The Power of Witness Reduction

Sanjay Gupta*
Department of Computer and Information Sciences
The Ohio State University
Columbus, Ohio 43210

Abstract

Witness reduction has played a crucial role in several recent results in complexity theory. These include Toda's result that $PH \subseteq BP \oplus P$, the "collapsing" of $PH$ into $\oplus P$ with high probability; Toda and Ogiwara's results which "collapses" $PH$ into various counting classes with high probability; and hard functions for $\#P$ studied by Ogiwara and Hemachandra. Ogiwara and Hemachandra's results establish a connection between functions being hard for a class of functions and functions interacting with the class to effect witness reduction. In fact, we believe that the ability to achieve some form of witness reduction is what makes a function hard for a class of functions. To support our thesis we define new function classes and obtain results analogous to those of Ogiwara and Hemachandra. We also introduce the notion of randomly hard functions and obtain similar results.

1 Introduction

Acceptance criteria for nondeterministic machines (NTMs) is defined by some threshold on the range of a witness function. Usually, the witness function is the number of accepting paths of the machine, while the threshold varies with the class. For example, for the class $NP$, the witness function is indeed, number of accepting paths and the threshold is 'greater than or equal to 1'; that is, the acceptance criteria is 'at least one accepting computation'. By witness reduction, we mean that the threshold applied to a witness function is reduced.

Consider the class $NP$. A very strong form of witness reduction would, given an arbitrary NTM $M$, argue that there is another NTM $M'$ such that $M$ and $M'$ accept the same language and whenever $M'$ accepts, it accepts on only one computation. Of course, if this type of witness reduction were possible, then $NP = UP$, an unlikely event.

One of the most important uses of witness reduction is to collapse hierarchies. As a very simple example, consider Figure 1. Suppose that the top tree corresponds to a $C_n^A$ computation; that is, the top tree accepts if and only if exactly $f(x)$ of its computations query a string $y \in A$, where $f \in PF$. Now, suppose that $A$ can be accepted by an NTM meeting the severe witness reduction constraints of $UP$; that is, $A \in UP$. Then, the number of strings $y \in A$ queried by the top machine is exactly the same as the total number of accepting compu-
tions at the bottom of all of the level 2 trees, so that Figure 1 can be viewed as one large $\mathcal{C}_e P$ tree, collapsing $\mathcal{C}_e UP$ into $\mathcal{C}_e P$.

As another example, suppose that the top tree of Figure 1 again corresponds to a $\mathcal{C}_e A$ computation. Let $A \in \exists P$ and on input $x$ let the length of queries made to the set $A$ at level 1 be bounded by some polynomial $p(|x|)$. Now, suppose it is possible to make a guess $W$ with a high probability, where $W$ is bounded by some polynomial in $|x|$, so that given $W$, each of the strings of $A$ up to length $p(|x|)$ are accepted by an NTM meeting the witness reduction constraints of $UP$. Then, the number of strings $y \in A$ queried by the top machine is exactly the same as the total number of accepting computations at the bottom of all of the level 2 trees, for each of the right guesses $W$. Hence, the existential quantifier of $\mathcal{C}_e \exists P$ can be collapsed into $\mathcal{C}_e$ with a high probability. This is illustrated in Figure 2.

Please be warned that witness reduction does not literally mean reducing the number of accepting computations as in the previous two examples. It can be much more complicated than this. For example, let $L \in NP$ with the witness function 'number of accepting paths' and the threshold 'greater than or equal to 1'. Now, change the witness function to 'number of accepting paths $\text{Mod}_2$', so that the range of the witness function is $\{0,1\}$ and the threshold of this new witness function to 'equal to 1'; that is, the new acceptance criteria is odd number of accepting computations. Using Valiant and Vazirani's [16] reduction it is possible to construct polynomial number of machines so that one of them yields a threshold value 1 under the new witness function, with a high probability. Now, using the fact that $\oplus P$ is closed under Turing reduction[7], all of these machines can be merged into one machine with the acceptance criteria 'odd number of accepting computations'. This gives that $NP \subseteq BP.\oplus P$ or,
This complicated form of witness reduction of $NP \subseteq BP \oplus P$ was then used by Toda [13] to collapse $PH$ in $BP \oplus P$. To see how this works, using the witness function ‘number of rejecting paths’, the number of witnesses for non-membership in $VP$ can be reduced from many to one, with a high probability. This yields $VP \subseteq BP \oplus P$.

Now consider a two level tree corresponding to $VP$. Each of the level 2 trees corresponding to $VP$ acceptance criteria can be replaced by trees corresponding to $BP \oplus P$ acceptance criteria. Also, due to the second amplification lemma [11], one random guess is sufficient for each of the level 2 trees. Thus, $VP$ is simplified to $BP \oplus P$ with a high probability.

Again applying Valiant and Vazirani’s result to level 1 trees, and using the fact that $\oplus P$ is closed under Turing reductions, the acceptance criteria for level 1 can be changed from $\exists \oplus P$ to $\oplus \oplus P$, with a high probability. Now, that the witness function ‘number of accepting paths $Mod_2$’ is closed under composition\(^1\) allows collapsing of the two levels into one, with a high probability. Note that if the witness function is not the identity function, then it should be closed under composition for the collapse to occur.

This process can be iterated finite number of times yielding Toda’s result, so that any finite sequence of alternating $\exists$ and $\forall$ quantifiers can be collapsed into $\oplus P$ with a high probability. The above process also yields that $PH \subseteq BP$ for any prime number $k$, using the fact that $Mod_k P$ is closed under Turing reduction for any prime number $k$[8] and also under composition.

In the above example, note that $\oplus P$ served two purposes. Firstly, it allowed amplification of probability due to its closure under Turing reductions and secondly, it allowed the final composition of witness function to collapse the two levels into one.

Now consider the recent result of Toda and Ogiwara [14]. This uses a much simpler form of witness reduction. Again consider a two level tree of Figure 1. Suppose with one random guess (of size polynomial in the length of the input), we can reduce the number of witnesses of each of the level 2 trees, from many to one with a high probability. Then, the count of accepting paths at level 1 is same as the count of accepting paths at level 2. Hence, the two levels can be merged into one, yielding the same count of accepting paths at the bottom of all the trees of level 2. Clearly, this process can be iterated, the only problem is how to reduce the number of witnesses to one. With a very ingenious trick of taking the product of number of accepting paths minus one, Toda and Ogiwara were able to achieve this reduction, with an arbitrarily high probability. However, there process yields an additive factor of $2^{d(|z|)}$, which can be factored out by knowing the count of number of accepts. This allowed them to prove results of the form, $C.PH \subseteq BP.C$, for various counting classes $C$.

Viewing Toda and Ogiwara’s [14] result as an application of witness reduction, we note that the whole process could be simplified by changing the witness function from ‘number of accepting paths’ to ‘number of accepting paths minus number of rejecting paths(AR function)’. Let $L \in \exists P$ be accepted by a NTM $M$. Then, on input $x \in L$, using Valiant and Vazirani’s [16] reduction, it is possible to construct a polynomial number of nondeterministic machines $M_i$, so that one of them has only one accepting path, with an arbitrarily high probability. On the other hand, if $x \notin L$ then

\(^1\)(a_1 Mod_2 + \ldots + a_k Mod_2) Mod_2 = (a_1 + \ldots + a_k) Mod_2$, where $a_1, \ldots, a_k$ correspond to number of accepting paths for level 2 trees
each of the machine has no accepting paths. Now change the witness function to the $AR$ function and trivially modify $M_i$ to obtain $M'_i$, so that $AR(M'_i, x) = Acc(M_i, x)$ for each machine. Given that the $AR$ function is closed under addition, subtraction and multiplication, we can construct a new machine $M^*$ such that 

$$AR(M^*, x) = \begin{cases} 1 & \text{iff } x \in L \\
 0 & \text{iff } x \notin L, \end{cases}$$

with an arbitrarily high probability. Again, this is an instance of witness reduction with a high probability, using $AR$ function. The same can be done for $VP$.

