[Sch89] U. Schöning. Probabilistic Complexity Classes and Lowness. *Journal of Computer and System Sciences*, 39:84-100, 1989.

[Sim75] J. Simon. *On some central problems in Computational Complexity.* Ph.D. thesis. Cornell University, Ithaca, NY, January 1975. Available as Cornell Department of Computer Science Technical Report, TR 75-224.

[Tod89] S. Toda. On the computational power of PP and $\oplus P$. In *The Proceedings of the 30th Annual IEEE Symposium on Foundations of Computer Science*, pages 514-519, 1989.

[TO90] S. Toda and M. Ogiwara. Counting classes are at least as hard as the polynomial-time hierarchy. Manuscript, July, 1990.

[Tor88] J. Torán. *Structural Properties of the Counting Hierarchies.* Ph.D. thesis, Universitat Politècnica de Catalunya, Barcelona, Spain, 1988.

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

References

[BRS90] R. Beigel, N. Reingold and D. Spielman. PP is closed under intersection. Technical Report YALEU/DCS/TR-803, Yale University, Department of Computer Science, New Haven, CT, June 1990.

[FFK90] S. Fenner, L. Fortnow, and S. Kurtz. Gap-definable counting classes. Technical Report 90-32, University of Chicago, Department of Computer Science, Chicago, IL, November 1990.

[FR90] L. Fortnow and N. Reingold. PP is closed under truth-table reductions. Technical Report 90-30, University of Chicago, Department of Computer Science, Chicago, IL, September, 1990.

[Gup90] S. Gupta. A note on the Counting hierarchy. Technical Report, The Ohio State University, Department of Computer and Information Sciences, OSU-CISRC-8/90-TR24, 1990.

[Gup91] S. Gupta. New domains of interpretation for nondeterministically defined complexity classes. (In preparation)

[OH90] M. Ogiwara and L.A. Hemachandra. A complexity theory for closure properties. Technical Report C-99, Tokyo Institute of Technology, 1990. To appear in Structure in Complexity Theory Conference.

[PZ83] C. Papadimitriou and S. Zachos. Two remarks on the power of counting. In *Proceedings 6th GI Conference on Theoretical Computer Science*, pages 269-276. Springer-Verlag *Lecture Notes in Computer Science # 145*, 1983.

[Reg82] K. Regan. Enumeration problems. Manuscript, 1982.

[RR90] K. Regan and J.S. Royer. A simpler proof of $PH \subseteq BP[\oplus P]$. Manuscript, August, 1990.

6 Concluding Remarks

One of the motivations for defining new domains$(\mathcal{Z}, \mathcal{Q})$ 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.

Some results for these new interpretations of complexity classes that may be of immediate interest are the following (slightly stronger) analogues of Toda and Ogiwara's [TO90] meta theorem:

Theorem 6.1 *Let K be any class of sets and let F be any function in $\mathcal{Z}$NUM.$\exists$.K. Then, for every polynomial e, there exist a function $H \in \mathcal{Z}\#\mathrm{P}^K$ and a polynomial b such that for all x, $Prob(w \in \{0,1\}^{b(|x|)} \mid H(x\#w) = F(x)) \geq 1 - \frac{1}{2^{e(|x|)}}$.*

Theorem 6.2 *Let K be any class of sets and let F be any function in $\mathcal{Q}$NUM.$\exists$.K. Then, for every polynomial e, there exist a function $H \in \mathcal{Q}\#\mathrm{P}^K$ and a polynomial b such that for all x, $Prob(w \in \{0,1\}^{b(|x|)} \mid H(x\#w) = F(x)) \geq 1 - \frac{1}{2^{e(|x|)}}$.*

These meta theorems can be used to produce "collapses" of PH into various counting classes. For example, using the above, it is easy to prove that $\mathcal{Z}\mathrm{CP}.PH \subseteq \widehat{BP}.\mathcal{Z}\mathrm{CP}$. These results, together with the proofs of the various propositions stated in this paper are studied in [Gup91].

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.

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 $\mathcal{Z}\#\mathrm{P}$ and $\mathcal{Q}\#\mathrm{P}$. 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) $\mathcal{Z}\mathrm{C}_{=}\mathrm{P} \subseteq \widehat{BP}.\mathcal{Z}\mathrm{UP} \Rightarrow CH = \widehat{BP}.\mathcal{Z}\mathrm{UP}$.

Theorem 5.2 (Random closure iff random witness reduction) $\mathcal{Z}\mathrm{C}_{=}\mathrm{P} \subseteq \widehat{BP}.\mathcal{Z}\mathrm{UP} \Leftrightarrow$ $\mathcal{Z}\#\mathrm{P}$ *is closed under composition with* $\mathcal{Z}\#\mathrm{P}$ *randomly.*

Theorem 5.3 (Randomly hard functions for $\mathcal{Z}\#\mathrm{P}$**)** *Proper subtraction*($\ominus$)*, integer division*($\div$) *and* $span_k$*, for some* $k \geq 2$*, are* $\mathcal{Z}\#\mathrm{P}$*-hard for* $\mathcal{Z}\#\mathrm{P}$ *randomly.*

Corollary 5.4 $\mathcal{Z}\#\mathrm{P}$ *is closed under composition with* $\mathcal{Z}\#\mathrm{P}$ *randomly* $\Leftrightarrow$ $\mathcal{Z}\#\mathrm{P}$ *is closed under compositiion with* PF *randomly.*

Theorem 5.5 (Random closure iff random witness reduction) $\mathcal{Q}\mathrm{C}_{=}\mathrm{P} \subseteq \widehat{BP}.\mathcal{Q}\mathrm{UP} \Leftrightarrow$ $\mathcal{Q}\#\mathrm{P}$ *is closed under composition with* $\mathcal{Q}\#\mathrm{P}$ *randomly.*

Theorem 5.6 (Randomly hard functions for $\mathcal{Q}\#\mathrm{P}$**)** *Proper subtraction*($\ominus$)*, integer division*($\div$) *and* $span_k$*, for some* $k \geq 2$*, are* $\mathcal{Q}\#\mathrm{P}$*-hard for* $\mathcal{Q}\#\mathrm{P}$ *randomly.*

