Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 107 (2005)

Retraction of Wigderson-Xiao, "A Randomness-Efficient Sampler for Matrix-valued Functions and Applications", ECCC TR05-107

Avi Wigderson David Xiao

August 27, 2006

Abstract

We discovered an error in the proof of the main theorem of *A Randomness-Efficient Sampler for Matrix-valued Functions and Applications*, which appears as ECCC TR05-107 [WX05a], and also appeared in FOCS [WX05b]. We describe it below. This error invalidates all of the results concerning the expander walk sampler for matrix-valued functions.

Nevertheless, we are able to use a different technique to prove the main applications of the sampler that appear in that paper. These include a deterministic algorithm for constructing logarithmic-degree Cayley graphs on any group (derandomizing Alon-Roichman's theorem [AR94]), and for the quantum hypergraph cover problem, described in Ahlswede-Winter [AW02]. We state the correct result - the manuscript with their proof, under the title *Derandomizing the AW matrix-valued Chernoff bound using pessimistic estimators and applications*, is available as ECCC TR06-105 [WX06] and also will appear on our homepages

1 Error in the proof of the main theorem

We discovered a (seemingly fatal) error in the proof of the main theorem of [WX05a]. This invalidates all the expander walk sampler results of [WX05a]. Fortunately the main applications survive via a completely different technique.

The error in [WX05a] is in the application of the Golden-Thompson inequality. The following derivation, which appears in the proof of Theorem 3.6 at the top of page 12 of [WX05a], is incorrect:

$$\mathbb{E}[\mathrm{Tr}(\exp\left(t\sum_{i=1}^{k} f(Y_i)\right))] \leq \mathbb{E}[\mathrm{Tr}(\prod_{i=1}^{k}\exp(tf(Y_i)))] \tag{1.1}$$

where the Y_i are the steps in a random expander walk and the expectation is over all walks. This is incorrect because the Golden-Thompson inequality does not generalize to more than two terms, i.e. the following does *not* hold in general for real symmetric matrices A, B, C:

$$\mathrm{Tr}(\exp(A+B+C)) \leq \mathrm{Tr}(\exp(A)\exp(B)\exp(C))$$

and it is not hard to come up with counterexamples.

The false inequality above is not needed in full generality for the proof. In the notation of [WX05a], it would suffice to prove

$$\mathrm{Tr}(\mathbb{E}[\exp(t\sum_{i=2}^{k} f(Y_i))\exp(tf(Y_1))]) \leq \|\tilde{A}\tilde{D}_t\| \cdot \mathrm{Tr}(\mathbb{E}[\exp(t\sum_{i=2}^{k} f(Y_i))])$$

or even only

$$\mathrm{Tr}(\mathbb{E}[\exp(t\sum_{i=1}^{k} f(Y_i))]) \leq d\|\tilde{A}\tilde{D}_t\|^k$$

ISSN 1433-8092

since the analysis of the above norm $\|\tilde{A}\tilde{D}_t\|$ via perturbation theory remains correct.

We do know that both the previous inequalities hold when the normalized adjacency matrix of the graph $A = J/n$ where J is the all 1's matrix, i.e. we sample from the complete graph, which corresponds to independent sampling. We do not know counter-examples for either of these inequalities for sampling according to an expander walk, namely for A is the random walk matrix on any regular graph. Thus, as far as we know, our main Theorem 3.6 of [WX05a] may be true as stated.

Our attempts to prove even weaker versions of Theorem 3.6 that would suffice for the applications failed.

2 Surviving results

All applications of the sampler listed in the paper do hold, though via a completely different proof. These theorems are stated below. For definitions, details, and proofs, see the paper *Derandomizing the AW matrix-valued Chernoff bound using pessimistic estimators and applications*, which is available as an ECCC report [WX06] and also will appear on the authors' websites.

Theorem 2.1 (Corresponds to Theorem 1.2 of [WX05a]). *Fix* $\gamma < 1$. *There exists an algorithm that, given a group* H *of size* n *as a multiplication table, constructs a symmetric multi-set* $S \subseteq H$ *of size* $|S| = O(\frac{1}{\gamma^2}\log n)$ *such that the second-largest eigenvalue of the Cayley graph* $\mathrm{Cay}(H; S)$ *is at most* γ. *The algorithm runs in time* $\mathrm{poly}(n)$.

Corollary 2.2 (Corresponds to Corollary 1.3 of [WX05a]). *Given an arbitrary group* H *of size* n*, one can construct in time* $\mathrm{poly}(n)$ *a* homomorphism tester *for functions on* H *which uses only* $\log n + \log\log n + O(1)$ *random bits.*

Theorem 2.3 (Supersedes Theorem 4.5 of [WX05a]). *Suppose we are given* $\Gamma = (\mathcal{V}, \mathcal{E})$ *a quantum hypergraph with fractional cover number* $\tilde{c}(\Gamma)$*, with* $|\mathcal{V}| = d$ *and* $|\mathcal{E}| = n$. *Then we can find an integer cover of* Γ *of size* $k = \tilde{c}(\Gamma) \cdot O(\log d)$ *in time* $\mathrm{poly}(n, d)$.

In addition, all of the theorems of [WX05a] still hold when restricted to real-valued functions, since Inequality 1.1 holds in the one-dimensional case. In particular, Theorem C.1 of [WX05a] holds for real-valued functions, which was used by Zuckerman [Zuc05]. We do not state our version here, as an even better version was proven by Healy [Hea06].

References

[AW02] R. Ahlswede and A. Winter. Strong Converse for Identification via Quantum Channels. *IEEE Transactions on Information Theory*, 48(3):569–579, 2002.

[AR94] N. Alon and Y. Roichman. Random Cayley Graphs and Expanders. *RSA: Random Structures & Algorithms*, 5, 1994.

[Hea06] A. Healy. Randomness-Efficient Sampling within $\mathbf{NC}^1$. ECCC Report TR06-058, 2006.

[WX05a] A. Wigderson and D. Xiao. A randomness-efficient sampler for matrix-valued functions and applications. ECCC Report TR05-107, 2005.

[WX05b] A. Wigderson and D. Xiao. A randomness-efficient sampler for matrix-valued functions and applications. In *Proc. 46th FOCS*, 2005.

[WX06] A. Wigderson and D. Xiao. Derandomizing the AW matrix-valued Chernoff bound using pessimistic estimators and applications. ECCC Report TR06-105, 2006.

[Zuc05] D. Zuckerman. Linear Degree Extractors and the Inapproximability of Max Clique and Chromatic Number. ECCC Report TR05-100, 2005.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de/