行政院國家科學委員會專題研究計畫　成果報告

解隨機化之研究(3/3)

計畫類別：個別型計畫
計畫編號：NSC94-2213-E-009-007-
執行期間：94 年 08 月 01 日至 95 年 07 月 31 日
執行單位：國立交通大學資訊工程學系(所)

計畫主持人：蔡錫鈞

計畫參與人員：吳信龍，李佳蓉，謝旻錚，余謝銘

報告類型：完整報告
報告附件：出席國際會議研究心得報告及發表論文
處理方式：本計畫可公開查詢

中　華　民　國 95 年 9 月 19 日

行政院國家科學委員會補助專題研究計畫 ■ 成 果 報 告
□期中進度報告

解隨機化之研究

計畫類別：■ 個別型計畫　□ 整合型計畫
計畫編號：NSC　94-2213-E-009-007
執行期間：　92　年　8　月　1　日至　95　　年　7　月　31　日

計畫主持人：蔡錫鈞 教授
共同主持人：
計畫參與人員： 吳信龍、李佳蓉、謝旻錚、余謝銘

成果報告類型(依經費核定清單規定繳交)：□精簡報告　■完整報告

本成果報告包括以下應繳交之附件：
□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
□出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究計畫、列管計畫及下列情形者外，得立即公開查詢
□涉及專利或其他智慧財產權，□一年□二年後可公開查詢

執行單位：

中　華　民　國　95　年　7　月　31　日

中文摘要

我們研究解隨機化相關問題。虛擬亂數產生器(Pseudo-random number generator)在下列問題中扮演了重要的角色：是否每一個在問題類 BPP 中的問題都有一個多項式時間的確定式演算法能解決。(稱為 BPP 的解隨機化。) 為了構造偽亂數產生器，通常我們需要經由一些函數難度上的假設出發去建構此產生器。在本計畫，我們將探討不同的函數難度上的假設與偽亂數產生器之關係。我們特別探討下列主題：

(一) 難度放大器之構造的不可能結果；

(二) 在 NP 問題類之難度放大問題與構造；

(三) 建立虛擬亂數產生器與不同函數難度上的假設間之關係；

(四) 對於更限制一類電路分辨者，構造一虛擬亂數產生器使其無法分辨。

關鍵詞：隨機計算(randomized computation)、難度放大(hardness amplification)、解隨機化(derandomization)、虛擬亂數產生器(Pseudo-random number generator)

英文摘要

We study the Derandomization. Pseudorandom number generators play an important role in whether every problem in BPP can be transformed into P (Derandomization of BPP). To construct pseudorandom generators, one need to start from some hardness assumptions. In this project, we study the the relationship between these various hardness assumptions and pseudorandomness. Particularly, we study the following topics.

- The impossibility results of hardness amplification.
- Construction of an efficient procedure for hardness amplification within NP.
- To establish the relationship between various hardness assumptions and pseudorandomness.
- Construction of an efficient pseudorandom generator against restricted classes of circuits.

Keywords：Randomized computation, Hardness Amplification, Derandomization, Pseudorandom number Generators

Index

1 Introduction

1.1 Background

Understanding the power of randomness in computation is one of the central topics in theoretical computer science. A major open question is the BPP versus P question, asking whether or not all randomized polynomial-time algorithms can be converted into deterministic polynomial-time ones. A standard approach to derandomizing BPP relies on constructing the so-called pseudorandom generators (PRG), which stretch a short random seed into a long pseudorandom string that looks random to circuits of polynomial size. So far, all known constructions of PRG are based on unproven assumptions of the nature that certain functions are hard to compute. The idea of converting hardness into pseudorandomness first appeared implicitly in the work of Blum and Micali [BM82] and Yao [Yao82]. This was made explicit by Nisan and Wigderson [NW94], who showed how to construct a PRG based on a Boolean function which is hard in an average-case sense. To get a stronger result, one would like to relax the hardness assumption, and a series of research [NW94, BFNW93, Im95] then worked on how to transform a function into a harder one. Finally, Impagliazzo and Wigderson [IW97] were able to convert a function in E that is hard in worst case into one that is hard in average case, both against circuits of exponential size. As a result, they obtained BPP = P under the assumption that some function in E cannot be computed by a circuit of sub-exponential size. Simpler proofs and better trade-offs have been obtained since then [STV01, ISW00, SU01, Uma03].

