Electronic Colloquium on Computational Complexity - Reports Series 1995 - available via:
ECCC
TR95-035
FTP: ftp.eccc.uni-trier.de:/pub/eccc/
WWW: http://www.eccc.uni-trier.de/eccc/
Email: ftpmail@ftp.eccc.uni-trier.de with subject 'help eccc'

Closure Properties of GapP and #P

Richard Beigel*
Yale University

June 28, 1995

Abstract

We classify the univariate functions that are relativizable closure properties of GapP, solving a problem posed by Hertrampf, Vollmer, and Wagner (Structures '95). We also give a simple proof of their classification of univariate functions that are relativizable closure properties of #P.

1. Introduction

An operator H is a closure property of a class G of functions if, for all g in G, Hg belongs to G. An operator H is a relativizable closure property of a class G of functions if, for all oracles A, for all g in G^A, Hg belongs to G^A.

Closure properties of #P and GapP, studied in [4, 5], yield important closure properties of various counting classes. Hertrampf, Vollmer, and Wagner [6] considered the special case where $Hg = f \circ g$ for some function f of a single variable. It is known [4, 5] that $\#P$ and GapP are closed under addition and under $f(n) = \binom{n}{k}$; GapP is also closed under subtraction. Therefore, if a univariate function f is a linear combination of binomial coefficients then GapP is closed under f; if, in addition, f is a positive linear combination of binomial coefficients then #P is closed under f as well. A relativized converse is hinted at by several oracle constructions involving counting classes (e.g., [1, 3, 2]) that hinge on the nonexistence of such polynomials. However, an exact characterization of the univariate functions that are relativizable closure properties of #P was unknown until Hertrampf, Vollmer, and Wagner [6] proved that they are exactly the positive linear combinations of binomial coefficients.

In this note, we prove that the univariate functions that are relativizable closure properties of GapP are exactly the linear combinations of binomial coefficients. In addition, we give a simple proof of Hertrampf et al's result for #P. (Hertrampf et al also consider multivariate functions — see Section 4.)

*Yale University, Dept. of Computer Science, P.O. Box 208285, New Haven, CT 06520-8285, USA. Email: beigel-richard@cs.yale.edu. Research supported in part by the National Science Foundation under grants CCR-8958528 and CCR-9415410.

2. Terminology

We write Accept(M, x) to denote the number of accepting paths of nondeterministic TM M on input x and Reject(M, x) to denote the number of rejecting paths of nondeterministic TM M on input x. We write Gap(M, x) to denote Accept$(M, x) -$ Reject(M, x). We write NPTM as a shorthand for "nondeterministic polynomial time–bounded Turing machine." A function h is in GapP if there is an NPTM M such that, for all x, $h(x) = \mathrm{Gap}(M, x)$. These concepts are relativized in the standard way by allowing M access to an oracle A.

3. Results

Lemma 1 is well known [7, 2]:

Lemma 1. *Let h be a degree-d polynomial, having integer coefficients, in variables $a_1, \ldots, a_m$. If h is a symmetric function, then there exist integers $c_0, \ldots, c_d$ such that*

$$h(a_1, \ldots, a_m) = \sum_{0 \leq i \leq d} c_i \binom{\sum_{1 \leq j \leq m} a_j}{i}.$$

Lemma 2. *Let f be a function from N to Z. If, for every oracle A and every function $g \in \#\mathrm{P}^A$ we have $f \circ g \in \mathrm{GapP}^A$, then there exists a finite sequence of integers $c_0, ..., c_k$ such that*

$$f(N) = \sum_{0 \leq i \leq k} c_i \binom{N}{i}.$$

Proof: This is a simple application of the polynomial method [2].

We define a function $g_A \in \#\mathrm{P}^A$:

$$g_A(x) = |\{y : |y| = |x| \text{ and } y \in A\}|.$$

Let f be a function from N to Z. Assume that for every A, $f \circ g_A \in \mathrm{GapP}^A$. Therefore, for every oracle A, there exists an oracle NPTM $M^{()}$ such that, for all x, $f(g_A(x)) = \mathrm{Gap}(M^A, x)$. By a standard diagonalization argument it follows that there exists a single oracle NPTM $M^{()}$ such that for all A, for all x, $f(g_A(x)) = \mathrm{Gap}(M^A, x)$.

