A Nonapproximability Result for Finite Function Generation

P. Jonsson

Department of Computer and Information Science, Linköping University, S-581 83 Linköping, Sweden

Abstract

We show that an optimization problem in connection with FINITE FUNCTION GENERATION is PSPACE-hard to approximate within an exponential lower bound.

Keywords: Computational complexity, approximation, function generation, PSPACE

1 Introduction

Approximation of NP-complete optimization problems has been a very active area of research for some years. However, approximability results for PSPACE-hard problems have only recently begun to appear in the literature [1,3,5]. In this paper, we study an optimization version of the FINITE FUNCTION GENERATION (FFG) problem. FFG is defined as follows:

INSTANCE: A triple $\langle A, F, h\rangle$ where A is a finite set, F is a collection of total functions on A and h is a total function on A.
QUESTION: Does there exist a sequence $\langle f_{i_1}, \ldots, f_{i_k}\rangle$ of functions taken from F such that $f_{i_1} \circ \ldots \circ f_{i_k} = h$?

The symbol $\circ$ denotes function composition, *i.e.*, $f \circ g(x) = f(g(x))$, and we assume that the functions are represented as explicit look-up tables. Kozen [4] has proved that FFG is PSPACE-complete. Next, we define a function $\mathcal{L}$ that computes the least number of functions that have to be composed in order to solve an FFG instance.

Definition 1 *Let* $\mathbf{S} = \{\Gamma ; \Gamma$ *is an FFG instance and* Γ *has a solution*$\}$. *Define the function* $\mathcal{L} : \mathbf{S} \to \mathbb{N}$ *such that*

$$\mathcal{L}(\Gamma) = \min\{|\omega| \, ; \, \omega \textit{ is a solution to } \Gamma\}.$$

$|\omega|$ denotes the number of functions in the sequence ω.

Obviously, it is meaningless to define $\mathcal{L}$ on instances which have no solutions. Let $\Gamma = \langle A, F, h\rangle$ be an instance of FFG and define $|\Gamma| = |A|$. We say that an algorithm T *approximates* $\mathcal{L}$ within some function $f : \mathbb{N} \to \mathbb{R}$ iff $\mathcal{L}(\Gamma) \leq T(\Gamma) \leq f(|\Gamma|) \cdot \mathcal{L}(\Gamma)$ for all $\Gamma \in \mathbf{S}$. A function g is PSPACE-hard iff PSPACE $\subseteq \mathrm{P}^g$, *i.e.*, if every language in PSPACE can be recognized in polynomial time with an oracle for g. By "approximating $\mathcal{L}$ within f is PSPACE-hard" we mean that, if T approximates $\mathcal{L}$ within f, then T is PSPACE-hard. In the rest of this paper, we prove PSPACE-hardness of approximating $\mathcal{L}$ within a certain exponential function.

2 Preliminaries

We begin by providing an upper bound on $\mathcal{L}$.

Lemma 2 *If $\Gamma = \langle A, F, h\rangle \in \mathbf{S}$ then $\mathcal{L}(\Gamma) \leq |\Gamma|^{|\Gamma|}$.*

Proof. Construct a directed graph $G = \langle V, E\rangle$ with the total functions from A to A as nodes. Insert an edge from v_i to v_j iff there exists a function $f \in F$ such that $f \circ v_i = v_j$. Let id_A denote the identity function on A. Obviously, there exists a path ω from id_A to the function h since Γ has a solution.

Without loss of generality, assume ω to be the shortest such path and observe that $|\omega| = \mathcal{L}(\Gamma)$. Furthermore, $|\omega| \leq |V|$ since ω is the shortest path between two nodes in the graph G. There are $|\Gamma|^{|\Gamma|}$ functions from A to A so $\mathcal{L}(\Gamma) \leq |\Gamma|^{|\Gamma|}$ and the lemma follows. $\Box$

A *cycle* is a permutation σ on a finite, ordered set $B = \{b_1, \ldots, b_n\}$ such that $\sigma(b_1) = b_2, \sigma(b_2) = b_3, \ldots, \sigma(b_n) = b_1$. We use the standard notation $(b_1, \ldots, b_n)$ to denote such a cycle. The *length* of a cycle σ is the size of the set on which it is defined. Let π be an arbitrary permutation on a finite set B. The *order* of π, $o(\pi)$, is the smallest integer $n > 0$ such that $\pi^n = \mathsf{id}_B$.