Note that hardness amplification is the major step in derandomizing BPP in the research discussed above, as the step from an average-case hard function to a PRG is relatively simple and has low complexity. We say that a Boolean function f is β–hard (or has hardness β) against circuits of size s if any such circuit attempting to compute f must make errors on at least β fraction of the input. The error bound β is the main parameter characterizing the hardness; the size bound s also reflects the hardness, but it plays a lesser role in our study. Formally, the task of hardness amplification is to transform a function $f : \{0,1\}^n \to \{0,1\}$ which is β–hard against circuits of size $s(n)$ into a function $f' : \{0,1\}^m \to \{0,1\}$ which is β'–hard against circuits of size $s'(m)$, with $\beta < \beta'$ and $s'(m)$ close to (usually slightly smaller than) $s(n)$. Normally, one would like to have m as close to n as possible, preferably with $m = \mathrm{poly}(n)$, so that one could have $s'(m)$ close to $s(m)$; otherwise, one would only be able to have the hardness of f' against much smaller circuits. Furthermore, one would like f' to stay in the same complexity class of f, so that one could establish the relation among hardness assumptions within the same complexity class.

Two issues come up from those works on hardness amplification. The first is on the complexity of the amplification procedure. All previous amplification procedures going from worst-case hardness ($\beta = 2^{-n}$) to average-case hardness ($\beta' = 1/2 - 2^{-\Omega(m)}$) need exponential time [BFNW93, IW97, STV01] (or slightly better, in linear space [KM02] or $\oplus\mathsf{ATIME}(O(1), n)$ [Vio04]). As a result, such a hardness amplification is only known for functions in high complexity classes. Then a natural question is: can it be done for functions in lower complexity classes? For example, given a function in NP which is worst-case hard, can we transform it into another function in NP which is average-case hard? Only for some range of hardness (e.g. starting from mild hardness, with $\beta = 1/\mathrm{poly}(n)$) is this known to be possible [Yao82, NW94, IW97, OD02, HVV04].

The second issue is that hardness amplification typically involves non-uniformity in the sense that hardness is usually measured against *non-uniform* circuits. In fact, one usually needs to start from a function which is hard against non-uniform circuits, even if one only wants to produce a

function which is hard against uniform Turing machines. This is why most results on hardness amplification are based on non-uniform assumptions (except [IW98, TV02]).

It is also known that from a PRG, one can obtain a worst-case hard function [NW94]. Therefore, in a high complexity class such as E, the notions of pseudrandomness and various degrees of hardness are equivalent. However, when we go down to a lower complexity class, such as NP, the picture among worst-case hardness, average-case hardness, and pseudorandomness is no longer clear. In fact, all the known transformations from a worst-case hard function to a mildly hard one or to a PRG require exponential time (or linear space) [IW97, STV01, KM99, ISW00, SU01, Uma03], and it appears very difficult to bring down the complexity.

1.2 Strongly and Weakly Black-Box Constructions.

According to the prior discussion, we would like to show that some kind of hardness amplification or PRG construction is indeed impossible. For this, we need to clarify what type of hardness amplification we are talking about, especially given the possibility that an average-case hard function may indeed exist.

One important type of hardness amplification is the (strongly) *black-box* hardness amplification from ε-hardness to $\bar{\varepsilon}$-hardness. First, the initial function f is given as a black box to construct the new function $\bar{f}$, in the sense that there is an oracle Turing machine $\textsc{Amp}^{(\cdot)}$ such that $\bar{f} = \textsc{Amp}^{f}$. Furthermore, the $\bar{\varepsilon}$-hardness of the new function $\bar{f}$ is also guaranteed in a black box way, in the sense that there is another oracle Turing machine $\textsc{Dec}^{(\cdot)}$ such that given any adversary A which computes $\bar{f}$ correctly on at least $(1-\bar{\varepsilon})$ fraction of inputs, $\textsc{Dec}$ using A as oracle can compute f correctly on at least $(1-\varepsilon)$ fraction of inputs. We call $\textsc{Amp}$ the encoding procedure and $\textsc{Dec}$ the decoding procedure. In fact, almost all previous constructions of hardness amplification were done in such a black-box way [Yao82, BFNW93, GNW95, Im95, IW97, STV01, KM99, OD02, HVV04]. As we will see, such type of hardness amplification has its limitation.