Let $M^{()}$ run in time $p(n)$. Let ℓ be the least positive integer such that for all $n \geq \ell$, $p(n) < 2^{n-1}$. Let $n \geq \ell$. Let $x = 0^n$. Let A contain no elements of length different from n. For $j = 1, \ldots, 2^n$, let $a_j = 1$ if the jth string of length n belongs to A, $a_j = 0$ otherwise. By standard techniques [2], the result of each path of M^A is obtained by evaluating a multilinear polynomial over $a_1, \ldots, a_{2^n}$ and identifying a result 1 with ACCEPT and -1 with REJECT; this polynomial has integer coefficients and degree $p(n)$ or less. Gap(M^A, x) is equal to the sum of these multilinear polynomials, which we denote by $h_n(a_1, \ldots, a_{2^n})$. Note that $g_A(x) = \sum_{1\le j\le 2^n} a_j$. Therefore, $f(\sum_{1\le j\le 2^n} a_j) = h_n(a_1, \ldots, a_{2^n})$, so h_n is a symmetric function. Therefore, by Lemma 1, there are integers $c_1, \ldots, c_{p(n)}$ such that

$$h_n(a_1, \ldots, a_{2^n}) = \sum_{0\le i\le p(n)} c_i \binom{\sum_{1\le j\le 2^n} a_j}{i},$$

so, for $0 \le N \le 2^n$,

$$f(N) = h_n(N) = \sum_{0\le i\le p(n)} c_i \binom{N}{i}.$$

Let $H_n(N) = \sum_{0\le i\le p(n)} c_i \binom{N}{i}$. Then, for $0 \le N \le 2^n$, $f(N) = H_n(N)$. For all $n \ge \ell$, the univariate polynomials H_n and H_{n+1} have the same value on at least 2^n points but both have degree less than 2^n, so $H_n = H_{n+1}$. Consequently, $H_n = H_\ell$ for all $n \ge \ell$. Therefore for all $N \ge 0$,

$$f(N) = H_\ell(N) = \sum_{0\le i\le p(\ell)} c_i \binom{N}{i}.$$

We complete the proof by letting $k = p(\ell)$. ∎

Because every #P function is a GapP function, the following is an immediate consequence of Lemma 2:

Theorem 3. *Let f be a function from $\mathbb{Z}$ to $\mathbb{Z}$. If, for every oracle A and every function $g \in \mathrm{GapP}^A$ we have $f \circ g \in \mathrm{GapP}^A$, then there exists a finite sequence of integers $c_0, \ldots, c_k$ such that*

$$f(N) = \sum_{0\le i\le k} c_i \binom{N}{i}.$$

The converse follows from well known closure properties of GapP [5]. We note that this characterization is not surprising because many oracle constructions for counting classes hinge on the nonexistence of polynomials of this type (for example, [1, 3, 2]).

Theorem 4 ([6]). *Let f be a function from $\mathbb{N}$ to $\mathbb{N}$. If, for every oracle A and every function $g \in \#\mathrm{P}^A$ we have $f \circ g \in \#\mathrm{P}^A$, then there exists a finite sequence of natural numbers $c_0, \ldots, c_k$ such that*

$$f(N) = \sum_{0\le i\le k} c_i \binom{N}{i}.$$

Proof: Define g_A as in the proof of Lemma 2. Let f be a function from N to N. Assume that for every A, $f \circ g_A \in \mathrm{GapP}^A$. As in the proof of Lemma 2, there exists an oracle NPTM $M^{()}$ such that for all A, for all x, $f(g_A(x)) = \mathrm{Gap}(M^A, x)$.

Let M run in time $p(n)$. Let ℓ be the least positive integer such that for all $n \geq \ell$, $p(n) < 2^{n-1}$. Let $n \geq \ell$. Let $x = 0^n$. Let A contain no elements of length different from n. For $j = 1, \ldots, 2^n$, let $a_j = 1$ if the jth string of length n belongs to A, $a_j = 0$ otherwise. Let $\overline{a}_j = 1 - a_j$.By standard techniques [2], the result of each path of M^A is obtained by evaluating a multilinear polynomial over $a_1, \ldots, a_{2^n}, \overline{a}_1, \ldots, \overline{a}_{2^n}$ and identifying a result 1 with ACCEPT and 0 with REJECT; this polynomial has nonnegative integer coefficients and degree $p(n)$ or less. $\mathrm{Gap}(M^A, x)$ is equal to the sum of these multilinear polynomials, which we denote by $h_n(a_1, \ldots, a_{2^n})$. Note that $g_A(x) = \sum_{1 \leq j \leq 2^n} a_j$. Therefore, $f(\sum_{1 \leq j \leq 2^n} a_j) = h_n(a_1, \ldots, a_{2^n})$, so h_n is a symmetric function. Therefore, by Lemma 1, there are integers $c_1, \ldots, c_{p(n)}$ such that

$$h_n(a_1, \ldots, a_{2^n}) = \sum_{0 \leq i \leq p(n)} c_i \binom{\sum_{1 \leq j \leq 2^n} a_j}{i}.$$

We will show that $c_i \geq 0$ for each i.