Corollary 5.7 $\mathcal{Q}\#\mathrm{P}$ *is closed under composition with* $\mathcal{Q}\#\mathrm{P}$ *randomly* $\Leftrightarrow$ $\mathcal{Q}\#\mathrm{P}$ *is closed under compositiion with* PF *randomly.*

$AR(\hat{M}_i^n, \langle x, y \rangle)$. 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 $\hat{M}_i^n$, the above product is 0 if any one guess $y_i \neq g_i(x)$. Hence,

$$AR(M^n, x) = AR(\hat{M}_1^n, \langle x, y_1 \rangle).AR(\hat{M}_2^n, \langle x, y_2 \rangle) \ldots AR(\hat{M}_k^n, \langle x, y_k \rangle)AR(\hat{M}_f^n, \langle y_1, y_2, \ldots, y_k \rangle)$$

$$AR(M^d, x) = AR(\hat{M}_1^n, \langle x, y_1 \rangle).AR(\hat{M}_2^n, \langle x, y_2 \rangle) \ldots AR(\hat{M}_k^n, \langle x, y_k \rangle)AR(\hat{M}_f^d, \langle y_1, y_2, \ldots, y_k \rangle)$$

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

Proof of Theorem 4.12 We show that closure of $\mathcal{Q}\#\mathrm{P}$ under composition with proper subtraction, integer division and span implies that $\mathcal{Q}\mathrm{C}_{=}\mathrm{P} \subseteq \mathcal{Q}\mathrm{UP}$. 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 $g_2(x) = 2^{p(|x|)} - 1$.

Given $L \in \mathcal{Q}\mathrm{C}_{=}\mathrm{P} = \mathcal{Z}\mathrm{C}_{=}\mathrm{P}$, as $\mathcal{Z}\#\mathrm{P}$ is closed under subtraction, there exists a $g \in \mathcal{Z}\#\mathrm{P}$ such that $x \in L \Leftrightarrow g(x) = 0$. Let $g_i(x) = 2.g(x), 2 \leq i \leq k$. Then, under the hypothesis, there exists $h \in \mathcal{Q}\#\mathrm{P}$, such that $h(x) = span_k(g(x), g_2(x), \ldots, g_k(x))$. Hence, $x \in L \Leftrightarrow h(x) = 1$ and $x \notin L \Leftrightarrow h(x) = 2$. Again, as $\mathcal{Q}\#\mathrm{P}$ is closed under subtraction, $h^*(x) = 2 - h(x) \in \mathcal{Q}\#\mathrm{P}$. Now, $x \in L \Leftrightarrow h^*(x) = 1$ and $x \notin L \Leftrightarrow h^*(x) = 0$ or, $L \in \mathcal{Q}\mathrm{UP}$. $\square$

5 Random witness reduction in $\mathcal{Z}\#\mathrm{P}$ and $\mathcal{Q}\#\mathrm{P}$

In the previous sections we studied random witness reduction in #P and then witness reduction in $\mathcal{Z}\#\mathrm{P}$ and $\mathcal{Q}\#\mathrm{P}$. The concept of random witness reduction in $\mathcal{Z}\#\mathrm{P}$ and $\mathcal{Q}\#\mathrm{P}$ is analogous

Then, as shown before in Theorem 4.8(Claim 1), each $L_i \in \mathcal{Z}\mathrm{C}_{=}\mathrm{P}$.

Under our hypothesis, $\mathcal{Z}\mathrm{C}_{=}\mathrm{P} = \mathcal{Q}\mathrm{C}_{=}\mathrm{P} \subseteq \mathcal{Q}\mathrm{UP}$, there exists NTM pairs $(\hat{M}_i^n, \hat{M}_i^d)$, $1 \leq i \leq k$, 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,

$$\langle x, y \rangle \in L_i \Leftrightarrow \frac{AR(\hat{M}_i^n, x)}{AR(\hat{M}_i^d, x)} = 1$$

$$\langle x, y \rangle \notin L_i \Leftrightarrow AR(\hat{M}_i^n, x) = 0$$

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

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

1. Input x.
2. Guess $y_i = \frac{n_i}{d_i}, -2^{p_i^n(|x|)} \leq n_i \leq 2^{p_i^n(|x|)}, 1 \leq d_i \leq 2^{p_i^d(|x|)}, 1 \leq i \leq k$(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 $\hat{M}_i^n$ 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 $\hat{M}_i^n$ on $\langle x, y_i \rangle$.
4. Run $M_f^n[M_f^d]$ 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

$$AR(M^n, x) = \sum_{y_1, y_2, \ldots, y_k} [AR(\hat{M}_1^n, \langle x, y_1 \rangle).AR(\hat{M}_2^n, \langle x, y_2 \rangle) \ldots AR(\hat{M}_k^n, \langle x, y_k \rangle) AR(\hat{M}_f^n, \langle y_1, y_2, \ldots, y_k \rangle)]$$

$$AR(M^d, x) = \sum_{y_1, y_2, \ldots, y_k} [AR(\hat{M}_1^n, \langle x, y_1 \rangle).AR(\hat{M}_2^n, \langle x, y_2 \rangle) \ldots AR(\hat{M}_k^n, \langle x, y_k \rangle) AR(\hat{M}_f^d, \langle y_1, y_2, \ldots, y_k \rangle)]$$

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 $AR(\hat{M}_i^n, \langle x, y \rangle)$ and each C_i that rejects contributes a -1 in

4.3 Witness reduction in $\mathcal{Q}\#\mathrm{P}$

Theorem 4.11 (Closure if and only if witness reduction) $\mathcal{Q}\mathrm{C}_{=}\mathrm{P} \subseteq \mathcal{Q}\mathrm{UP} \Leftrightarrow \mathcal{Q}\#\mathrm{P}$ *is closed under composition with* $\mathcal{Q}\#\mathrm{P}$.

Theorem 4.12 (Hard functions for $\mathcal{Q}\#\mathrm{P}$) *Proper subtraction($\ominus$), integer division($\div$) and* $span_k, k \geq 2$, *are* $\mathcal{Q}\#\mathrm{P}$*-hard for* $\mathcal{Q}\#\mathrm{P}$.