One relaxation is the so-called *weakly black-box* hardness amplification, in which the hardness proof is no longer required to be done in a black-box way (dropping the requirement of having a decoding procedure). Precisely, its hardness proof is only to show the following statement: if there is an efficient adversary A computing $\bar{f}$ correctly on at least $(1-\bar{\varepsilon})$-fraction of inputs, then there exists an efficient adversary B which computes the initial function f on at least $(1-\varepsilon)$ fraction of inputs. Note that the analysis is arbitrary and hence is not necessarily restricted in a black-box way. In this sense, this weakly model is a natural relaxation of strongly black-box model. The difference between strongly and weakly black-box models is remarkable especially when an average-case hard function indeed exists. A hardness proof of the weakly black-box model may just to show that the resulting function $\bar{f}$ is close to that average-case hard one. Hence this sufficiently fulfills the statement of hardness proof. However, this proof approach is not allowed for the strongly black-box model. Again, as we will see, the weakly black-box hardness amplification also has its limitation when it is unable to embed any average-case (or mildly) hard function in itself.

Similarly, one can consider black-box construction of a PRG from a hard function, which builds a PRG from a hard function in a black-box way. Again, almost all previous PRG constructions were done in such a black-box way [IW97, STV01, KM99, ISW00, SU01, Uma03]. We will also consider black-box construction of a hard function from a PRG, which builds a hard function from a PRG in a black-box way. The construction of [NW94] was indeed a black-box one. Now we can back to the relationship among pseudorandomness and various degrees of hardness within NP (or PH).

2 Goal of this Research

Our goal in this project is to study the the following topics.

- The impossibility results of hardness amplification.
- To construct an efficient procedure for hardness amplification within NP.
- To establish the relationship between various hardness assumptions and pseudorandomness.
- To construct an efficient pseudorandom generator against restricted classes of circuits.

3 Previous Results

3.1 Hardness Amplification and Pseudorandomness

Viola [Vio04] gave the first lower bound on the complexity required for black-box hardness amplification. He showed that to transform a worst-case hard function f into a mildly hard function f', both against circuits of size $2^{o(n)}$, the encoding procedure Amp cannot possibly belong to the complexity class $\mathsf{ATIME}(O(1), 2^{o(n)})$. This rules out the possibility of doing such hardness amplification in PH, which explains why previous such procedures all require a high computational complexity. He also showed a similar lower bound for black-box construction of PRG from a worst-case hard function.

Trevisan and Vadhan [TV02] observed that a black-box hardness amplification from worst-case hardness corresponds to an error-correcting code with some list-decoding property. Then results from coding theory can be used to show that for any such amplification from worst-case hardness to hardness $(1-\varepsilon)/2$, the decoding procedure Dec must need $\Omega(\log(1/\varepsilon))$ bits of advice in order to compute f. This explains why almost all previous hardness amplification results were done in a non-uniform setting, except [IW98, TV02] which did not work in a black-box way.

There were also impossibility results on weaker types of hardness amplification, from worst-case hardness to average-case hardness. Bogdanov and Trevisan [BT03] considered hardness amplification for functions in NP in which the black-box requirement on the *encoding* procedure is dropped. They showed that the decoding procedure cannot be computed non-adaptively in polynomial time unless PH collapses.

The other possibility is to consider weakly black-box hardness amplification, in which the constraint on the decoding procedure is dropped, while the encoding procedure is still required to be done in a black-box way. Viola [Vio05a] proved that if a weakly black-box procedure amplifying from worst-case hardness to mild hardness can be realized in PH, then one can obtain from it a mildly hard function computable in PH. Although this can be seen as a negative result, it does not rule out the possibility of such a weakly black-box hardness amplification. In fact, it appears difficult to establish impossibility results for such a hardness amplification. This is because if an average-case hard function indeed exists, an amplification procedure may simply ignore the initial hard function and compute the average-case function from scratch. This raises the question: can one prove any meaningful impossibility result for weakly black-box hardness amplification?

All these results discussed above are basically on the difficulty of amplifying from a worst-case hard (or even slightly harder) function into a mildly hard one. On the other hand, in polynomial time one can transform a mildly hard function into an average-case hard one [IW97], or to construct

a PRG from an average-case hard function [NW94]. In fact, each of them can be done in a strongly black-box way, with both the encoding and decoding procedures realized in P.