Now it is possible to collapse a finite number of quantifiers (which correspond to different levels of guess tree) into one, with an arbitrarily high probability. This yields a stronger result than Toda and Ogiwara: for all $L \in PH$ and any polynomial $q$, there exists a NTM $M$ such that

$$\Pr\left( x \in L \Rightarrow AR(M, x \# W) = 1 \text{ and from any other number to } 0 \right) \geq (1 - \frac{1}{2^{q(|x|)}})$$

where $W$ is chosen uniformly from $\{0, 1\}^{M(|x|)}$ for some polynomial $b$. It is not difficult to see that all the results of Toda and Ogiwara are easy corollaries to this new result.

The theme of witness reduction has also appeared in the recent work of Ogiwara and Hemachandra[14]. They introduced the idea of a function being hard for a class of functions. For example, Ogiwara and Hemachandra showed that $\#P$ is closed under composition with division, subtraction, and certain other functions as well, if and only if $\#P$ is closed under composition with all $\#P$ functions. In addition, they show the interesting result that $\#P$ is closed under composition with these functions if and only if $PH = CH = UP$. More explicitly, Ogiwara and Hemachandra show that a function is hard for $\#P$ if and only if the interaction between the function and the class $\#P$ can reduce the number of accepting computations of NTMs from an exact number to 1 and from any other number to 0. Thus, the hard functions for $\#P$ are those that can effect this very strong witness reduction in $\#P^2$. In fact, we believe that this is exactly what makes a function hard for a class of functions: the ability of the function to interact with the class to effect appropriate types of witness reduction.

In this paper we build on the work of Ogiwara and Hemachandra[14] in two ways. First, we introduce the idea of a function being randomly hard for a class of functions. We then show that each of the functions proved by Ogiwara and Hemachandra to be hard for $\#P$ are also randomly hard for $\#P$. Carrying along the central theme that hardness is due to witness reduction, we show that a function is randomly hard for $\#P$ if and only if the functions can be used to achieve the corresponding random versions of the witness reduction that Ogiwara and Hemachandra achieved for $\#P$, and the corresponding random collapses: $CH = PH = \overline{BPP} = UP$.

Our second extension to the work of Ogiwara and Hemachandra is aimed at supporting the theme of witness reduction being the reason for functions being hard for a class of functions. We do this by considering two different witness functions other than 'number of accepting paths'. In particular, we consider not only number of accepting paths as witness functions, but also the AR function and the ratio of two AR functions. The AR functions are closed under composition with subtraction while the ratio of two AR functions is closed under composition with subtraction and division. However, proper subtraction and integer division, which reduce witnesses even in these

---

\[\text{Also, it is interesting to note that the witness reduction achieved by Ogiwara and Hemachandra is stronger than that of Toda, and hence produces stronger collapses.}\]
new domains, do turn out to be hard functions for these new classes of functions. Thus, in the new domains, hardness is once again associated with some form of witness reduction.

This paper is organized as follows: in Section 3 we introduce and formalize the notion of randomly hard functions for \( \#P \). We study what sort of collapses are produced by random witness reduction. Then we show that division, subtraction and span are randomly hard functions for \( \#P \).

In Section 4 we let the witness functions be AR function and then, the ratio of two AR functions. We again show that proper subtraction, integer division and span are hard functions for even these new witness functions. Finally, in Section 5, we state similar results about random witness reduction with the new witness functions - AR function and the ratio of two AR functions.

## 2 Preliminaries

Our model of computation is polynomial time bounded Turing machines. All our languages are over a fixed alphabet \( \Sigma \), containing at least two symbols \( \{0, 1\} \). The set of natural numbers, the set of integers, and the set of rational numbers, are denoted by \( \mathbb{N}, \mathbb{Z} \) and \( \mathbb{Q} \), respectively. We denote by \( PF \) the class of polynomial time computable functions. For a string, \( x \in \Sigma^* \), \( |x| \) denotes its length and for a set \( A \subseteq \Sigma^* \), \( |A| \) denotes its cardinality. We also use the standard pairing function \( \langle \cdot, \cdot \rangle \).

We define the following functions on nondeterministic Turing machines (NTMs).

**Definition 2.1** Given a nondeterministic machine \( N \), let \( \text{Acc}(N, x) \) = number of accepting paths of \( N \) on input \( x \), and \( \text{Rej}(N, x) \) = number of rejecting paths of \( N \) on input \( x \). Now, let \( \text{AR}(N, x) = \text{Acc}(N, x) - \text{Rej}(N, x) \).

Note that AR functions were used extensively to show closure properties for \( PP[1, 3, 4] \). We review the definitions of complexity classes that we will discuss in this paper.

**Definition 2.2**

1. A function \( f : \Sigma^* \rightarrow \mathbb{N} \) is in \( \#P \) iff there exists a polynomial time-bounded nondeterministic machine \( M \) such that for all \( x \), \( f(x) = \text{Acc}(M, x) \).

2. A language \( L \in NP \) iff there exists \( f \in \#P \) such that, for all \( x, x \in L \iff f(x) > 0 \).

3. A language \( L \in UP \) iff there exists \( f \in \#P \) such that, for all \( x, x \in L \iff f(x) = 1 \) and \( x \notin L \iff f(x) = 0 \).

4. A language \( L \in C_{#P} \) iff there exists \( f \in \#P \), and a \( g \in PF \) such that, for all \( x, x \in L \iff g(x) = f(x) \).

Next, we review the definitions of some standard operators.

**Definition 2.3**

1. For a class \( K \), \( \exists K \) is the class of languages defined as follows: a set \( L \) is in \( \exists K \) if there exists a polynomial \( p \) and a set \( A \in K \) such that for every \( x \in \Sigma^* \),

   \[
   x \in L \iff \|\{y \mid |y| = p(|x|) \land (x, y) \in A\}\| \geq 1.
   \]

2. For a class \( K \), \( \forall K \) is the class of languages defined as follows: a set \( L \) is in \( \forall K \) if there exists a polynomial \( p \) and a set \( A \in K \) such that for every \( x \in \Sigma^* \),

   \[
   x \in L \iff \|\{y \mid |y| = p(|x|) \land (x, y) \in A\}\| = 2^{p(|x|)}.
   \]

3. For a class \( K \), \( C_{#K} \) is the class of languages defined as follows: a set \( L \) is in \( C_{#K} \) if there exists a polynomial \( p \), a \( f \in \)
4. For a class $K$, $C_{n}K$ is the class of languages defined as follows: a set $L$ is in $C_{n}K$ if there exists a polynomial $p$, $f \in PF$, and a set $A \in K$ such that for every $x \in \Sigma^*$,

$$x \in L \iff \|\{y \mid |y| = p(|x|)\mathrm{and}(x,y) \in A\}\| \geq f(x).$$

Below are the definitions of two standard hierarchies, the polynomial time hierarchy (PH) and the polynomial time counting hierarchy (CH).

**Definition 2.4**

1. $P \in PH$.

2. If $K \in PH$, then $\exists K \in PH$ and $\forall K \in PH$.

3. PH consists of only the sets described by 1 and 2.

**Definition 2.5**

1. $P \in CH$.

