construct a string of length $m' = (m(n))^3$ with high $\mathrm{CND}^{q'}$ complexity in the polynomial hierarchy. Indeed, checking that a string has maximal CND complexity can be done with a Σ_2^p

oracle. Thus the lexicographically first string of length m' with maximal CND complexity, call it r^*, can be found with a Σ_3^p oracle by doing a prefix search. This means that $\mathrm{C}^{q',\Sigma_3^p}(r^*) = O(\log n)$. As the hypothesis of the theorem implies PH $\subseteq$ BPP, and following the proof that $\mathrm{BPP}^{\mathrm{BPP}} = \mathrm{BPP}$, we obtain $\mathrm{CBP}^{q''}(r^*) = O(\log n)$. Finally applying the second hypothesis of the theorem we have $\mathrm{C}^p(r^*) = O(\log n)$.

Thus to decide if $x \in L$ we evaluate $M'(x, U(p))$ for all programs p of length $d \log n$ for some constant d. We reject if and only if M' rejects on all these computations. U will output r^* for one of these programs p and by the above argument, if $x \in L$ then $M'(x, r^*)$ must accept. □

Proof. (Theorem Theorem 6.1) Two consequences follow from assumption (*)

- $\mathrm{C}^p(x \mid y) \leq \mathrm{CBP}^q(x \mid y) + O(\log n)$
- $\mathrm{C}^p(x \mid y) \leq \mathrm{CND}^q(x \mid y) + O(\log n)$

The second item is shown in (FK96) to imply NP = RP. This fact can be proven as follows. If ϕ if a formula with exactly one satisfying assignment a then $\mathrm{CND}^q(a \mid \phi) = O(1)$. Thus printing complexity being less than nondeterministic distinguishing complexity gives that unique SAT can be solved in polynomial time, and so by Valiant-Vazirani (VV86) NP = RP. We can now apply the Lemma Lemma 6.2 to obtain P = NP. □

A corollary of Lemma Lemma 6.2 is that polynomial time symmetry of information implies BPP $\neq$ EXP. We first need the following lemma.

Lemma 6.3. *If (SMI) holds for polynomial time printing complexity, then for every polynomial q there is a polynomial p such that for all x, $\mathrm{C}^p(x) \leq \mathrm{CBP}^q(x) + O(\log |x|)$.*

Proof. Suppose that $\mathrm{CBP}^q(x) = k$. This means there is a program p of length k such that $U(p, r) = x$ for at least 2/3 of the strings $r \in \{0,1\}^{q(n)}$. By counting, it must be the case that $\mathrm{C}(r \mid x) \geq |r| - O(1)$ for one of these strings r, call it r^*. Using (SMI), there is a polynomial p for which

$$\mathrm{C}^q(r^*) + \mathrm{C}^q(x \mid r^*) \geq \mathrm{C}^p(x) + \mathrm{C}^p(r^* \mid x) - O(\log n).$$

As $\mathrm{C}^q(r^*) = \mathrm{C}^p(r^* \mid x) + O(1)$ this implies $\mathrm{C}^p(x) \leq k + O(\log n)$. □

Corollary 6.4. *If for every polynomial q there exists a polynomial p such that for every x, $\mathrm{C}^p(x) \leq \mathrm{CBP}^q(x) + O(\log |x|)$, then* BPP $\neq$ EXP. *In particular, if (SMI) holds for polynomial time printing complexity then* BPP $\neq$ EXP.

Proof. Suppose, for contradiction, that EXP $\subseteq$ BPP. This implies that NP $\subseteq$ BPP, and thus by Lemma Lemma 6.2 that P = NP. We now have EXP $\subseteq$ BPP $\subseteq$ $\mathrm{NP}^{\mathrm{NP}}$ = P a contradiction to the time hierarchy theorem. □

We now turn to relativizations to help us find a good candidate hypothesis, weaker than P = NP, which would imply symmetry of information. As we know that symmetry of information implies the nonexistence of cryptographic one-way functions, it is natural to ask if the converse holds. This is a tantalizing hypothesis as it is known that the nonexistence of one-way functions does imply a strong compression result (Wee04, Theorem 6.3). We show that this implication does not hold in every relativized world. That is, we show there is an oracle X such that $\mathrm{P}^X = \mathrm{UP}^X$ yet symmetry of information does not hold relative to X.

Theorem 6.5. *There is an oracle X such that $\mathrm{P}^X = \mathrm{UP}^X$ yet symmetry of information does not hold relative to X.*

Proof. Let X be an oracle where $\mathrm{P}^X = \mathrm{UP}^X$ and $\mathrm{P}^X \neq \mathrm{NP}^X$. Such an oracle is constructed in (BBF98). With respect to this oracle $\mathrm{NP}^X = \mathrm{RP}^X$. Suppose also that symmetry of information holds relative to X. As the proofs of Lemma Lemma 6.2 and Lemma Lemma 6.3 relativize, this would then imply $\mathrm{P}^X = \mathrm{NP}^X$, a contradiction. □

Acknowledgements

We would like to thank Leonid Levin, and Paul Vitanyi for anecdotes on the early days of symmetry of information, and Harry Buhrman and Lance Fortnow for helpful comments on (BF95) and (BFL02) and the modern history of the problem. We thank Harry Buhrman and Dieter van Melkebeek for beneficial comments and conversations about Sect. Section 5. The first author would like to thank Peter Bro Miltersen for his hospitality and many fruitful discussions during a visit in which part of this work took place. We also thank Detlef Ronneburger for sharing his result on Kt complexity and Michal Koucky for pointing out this result to us.