Finally, to complete the circle, one can transform a PRG back to a worst-case hard function [NW94]. Note that the above transformation can be done in a black-box way, in which the decoding procedure is realized in P while the encoding procedure needs the complexity of NP. This raises the following two questions. First, can the complexity of the encoding procedure be reduced? Next, since the transformation from worst-case hardness to average-case hardness seems to require high complexity, can we transform a PRG directly into an average-case hard function, using a low-complexity procedure, say in NP (or even in P)?

3.2 Hardness Amplification within NP

It remains open for lower complexity classes. In fact, there are results showing that the same techniques used for high complexity classes can not be used for the class NP to obtain average-case hardness when starting from worst-case hardness [BT03] or even starting slightly below mild hardness [Vio04, LTW05, Vio05a].

So we focus on the task of transforming mild hardness to average-case hardness for the complexity class NP. One attempt is to use Yao's XOR lemma [Yao82, GNW95], which transforms a given function $f : \{0,1\}^n \to \{0,1\}$ into a function $f' : (\{0,1\}^n)^k \to \{0,1\}$ defined by $f'(x_1, \cdots, x_k) = f(x_1) \oplus \cdots \oplus f(x_k)$. However, we do not know if this works here, since we do not know if NP is closed under the XOR operation. O'Donnell [OD02] gave the first result along this line, showing how to convert any balanced function $f \in \mathsf{NP}$ which is mildly hard for polynomial-size circuits into another $f' \in \mathsf{NP}$ which is $(1/2 - 1/n^{1/2-\alpha})$-hard for polynomial-size circuits, for any constant $\alpha > 0$. He considered transformations of the form: $f'(x_1, \ldots, x_k) = C(f(x_1), \ldots, f(x_k))$, where C is a polynomial-time computable *monotone* function. Then he used the "tribes" function and the "recursive majority" function, and took their composition as the function C. Recently, Healy et al. [HVV04] were able to amplify hardness beyond $1/2 - 1/\mathrm{poly}(n)$, showing how to convert any balanced function in NP which is mildly hard for circuits of size $s(n)$ into one in NP which is $(1/2 - 1/s'(n))$-hard for circuits of size $s'(n)$, with $s'(n) = s(n^{1/2})^{\Omega(1)}$. In particular, $s'(n) = n^{\omega(1)}$ when $s(n) = n^{\omega(1)}$, $s'(n) = 2^{n^{\Omega(1)}}$ when $s(n) = 2^{n^{\Omega(1)}}$, and $s'(n) = 2^{\Omega(n^{1/2})}$ when $s(n) = 2^{\Omega(n)}$. A key source of their improvement came from derandomizing O'Donnell's proof (the other source being nondeterminism). They observed that the function C used by O'Donnell can be computed by a small-size read-once branching program and thus can be fooled by the pseudorandom generator of Nisan [Nis91]. Unfortunately, this generator becomes the bottleneck of their approach when $s(n) = 2^{\Omega(n)}$, which prevents them from achieving the goal of having $s'(n) = 2^{\Omega(n)}$.

3.3 Pseudorandom Generators fooling Restricted Classes of Circuits

A pseudorandom generator (PRG) is an efficiently computable function which maps a short random input to a long pseudorandom output which is hard for small boolean circuits to distinguish from truly uniform distribution. Pseudorandom generators play an important role in the theory of computation such as derandomization of randomized algorithms. The first pseudorandom generator for derandomization is constructed by Nisan and Wigderson [NW94] based on a boolean function which is hard for subexponential circuits to approximate. However it is unknown about the existence of such a hard function so far.

When we consider more restricted circuits such as AC^0 circuits, i.e. constant depth circuits with unbounded fanin, one can find an explicit function that is hard for AC^0 circuits to approximate. In fact, parity function is hard for subexponential AC^0 circuits to approximate [Has86]. Therefore, it is interesting to ask whether one can construct a pseudorandom generator fooling AC^0 circuits based on parity function. This is positively answered by Nisan [Nis91]. In [Nis91], parity function is plugged into the Nisan-Wigderson construction to achieve a pseudorandom generator fooling small AC^0 circuits.

Even when AC^0 circuits are allowed to use few symmetric gates (i.e. the gate depending only on the weight of its fanin), there is still an explicit function that is hard to approximate for these kinds of circuits. Viola [Vio05b] shows that there exists an explicit function which is hard to approximate by AC^0 circuits of size $n^{O(\log n)}$ and with $O(\log^2 n)$ symmetric gates. Subsequently Viola plugs this function into the Nisan-Wigderson construction to obtain a pseudorandom generator for AC^0 circuits of size $n^{O(\log n)}$ and with $O(\log^2 n)$ symmetric gates [Vio05b].