2. If $K \in CH$, then $\exists K \in CH$, $\forall K \in CH$ and $C.K \in CH$.

3. CH consists of only the sets described by 1 and 2.

The following results are well-known. Note that part 2 can be proved from the definitions and part 1.

**Proposition 2.6**

1. $C_{n}.C.K = C_{n}.C_{m}.K$, for any class $K \in CH$.

2. $CH = \cup_{k>0} C_k \ldots C_k P = \cup_{k>0} C_k \ldots C_k P$.

3. $[12] L \in C_{m}P$ iff there exists a nondeterministic polynomial-time Turing machine $M$ and a polynomial $p$ such that for every $x \in \Sigma^*$,

   (a) $Acc(M,x) + Rej(M,x) = 2^{p(|x|)+1}$.
   (b) $x \in L$ iff $Acc(M,x) = 2^{p(|x|)}$.
   (c) $x \notin L$ iff $0 < Acc(M,x) < 2^{p(|x|)}$.

The following definitions are slightly modified versions of the definitions originally introduced by Ogiwara and Hemachandra [6]. We assume throughout that all functions are total.

**Definition 2.7**

1. Let $DF$ be a class of functions. Let $i \geq 1$ and let $f : N^i \rightarrow N$. $DF$ is closed under outermost composition with $f$ iff

$$\forall g_1, \ldots, g_i \in DF \\\lambda x.f(g_1(x), \ldots, g_i(x)) \in DF.$$

2. Let $DF$ and $CF$ be classes of functions.

We say that $DF$ is closed under composition with $CF$ iff

$\forall f \in CF [DF \text{ is closed under composition with } f]$.

3. Let $DF$ and $CF$ be classes of functions. Let $f \in CF$. Then, $f$ is $CF$-hard for $DF$ iff

$[DF \text{ is closed under composition with } f \Rightarrow DF \text{ is closed under composition with } CF]$.

We use outermost composition to imply that $f$ cannot appear as an argument to a function, including itself. Henceforth, we will use only "composition" to imply this restriction.

One reason for modifying the original definitions is that very simple $PF$-functions like subtraction, division, and span, when composed with $\#P$ functions, turn out to be hard for $\#P$. Thus, it is not necessarily true that if a $PF$-function is hard for $\#P$ then $\#P = PF$. 

---

4The reader is cautioned that the original proof contains a fixable error.

---

48
Definition 2.8 1. For any two $a, b \in \mathbb{Q}$, let $a \ominus b$ (proper subtraction) denote $\max(0, a - b)$.

2. For any two $a, b \in \mathbb{Q}, b \neq 0$, let $a \div b$ (integer division) denote $\left\lfloor \frac{a}{b} \right\rfloor$.

3. For each number $k \geq 2$, and $a_1, \ldots, a_k \in \mathbb{Q}$, let $\text{span}_k(a_1, \ldots, a_k)$ denote the number of distinct values in $\{a_1, a_k, \ldots, a_k\}$.

The following are parts of the main theorem proved in Ogiwara and Hemachandra [6].

Theorem 2.9 (Witness reduction implies collapsing) $\mathbb{C}_P \subseteq UP \Rightarrow CH = PH = UP$.

Theorem 2.10 (Closure iff witness reduction) $\mathbb{C}_P \subseteq UP \Leftrightarrow \#P$ is closed under composition with $\#P$.

Theorem 2.11 (Hard functions for $\#P$) Proper subtraction $(\ominus)$, integer division $(\div)$ and $\text{span}_k$, for some $k \geq 2$, are $\#P$-hard for $\#P$ (on $N$).

Corollary 2.12 (To Theorem 2.11) $\#P$ is closed under composition with $\#P$. $\#P$ is closed under composition with $PF$.

We have reproduced only parts of the original theorem from Ogiwara and Hemachandra to cluttering the theme of the paper. For example, Ogiwara and Hemachandra [6] have also shown that weak plurality and strong plurality are $\#P$-hard. All our main results look similar to the above theorems, the theme running through all the results being “witness reduction”.

3 Random witness reduction in $\#P$

As stated in the introduction, several interesting “collapses” of $PH$ into other classes have been obtained by using the random witness reduction constructed by Valiant and Vazirani [16]. In each case, it was possible to amplify the probability of reduction by using appropriate classes -$\oplus P[13]$ and counting classes [14].

We study a stronger form of random witness reduction - reducing witnesses from a fixed number to one and from any other number to zero with an arbitrarily high probability. This is exactly the condition needed to make a function randomly hard for $\#P$. We obtain results analogous to those of Ogiwara and Hemachandra [6]: witness reduction with a very high probability collapses $PH$ and $CH$ to $UP$ with a very high probability. Also, random division, random subtraction, etc, which reduce witnesses with a very high probability turn out to be randomly hard for $\#P$.

The concept of randomly hard functions is motivated by the notion of hard closure properties introduced by Ogiwara and Hemachandra [6] and the $BP$ operator introduced by Toda and Ogiwara [14]. Essentially, $BP$ is same as the standard $BP$ operator, except that “free amplification” is provided in the definition of $BP$.

Definition 3.1 1. Let $DF$ be a class of functions. Let $i \geq 1$ and let $f : N^i \rightarrow N$. $DF$ is closed under composition with $f$ randomly iff for all polynomials $e$, for all $g_1, g_2, \ldots, g_i \in DF$, there exists an $h \in DF$ and a polynomial $b$, such that, for all $x$,

$$
\text{Prob}(h(x\#w) = f(g_1(x), g_2(x), \ldots, g_i(x))) \geq 1 - \frac{1}{2^e(|x|)}
$$
where, \( w \in \{0,1\}^{4l(n)} \) is chosen uniformly.

Equivalently, we say that \( \mathcal{D} \) is closed under composition with \( f \) with an arbitrarily high probability.

2. Let \( \mathcal{D} \) and \( \mathcal{C} \) be classes of functions. We say that \( \mathcal{D} \) is closed under composition with \( \mathcal{C} \) randomly if \( \forall f \in \mathcal{C} \), \( \mathcal{D} \) is closed under composition with \( f \) randomly.

3. Let \( \mathcal{D} \) and \( \mathcal{C} \) be classes of functions. Let \( f \in \mathcal{C} \). Then, \( f \) is \( \mathcal{C} \)-hard for \( \mathcal{D} \) randomly if \( \forall f \in \mathcal{C} \), \( \mathcal{D} \) is closed under composition with \( f \) randomly.

The following definition was first introduced by Toda and Ogiwara in [14].

**Definition 3.2** \( L \in \overline{B^P}.K \) if, for all polynomials \( e \), there exists \( A \in K \) and a polynomial \( b \), such that, for all strings \( z \),

\[
\text{Prob}(x \# w \in A \Leftrightarrow x \in L) \geq 1 - \frac{1}{2^e(|z|)}
\]

where \( w \in \{0,1\}^{4l(|z|)} \) is chosen uniformly.

Our proofs in this section use the following proposition, which is easy to prove directly from the definitions. Part 1 of the proposition can also be viewed as a weaker version of the operator interchange lemma proved by Regan and Royer [10].

**Proposition 3.3**

1. \( \mathcal{C}_e B^P . UP \subseteq \overline{B^P}.C.e. UP = \overline{B^P}.C.P \).

2. \( \overline{B^P}.B^P . K = \overline{B^P}.K \).

Now we state our results for random witness reduction, which are analogous to witness reduction results of Ogiwara and Hemachandra [6].

**Theorem 3.4** (Random witness reduction implies collapsing) \( \#P \subseteq \overline{B^P}.UP \Rightarrow \mathcal{C}H = \mathcal{P}H = \overline{B^P}.UP \).

