A Randomness-Efficient Sampler for Matrix-valued Functions and Applications

Avi Wigderson
Institute for Advanced Study
Princeton, NJ 08540
avi@ias.edu

David Xiao
Princeton University
Princeton, NJ 08544
dxiao@cs.princeton.edu

Abstract

In this paper we give a randomness efficient sampler for matrix-valued functions. Specifically, we show that a random walk on an expander approximates the recent Chernoff-like bound for matrix-valued functions of Ahlswede and Winter [1], in a manner which depends optimally on the spectral gap. The proof uses perturbation theory, and is a generalization of Gillman's and Lezaud's analysis of the Ajtai-Komlos-Szemeredi sampler for real-valued functions [11, 21, 2].

Derandomizing our sampler gives a few applications, yielding deterministic polynomial time algorithms for problems in which derandomizing independent sampling gives only quasi-polynomial time deterministic algorithms. The first (which was our original motivation) is to a polynomial-time derandomization of the Alon-Roichman theorem [4, 20, 22]: given a group of size n, find $O(\log n)$ elements which generate it as an expander. This implies a second application - efficiently constructing a randomness-optimal homomorphism tester, significantly improving the previous result of Shpilka and Wigderson [29]. The third is to a "non-commutative" hypergraph covering problem - a natural extension of the set-cover problem which arises in quantum information theory (e.g. [1, 16]), in which we effciently attain the integrality gap when the fractional semi-definite relaxation cost is constant.

1. Introduction

1.1. Background

The Chernoff bound [8] and its variants are among the most useful mathematical results, and in particular are extremely useful in theoretical computer science. Roughly stated, it says that if we wish to estimate the mean of a bounded real function on some domain V, the average of the values at k independent samples deviates from the true mean (by a small additive constant) only with error probability bounded by $2^{-\Omega(k)}$. Note that if every sample requires r random bits, this sampling procedure requires a total of rk random bits to achieve error $2^{-\Omega(k)}$.

A remarkable construction and analysis of Ajtai, Komlos and Szemeredi [2] suggested a way of achieving essentially the same error using only $r + O(k)$ bits. The idea is to impose a good constant degree *expander* graph G on the vertex set V, and select k (highly dependent) samples by taking a random path of length k in this graph. The analysis of this sampler due to Gillman [11], which is the first to consider sampling any bounded real function (see also [18, 21]), shows that the error is bounded by $2^{-\Omega(\varepsilon k)}$, where ε is the *spectral gap* of the random walk on the expander G. The fact that explicit families of constant degree expanders with constant spectral gap are known [10, 24, 23, 27] show that such a randomness-efficient sampler can be efficiently implemented.

This sampler has become a paramount tool in theoretical computer science. Indeed, it has found a large number of applications in such a variety of areas as deterministic amplification [9, 17], security amplification in cryptography [14], hardness of approximation [5, 3], extractor construction (e.g. see surveys [26, 13, 28]), construction of efficient error-correcting codes [30, 7], construction of ε-biased spaces [25] and much more. In algorithmic applications, including some of the ones above, often both r and k are $O(\log n)$ where $n = |V|$ is the input size of the problem, so derandomizing simply (i.e. enumerating all possible values of the random bits) the independent sampling requires quasi-polynomial time, while the AKS-sampler can be derandomized in polynomial time.

Recently, a Chernoff-like bound was introduced by Ahlswede and Winter [1] for matrix-valued random variables. Here we seek to estimate the average of a function from V to $d \times d$ complex Hermitian[1] matrices of bounded norm. The [1] generalization of the Chernoff bound states that the average of k independent points deviates significantly in norm from the mean with probability bounded by

[1] For all practical purposes the reader can think of real symmetric matrices.