4 Our Results

We mainly focus on hardness amplification and its relation to pseudorandom generators. The following is the description of our research.

4.1 Strongly Black-Box Hardness Amplification

Previous lower bound results only address hardness in a specific range. However, whether or not one can amplify hardness beyond this range is also a natural and interesting question. For example, it is known that a black-box hardness amplification from hardness $1/\mathrm{poly}(n)$ to average-case hardness can be realized in polynomial time [Yao82, GNW95, Im95, IW97]. Can such a hardness amplification be realized in a lower complexity class, such as AC^0? Can it start from hardness below $1/\mathrm{poly}(n)$ and still be realized in polynomial time? Can it be done in a uniform way (with a uniform decoding procedure) if we drop the complexity constraint? In general, how does the quality of a hardness amplification (the amount of hardness increased) determine its inherent complexity or non-uniformity? These questions will all be answered in this paper. We generalize previous results [Vio04, TV02] and consider hardness amplification in a much broader spectrum: from hardness $(1-\delta)/2$ to hardness $(1-\delta^k)/2$, for general $\delta \in (0,1)$ and $k \in \mathbb{N}$.

Our first result addresses both the complexity issue and the non-uniformity issue in the same framework, showing how complexity constraints on the encoding procedure result in the inherent non-uniformity of the decoding procedure. Formally, we prove that if the encoding procedure Amp for such a hardness amplification is computed by a circuit of depth d and size $2^{o(k^{1/d})}$, the decoding procedure Dec must need an advice of length $2^{\Omega(n)}$. As a result, with $\textsc{Amp} \in \mathsf{PH}$ when $k = n^{\omega(1)}$ or with $\textsc{Amp} \in \mathsf{ATIME}(O(1), 2^{o(n)})$ when $k = 2^{\Omega(n)}$, such a hardness amplification is impossible if the hardness is measured against circuits of size $2^{o(n)}$.

Our lower bound is almost tight as the well known XOR lemma [Yao82, GNW95] can achieve such a hardness amplification with Amp realized by a circuit of depth $O(d)$ and size $2^{O(k^{1/d})}$ and Dec using an advice of length $\mathrm{poly}(n/\delta^k)$. Note that Viola's result in [Vio04] is a special case of ours, because he only addressed explicitly the specific case with $(1-\delta)/2 = 2^{-n}$ and $(1-\delta^k)/2 = 1/\mathrm{poly}(n)$ (or equivalently, $\delta = 1 - 2^{-n+1}$ and $k = 2^{\Omega(n)}$). Although it seems that his technique can be extended to show lower bounds when $(1-\delta)/2$ is small enough, but beyond that,

say with $(1-\delta)/2 = \Omega(1)$, it fails to give a meaningful bound. We can cover this case: our result implies that no AC^0 circuit can realize a black-box hardness amplification, say, from hardness $1/3$ to hardness $1/2 + 2^{-n^{\Omega(1)}}$. On the other hand, our result when restricted to worst-case to average-case hardness amplification is incomparable to those of [BT03] and [Vio05a]. Finally, two interesting facts follow from our result. First, it is impossible to produce in a black-box way a function which is $(1-\delta^k)/2$–hard against a uniform low complexity class, say $\mathsf{DTIME}(O(1))$, even if we start from a function which is $(1-\delta)/2$–hard against a uniform but arbitrarily high complexity class equipped with an advice of length $2^{o(n)}$, say $\mathsf{DTIME}(2^{2^n})/2^{o(n)}$. On the other hand, it is easy to show that hard functions against $\mathsf{DTIME}(O(1))$ do exist. This demonstrates one severe weakness of black-box hardness amplifications. Second, when amplifying hardness from $(1-\delta)/2$ to $(1-\delta^k)/2$, the complexity of such amplification is determined mainly by the parameter k; a larger value of k results in a higher complexity requirement, for typical values of δ.

Note that our lower bound above vanishes for $d = \Omega(\log k)$. Our second result deals with this issue. We show that if the encoding procedure is computed by a nondeterministic circuit of size $o(k/\log k)$, even with arbitrary depth, the decoding procedure Dec must need an advice of length $2^{\Omega(n)}$. As a result, in nondeterministic polynomial time, one can not amplify hardness from $(1-\delta)/2$ to hardness $(1-\delta^k)/2$ for any super-polynomial k (for example, from hardness below $1/\mathrm{poly}(n)$ to hardness $\Omega(1)$).