**Theorem 3.5** (Random closure iff random witness reduction) \( \#P \subseteq \overline{B^P}.UP \Leftrightarrow \#P \) is closed under composition with \( \#P \) randomly.

**Theorem 3.6** (Randomly hard functions for \( \#P \)) Proper subtraction(\( \Theta \)), integer division(\( \div \)) and span, for some \( k \geq 2 \), are \( \#P \)-hard for \( \#P \) randomly on \( N \).

**Corollary 3.7** \( \#P \) is closed under composition with \( \#P \) randomly.

**Proof of Theorem 3.4** \( \#P \subseteq \overline{B^P}.UP \) implies that \( \mathcal{C}_e \mathcal{C}_e P \subseteq \overline{B^P}.C.e. UP \subseteq \overline{B^P}.C.P \subseteq \overline{B^P}.UP \), using Proposition 3.3. Iterating this process gives \( \forall k(\mathcal{C}_e \mathcal{C}_e \mathcal{C}_e P \subseteq \overline{B^P}.UP) \).

**Proof of Theorem 3.5** Let \( e \) be a polynomial and \( f \in \#P \) (witnessed by NTM \( M_f \)) be a \( k \)-ary function. Let \( g_1, g_2, \ldots, g_k \in \#P \) be witnessed by NTMs \( M_1, M_2, \ldots, M_k \), time bounded by polynomials \( p_1, p_2, \ldots, p_k \), respectively.

Now define the following languages as graphs of the functions \( g_1, g_2, \ldots, g_k \):

\[
L_i = \{(x,y) | y = g_i(x)\}, \text{ for } i = 1, 2, \ldots, k
\]

**Claim 1:** \( L_i \in \#P, \text{ for } i = 1, 2, \ldots, k. \)

**Proof.** The following NTM \( M_i \) accepts \( L_i \).

1. Input \( (x,y) \). Assume that \( 0 \leq y \leq 2^{e(|z|)} \).

2. Guess \( b \in \{0,1\} \).

3. if \( b = 0 \) then simulate \( M_i \) on \( x \). \( M_i^* \) accepts if \( M_i \) accepts.
4. if $b = 1$ then guess $l \in \{0, 1, 2, \ldots, 2^{|l_1|}\}$.
   If $y \leq l$ then reject else accept.

Note that $\text{Acc}(M^*_f, (x, y)) = 2^{|l_1|} \iff y = g_i(x) \iff x \in L_i$. □

Now, under our hypothesis, each $L_i \in \overline{BPP}$. Choose a polynomial $e^*$ such that

\[ (1 - \frac{1}{2^{|l_1|}}) \geq (1 - \frac{1}{2^{|l_1|}}) \text{ or } 2^{e^*(n)} \geq \frac{2^{|l_1|}}{e} \text{, for all } n. \]

Then, there exists a set $A; \in \overline{UP}$, and a polynomial $b$ such that for all $x$,

\[ \text{Prob}((x, y) \#w \in A_i \iff (x, y) \in L_i) \geq 1 - \frac{1}{2^{e^*(|l_1|)}}. \]

Let NTM $M_{A_i}$ accept the set $A_i \in \overline{UP}$. Thus,

\[ \text{Prob}(x, y) \#w \in A_i \iff (x, y) \in L_i \geq 1 - \frac{1}{2^{e^*(|l_1|)}}. \]

where $w \in \{0, 1\}^{b(|(x, y)|)}$ is chosen uniformly.

Now we construct a NTM $M$ such that $\text{Acc}(M, x \#w) = f(g_1(x), \ldots, g_k(x))$, with error probability less than $\frac{1}{2^{e^*(|l_1|)}}$. Choose a polynomial $b(n)$ such that $b(|x|) \geq \max_{1 \leq i \leq k} b_i(|(x, 1^{b(n)}|))$ and let $w \in \{0, 1\}^{b(|l_1|)}$ be selected uniformly.

NTM $M$

1. Input $x \#w$.
2. Guess $y_i \in \{0, 1, 2, \ldots, 2^{|l_1|}\}$, for each $i = 1, 2, \ldots, k$.
3. Let $w_i$ = prefix of $w$ such that $|w_i| = b_i(|(x, y_i)|)$.
4. Simulate NTM $M_{A_i}$ on $(x, y_i) \#w_i$ sequentially, for each $i = 1, 2, \ldots, k$.
5. If any $M_{A_i}$ rejects then $M$ rejects and halts.
6. If for every $i = 1, 2, \ldots, k$, $M_{A_i}$ accepts, then $M$ simulates $M_f$ on $(y_1, y_2, \ldots, y_k)$ and accepts iff $M_f$ accepts.

Claim 2:

\[ \text{Prob}(\text{Acc}(M, x \#w) = f(g_1(x), \ldots, g_k(x))) \geq 1 - \frac{1}{2^{e^*(|l_1|)}} \text{ where, } w \in \{0, 1\}^{k|l_1|} \text{ is chosen uniformly.} \]

Proof. Due to our choice of $b$, for all $i, 1 \leq i \leq k$ and for each $y$ we have,

\[ \text{Prob} \left( (x, y) \in L_i \iff \text{Acc}(M_{A_i}, (x, y) \#w) = 1 \right) \geq 1 - \frac{1}{2^{e^*(|l_1|)}} \]

or,

\[ \text{Prob} \left( \bigwedge_{i=1}^{k} \left( (x, y) \in L_i \iff \text{Acc}(M_{A_i}, (x, y) \#w) = 1 \right) \right) \geq 1 - \frac{1}{2^{k e^*(|l_1|)}} \]

where, $w \in \{0, 1\}^{k|l_1|}$ is chosen uniformly.

Let $w \in \{0, 1\}^{b(|l_1|)}$ be such that the conjunctive condition holds. The probability of choosing such a $w$ is at least $1 - \frac{1}{2^{e^*(|l_1|)}}$. For such a $w$, the conjunctive condition implies that on an incorrect guess $y_i \neq g_i(x)$, for some $i$, each computation of $M_{A_i}$ rejects, and hence $M$ rejects and halts (at step 5 of NTM $M$). On the other hand, on the unique path corresponding to the correct guesses, $y_i = g_i(x)$, for all $i$, $\text{Acc}(M_{A_i}, (x, y_i) \#w) = 1$. Hence, for a correct guess $w$, there is exactly one path of NTM $M$ (at Step 6) that accepts and simulates $M_f$ with all the correct guesses $y_i = g_i(x), 1 \leq i \leq k$. This proves our claim. □

[\iff] If #P is closed under #P, then it is surely closed under proper subtraction. We will show that this implies $\mathbb{C}_{\overline{P}} \subseteq \overline{BPP}$.

Let $L \in \mathbb{C}_{\overline{P}}$. By Proposition 2.6 there exists a NTM $M$ and a polynomial $p$ such that

\[ x \in L \iff \text{Acc}(M, x) = 2^{p(|l_1|)} \]
Let \( g_1(x) = \text{Acc}(M, x) \in \#P \) and \( g_2(x) = 2^{2\lceil |x| \rceil} - 1 \). Note that \( x \in L \iff g_1(x) \land g_2(x) = 1 \) and \( x \not\in L \iff g_1(x) \lor g_2(x) = 0 \). Under our hypothesis, for each polynomial \( e \), there exists a \( h \in \#P \) and a polynomial \( b \) such that,

\[
\text{Prob}(h(x \# w) = g_1(x) \land g_2(x)) \geq 1 - \frac{1}{2^{e(|x|)}}
\]

where, \( w \in \{0, 1\}^{k(|x|)} \) is chosen uniformly.