Corollary 4.13 *(To Theorem 4.12)*$\mathcal{Q}\#\mathrm{P}$ *is closed under composition with* $\mathcal{Q}\#\mathrm{P} \Leftrightarrow$ $\mathcal{Q}\#\mathrm{P}$ *is closed under composition with PF.*

Proof of Theorem 4.11 [$\Longleftarrow$] Let $L \in \mathcal{Q}\mathrm{C}_{=}\mathrm{P}$. Then, by Proposition 4.6, there exists a NTM M and a polynomial p such that

$$x \in L \Leftrightarrow AR(M,x) = 2^{p(|x|)}$$

$$x \notin L \Leftrightarrow 0 \leq AR(M,x) < 2^{p(|x|)}$$

Let $g_1(x) = AR(M,x)$ and $g_2(x) = 2^{p(|x|)}$. Under the hypothesis, since integer division is a $\mathcal{Q}\#\mathrm{P}$-function, there exists $h \in \mathcal{Q}\#\mathrm{P}$ such that $h(x) = \lfloor g_1(x)/g_2(x) \rfloor$. Thus,

$$x \in L \Leftrightarrow h(x) = 1$$

$$x \notin L \Leftrightarrow h(x) = 0.$$

Hence, h witnesses that $L \in \mathcal{Q}\mathrm{UP}$.

[$\Longrightarrow$] Let $f \in \mathcal{Q}\#\mathrm{P}$ be a k-ary function, witnessed by a NTM pair (M_f^n, M_f^d). Let $g_1, g_2, \ldots, g_k \in \mathcal{Q}\#\mathrm{P}$ be witnessed by NTM pairs $(M_1^n, M_1^d), (M_2^n, M_2^d), \ldots, (M_k^n, M_k^d)$, respectively, each polynomial time bounded. Define the following languages as graphs of the above functions:

$$L_i = \{\langle x, y \rangle | y = g_i(x) = AR(M_i^n, x)\}, 1 \leq i \leq k$$

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 $AR(M_i^{**}, \langle x, y \rangle)$ and each C_i that rejects contributes a -1 in $AR(M_i^{**}, \langle x, y \rangle)$.

By the definition of M_i^{**}, the above product is 0 if any one guess $y_i \neq g_i(x)$. Also, $AR(M_i^{**}, \langle x, y \rangle) = 1$ if $y = g_i(x)$. Hence,

$$AR(M, x) = AR(M_f, \langle g_1(x), g_2(x), \ldots, g_k(x) \rangle)$$

Also, the running time of NTM M is bounded by some polynomial. $\square$

Proof of Theorem 4.9 We show that closure of $\mathcal{Z}\#\mathrm{P}$ under composition with proper subtraction, integer division and span implies that $\mathcal{Z}\mathrm{C}_{=}\mathrm{P} \subseteq \mathcal{Z}\mathrm{UP}$. Hence, by Theorem 4.8, we are done.

Let $L \in \mathcal{Z}\mathrm{C}_{=}\mathrm{P}$. Hence, there exists a $g \in \mathcal{Z}\#\mathrm{P}$ and a polynomial p such that $x \in L \Leftrightarrow g(x) = 2^{p(|x|)}$ and $x \notin L \Leftrightarrow 0 \leq g(x) < 2^{p(|x|)}$. Let $g_2(x) = 2^{p(|x|)} - 1$. Then, by the hypothesis, $h = g \ominus g_2 \in \mathcal{Z}\#\mathrm{P}$ and $x \in L \Leftrightarrow h(x) = 1$ and $x \notin L \Leftrightarrow h(x) = 0$. Thus, $L \in \mathcal{Z}\mathrm{UP}$. This shows that proper subtraction is hard for $\mathcal{Z}\#\mathrm{P}$.

Let $g_2(x) = 2^{p(|x|)}$. Then, under the hypothesis $h = g \div g_2 \in \mathcal{Z}\#\mathrm{P}$ and $x \in L \Leftrightarrow h(x) = 1$ and $x \notin L \Leftrightarrow h(x) = 0$. Thus, $L \in \mathcal{Z}\mathrm{UP}$. This shows that integer division is hard for $\mathcal{Z}\#\mathrm{P}$.

Given $L \in \mathcal{Z}\mathrm{C}_{=}\mathrm{P}$, as $\mathcal{Z}\#\mathrm{P}$ is closed under subtraction, there exists a $g \in \mathcal{Z}\#\mathrm{P}$ such that $x \in L \Leftrightarrow g(x) = 0$. Let $g_i(x) = 2.g(x), 2 \leq i \leq k$. Then, under the hypothesis, there exists $h \in \mathcal{Z}\#\mathrm{P}$, such that $h(x) = span_k(g, g_2, \ldots, g_k)$. Hence, $x \in L \Leftrightarrow h(x) = 1$ and $x \notin L \Leftrightarrow h(x) = 2$. Again, as $\mathcal{Z}\#\mathrm{P}$ is closed under subtraction, $h^*(x) = 2 - h(x) \in \mathcal{Z}\#\mathrm{P}$. Now, $x \in L \Leftrightarrow h^*(x) = 1$ and $x \notin L \Leftrightarrow h^*(x) = 0$ or, $L \in \mathcal{Z}\mathrm{UP}$. $\square$

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, $L_i \in \mathcal{Z}\mathrm{C}_{=}\mathrm{P}$. $\square$

Under our hypothesis, there exists a NTM $M_i^{**}, 1 \leq i \leq k$ such that

$$\langle x, y\rangle \in L_i \Leftrightarrow AR(M_i^{**}, \langle x, y\rangle) = 1$$

$$\langle x, y\rangle \notin L_i \Leftrightarrow AR(M_i^{**}, \langle x, y\rangle) = 0$$

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

NTM M

1. Input x.

2. Guess $y_i, -2^{p_i(|x|)} \leq y_i \leq 2^{p_i(|x|)}, 1 \leq i \leq k$.

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

$$AR(M, x) = \sum_{y_1, y_2, \ldots, y_k} [AR(M_1^{**}, \langle x, y_1\rangle).AR(M_2^{**}, \langle x, y_2\rangle) \ldots AR(M_k^{**}, \langle x, y_k\rangle) AR(M_f, \langle y_1, y_2, \ldots, y_k\rangle)]$$

Corollary 4.10 *(to Theorem 4.9)$\mathcal{Z}\#\mathrm{P}$ is closed under composition with $\mathcal{Z}\#\mathrm{P} \Leftrightarrow$ $\mathcal{Z}\#\mathrm{P}$ is closed under composition with PF.*