Our third result shows that even without any complexity constraint on the encoding or decoding procedure, amplification between certain range of hardness is still inherently non-uniform. One can derive this for the case of amplifying hardness beyond $1/4$, using Plotkin bound [Plo60] from coding theory. We obtain a quantitative bound on the non-uniformity for a general range of hardness amplification. We show that to amplify from hardness $(1-\delta)/2$ to hardness $(1-\varepsilon)/2$, the decoding procedure Dec must need an advice of $\Omega(\log(\delta^2/\varepsilon))$ bits. Thus, when $\varepsilon = \delta^k$, an advice of length $\Omega(k\log(1/\delta))$ is necessary, and when $\varepsilon \le c\delta^2$ for some constant c, such hardness amplification must be inherently non-uniform. Our result generalizes that of Trevisan and Vadhan [TV02].

Finally, we derive similar lower bounds on black-box constructions of PRG from any function with a given hardness.

4.2 The Relationship between Mild Hardness and Pseudorandomness

Our result provides strongly black-box constructions of average-case hard functions from PRGs. As a result, we build the equivalence between PRG and average-case hardness within NP Then, we also derive negative results for weakly black-box hardness amplification. Therefore, we widen the gap between worst-case and mild hardness within NP.

First, we give strongly black-box constructions of average-case hard functions from PRGs. The first construction has the encoding procedure realized in NP and the decoding procedure realized in P/poly (or randomized polynomial time). This improves the result of [NW94] which, using an encoding procedure in NP as well, obtains only a worst-case hard function. A natural question then is: can we further reduce the complexity of the encoding procedure, or can we prove a complexity lower bound? We give a partial answer to this by providing another strongly black-box construction with the encoding procedure realized in P but at the expense of increasing the complexity of the decoding procedure to NP, which rules out the possibility of proving a complexity lower bound for the encoding procedure without restricting the complexity of the decoding procedure. This still leaves open the question of whether or not one can have both the encoding and decoding procedures realized in P. Our positive results also imply some impossibility results. By combining

with the impossibility results of strongly black-box hardness amplification in [**?**, LTW05] and our following impossibility results of weakly black-box hardness amplification, respectively, we can obtain corresponding impossibility results of black-box PRG constructions from hard functions.

4.3 Weakly Black-Box Hardness Amplification

We prove that if a weakly black-box hardness amplification realized in $\mathsf{TIME}(t)$ can amplify hardness by an $\omega(t)$ factor, from $o(\varepsilon/t)$ to ε, then it must embed in it a function computable in $\mathsf{TIME}(t)$ with hardness about ε. Note that a function in $\mathsf{TIME}(t)$ cannot be hard against a class containing $\mathsf{TIME}(t)$. Therefore, we obtain an unconditional impossibility result: it is impossible to use a procedure in $\mathsf{TIME}(t)$ to transform a function which is $o(\varepsilon/t)$-hard against the class $\mathcal{C} = \mathsf{SIZE}(2^{n/3})$ into a function which is ε-hard against a class $\bar{\mathcal{C}} \supseteq \mathsf{TIME}(t)$. This rules out the possibility of using a low-complexity procedure to do such a hardness amplification for high-complexity functions. Note that when $t = 2^{o(n)}$, this gives an impossibility result for amplifying from worst-case hardness to mild hardness in sub-exponential time. We also extend this impossibility result to the case with $\mathcal{C}$ being any uniform complexity class equipped with an advice of length at most $2^{n/3}$. This says that such a weakly hardness amplification, just as in the strongly black-box case [LTW05], must also be highly non-uniform in nature: it is impossible to have such a weakly hardness amplification if one start from an initial function which is hard against any complexity class with only $2^{n/3}$ bits of non-uniformity (even of arbitrarily high uniform complexity). Second, we prove that if a weakly black-box hardness amplification realized in NP ($\Sigma_k\mathsf{P}$, respectively) can amplify hardness beyond a polynomial factor, from $\varepsilon^2/n^{\omega(1)}$ to ε, then one can obtain from it a function computable in NP ($\Sigma_k\mathsf{P}$, respectively) with hardness about ε. This improves the result in [Vio05a], as the hard function obtained there seems to need at least the complexity of $\Sigma_{k+1}\mathsf{P}$, one level higher then ours in PH. Again, this enables us to derive an unconditional impossibility result: it is impossible to use a procedure in NP ($\Sigma_k\mathsf{P}$, respectively) for such a hardness amplification, if the new function's hardness is measured against a class containing $\mathsf{NP}/\mathrm{poly}$ ($\Sigma_k\mathsf{P}$, respectively), when the initial function is hard against a uniform complexity class equipped an advice of length $2^{n/3}$. Note that this excludes the possibility of having such a hardness amplification from worst-case hardness to mild hardness for functions in NP.