Theorem 3 *Given any permutation π on a finite set B, the set B may be divided into disjoint subsets such that π is a cycle on each subset. Furthermore, the order of π is the least common multiple of the lengths of these cycles.*

The proof of Theorem 3 appears in [2]. The next lemma contains the construction that underlies the proof of the main theorem.

Lemma 4 *For arbitrary $n \geq 20$, there exists a set B and a permutation π on B satisfying $|B| \leq 2n^2 \ln n - n$ and $o(\pi) \geq n!$ where $n!$ denotes the factorial of n and $\ln(n)$ the natural logarithm of n.*

Proof. Let p_i, $i \geq 1$, denote the primes with $p_1 = 2$, $p_2 = 3$ and so on. If σ is a cycle on a set A and π is a cycle on a set A' then we can compose σ and π with function composition and obtain a permutation on $A \cup A'$. Let $B = \bigcup_{i=1}^{n} \{b_1^i, \ldots, b_{p_i}^i\}$ where $b_j^i = b_\ell^k$ iff both $i = k$ and $j = \ell$. Further, let $\pi = (b_1^1, b_2^1) \circ (b_1^2, \ldots, b_{p_2}^2) \circ \ldots \circ (b_1^n, \ldots, b_{p_n}^n)$ and note that π is a permutation on B.

We begin by showing that $|B| \leq 2n^2 \ln n - n$. Clearly, $|B| = \sum_{i=1}^{n} p_i$. Rosser and Schoenfield [6] have established the bound $p_n < n(\ln n + \ln\ln n - 1/2)$ for $n \geq 20$. Hence, $|B| = \sum_{i=1}^{n} p_i \leq n \cdot p_n \leq n^2(\ln n + \ln\ln n - 1/2) \leq 2n^2 \ln n - n$.

We continue by proving that $o(\pi) \geq n!$. By definition, $(b_1^1, b_2^1), \ldots, (b_1^n, \ldots, b_{p_n}^n)$ are the disjoint cycles of π. Theorem 3 states that $o(\pi)$ is the least common multiple of $p_1, \ldots, p_n$. Since $p_1, \ldots, p_n$ are distinct primes, the least common multiple of them is $\prod_{i=1}^{n} p_i$. It follows that $\prod_{i=1}^{n} p_i \geq n!$ since $p_i \geq i$ for $i \geq 1$. $\square$

3 Non-approximability of $\mathcal{L}$

We can now prove the main theorem.

Theorem 5 *$\mathcal{L}$ is* PSPACE*-hard to approximate within some function $f(n) \in 2^{\Omega(n \log n)}$ where $\log(n)$ denotes the 2-logarithm of n.*

Proof. Polynomial-time reduction from the PSPACE-complete problem FFG. Arbitrarily choose an instance $\Gamma = \langle A, F, h \rangle$ of FFG such that $|\Gamma| \geq 20$ and $F = \{f_1, \ldots, f_p\}$. Let $m = |\Gamma|$. We define $\Gamma' = \langle A', F', h' \rangle$ as follows: Let $B = \{b_1, \ldots, b_k\}$ be a set such that

(i) $A \cap B = \emptyset$; and
(ii) $k \leq 2(m^2)^2 \ln(m^2) - m^2 = 4m^4 \ln m - m^2$; and
(iii) there exists an permutation π on B such that $o(\pi) \geq (m^2)!$.

By Lemma 4, since $m \geq 20$, we know that such a B and π exist. Note that $|A \cup B| = 4m^4 \ln m - m^2 + m$. Choose a set C such that A, B and C are disjoint and $|A \cup B \cup C| = 4m^4 \ln m$. Let $A' = A \cup B \cup C$ and $n = |A'|$. The only reason for introducing C is to ensure that $n = 4m^4 \ln m$ holds.

Let $F' = \{f'_1, \ldots, f'_p, G', \pi'\}$ be a collection of functions on A', defined as follows:

$$f'_i(x) = \begin{cases} f_i(x) & \text{if } x \in A \\ x & \text{if } x \in B \cup C \end{cases}$$

$$G'(x) = \begin{cases} h(x) & \text{if } x \in A \\ \pi(x) & \text{if } x \in B \\ x & \text{if } x \in C \end{cases}$$

$$\pi'(x) = \begin{cases} x & \text{if } x \in A \cup C \\ \pi(x) & \text{if } x \in B \end{cases}$$

Finally, define the function h' as

$$h'(x) = \begin{cases} h(x) & \text{if } x \in A \\ x & \text{if } x \in B \cup C \end{cases}$$

It is obvious that we can transform $\langle A, F, h\rangle$ to $\langle A', F', h'\rangle$ in polynomial time since $n = 4m^4 \ln m$. We continue by showing two properties of Γ'.