Proof of Theorem 4.7 $\mathcal{Z}\mathrm{C}_{=}\mathrm{P} \subset \mathcal{Z}\mathrm{UP}$ implies that $\mathrm{C}_{=}.\mathrm{C}_{=}.P \subseteq \mathrm{C}_{=}.\mathcal{Z}\mathrm{C}_{=}\mathrm{P} \subseteq \mathrm{C}_{=}.\mathcal{Z}\mathrm{UP} \subseteq \mathcal{Z}\mathrm{C}_{=}\mathrm{P} \subseteq \mathcal{Z}\mathrm{UP}$, using Propositions 4.6. Iterating this process it is easy to prove that $\underbrace{\mathrm{C}_{=} \ldots \mathrm{C}_{=}\mathrm{C}_{=}}_{k}\mathrm{P} \subseteq \mathcal{Z}\mathrm{UP}, k \geq 1$. $\square$

Proof of Theorem 4.8 [$\Longleftarrow$] Let $L \in \mathcal{Z}\mathrm{C}_{=}\mathrm{P}$. Then by Proposition 4.6 there exists a NTM M and a polynomial p such that

$$x \in L \Leftrightarrow AR(M,x) = 2^{p(|x|)}$$

$$x \notin L \Leftrightarrow 0 \leq AR(M,x) < 2^{p(|x|)}$$

Let $g_1(x) = AR(M,x)$ and $g_2(x) = 2^{p(|x|)}$. Under the hypothesis, since integer division is a $\mathcal{Z}\#\mathrm{P}$-function, there exists $h \in \mathcal{Z}\#\mathrm{P}$ such that $h(x) = \lfloor g_1(x)/g_2(x) \rfloor$. Thus,

$$x \in L \Leftrightarrow h(x) = 1$$

$$x \notin L \Leftrightarrow h(x) = 0.$$

Hence, $h \in \mathcal{Z}\#\mathrm{P}$ witnesses that $L \in \mathcal{Z}\mathrm{UP}$.

[$\Longrightarrow$] Let $f \in \mathcal{Z}\#\mathrm{P}$ be a k-ary function witnessed by NTM M_f. Let $g_1, g_2, \ldots, g_k \in \mathcal{Z}\#\mathrm{P}$ 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.

$$L_i = \{\langle x,y \rangle | y = g_i(x) = AR(M_i,x)\}, 1 \leq i \leq k$$

Claim 1: $L_i \in \mathcal{Z}\mathrm{C}_{=}\mathrm{P}$

Proof: The following NTM M_i^* accepts L_i.

1. Input $\langle x,y \rangle$. We assume that $-2^{p_i(|x|)} \leq y \leq 2^{p_i(|x|)}$.

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

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

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

□

4.2 Witness reduction in $\mathcal{Z}\#\mathrm{P}$

Theorem 4.7 (Witness reduction implies collapsing) $\mathcal{Z}\mathrm{C}_{=}\mathrm{P} \subset \mathcal{Z}\mathrm{UP} \Rightarrow CH = \mathcal{Z}\mathrm{UP}$.

Theorem 4.8 (Closure if and only if witness reduction) $\mathcal{Z}\mathrm{C}_{=}\mathrm{P} \subseteq \mathcal{Z}\mathrm{UP} \Leftrightarrow \mathcal{Z}\#\mathrm{P}$ *is closed under composition with* $\mathcal{Z}\#\mathrm{P}$.

Theorem 4.9 (Hard functions for $\mathcal{Z}\#\mathrm{P}$) *Proper subtraction($\ominus$), integer division($\div$) and* $span_k, k \geq 2$, *are* $\mathcal{Z}\#\mathrm{P}$*-hard for* $\mathcal{Z}\#\mathrm{P}$.

The definition of the class $\mathrm{C_{=}P}$ is slightly different from the standard one; however, they both yield the same class. Also, note that the class $\mathcal{Z}\#\mathrm{P}$ is same as the class GapP defined by Fenner, Fortnow and Kurtz [FFK90].

The following propositions can be easily proved from the definitions.

Proposition 4.4 *1.* $\#\mathrm{P} \subseteq \mathcal{Z}\#\mathrm{P} \subseteq \mathcal{Q}\#\mathrm{P}$.

2. $\mathrm{P}^{\#\mathrm{P}} = \mathrm{P}^{\mathcal{Z}\#\mathrm{P}} = \mathrm{P}^{\mathcal{Q}\#\mathrm{P}}$.

3. $\mathrm{C_{=}P} \subseteq \mathcal{Z}\mathrm{C_{=}P} \subseteq \mathcal{Q}\mathrm{C_{=}P}$.

4. $\mathrm{UP} \subseteq \mathcal{Z}\mathrm{UP} \subseteq \mathcal{Q}\mathrm{UP}$.

Proposition 4.5 *1. [Reg82]* $\#\mathrm{P}$ *is closed under composition with addition and multiplication.*

2. $\mathcal{Z}\#\mathrm{P}$ *is closed under composition with addition, multiplication and subtraction.*

3. $\mathcal{Q}\#\mathrm{P}$ *is closed under composition with addition, multiplication, subtraction and division (by a non-zero* $\mathcal{Q}\#\mathrm{P}$ *function).*

We outline the proof of the following proposition.

Proposition 4.6 *1.* $\mathcal{Z}\mathrm{C_{=}P} = \mathcal{Q}\mathrm{C_{=}P}$.

2. $\mathrm{C_{=}}.\mathcal{Z}\mathrm{UP} \subseteq \mathcal{Z}\mathrm{C_{=}P}$.

3. Let $L \in \mathcal{Z}\mathrm{C_{=}P} = \mathcal{Q}\mathrm{C_{=}P}$. *Then, there exists a NTM* M *and a polynomial* p *such that, for all* x, $x \in L \Leftrightarrow AR(M,x) = 2^{p(|x|)}$ *and* $x \notin L \Leftrightarrow 0 \leq AR(M,x) < 2^{p(|x|)}$.

Proof.