4.4 Hardness Amplification Within NP

We study the problem of hardness amplification in NP. We prove that if there is a balanced function in NP such that any circuit of size $s(n) = 2^{\Omega(n)}$ fails to compute it on a $1/\mathrm{poly}(n)$ fraction of inputs, then there is a function in NP such that any circuit of size $s'(n)$ fails to compute it on a $1/2 - 1/s'(n)$ fraction of inputs, with $s'(n) = 2^{\Omega(n^{2/3})}$. This improves the result of Healy et al. (STOC'04), which only achieves $s'(n) = 2^{\Omega(n^{1/2})}$ for the case with $s(n) = 2^{\Omega(n)}$.

4.5 Jensen-Shannon Divergence and Variational Distance

We study the distance measures between two probability distributions via two different distance metrics, a new metric induced from Jensen-Shannon Divergence[DS03] and the well known L_1 metric. We show that several important results and constructions in computational complexity under the L_1 metric carry over to the new metric, such as Yao's next-bit predictor [Yao82], the existence of extractors [Tre99], the leftover hash lemma [Sti02] and the construction of expander

graph based extractor. Finally we show that the useful parity lemma [Vaz87] in studying pseudo-randomness does not hold in the new metric.

References

[BFNW93] László Babai, Lance Fortnow, Noam Nisan, and Avi Wigderson. BPP has subexponential time simulations unless EXPTIME has publishable proofs. *Computational Complexity*, 3(4), pages 307–318, 1993.

[BM82] Manuel Blum and Silvio Micali. How to generate cryptographically strong sequences of pseudo random bits. In *Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science*, pages 112–117, 1982.

[BT03] Andrej Bogdanov and Luca Trevisan. On worst-case to average-case reductions for NP problems. In *44th Annual Symposium on Foundations of Computer Science*, Cambridge, Massachusetts, pages 11–14, 2003.

[DS03] D. M. Endres and J. E. Schindelin. A New Metric for Probability Distributions. *IEEE Transaction on Information Theory*, vol 49, pp.1858-60. July 2003.

[FSS84] Merrick L. Furst, James B. Saxe, and Michael Sipser. Parity, circuits, and the polynomial-time hierarchy. *Mathematical Systems Theory*, 17(1), pages 13–27, 1984.

[GNW95] Oded Goldreich, Noam Nisan, and Avi Wigderson. On Yao's XOR lemma. Technical Report TR95–050, Electronic Colloquium on Computational Complexity, 1995.

[GV05] Venkatesan Guruswami and Salil Vadhan. A lower bound on list size for list decoding. In *Proceedings of the 8th International Workshop on Randomization and Computation (RANDOM '05)*, pages 318–329, 2005.

[Has86] Johan Håstad. *Computational limitations for small depth circuits*. PhD thesis, MIT Press, 1986.

[HVV04] Alexander Healy, Salil P. Vadhan, and Emanuele Viola. Using nondeterminism to amplify hardness. In *Proceedings of the 36th ACM Symposium on Theory of Computing*, pages 192–201, 2004.

[Im95] Russel Impagliazzo. Hard-core distributions for somewhat hard problems. In *Proceedings of the 36th Annual IEEE Symposium on Foundations of Computer Science*, pages 538–545, 1995.

[ISW00] Russell Impagliazzo, Ronen Shaltiel, and Avi Wigderson. Extractors and pseudo-random generators with optimal seed length. In *Proceedings of the 32nd ACM Symposium on Theory of Computing*, pages 1–10, 2000.

[IW97] Russel Impagliazzo and Avi Wigderson. P=BPP if E requires exponential circuits: derandomizing the XOR lemma. In *Proceedings of the 29th ACM Symposium on Theory of Computing*, pages 220–229, 1997.

[IW98] Russel Impagliazzo and Avi Wigderson. Randomness vs. time: de-randomization under a uniform assumption. In *Proceedings of the 39th Annual IEEE Symposium on Foundations of Computer Science*, pages 734–743, 1998.