Then, for a correct choice of \( w \), we have \( h(x \# w) = 1 \iff x \in L \) and \( h(x \# w) = 0 \iff x \not\in L \). Let \( A = \{x \# w | h(x \# w) = 1\} \). Then \( A \subseteq \text{UP} \).

Thus, for all \( e \), there exists \( A \subseteq \text{UP} \) and a polynomial \( b \) such that

\[
\text{Prob}(x \# w \in A \iff x \in L) \geq 1 - \frac{1}{2^{e(|x|)}}
\]

This completes the proof of the theorem. \( \square \)

**Proof of Theorem 3.6** We will show that if \( \#P \) is closed under composition with proper subtraction, integer division, or \( \text{span}_k \), for some \( k \geq 2 \), randomly, then \( \text{QP} \subseteq \text{BP} \cdot \text{UP} \). This together with Theorem 3.5 proves the theorem.

As part of the proof of Theorem 3.5 we have already shown that if \( \#P \) is closed under composition with proper subtraction randomly, then \( \#P \subseteq \text{BP} \cdot \text{UP} \). The proof that integer division is \( \#P \)-hard for \( \#P \) randomly, is quite similar to that of proper subtraction; just take \( g_2(x) = 2^{2\lceil |x| \rceil} \).

Now we show that \( \text{span}_k \), \( k \geq 2 \), is randomly hard for \( \#P \). Let \( L \subseteq \text{QP} \). Then by Proposition 2.6, there exists a NTM \( M \) and a polynomial \( p \) such that

\[
x \in L \iff \text{Acc}(M, x) = 2^{p(|x|)}
\]

\[
x \not\in L \iff \text{Acc}(M, x) < 2^{p(|x|)}
\]

Let \( g_1(x) = 2 \cdot \text{Acc}(M, x) \), \( g_2(x) = 2^{p(|x|)} + \text{Acc}(M, x) \), \( g_i(x) = g_2(x) \), for \( i = 3, \ldots, k \).

Then, \( g_1(x) = g_2(x) = 2^{2\lceil |x| \rceil} \iff \text{Acc}(M, x) = 2^{2\lceil |x| \rceil} \iff x \in L \). Thus,

\[
x \in L \iff \mathbf{span}(g_1(x), \ldots, g_k(x)) = 1
\]

\[
x \not\in L \iff \mathbf{span}(g_1(x), \ldots, g_k(x)) = 2
\]

Under our hypothesis, for all polynomials \( e \), there exists a NTM \( M^* \), a polynomial \( b_1 \), and \( h_1 \in \#P \) such that,

\[
\text{Prob}(h_1(x \# w_1) = \mathbf{span}_k(g_1(x), \ldots, g_k(x))) \geq 1 - \frac{1}{2^{e(|x|)}}
\]

or,

\[
\text{Prob}(x \in L \iff h_1(x \# w_1) = 1) \geq 1 - \frac{1}{2^{e(|x|)}}
\]

where, \( w_1 \in \{0, 1\}^{b_1(|x|)} \) is chosen uniformly.

Again using the hypothesis, there exists a polynomial \( b_2 \) and \( h \in \#P \) such that,

\[
\text{Prob}(h(x \# w_1 \# w_2) = \mathbf{span}(h_1(x \# w_1), 2)) \geq 1 - \frac{1}{2^{e(|x|)}}
\]

where, \( w_2 \in \{0, 1\}^{b_2(|x| \# w_1)} \) is chosen uniformly.

Note that, \( h(x) = 1 \iff h_1(x) = 2 \) and \( h(x) = 2 \iff h_1(x) = 1 \). Let \( b(n) = b_1(n) + b_2(n + b_1(n)) \).

Thus,

\[
\text{Prob}(x \not\in L \iff h(x \# w_1 \# w_2) = 1) \geq (1 - \frac{1}{2^{e(|x|)}})^2
\]

where \( w_1 w_2 \in \{0, 1\}^{b(|x| \# w_1)} \).

Let \( h \in \#P \) be witnessed by NTM \( M^* \). Now, construct \( M^{**} \), which guesses two computations of \( M^* \) and accepts if both the computations accept. Let \( A = \{x \# w_1 \# w_2 | \text{Acc}(M^{**}, x \# w_1 \# w_2) = 1\} \). Then

\[
52
\]
A ∈ UP. Thus, for all e, there exists A ∈ UP and a polynomial b such that

\[ \text{Prob}(x \# w / A \Rightarrow x \in L) \geq (1 - \frac{1}{2^{m[l][l]}})^2 \]

where \( w_1 w_2 \in \{0,1\}^{4[l][l]} \) is chosen uniformly. Choosing an appropriate e completes the proof.

As an additional comment we note that the class \( \overline{BP}.UP \) is the only class we are aware of that lies between \( BPP \) and \( PP \). Clearly, it lies in the \( PH \), using quantifier simulation [11].

4 Witness reduction in \( Z#P \) and \( Q#P \)

In this section we first ask the question: what makes subtraction a hard function for \#P? To this end, we define a class \( Z#P \), which is very similar to \#P, except that it is closed under composition with subtraction. Does this imply that \( Z#P \) is closed under composition with \( Z#P \)? Not really, because subtraction in \( Z#P \) does not reduce witnesses. However, proper subtraction, as well as integer division, reduces witnesses even in \( Z#P \), and hence turn out to be \( Z#P \)-hard for \( Z#P \).

Next, we ask the question: what makes division a hard function for \#P and \( Z#P \)? We define a class \( Q#P \), which is similar to \( Z#P \) and \#P, except that it is closed under composition with division. However, integer division, which again reduces witnesses in \( Q#P \), turns out to be \( Q#P \)-hard for \( Q#P \). These examples provide more evidence for the thesis that it is the ability of a function to interact with a class of functions to effect witness reduction is what makes functions hard.

4.1 Definitions and preliminaries

We repeat the definitions of \#P etc. to make comparisons with the new classes \( Z#P \) and \( Q#P \).

Definition 4.1

1. A function \( f : \Sigma^* \rightarrow \mathbb{N} \) is in \#P iff there exists a polynomial time-bounded nondeterministic machine \( M \) such that for all \( x \), \( f(x) = \text{Acc}(M, x) \).

2. A function \( f : \Sigma^* \rightarrow \mathbb{Z} \) is in \( Z#P \) iff there exists a polynomial time-bounded nondeterministic machine \( M \) such that for all \( x \), \( f(x) = \frac{\text{AR}(M^d, x)}{\text{AR}(M^d, x)} \).

3. A function \( f : \Sigma^* \rightarrow \mathbb{Q} \) is in \( Q#P \) iff there exists a pair of polynomial time-bounded nondeterministic machines \( (M^n, M^d) \) such that for all \( x \), \( f(x) = \frac{\text{AR}(M^n, x)}{\text{AR}(M^d, x)} \).

Definition 4.2

1. A language \( L \in \mathbb{C}_P \) iff there exists a function \( f \in PF, f : \Sigma^* \rightarrow \mathbb{N} \), and \( g \in \#P \) such that, for all \( x \), \( x \in L \Leftrightarrow g(x) = f(x) \).

2. A language \( L \in \mathbb{Z}_P \) iff there exists a function \( f \in PF, f : \Sigma^* \rightarrow \mathbb{Z} \), and \( g \in \#P \) such that, for all \( x \), \( x \in L \Leftrightarrow g(x) = f(x) \).

3. A language \( L \in \mathbb{Q}_P \) iff there exists a function \( f \in PF, f : \Sigma^* \rightarrow \mathbb{Q} \), and \( a \in \#P \) such that, for all \( x \), \( x \in L \Leftrightarrow g(x) = f(x) \).