Definition 4.1 *1. A function $f : \Sigma^* \longmapsto \mathcal{N}$ is in $\#\mathrm{P}$ iff there exists a polynomial time-bounded nondeterministic machine M such that $f(x) = Acc(M, x)$, for all x.*

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

3. A function $f : \Sigma^* \longmapsto \mathcal{Q}$ is in $\mathcal{Q}\#\mathrm{P}$ iff there exists a pair of polynomial time-bounded nondeterministic machines (M^n, M^d) such that $AR(M^d, x) \neq 0$ and $f(x) = \frac{AR(M^n,x)}{AR(M^d,x)}$, for all x.

Definition 4.2 *1. A language $L \in \mathrm{C}_{=}\mathrm{P}$ iff there exists a function $f \in PF$, $f : \Sigma^* \longmapsto \mathcal{N}$, and $g \in \#\mathrm{P}$ such that, for all x, $x \in L \Leftrightarrow g(x) = f(x)$.*

2. A language $L \in \mathcal{Z}\mathrm{C}_{=}\mathrm{P}$ iff there exists a function $f \in PF$, $f : \Sigma^* \longmapsto \mathcal{Z}$, and $g \in \mathcal{Z}\#\mathrm{P}$ such that, for all x, $x \in L \Leftrightarrow g(x) = f(x)$.

3. A language $L \in \mathcal{Q}\mathrm{C}_{=}\mathrm{P}$ iff there exists a function $f \in PF$, $f : \Sigma^* \longmapsto \mathcal{Q}$, and a $g \in \mathcal{Q}\#\mathrm{P}$ such that, for all x, $x \in L \Leftrightarrow g(x) = f(x)$.

Definition 4.3 *1. A language $L \in \mathrm{UP}$ iff there exists a $g \in \#\mathrm{P}$ such that, for all x, $x \in L \Leftrightarrow g(x) = 1$ and $x \notin L \Leftrightarrow g(x) = 0$.*

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

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

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, $\mathcal{Z}NP$ is the class of languages such that there exists a $g \in \mathcal{Z}\#\mathrm{P}$ such that $x \in L \Leftrightarrow g(x) > 0$ and $x \notin L \Leftrightarrow g(x) = 0$.

where $w_1 w_2 \in \{0,1\}^{b(|x|)}$ is chosen uniformly. Choosing an appropriate e completes the proof. □

As an additinal comment we note that the class $\widehat{BP}$.UP is the only class we are aware of that lies between BPP and PP. Clearly, it lies in the PH, using quantifier simulation [Sch89].

4 Witness reduction in $\mathcal{Z}\#\mathrm{P}$ and $\mathcal{Q}\#\mathrm{P}$

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

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

4.1 Definitions and preliminaries

We repeat the definition of #P etc. to make comparisons with the new classes $\mathcal{Z}\#\mathrm{P}$ and $\mathcal{Q}\#\mathrm{P}$.

$$x \notin L \Leftrightarrow Acc(M,x) < 2^{p(|x|)}$$

Let $g_1(x) = 2.Acc(M,x)$, $g_2(x) = 2^{p(|x|)} + Acc(M,x)$, $g_i(x) = g_2(x)$, for $i = 3, \ldots, k$. Then, $g_1(x) = g_2(x) = 2.2^{p(|x|)} \Leftrightarrow Acc(M,x) = 2^{p(|x|)} \Leftrightarrow x \in L$. Thus,

$$x \in L \Leftrightarrow span(g_1(x), \ldots, g_k(x)) = 1$$

$$x \notin L \Leftrightarrow span(g_1(x), \ldots, g_k(x)) = 2$$

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

$$Prob(h_1(x\#w_1) = span_k(g_1(x), \ldots, g_k(x))) \geq 1 - \frac{1}{2^{e(|x|)}}$$

$$\text{or, } Prob(x \in L \Leftrightarrow h_1(x\#w_1) = 1 \wedge x \notin L \Leftrightarrow h_1(x\#w_1) = 2) \geq 1 - \frac{1}{2^{e(|x|)}}$$

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,

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

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

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

$$Prob(x \in L \Leftrightarrow h(x\#w_1\#w_2) = 2 \wedge x \notin L \Leftrightarrow h(x\#w_1\#w_2)) = 1 \geq (1 - \frac{1}{2^{e(|x|)}})^2$$

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

Let $h \in$ #P be witnessed by NTM M^*. Now, construct M^{**}, which guesses two computations of M^* and accepts iff both the computations accept. Let $A = \{x\#w_1w_2 | Acc(M^{**}, x\#w_1\#w_2) = 1\}$. Then $A \in$ UP. Thus, for all e, there exists $A \in$ UP and a polynomial b such that

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

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

$$x \in L \Leftrightarrow Acc(M,x) = 2^{p(|x|)}$$

$$x \notin L \Leftrightarrow Acc(M,x) < 2^{p(|x|)}$$

Let $g_1(x) = Acc(M,x) \in \#\text{P}$ and $g_2(x) = 2^{p(|x|)} - 1$. Note that $x \in L \Leftrightarrow g_1(x) \ominus g_2(x) = 1$ and $x \notin L \Leftrightarrow g_1(x) \ominus g_2(x) = 0$. Under our hypothesis, for each polynomial e, there exists a $h \in \#\text{P}$ and a polynomial b such that,

$$Prob(h(x\#w) = g_1(x) \ominus g_2(x)) \geq 1 - \frac{1}{2^{e(|x|)}}$$

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

Then, for a correct choice of w, we have $h(x\#w) = 1 \Leftrightarrow x \in L$ and $h(x\#w) = 0 \Leftrightarrow x \notin L$. Let $A = \{x\#w | h(x\#w) = 1\}$. Then $A \in \text{UP}$. Thus, for all e, there exists $A \in \text{UP}$ and a polynomial b such that

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

This completes the proof of the theorem. $\square$

Proof of Theorem 3.6 We will show that if #P is closed under compostion with proper subtraction, integer division, or $span_k$, for some $k \geq 2$, randomly, then $\text{C}_{=}\text{P} \subseteq \widehat{BP}.\text{UP}$. 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 $\text{C}_{=}\text{P} \subseteq \widehat{BP}.\text{UP}$. The proof that integer division is #P-hard for #P randomly, is quite similar to that of proper subtraction; just take $g_2(x) = 2^{p(|x|)}$.