[KM99] Adam Klivans and Dieter van Melkebeek. Graph nonisomorphism has subexponential size proofs unless the polynomial-time hierarchy collapses. In *Proceedings of the thirty-first annual ACM symposium on Theory of computing*, pages 659–667, 1999.

[KM02] Adam Klivans and Dieter van Melkebeek. Graph nonisomorphism has subexponential size proofs unless the polynomial-time hierarchy collapses. *SIAM Journal on Computing*, 31(5), pages 1501–1526, 2002.

[LMN93] Nathan Linial, Yishay Mansour, and Noam Nisan. Constant depth circuits, Fourier transform, and learnability. *Journal of the ACM*, 40(3), pages 607–620, 1993.

[LTW05] Chi-Jen Lu, Shi-Chun Tsai, and Hsin-Lung Wu. On the complexity of hardness amplification. In *Proceedings of the 20th Annual IEEE Conference on Computational Complexity*, pages 170–182, 2005.

[Nis91] Noam Nisan. Pseudorandom bits for constant depth circuits. *Combinatorica*, 11(1), pages 63–70, 1991.

[NW94] Noam Nisan and Avi Wigderson. Hardness vs randomness. *Journal of Computing System Science*, 49(2), pages 149–167, 1994.

[OD02] Ryan O'Donnell. Hardness amplification within NP. In *Proceedings of the 34th ACM Symposium on Theory of Computing*, pages 751–760, 2002.

[Plo60] M. Plotkin. Binary codes with specified minimum distance. *IEEE Transactions on Information Theory*, 6, pages 445–450, 1960.

[Sti02] D. R. Stinson. Universal hash families and the leftover hash lemma, and applications to cryptography and computing. *J. Combin. Math. Combin. Comput.* 42 (2002), 3-31.

[SU01] Ronen Shaltiel and Christopher Umans. Simple extractors for all min-entropies and a new pseudo-random generator. In *Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science*, pages 648–657, 2001.

[STV01] Madhu Sudan, Luca Trevisan, and Salil Vadhan. Pseudorandom generators without the XOR lemma. *Journal of Computer and System Sciences*, 62(2), pages 236–266, 2001.

[Tre99] L. Trevisan. Construction of extractors using pseudorandom generators. In *Proceedings of the 31st ACM Symposium on Theory of Computing*, 1999.

[Tre03] Luca Trevisan. List decoding using the XOR lemma. In *Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science*, pages 126–135, 2003.

[TV02] Luca Trevisan and Salil Vadhan. Pseudorandomness and average-case complexity via uniform reductions. In *Proceedings of the 17th Computational Complexity Conference*, pages 129–138, IEEE, 2002.

[Uma03] Christopher Umans. Pseudo-random generators for all hardnesses. *Journal of Computer and System Sciences*. 67(2), pages 419–440, 2003.

[Vaz87] U. Vazirani. Strong Communication Complexity of Generating Quasi-Random Sequences from Two Communicating Semi-Random Sources. *Combinatorica*, 7(4):375-392, 1987.

[Vio04] Emanuele Viola. The Complexity of Constructing Pseudorandom Generators from Hard Functions. In *Computational Complexity* , 13(3-4), pages 147–188, 2004.

[Vio05a] Emanuele Viola. On Constructing Parallel Pseudorandom Generators from One-Way Functions. In *Proceedings of the 20th Computational Complexity Conference*, pages 183–197, IEEE, 2005.

[Vio05b] Emanuele Viola. Pseudorandom bits for constant depth circuits wiht few arbitrary symmetric gates. In *Proceedings of the 20th Annual IEEE Conference on Computational Complexity*, pages 198–209, 2005.

[Yao82] Andrew Chi-Chih Yao. Theory and applications of trapdoor functions. In *Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science*, pages 80–91, 1982.

A Self-Evaluation of this Project

We have the following published or submitted papers shown in the following table.

Title	Published in /Submitted to
On the Complexity of Hardness Amplification	Published in Proceedings of the 20th Annual IEEE Conference on Computational Complexity, pages 170-182, 2005.
Pseudorandomness and Hardness within NP	Submitted to Theoretical Computer Science
Improved Hardness Amplification in NP	Submitted to Theoretical Computer Science
On the Jensen-Shannon Divergence	Published in IEEE Transactions on Information Theory 51(9): 3333-3336 (2005)

Table 1: Our published or submitted results