(i) If Γ has a solution, then $\mathcal{L}(\Gamma') \leq m^m$. Assume $h = f_{i_1} \circ \ldots \circ f_{i_j}$ where $f_{i_1}, \ldots, f_{i_j} \in F$. By Lemma 2, $j \leq m^m$. Thus, $h' = f'_{i_1} \circ \ldots \circ f'_{i_j}$ is a solution to Γ' containing less than m^m functions.

(ii) If Γ has no solution, then $\mathcal{L}(\Gamma') \geq (m^2)!$. Since Γ has no solution, there is no sequence $\langle f'_{i_1}, \ldots, f'_{i_j}\rangle$ such that $f'_{i_1} \circ \ldots \circ f'_{i_j}(x) = h(x)$ for arbitrary $x \in A$. Thus, we must use the function G' which satisfies $G'(x) = h(x)$ for $x \in A$. But G' has the side-effect $G'(x) = \pi(x)$ for $x \in B$. However, we can use the permutation π' to remedy this. Since we chose π such that $o(\pi) \geq (m^2)!$, we have that, for any integer ℓ such that $(\pi')^\ell \circ G' = h'$, it holds $\ell \geq (m^2)!$.

Hence, Γ' has a solution and $\mathcal{L}$ is defined on Γ'. Assume that L' is a function that approximates $\mathcal{L}$ within $((m^2)! - 1)/m^m$. If Γ has a solution then $\mathcal{L}(\Gamma') \leq m^m$. Hence,

$$L'(\Gamma') \leq m^m \cdot \frac{(m^2)! - 1}{m^m} = (m^2)! - 1.$$

Assume to the contrary that Γ has no solution. Then $\mathcal{L}(\Gamma') \geq (m^2)!$ and $L'(\Gamma') \geq (m^2)!$. Hence, Γ has a solution iff $L'(\Gamma') \leq (m^2)! - 1$. We can, thus, recognize every language in PSPACE in polynomial time with an oracle for L'. It remains to show that $\frac{(m^2)!-1}{m^m} \in 2^{\Omega(n \log n)}$.

We have that

$$\frac{(m^2)!-1}{m^m} \geq \frac{(m^2/\mathrm{e})^{m^2}-1}{m^m} = \frac{2^{m^2\log(m^2/\mathrm{e})}-1}{2^{m\log m}} \in 2^{\Omega(m^2\log m)}$$

by applying Sterling's formula. Since $n = 4m^4 \ln m$ it follows that $m^4 = n/(4\ln m) \geq n/(4\ln n)$ and $m \geq (n/(4\ln n))^{1/4}$. Furthermore, note that $m \geq n^{1/5}$ so

$$2^{\Omega(m^2\log m)} \subseteq 2^{\Omega(\sqrt{\frac{n}{4\ln n}}\cdot\ln(n^{1/5}))} \subseteq 2^{\Omega(\sqrt{n\log n})}$$

which concludes the proof. $\square$

Acknowledgements

Thanks to Thomas Drakengren, Christer Bäckström and the anonymous referees for helpful comments.

References

[1] A. Condon, J. Feigenbaum, C. Lund, and P. W. Shor. Probabilistically checkable debate systems and nonapproximability of PSPACE-hard functions. *Chicago Journal of Theoretical Computer Science*, (1995) article 4.

[2] M. Hall. *The theory of groups.* (The Macmillan Company, New York, 1959).

[3] H. Hunt III, M. Marathe, and R. Stearns. Generalized CNF satisfiability problems and non-efficient approximability, in: *Proc. 9th Structure in Complexity Theory Conf.* (1994) 356–366.

[4] D. Kozen. Lower bounds for natural proof systems, in: *Proc. 18th Ann. Symp. on Foundations of Comp. Sci.* (1977) 254–266.

[5] M. Marathe, H. Hunt III, R. Stearns, and V. Radhakrishnan. Hierarchical specifications and polynomial-time approximation schemes for PSPACE-complete problems, in: *Proc. 26th Ann. ACM Symp. on the Theory of Computing* (1994) 468–477.

[6] J. B. Rosser and L. Schoenfield. Approximate formulas for some functions of prime numbers. *Ill. J. of Math.* **6** (1962) 64–94.