Definition 4.3

1. A language \( L \in \text{UP} \) iff there exists a \( g \in \#P \) such that, for all \( x \), \( x \in L \Leftrightarrow g(x) = 1 \) and \( x \notin L \Leftrightarrow g(x) = 0 \).

2. A language \( L \in \text{ZUP} \) iff there exists a \( g \in \#P \) such that, for all \( x \), \( x \in L \Leftrightarrow g(x) = 1 \) and \( x \notin L \Leftrightarrow g(x) = 0 \).
3. A language \( L \in \mathbb{Q}UP \) if there exists a \( g \in \mathbb{Q}\#P \) such that, for all \( x, x \in L \iff g(x) = 1 \) and \( x \notin L \iff g(x) = 0 \).

Note that it is possible to redefine any class of languages, originally defined in terms of number of accepting paths of a NTM, under a new domain of interpretation - integers or rational numbers - as above. For example, \( ZNP \) is the class of languages such that there exists a \( g \in \mathbb{Z}\#P \) such that \( x \in L \iff g(x) > 0 \) and \( x \notin L \iff g(x) = 0 \).

The definition of the class \( C_\varepsilon P \) is slightly different from the standard one; however, both definitions yield the same class. Also, note that the class \( \mathbb{Z}\#P \) is same as the class GapP defined by Fenner, Fortnow and Kurtz [2].

The following propositions can be easily proved from the definitions.

**Proposition 4.4**

1. \( \#P \subseteq \mathbb{Z}\#P \subseteq \mathbb{Q}\#P \).
2. \( p\#P = p\mathbb{Z}\#P = p\mathbb{Q}\#P \).
3. \( C_\varepsilon P \subseteq Z_\varepsilon P \subseteq Q_\varepsilon P \).
4. \( UP \subseteq \mathbb{Z}UP \subseteq \mathbb{Q}UP \).

**Proposition 4.5**

1. \( [9] \#P \) is closed under composition with addition and multiplication (on \( N \)).
2. \( \mathbb{Z}\#P \) is closed under composition with addition, multiplication and subtraction (on \( Z \)).
3. \( \mathbb{Q}\#P \) is closed under composition with addition, multiplication, subtraction and division (by a non-zero \( \mathbb{Q}\#P \) function)/(Q).

We outline the proof of the following proposition.

**Proposition 4.6**

1. \( Z_\varepsilon P = Q_\varepsilon P \).
2. \( C_\varepsilon \mathbb{Z}UP \subseteq Z_\varepsilon P \).

3. Let \( L \in Z_\varepsilon P = Q_\varepsilon P \). Then, there exists a NTM \( M \) and a polynomial \( p \) such that, for all \( x, x \in L \iff AR(M, x) = 2^{p(|x|)} \) and \( x \notin L \iff 0 \leq AR(M, x) < 2^{p(|x|)} \).

**Proof.**

1. The left to right containment is obtained by taking the denominator NTM for \( Q_\varepsilon P \) to have exactly one accept on all inputs. To see that \( Q_\varepsilon P \subseteq Z_\varepsilon P \), note that \( L \in Q_\varepsilon P \) if there exists a \( g \in \mathbb{Q}\#P \) such that, \( x \in L \iff g(x) = 0 \), as \( \mathbb{Q}\#P \) is closed under composition with subtraction. Let \( g \in \mathbb{Q}\#P \) be witnessed by the pair of NTM \( (M^n, M^d) \). The numerator NTM \( M^n \) witnesses \( L \in Z_\varepsilon P \) using a threshold of 0.

2. Let \( L \in \mathbb{C}_\varepsilon \mathbb{Z}UP \). Then there exists a set \( A \in \mathbb{Z}UP \), and a polynomial \( p \in PF \), and a polynomial \( f \) such that \( x \in L \iff \|\{y \mid |y| = p(|x|), (x, y) \in A\}|| = f(x) \). Let \( A \) be accepted by a NTM \( M_A \). Then, \( (x, y) \in A \iff AR(M_A, (x, y)) = 1 \) and \( (x, y) \notin A \iff AR(M_A, (x, y)) = 0 \). Construct NTM \( M \) which, on input \( x \), guesses \( y \), \( |y| = p(|x|) \) and simulates \( M_A \) on \( (x, y) \). It is easy to see that, \( AR(M, x) = f(x) \iff x \in L \).

3. Let \( L \in Z_\varepsilon P \) be witnessed by a NTM \( M \), time bounded by a polynomial \( q \), and \( f \in PF \). Let \( h(x) = AR(M, x) \in \mathbb{Z}\#P \). As \( \mathbb{Z}\#P \) is closed under subtraction and multiplication, let \( h^*(x) = -(AR(M, x) - f(x))^2 + 2^{q(|x|)} \in \mathbb{Z}\#P \) be witnessed by NTM \( M^* \). The NTM \( M^* \) has the required properties.

4.2 **Witness reduction in \( \mathbb{Z}\#P \)**
Theorem 4.7 (Witness reduction implies collapsing) \( Z_{\#}P \subset ZUP \Rightarrow CH = ZUP \).

Theorem 4.8 (Closure iff witness reduction) \( Z_{\#}P \subseteq ZUP \Leftrightarrow Z_{\#}P \text{ is closed under composition with } Z_{\#}P \).

Theorem 4.9 (Hard functions for \( Z_{\#}P \)) Proper subtraction(\( \ominus \)), integer division(\( \div \)) and spank, \( k_2 \), \( k_1 \), are \( Z_{\#}P \)-hard for \( Z_{\#}P(Z) \).

Corollary 4.10 (to Theorem 4.9) \( Z_{\#}P \) is closed under composition with \( Z_{\#}P \).

Proof of Theorem 4.7 \( Z_{\#}P \subset ZUP \) implies that \( C_{\#}L \subset C_{\#}P \subset C_{\#}L_{\#} \subset C_{\#}L \subset ZUP \), using Propositions 4.6. Iterating this process it is easy to prove that \( C_{\#}L_{\#} \subset^{k} ZUP \), \( k \geq 1 \). \( \Box \)

Proof of Theorem 4.8 \( \leftarrow \) Let \( L \in Z_{\#}P \). Then by Proposition 4.6 there exists a NTM \( M \) and a polynomial \( p \) such that
\[
\begin{align*}
x \in L \Leftrightarrow & AR(M, x) = 2^p(|x|) \\
x \notin L \Leftrightarrow & 0 \leq AR(M, x) < 2^p(|x|)
\end{align*}
\]
Let \( g_1(x) = AR(M, x) \) and \( g_2(x) = 2^p(|x|) \). Under the hypothesis, since integer division is a \( Z_{\#}P \)-function, there exists \( h \in Z_{\#}P \) such that \( h(x) = [g_1(x)/g_2(x)] \). Thus,
\[
\begin{align*}
x \in L \Leftrightarrow & h(x) = 1 \\
x \notin L \Leftrightarrow & h(x) = 0.
\end{align*}
\]
Hence, \( h \in Z_{\#}P \) witnesses that \( L \in ZUP \).

\( \Rightarrow \) Let \( f \in Z_{\#}P \) be a \( k \)-ary function witnessed by NTM \( M_f \). Let \( g_1, g_2, \ldots, g_k \in Z_{\#}P \) be witnessed by NTMs \( M_1, M_2, \ldots, M_k \), each polynomial time bounded by \( p_1, p_2, \ldots, p_k \), respectively. Define the following languages as graphs of the above functions.
\[
L_i = \{(x, y) | y = g_i(x) = AR(M_i, x)\}, 1 \leq i \leq k.
\]

Claim 1: \( L_i \in Z_{\#}P \)

Proof: The following NTM \( M_i^* \) accepts \( L_i \).