Now we show that $span_k, k \geq 2$, is randomly hard for #P. Let $L \in \text{C}_{=}\text{P}$. Then by Proposition 2.6, there exists a NTM M and a polynomial p such that

$$x \in L \Leftrightarrow Acc(M,x) = 2^{p(|x|)}$$

4. Simulate NTM M_{A_i} on $\langle x, y_i\rangle \# w_i$ 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 $\langle y_1, y_2, \ldots, y_k\rangle$ and accepts iff M_f accepts.

Claim 2: $Prob(Acc(M, x\#w) = f(g_1(x), g_2(x), \ldots, g_k(x))) \geq 1 - \frac{1}{2^{e(|x|)}}$, where, $w \in \{0,1\}^{b(|x|)}$ is chosen uniformly.

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

$$Prob\left(\begin{array}{l} \langle x, y\rangle \in L_i \Leftrightarrow Acc(M_{A_i}, \langle x, y\rangle \# w) = 1 \\ \\ \langle x, y\rangle \notin L_i \Leftrightarrow Acc(M_{A_i}, \langle x, y\rangle \# w) = 0 \end{array}\right) \geq 1 - \frac{1}{2^{e^*(|x|)}}$$

or,

$$Prob\left(\bigwedge_{i=1}^{k}\left(\begin{array}{l} \langle x, y_i\rangle \in L_i \Leftrightarrow Acc(M_{A_i}, \langle x, y_i\rangle \# w) = 1 \\ \\ \langle x, y_i\rangle \notin L_i \Leftrightarrow Acc(M_{A_i}, \langle x, y_i\rangle \# w) = 0 \end{array}\right)\right) \geq (1 - \frac{k}{2^{e^*(|x|)}}) \geq 1 - \frac{1}{2^{e(|x|)}}$$

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

Let $w \in \{0,1\}^{b(|x|)}$ be such that the conjunctive condition holds. The probability of choosing such a w is at least $1 - \frac{1}{2^{e(|x|)}}$. 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 corresoponding to the correct guesses, $y_i = g_i(x)$, for all i, $Acc(M_{A_i}, \langle x, y_i\rangle \# w) = 1$. 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. □

[$\Longleftarrow$] If #P is closed under #P, then it is surely closed under proper subtraction. We will show that this implies C$_=$P $\subseteq \widehat{BP}$.UP.

1. Input $\langle x, y \rangle$. Assume that $0 \leq y \leq 2^{p_i(|x|)}$.

2. Guess $b \in \{0, 1\}$.

3. if $b = 0$ then simulate M_i on x. M_i^* accepts iff M_i accepts.

4. if $b = 1$ then guess $l \in \{0, 1, 2, \ldots, 2^{p_i(|x|)}\}$. If $y \leq l$ then reject else accept.

Note that $Acc(M_i^*, \langle x, y \rangle) = 2^{p_i(|x|)} \Leftrightarrow y = g_i(x) \Leftrightarrow x \in L_i$. $\square$

Now, under our hypothesis, each $L_i \in \widehat{BP}$.UP. Choose a polynomial e^* such that $(1 - \frac{k}{2^{e^*(n)}}) \geq (1 - \frac{1}{2^{e(n)}})$ or, $2^{e^*(n)} \geq \frac{2^{e(n)}}{k}$, for all n. Then, there exists a set $A_i \in$ UP, and a polynomial b_i such that for all x,

$$Prob(\langle x, y \rangle \# w \in A_i \Leftrightarrow \langle x, y \rangle \in L_i) \geq 1 - \frac{1}{2^{e^*(|x|)}}$$

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

$$Prob \left(\begin{array}{l} \langle x, y \rangle \in L_i \Leftrightarrow Acc(M_{A_i}, \langle x, y \rangle \# w) = 1 \\ \\ \langle x, y \rangle \notin L_i \Leftrightarrow Acc(M_{A_i}, \langle x, y \rangle \# w) = 0 \end{array} \right) \geq 1 - \frac{1}{2^{e^*(|x|)}}$$

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

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

NTM M

1. Input $x \# w$.

2. Guess $y_i \in \{0, 1, 2, \ldots, 2^{p_i(|x|)}\}$, for each $i = 1, 2, \ldots, k$.

3. Let $w_i =$ prefix of w such that $|w_i| = b_i(|\langle x, y_i \rangle|)$.

2. $\widehat{BP}.\widehat{BP}.K = \widehat{BP}.K$.

Now we state our results for random witness reduction, which are analogous to witness reduction results of Ogiwara and Hemachandra [OH90].

Theorem 3.4 (Random witness reduction implies collapsing) $\mathrm{C_{=}P} \subseteq \widehat{BP}.\mathrm{UP} \Rightarrow CH = PH = \widehat{BP}.\mathrm{UP}$.

Theorem 3.5 (Random closure if and only if random witness reduction) $\mathrm{C_{=}P} \subseteq \widehat{BP}.\mathrm{UP}$ $\Leftrightarrow$ #P *is closed under composition with* #P *randomly.*

Theorem 3.6 (Randomly hard functions for #P**)** *Proper subtraction*($\ominus$)*, integer division*($\div$) *and* $span_k$*, for some* $k \geq 2$*, are* #P*-hard for* #P *randomly.*

Corollary 3.7 #P *is closed under composition with* #P *randomly* $\Leftrightarrow$ #P *is closed under compositiion with PF randomly.*

Proof of Theorem 3.4 $\mathrm{C_{=}P} \subseteq \widehat{BP}.\mathrm{UP}$ implies that $\mathrm{C_{=}}.\mathrm{C_{=}}.\mathrm{P} \subseteq \mathrm{C_{=}}.\widehat{BP}.\mathrm{UP} \subseteq \widehat{BP}.\mathrm{C_{=}}.\mathrm{UP} = \widehat{BP}.\mathrm{C_{=}P} \subseteq \widehat{BP}.\widehat{BP}.\mathrm{UP} = \widehat{BP}.\mathrm{UP}$, using Proposition 3.3. Iterating this process gives $\forall k[\underbrace{\mathrm{C_{=}} \ldots \mathrm{C_{=}}}_{k}\mathrm{P} \subseteq \widehat{BP}.\mathrm{UP}]$. $\square$

Proof of Theorem 3.5[$\Longrightarrow$] 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 $g_1, g_2, \ldots, g_k$:

$$L_i = \{\langle x, y\rangle | y = g_i(x)\}, i = 1, 2, \ldots, k$$

Claim 1: $L_i \in \mathrm{C_{=}P}$, for $i = 1, 2, \ldots, k$.