References

[Aar] S. Aaronson. The complexity zoo. http://www.cs.berkeley.edu/ /~aaronson/zoo.html.

[ABK$^+$02] E. Allender, H. Buhrman, M. Koucky, D. van Melkebeek, and D. Ronneburger. Power from random strings. In *Proceedings of the 47th IEEE Symposium on Foundations of Computer Science*, pages 669–678. IEEE, 2002.

[Bab85] L. Babai. Trading group theory for randomness. In *Proceedings of the 17th ACM Symposium on the Theory of Computing*, pages 421–429. ACM, 1985.

[BBF98] R. Beigel, H. Buhrman, and L. Fortnow. NP might not be as easy as detecting unique solutions. In *Proceedings of the 30th ACM Symposium on the Theory of Computing*, pages 203–208. ACM, 1998.

[BF95] H. Buhrman and L. Fortnow. Distinguishing complexity and symmetry of information. Technical Report TR-95-11, Department of Computer Science, The University of Chicago, 1995.

[BFL02] H. Buhrman, L. Fortnow, and S. Laplante. Resource bounded Kolmogorov complexity revisited. *SIAM Journal on Computing*, 31(3):887–905, 2002.

[BJP93] J. Buhler, H. W. Lenstra Jr., and C. Pomerance. Factoring integers with the number field sieve. In A. K. Lenstra and Jr. H. W. Lenstra, editors, *The Development of the Number Field Sieve*, volume 1554 of *Lecture Notes in Mathematics*, pages 50–94. Springer-Verlag, 1993.

[BLM00] H. Buhrman, S. Laplante, and P.B. Miltersen. New bounds for the language compression problem. In *Proceedings of the 15th IEEE Conference on Computational Complexity*, pages 126–130. IEEE, 2000.

[BLvM04] H. Buhrman, T. Lee, and D. van Melkebeek. Language compression and pseudorandom generators. In *Proceedings of the 19th IEEE Conference on Computational Complexity*. IEEE, 2004.

[FGM$^+$89] M. Fürer, O. Goldreich, Y. Mansour, M. Sipser, and S. Zachos. On completeness and soundness in interactive proof systems. In S. Micali, editor, *Randomness and Computation*, volume 5 of *Advances in Computing Research*, pages 429–442. JAI Press, Greenwich, 1989.

[FK96] L. Fortnow and M. Kummer. On resource-bounded instance complexity. *Theoretical Computer Science A*, 161:123–140, 1996.

[JSV97] T. Jiang, J. Seiferas, and P. Vitányi. Two heads are better than two tapes. *Journal of the ACM*, 44(2):237–256, 1997.

[Ko82] K. Ko. Some observations on the probabilistic algorithms and NP-hard problems. *Information Processing Letters*, 14(1):39–43, 1982.

[Lev73] L. A. Levin. Universal search problems. *Problems Information Transmission*, 9(3):265–266, 1973.

[Lev04] L. A. Levin. Personal communication, 2004.

[LM93] L. Longpré and S. Mocas. Symmetry of information and one-way functions. *Information Processing Letters*, 46(2):95–100, 1993.

[LV97] M. Li and P. Vitányi. *An Introduction to Kolmogorov Complexity and its Applications*. Springer-Verlag, New York, second edition, 1997.

[LW95] L. Longpré and O. Watanabe. On symmetry of information and polynomial time invertibility. *Information and Compuation*, 121(1):14–22, 1995.

[NW94] N. Nisan and A. Wigderson. Hardness vs. randomness. *Journal of Computer and System Sciences*, 49:149–167, 1994.

[Ron04] D. Ronneburger. Personal communication, 2004.

[RRV02] R. Raz, O. Reingold, and S. Vadhan. Extracting all the randomness and reducing the error in Trevisan's extractors. *Journal of Computer and System Sciences*, 65(1):97–128, 2002.

[Sip83] M. Sipser. A complexity theoretic approach to randomness. In *Proceedings of the 15th ACM Symposium on the Theory of Computing*, pages 330–335. ACM, 1983.

[Tre01] L. Trevisan. Construction of extractors using pseudo-random generators. *Journal of the ACM*, 48(4):860–879, 2001.

[TVZ04] L. Trevisan, S. Vadhan, and D. Zuckerman. Compression of samplable sources. In *Proceedings of the 19th IEEE Conference on Computational Complexity*, pages 1–15. IEEE, 2004.

[VV86] L. G. Valiant and V. V. Vazirani. NP is as easy as detecting unique solutions. *Theoretical Computer Science*, 47:85–93, 1986.

[VV02] N. Vereshchagin and P. Vitányi. Kolmogorov's structure function with an application to the foundations of model selection. In *Proceedings of the 47th IEEE Symposium on Foundations of Computer Science*, pages 751–760. IEEE, 2002.

[Wee04] H. Wee. On pseudoentropy versus compressibility. In *Proceedings of the 19th IEEE Conference on Computational Complexity.* IEEE, 2004.

[ZL70] A. Zvonkin and L. Levin. The complexity of finite objects and the algorithmic concepts of information and randomness. *Russian Mathematical Surveys*, 25:83–124, 1970.

Troy Lee
CWI and University of Amsterdam
Kruislaan 413, Amsterdam 1098SJ, The Netherlands
Troy.Lee@cwi.nl

Andrei Romashchenko
Institute for Information Transmission Problems
Bolshoy Karetny 19, Moscow 101447, Russia
anromash@mccme.ru