1. Input \( \langle x, y \rangle \). We assume that \( -2^p(|x|) \leq y \leq 2^p(|x|) \).
2. Guess \( b \in \{0, 1\} \).
3. If \( b = 0 \) then \( M_i^* \) simulates \( M_i \) on \( x \) and accepts iff \( M_i \) accepts.
4. If \( b = 1 \) then \( M_i^* \) nondeterministically branches into a tree with (number of accepts - number of rejects) equal to \( -y \).

Note that \( AR(M_i^*, \langle x, y \rangle) = 0 \Leftrightarrow y = AR(M_i, x) \Leftrightarrow \langle x, y \rangle \in L_i \). Hence, \( L_i \in Z_{\#}P \).

Under our hypothesis, there exists a NTM \( M_{i^*}, 1 \leq i \leq k \) such that
\[
\begin{align*}
\langle x, y \rangle \in L_i & \Leftrightarrow AR(M_{i^*}, \langle x, y \rangle) = 1 \\
\langle x, y \rangle \notin L_i & \Leftrightarrow AR(M_{i^*}, \langle x, y \rangle) = 0
\end{align*}
\]

Now we construct NTM \( M \) which witnesses that \( f(g_1, g_2, \ldots, g_k) \in Z_{\#}P \).

NTM \( M \)

1. Input \( x \).
2. Guess \( y_i, -2^p(|x|) \leq y_i \leq 2^p(|x|), 1 \leq i \leq k \).
3. Run \( M_{i^*} \) on \( \langle x, y_i \rangle, 1 \leq i \leq k \), sequentially. This follows some computations \( C_1, C_2, \ldots, C_k \), where \( C_i \) is a computation of \( M_{i^*} \) on \( \langle x, y_i \rangle \).
4. Run \( M_f \) on \( \langle y_1, y_2, \ldots, y_k \rangle \) following a final computation \( C_{k+1} \).
5. The computation \( C_1, C_2, \ldots, C_k, C_{k+1} \) of \( M \) accepts iff an even number of \( C_1, C_2, \ldots, C_k, C_{k+1} \) reject.
It is not difficult to see that
\[ AR(M, x) = \sum_{y_1, y_2, \ldots, y_k} [AR(M_i^{**}, (x, y_1)) \cdots AR(M_k^{**}, (x, y_k))] \]
where the sum is taken over all the guesses \( y_1, y_2, \ldots, y_k \). This is because each \( C_i \) that accepts contributes a +1 in \( AR(M_i^{**}, (x, y)) \) and each \( C_i \) that rejects contributes a -1 in \( AR(M_i^{**}, (x, y)) \).

By the definition of \( M_i^{**} \), the above product is 0 if any one guess \( y_i \neq g_i(x) \). Also, \( AR(M_i^{**}, (x, y)) = 1 \) if \( y = g_i(x) \). Hence,
\[ ANM, 2) = \sum_{y_1, y_2, \ldots, y_k} AR(M_f, (y_1, y_2, \ldots, y_k)) \]
where the sum is taken over all the guesses \( y_1, y_2, \ldots, y_k \).

The running time of NTM \( M \) is bounded by some polynomial.

Proof of Theorem 4.9 We show that closure of \( \text{ZC} \) under composition with proper subtraction, integer division and \( \text{span} \), \( k \geq 2 \), is \( \text{hard} \) for \( \text{ZC} \).

Let \( L \in \text{ZC} \). Hence, there exists a \( g \in \text{ZC} \) and a polynomial \( p \) such that \( z \in L \iff g(z) = 2^{p(|z|)} \) and \( z \notin L \iff 0 \leq g(z) < 2^{p(|z|)} \). Let \( g_1(z) = 2^{p(|z|)} - 1 \). Then, under the hypothesis, \( h = g_1 g_2 \in \text{ZC} \) and \( z \in L \iff h(z) = 1 \) and \( z \notin L \iff h(z) = 0 \). Thus, \( L \in \text{ZUP} \). This shows that proper subtraction is hard for \( \text{ZC} \).

Given \( L \in \text{ZC} \), as \( \text{ZC} \) is closed under subtraction, there exists a \( g \in \text{ZC} \) such that \( x \in L \iff g(x) = 0 \). Let \( g_i(x) = 2^{p(|z|)} - 1 \). Then, under the hypothesis, \( h \in \text{ZC} \), such that \( h(x) = \text{span} g_1, g_2, \ldots, g_k \). Hence, \( x \in L \iff h(x) = 1 \) and \( x \notin L \iff h(x) = 0 \). Thus, \( L \in \text{ZUP} \). This shows that integer division is hard for \( \text{ZC} \).

4.3 Witness reduction in \( \text{Q} \)

Theorem 4.11 (Closure iff witness reduction) \( \text{Q} \subseteq \text{QUP} \iff \text{Q} \) is closed under composition with \( \text{Q} \).

Theorem 4.12 (Hard functions for \( \text{Q} \))
Proper subtraction(\( - \)), integer division(\( + \)) and \( \text{span} \), \( k \geq 2 \), are \( \text{hard} \) for \( \text{Q} \) (on \( Q \)).

Corollary 4.13 (To Theorem 4.12) \( \text{Q} \) is closed under composition with \( \text{Q} \) and \( \text{Q} \) is closed under composition with \( \text{PF} \).

Proof of Theorem 4.11 \([\iff]\) Let \( L \in \text{Q} \). Then, by Proposition 4.6, there exists a NTM \( M \) and a polynomial \( p \) such that
\[ x \in L \iff AR(M, x) = 2^{p(|z|)} \]
\[ x \notin L \iff 0 \leq AR(M, x) < 2^{p(|z|)} \]

Let \( g_1(x) = AR(M, x) \) and \( g_2(x) = 2^{p(|z|)} \).

Let \( g_1(x) \) be a \( k \)-ary function, witnessed by a NTM pair \( (M_1, M_2) \). Let \( g_1, g_2, \ldots, g_k \in \text{Q} \) be witnessed by NTM pairs \( (M_1, M_2), (M_3, M_4), \ldots, (M_{2k}, M_{2k+1}) \), respectively, each polynomial time bounded. Define the following languages as graphs of the above functions:
\[ L_i = \{(x, y) \mid y = g_i(x) = AR(M_i, x)\}, 1 \leq i \leq k \]
Then, as shown before in Theorem 4.8 (Claim 1), each $L_i \in \mathbb{Z}_2 \mathbb{P}$.

Under our hypothesis, $\mathbb{Z}_2 \mathbb{P} = \mathbb{Q}_2 \mathbb{P} \subseteq \mathbb{Q}_{UP}$, there exists NTM pairs $(\hat{M}^n_i, \hat{M}^d_i)$, $1 \leq i \leq k$, each polynomial time bounded by $(p_1^n, p_1^d), (p_2^n, p_2^d), \ldots, (p_k^n, p_k^d)$, such that,

$$(x, y) \in L_i \iff \frac{AR(\hat{M}^n_i, x)}{AR(\hat{M}^d_i, x)} = 1$$

$$(x, y) \notin L_i \iff AR(\hat{M}^n_i, x) = 0$$

Now we construct NTM $(M^n, M^d)$ which witness that $f(g_1, g_2, \ldots, g_k) \in \mathbb{Q}_{#P}$.