Proof. The following NTM M_i^* accepts L_i.

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

$$Prob(h(x\#w) = f(g_1(x), g_2(x), \ldots, g_i(x))) \geq 1 - \frac{1}{2^{e(|x|)}}$$

where, $w \in \{0,1\}^{b(|x|)}$ is chosen uniformly. Equivalently, we say that $\mathcal{DF}$ is closed under composition with f with an arbitrarily high probability.

2. Let $\mathcal{DF}$ and $\mathcal{CF}$ be classes of functions. We say that $\mathcal{DF}$ is closed under composition with $\mathcal{CF}$ randomly iff
$\forall f \in \mathcal{CF}$ [$\mathcal{DF}$ is closed under composition with f randomly].

3. Let $\mathcal{DF}$ and $\mathcal{CF}$ be classes of functions. Let $f \in \mathcal{CF}$. Then, f is $\mathcal{CF}$-hard for $\mathcal{DF}$ randomly iff
[$\mathcal{DF}$ is closed under composition with f randomly $\Rightarrow$ $\mathcal{DF}$ is closed under composition with $\mathcal{CF}$ randomly].

The following definition was first introduced by Toda and Ogiwara in [TO90].

Definition 3.2 *$L \in \widehat{BP}.K$ iff, for all polynomials e, there exists $A \in K$ and a polynomial b, such that, for all strings x,*

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

where, $w \in \{0,1\}^{b(|x|)}$ 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 [RR90].

Proposition 3.3 *1.* $\mathrm{C}_{=}.\widehat{BP}.\mathrm{UP} \subseteq \widehat{BP}.\mathrm{C}_{=}.\mathrm{UP} = \widehat{BP}.\mathrm{C}_{=}\mathrm{P}$.

We have reproduced only parts of the above theorem to avoid cluttering the theme of the paper with unneccessary details. For example, Ogiwara and Hemachandra [OH90] 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 [VV86]. In each case, it was possible to amplify the probability of reduction, by using appropriate classes - $\oplus P$[Tod89] and counting classes[TO90]. We ask the question: what sort of collapses will be produced if the probability of witness reduction was arbitrarily high in the first place? It turns out that, if it were possible to reduce witnesses from many to one, with a high probability then PH collapses to its second level. As this result is fairly easy to prove, we do not state the proof here.

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 very analogous to those of Ogiwara and Hemachandra [OH90]. 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.

Now, we introduce the notion of randomly hard functions. The concept is motivated by the notion of hard closure properties introduced by Ogiwara and Hemachandra [OH90] and the $\widehat{BP}$ operator introduced by Toda and Ogiwara [TO90]. Essentially, $\widehat{BP}$ is same as the standard BP operator, except that "free amplification" is provided in the definition of $\widehat{BP}$.

2. *Let $\mathcal{DF}$ and $\mathcal{CF}$ be classes of functions. We say that $\mathcal{DF}$ is closed under composition with $\mathcal{CF}$ iff*
   $\forall f \in \mathcal{CF}$ *[$\mathcal{DF}$ is closed under composition with f].*

3. *Let $\mathcal{DF}$ and $\mathcal{CF}$ be classes of functions. Let $f \in \mathcal{CF}$. Then, f is $\mathcal{CF}$-hard* [3] *for $\mathcal{DF}$ iff [$\mathcal{DF}$ is closed under composition with $f \Rightarrow \mathcal{DF}$ is closed under composition with $\mathcal{CF}$].*

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

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

3. *For each number $k \geq 2$, and $a_1, \ldots, a_k \in \mathcal{Q}$, let $span_k(a_1, \ldots, a_k)$ 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 [OH90].

Theorem 2.9 (Witness reduction implies collapsing) $\subseteq_{=}\mathrm{P} \subseteq UP \Rightarrow CH = PH = UP$.

Theorem 2.10 (Closure if and only if witness reduction) $\subseteq_{=}\mathrm{P} \subseteq UP \Leftrightarrow \#\mathrm{P}$ *is closed under composition with* $\#\mathrm{P}$.

Theorem 2.11 (Hard functions for $\#\mathrm{P}$) *Proper subtraction($\ominus$), integer division($\div$) and $span_k$, for some $k \geq 2$, are $\#\mathrm{P}$-hard for $\#\mathrm{P}$.*

Corollary 2.12 *(To Theorem 2.11)$\#\mathrm{P}$ is closed under composition with $\#\mathrm{P} \Leftrightarrow \#\mathrm{P}$ is closed under composition with PF.*

[3] 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 $\#\mathrm{P} = PF$.

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 $\mathrm{C}.K \in CH$.

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. [Tor88] $\mathrm{C}_{=}.\mathrm{C}.K = \mathrm{C}_{=}.\mathrm{C}_{=}.K$, for any class $K \in CH$[1].*

2. $CH = \cup_{k>0} \underbrace{\mathrm{C} \ldots \mathrm{C}}_{k} \mathrm{P} = \cup_{k>0} \underbrace{\mathrm{C}_{=} \ldots \mathrm{C}_{=}}_{k} \mathrm{P}$.

3. [Sim75] L is in $\mathrm{C}_{=}\mathrm{P}$ 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) $x \in L$ iff $0 < Acc(M,x) < 2^{p(|x|)}$.

The following definitions are slightly modified versions of the ones originally used by Ogiwara and Hemachandra [OH90]. We assume throughout that all functions are total.

Definition 2.7 *1. Let $\mathcal{DF}$ be a class of functions. Let $i \geq 1$ and let $f : \mathcal{N}^i \longmapsto \mathcal{N}$. $\mathcal{DF}$ is closed under outermost composition[2] with f iff*

$$\forall g_1, g_2, \ldots, g_i \in \mathcal{DF}[\lambda x.f(g_1(x), \ldots, g_i(x))] \in \mathcal{DF}$$

[1]The reader is cautioned that the original proof contains a fixable error.

[2]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.

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

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

Next, we review the definitions of some standard operators.