The function h is a positive linear combination of terms of the form

$$t(a_1, \ldots, a_{2^k}) = \prod_{i \in U} a_i \prod_{i \in V} \overline{a}_i .$$

where $U \cap V = \emptyset$ and $|U \cup V| \leq k$. Call t a U-term if the product of positive literals is taken over the set U. If we set $a_i = 1$ iff $i \in U$, that makes $t(a_1, \ldots, a_{2^k}) = 1$ for all U-terms t and $t(a_1, \ldots, a_{2^k}) \geq 0$ for all other U-terms. Therefore the number of terms with a fixed U is bounded by $f(|U|)$. Now suppose that $c_m < 0$ for some m. That means that when we expand the terms in h we get every product of the form $-a_{i_1} \cdots a_{i_m}$ where $i_1 < \cdots < i_m$. These products can only come from U-terms where $|U| \leq m - 1$. The total number of such terms is bounded by $\sum_{0 \leq i \leq m-1} f(i) \binom{2^n}{i} = O\left(\binom{2^n}{m-1}\right)$, and each of those term contributes at most k products of the desired form, for a total of $O\left(\binom{2^n}{m-1}\right)$. However there are $\binom{2^n}{m}$ products of the form $-a_{i_1} \cdots a_{i_m}$, so we have $\binom{2^n}{m} = O\left(\binom{2^n}{m-1}\right)$. This contradiction implies that $c_m \geq 0$.

Continuing as in the proof of Lemma 2, we obtain

$$f(N) = \sum_{0 \leq i \leq p(\ell)} c_i \binom{N}{i}.$$

∎

Define a function ∇f by $(\nabla f)(n) = f(n+1) - f(n)$.

Corollary 5. *f is a relativizable closure property of #P iff ∇f is a relativizable closure property of #P.*

On the surface, this is a surprising corollary because ∇ is not a relativizable closure property of #P. In contrast, the corresponding statement for GapP is obvious (even unrelativized).

4. Extension

Finally we note that analogous results hold for functions f of any fixed number of variables.

Theorem 6. *Let f be a function from $\mathbb{Z}^d$ to $\mathbb{Z}$. If, for every oracle A and every d-tuple of function $g_1, \ldots, g_d$ in* GapP^A *we have $f \circ (g_1, \ldots, g_d) \in \mathrm{GapP}^A$, then there exists a positive integer k and collection of integers $c_{i_1 \cdots i_d}$ such that*

$$f(N) = \sum_{0 \le i_1, \ldots, i_d \le k} c_{i_1 \cdots i_d} \binom{N}{i_1} \cdots \binom{N}{i_d}.$$

Theorem 7 ([6]). *Let f be a function from $\mathbb{N}^d$ to $\mathbb{N}$. If, for every oracle A and every d-tuple of function $g_1, \ldots, g_d$ in $\#\mathrm{P}^A$ we have $f \circ (g_1, \ldots, g_d) \in \#\mathrm{P}^A$, then there exists a positive integer k and a collection of nonnegative integers $c_{i_1 \cdots i_d}$ such that*

$$f(N) = \sum_{0 \le i_1, \ldots, i_d \le k} c_{i_1 \cdots i_d} \binom{N}{i_1} \cdots \binom{N}{i_d}.$$

The proofs are very similar to the ones given for univariate fs. As they involve no new ideas, they are omitted.

Acknowledgments

We thank Bill Gasarch for proofreading and Uli Hertrampf, Heribert Vollmer, and Klaus Wagner for an advance copy of their paper.

References

[1] J. Aspnes, R. Beigel, M. Furst, and S. Rudich. The expressive power of voting polynomials. *Combinatorica*, 14(2):1–14, 1994.

[2] R. Beigel. The polynomial method in circuit complexity. In *Proceedings of the 8th Annual Conference on Structure in Complexity Theory*, pages 82–95, 1993.

[3] R. Beigel. Perceptrons, PP, and the polynomial hierarchy. *Comp. Complexity*, 4:339–349, 1994. Special issue devoted to the 4th Annual McGill Workshop on Complexity Theory.

[4] R. Beigel and J. Gill. Counting classes: Thresholds, parity, mods, and fewness. *Theoretical Computer Science*, 103(1):3–23, 1992.

[5] S. Fenner, L. Fortnow, and S. Kurtz. Gap-definable counting classes. In *Proceedings of the 6th Annual Conference on Structure in Complexity Theory*, pages 30–42. IEEE Computer Society Press, 1991.

[6] U. Hertrampf, H. Vollmer, and K. Wagner. On the power of number-theoretic operations with respect to counting. In *Proceedings of the 10th Annual Conference on Structure in Complexity Theory*, pages 299–314, 1995.

[7] M. L. Minsky and S. A. Papert. *Perceptrons*. MIT Press, Cambridge, MA, 1988. Expanded version of the original 1968 edition.