**NTM $M^n$ [and $M^d$]**

1. Input $x$.
2. Guess $y_i = \frac{y_i}{d_i} - 2^{n_i - |y_i|} \leq n_i \leq 2^{n_i - |y_i|}, 1 \leq d_i \leq 2^{n_i - |y_i|}, 1 \leq i \leq k$ (Note that it is possible to guess multiple $y_i$). If $n_i$ and $d_i$ are not relatively prime for some $i$, then guess $b \in \{0, 1\}$ and accept on $b = 1$ and reject on $b = 0$.
3. Run $\hat{M}^n_i[\hat{M}^d_i]$ on $(x, y_i), 1 \leq i \leq k$, sequentially. This follows some computations $C_1, C_2, \ldots, C_k$, where $C_i$ is a computation of $\hat{M}^n_i$ on $(x, y_i)$.
4. Run $M^n_i[M^d_i]$ on $(y_1, y_2, \ldots, y_k)$ following a final computation $C_{k+1}$.
5. The computation $C_1, C_2, \ldots, C_k, C_{k+1}$ of $M^n[M^d]$ accepts iff an even number of $C_1, C_2, \ldots, C_k, C_{k+1}$ reject.

It is not difficult to see that

$$AR(M^n, x) = \sum_{y_1, y_2, \ldots, y_k} [AR(\hat{M}^n_i, (x, y_i)) \ldots AR(\hat{M}^n_k, (x, y_k))] AR(\hat{M}^d_i, (y_1, y_2, \ldots, y_k))$$

and

$$AR(M^d, x) = \sum_{y_1, y_2, \ldots, y_k} [AR(\hat{M}^n_i, (x, y_i)) \ldots AR(\hat{M}^n_k, (x, y_k))] AR(\hat{M}^d_i, (y_1, y_2, \ldots, y_k))$$

where the sum is taken over all the guesses $y_1, y_2, \ldots, y_k$. This is because each $C_i$ that accepts contributes a $+1$ in $AR(\hat{M}^n_i, (x, y))$ and each $C_i$ that rejects contributes a $-1$ in $AR(\hat{M}^d_i, (x, y))$ and similarly for $\hat{M}^d_i$. Multiple guesses of $y_i$'s do not contribute to the value of $AR(M^n, x)$ or $AR(M^d, x)$.

By the definition of $\hat{M}^n_i$, the above product is $0$ if any one guess $y_i \neq g_i(x)$. Hence,

$$AR(M^n, x) = AR(\hat{M}^n_i, (x, y_1)) AR(\hat{M}^n_i, (x, y_2)) \ldots AR(\hat{M}^n_i, (x, y_k)) AR(\hat{M}^d_i, (y_1, y_2, \ldots, y_k))$$

and

$$AR(M^d, x) = AR(\hat{M}^n_i, (x, y_1)) AR(\hat{M}^n_i, (x, y_2)) \ldots AR(\hat{M}^n_i, (x, y_k)) AR(\hat{M}^d_i, (y_1, y_2, \ldots, y_k))$$

with the correct guesses $y_i = g_i(x)$ and $AR(\hat{M}^n_i, (x, y_i)) \neq 0, 1 \leq i \leq k$. Thus, $\frac{AR(M^n, x)}{AR(M^d, x)} = \frac{AR(\hat{M}^n_i, (y_1, y_2, \ldots, y_k))}{AR(\hat{M}^d_i, (y_1, y_2, \ldots, y_k))} = f(g_1(x), \ldots, g_k(x))$. Also, the running time of NTM $M$ is bounded by some polynomial.

**Proof of Theorem 4.12** We show that closure of $\mathbb{Q}_{#P}$ under composition with proper subtraction, integer division and span implies that $\mathbb{Q}_{CP} \subseteq \mathbb{Q}_{UP}$. Hence, by Theorem 4.11, we are done.

The proof for integer division was done as part of Theorem 4.11. The proof for proper subtraction is very similar, take $g_2(x) = 2^{n(|y|)} - 1$.

Given $L \in \mathbb{Q}_{CP} = \mathbb{Z}_{2} \mathbb{P}$, as $\mathbb{Z}_{2} \mathbb{P}$ is closed under subtraction, there exists a $g \in \mathbb{Z}_{2} \mathbb{P}$ such that $x \in L \iff g(x) = 0$. Let $g_i(x) = 2.g(x), 2 \leq i \leq k$. Then, under the hypothesis, there exists $h \in \mathbb{Q}_{#P}$, such that $h(x) = span_{k}(g(x), g_2(x), \ldots, g_k(x))$. Hence, $x \in L \iff h(x) = 1$ and $x \notin L \iff h(x) = 2$. Again, as $\mathbb{Q}_{#P}$ is closed under subtraction, $h^*(x) = 2 - h(x) \in \mathbb{Q}_{#P}$. Now, $x \in L \iff h^*(x) = 1$ and $x \notin L \iff h^*(x) = 0$ or, $L \in \mathbb{Q}_{UP}$. □
5 Random witness reduction in \( Z\#P \) and \( Q\#P \)

In the previous sections we studied random witness reduction in \( #P \) and then witness reduction in \( Z\#P \) and \( Q\#P \). The concept of random witness reduction in \( Z\#P \) and \( Q\#P \) is analogous to that of random witness reduction in \( #P \). For example, we can talk about closure of these function classes under composition with high probability, or, randomly hard functions for \( Z\#P \) and \( Q\#P \). Thus, the general definitions given in Section 3 can be applied to these new function classes.

Using the techniques of the sections 3 and 4, it is easy to see the results in this section. We obtain corresponding collapses and closures with high probability. This is a weaker form of witness reduction - hence it produces weaker collapses.

Theorem 5.1 (Random witness reduction implies collapsing) \( Z\#P \subseteq B\P \cdot Z\UP \Rightarrow CH = B\P \cdot Z\UP \).

Theorem 5.2 (Random closure iff random witness reduction) \( Z\#P \subseteq B\P \cdot Z\UP \Leftrightarrow Z\#P \) is closed under composition with \( Z\#P \) randomly.

Theorem 5.3 (Randomly hard functions for \( Z\#P \)) Proper subtraction(\( \ominus \)), integer division(\( \div \)) and span\(_k\), for some \( k \geq 2 \), are \( Z\#P \)-hard for \( Z\#P \) randomly (on \( Z \)).

Corollary 5.4 \( Z\#P \) is closed under composition with \( Z\#P \) randomly \( \Leftrightarrow Z\#P \) is closed under composition with \( PF \) randomly.

Theorem 5.5 (Random closure iff random witness reduction) \( Q\#P \subseteq Z\P \cdot Q\UP \Leftrightarrow Q\#P \) is closed under composition with \( Q\#P \) randomly.

Theorem 5.6 (Randomly hard functions for \( Q\#P \)) Proper subtraction(\( \ominus \)), integer division(\( \div \)) and span\(_k\), for some \( k \geq 2 \), are \( Q\#P \)-hard for \( Q\#P \) randomly (on \( Q \)).

Corollary 5.7 \( Q\#P \) is closed under composition with \( Q\#P \) randomly \( \Leftrightarrow Q\#P \) is closed under composition with \( PF \) randomly.

6 Concluding Remarks

One of the motivations for defining new domains(\( Z, Q \)) for interpretation of functions computed by NTMs was to study the reasons for existence of hard functions. However, as stated before, any class that is originally defined in terms of number of accepting paths of a NTM can be redefined, under a new interpretation. We believe that this is of independent interest. We have several interesting relations between classes defined in this fashion, which were not stated here as they are irrelevant to the theme of this paper. It remains to be seen if the enrichment of nondeterministic complexity classes, provided by these new domains, will bring us any closer to the goals of complexity theory.

Acknowledgements I am grateful to Timothy J. Long for scrutinizing the preliminary drafts of the paper, and more importantly, for his constant guidance and support.

References


port 90-32, University of Chicago, Department of Computer Science, Chicago, IL, November 1990.


