

# Improved derandomization of BPP using a hitting set generator

Oded Goldreich

Avi Wigderson

## Abstract

A hitting-set generator is a deterministic algorithm which generates a set of strings that intersects every dense set recognizable by a small circuit. A polynomial time hitting-set generator readily implies  $RP=P$ . Andreev et. al (ICALP'96 and JACM 1998) showed that if polynomial-time hitting-set generator in fact implies the much stronger conclusion  $BPP=P$ . We simplify and improve their (and later) constructions.