

Randomness-efficient Low Degree Tests and Short PCPs via Epsilon-Biased Sets

Eli Ben-Sasson^{*}

DEAS, Harvard University and
LCS, MIT
Cambridge, MA
eli@eecs.harvard.edu

Madhu Sudan[†]

Laboratory for Computer Science
Massachusetts Institute of Technology
Cambridge, MA
madhu@mit.edu.

Salil Vadhan[‡]

Harvard University,
Division of Engineering and Applied Sciences,
Maxwell Dworkin 337, 33 Oxford Street
Cambridge, MA 02138, USA.
salil@eecs.harvard.edu.

Avi Wigderson

Institute for Advanced Study, Princeton and the
Hebrew University, Jerusalem.
Address: Institute for Advanced Study, School of
Math., Einstein Drive, Princeton, NJ 08540.
avi@ias.edu

ABSTRACT

We present the first *explicit* construction of Probabilistically Checkable Proofs (PCPs) and Locally Testable Codes (LTCs) of fixed constant query complexity which have almost-linear ($= n \cdot 2^{\tilde{O}(\sqrt{\log n})}$) size. Such objects were recently shown to exist (nonconstructively) by Goldreich and Sudan [17]. Previous explicit constructions required size $n^{1+\Omega(\epsilon)}$ with $1/\epsilon$ queries.

The key to these constructions is a nearly optimal randomness-efficient version of the low degree test [32]. In a similar way we give a randomness-efficient version of the BLR linearity test [13] (which is used, for instance, in locally testing the Hadamard code).

The derandomizations are obtained through ϵ -biased sets for vector spaces over finite fields. The analysis of the derandomized tests rely on alternative views of ϵ -biased sets — as generating sets of Cayley expander graphs for the low degree test, and as defining linear error-correcting codes for the linearity test.

^{*}Supported by NSF grants CCR-0133096, CCR-9877049, CCR 0205390, and NTT Award MIT 2001-04.

[†]Supported in part by NSF Awards CCR 0205390, and NTT Award MIT 2001-04.

[‡]URL: <http://www.eecs.harvard.edu/~salil>. Supported by NSF grant CCR-0133096 and a Sloan Research Fellowship.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

STOC'03, June 9–11, 2003, San Diego, California, USA.
Copyright 2003 ACM 1-58113-674-9/03/0006 ...\$5.00.

Categories and Subject Descriptors

F.2.2 [Theory of Computation]: Analysis of Algorithms and Problem Complexity—*Nonnumerical Algorithms and Problems, Complexity of proof procedures*; E.4 [Data]: Coding and Information Theory

General Terms

Theory

Keywords

Probabilistically Checkable Proofs, Locally Testable Codes, Property Testing, Linearity Testing, Low Degree Testing

1. INTRODUCTION

Low degree testing, the problem of testing the proximity of a function to a family of low-degree functions has been a subject of intense examination in the past decade. On the one hand, this task opens up a wide range of intriguing mathematical questions. On the other hand, success in designing and analyzing efficient tests has led to great strides in the design of probabilistically checkable proofs (PCPs) and more recently, in new families of error-correcting codes called locally testable codes (LTCs). In this paper we explore the randomness requirement of such tests and reduce them significantly. Our results translate to explicit constructions of PCPs and LTCs of almost-linear size. We start with some background material.

1.1 PCPs

Probabilistically Checkable Proofs (PCPs) are by now a fundamental object of study in theoretical computer science. The essence of a PCP system is the PCP verifier — a probabilistic algorithm that is given a claimed theorem statement as input and is given oracle access to a purported proof of the theorem. The PCP verifier is allowed to query the proof