Definition 2.3 *1. For a class* K, $\exists.K$ *is the class defined in the following way: A set* L *is in* $\exists.K$ *if there exists a polynomial* p *and a set* $A \in K$ *such that for every* $x \in \Sigma^*$,

$$x \in L \Longleftrightarrow \|\{y \mid |y| = p(|x|) and \langle x, y\rangle \in A\}\| \geq 1.$$

2. *For a class* K, $\forall.K$ *is the class defined in the following way: A set* L *is in* $\forall.K$ *if there exists a polynomial* p *and a set* $A \in K$ *such that for every* $x \in \Sigma^*$,

$$x \in L \Longleftrightarrow \|\{y \mid |y| = p(|x|) and \langle x, y\rangle \in A\}\| = 2^{p(|x|)}.$$

3. *For a class* K, $\mathrm{C}.K$ *is the class defined in the following way: A set* L *is in* $\mathrm{C}.K$ *if there exists a polynomial* p, *a* $f \in PF$ *and a set* $A \in K$, *such that for every* $x \in \Sigma^*$,

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

4. *For a class* K, $\mathrm{C}_{=}.K$ *is the class defined in the following way: A set* L *is in* $\mathrm{C}_{=}.K$ *if there exists a polynomial* p, $f \in PF$, *and a set* $A \in K$ *such that for every* $x \in \Sigma^*$,

$$x \in L \Longleftrightarrow \|\{y \mid |y| = p(|x|) and \langle x, y\rangle \in A\}\| = f(x).$$

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

Definition 2.4 *1.* $P \in PH$.

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 Σ, 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 $\mathcal{N}$, $\mathcal{Z}$ and $\mathcal{Q}$, 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 $Acc(N,x)$ = number of accepting paths of N on input x, and $Rej(N,x)$ = number of rejecting paths of N on input x. Now, let $AR(N,x) = Acc(N,x) - Rej(N,x)$.*

Note that AR functions were used extensively, to show closure properties for PP[BRS90, FR90, Gup90]. We review the definitions of complexity classes that we will discuss in this paper.

Definition 2.2 *1. A function $f : \Sigma^* \longmapsto \mathcal{N}$ is in* #P *iff there exists a polynomial time-bounded nondeterministic machine M such that $f(x) = Acc(M,x)$, for all x.*

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

tions for #P, including division, subtraction, span, etc. For example, #P is closed under composition with division iff #P is closed under composition with every other #P function iff $PH = CH = UP$. We ask the question: what makes a function hard? Is there anything special about division or subtraction? Interestingly, the answer lies in the same underlying theme, witness reduction. A function is hard for #P if and only if it can reduce the number of witnesses from an exact number to one and from any other number to zero. Compared to one used by Toda [Tod89], this is a stronger form of witness reduction. Hence it produces stronger collapses.

In this paper we study different forms of witness reduction. We provide several different instances, besides the ones stated above, of this technique at work. We also formalize the notion of random witness reduction as well as randomly hard functions. We show that a function is hard randomly if and only if it can reduce the number of witnesses randomly from a fixed number to one and from any other number to 0. Random witness reduction leads to collapse with a very high probability.

To support our thesis that witness reduction is what makes a function hard, we vary the witness functions on nondeterministic machines and achieve the same results. In particular, we consider not only number of accepting paths as witness functions, but also number of accepting paths minus number of rejecting path (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 the new domains, turn out to be hard functions for these new classes of functions.

This paper is organized as follows: in Section 3 we introduce and formalize the notion of random witness reduction and 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.

1 Introduction

Witness reduction allows composition of functions and hence collapses hierarchies. This has been the underlying theme of several recent results in complexity theory. For example, Toda and Ogiwara's recent result [TO90] uses random witness reduction (SAT to USAT), originally defined by Valiant and Vazirani [VV86]. This reduction randomly reduces the number of witnesses to membership in a language (in NP) from many to one. Using exact counting, Toda and Ogiwara [TO90] were able to amplify the probability of the reduction so that, given exact counting, it is possible to reduce the number of witnesses to membership in a language (in NP) from many to one, with an arbitrarily high probability. This allows one to prove collapsing results such as $PP.PH \subseteq \widehat{BP}.PP$; that is, PH can be "collapsed" into PP with an arbitrarily high probability.

Membership in a language defined using nondeterministic machines is witnessed by certain functions on the machine, usually some "threshold" on number of accepting paths. By witness reduction, we mean that these function values are reduced. The form of witness reduction may vary depending on what the witness functions are, for membership in the language, and on how the witnesses are being reduced. The witness reduction from Valiant and Vazirani, for example, randomly reduces number of accepting paths from many to one.

Toda's initial result [Tod89], that $PH \subseteq BP.\oplus P$, is a different form of witness reduction. Here, the witness function is "number of accepting paths Mod_2" and the witnesses are reduced randomly. Again using Valiant and Vazirani's reduction, and given that $\oplus P$ is closed under Turing reductions [PZ83], it is possible to construct a nondeterministic machine M for any $L \in NP$, such that $x \in L \Leftrightarrow$number of accepting paths of M on x $Mod_2 = 1$ and $x \notin L \Leftrightarrow$number of accepting paths of M on x $Mod_2 = 0$, with an arbitrarily high probability. Now, the fact that $\oplus P$ is closed under composition "collapses" PH into $\oplus P$, with a high probability.

Ogiwara and Hemachandra [OH90] have recently shown certain functions to be hard func-

Abstract

We identify "Witness reduction" as the underlying theme of 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 have shown that subtraction, division, etc. are hard for #P in the sense that, if #P is closed under composition with subtraction and division then, it is closed under composition with every other #P function. We identify witness reduction as the reason for the existence of hard functions. To support our thesis we define new function classes which are apriori closed under composition with subtraction and division implying that subtraction and division do not reduce witnesses in these classes. However, proper subtraction and integer division do reduce witnesses in the new classes and turn out to be hard for these classes.

We also introduce and formalize the notion of random witness reduction and randomly hard functions and obtain results analogous to those of Ogiwara and Hemachandra.

The Power of Witness Reduction

Sanjay Gupta[1]

The Ohio State University

Department of Computer and Information Sciences

Columbus, Ohio 43210

sgupta@cis.ohio-state.edu

September 22, 1992

[1]This work was supported in part by NSF under Grant No. CCR-8909071.