New Direct-Product Testers and 2-Query PCPs

Russell Impagliazzo [*] Valentine Kabanets [†] Avi Wigderson [‡]

February 25, 2009

Abstract

The "direct product code" of a function f gives its values on all k-tuples $(f(x_1), \ldots, f(x_k))$. This basic construct underlies "hardness amplification" in cryptography, circuit complexity and PCPs. Goldreich and Safra [GS00] pioneered its local *testing* and its PCP application. A recent result by Dinur and Goldenberg [DG08] enabled for the first time testing proximity to this important code in the "list-decoding" regime. In particular, they give a 2-query test which works for *polynomially small* success probability $1/k^{\alpha}$, and show that no such test works below success probability $1/k$.

Our main result is a 3-query test which works for *exponentially small* success probability $\exp(-k^{\alpha})$. Our techniques (based on recent simplified decoding algorithms for the same code [IJKW08]) also allow us to considerably simplify the analysis of the 2-query test of [DG08]. We then show how to *derandomize* their test, achieving a code of polynomial rate, independent of k, and success probability $1/k^{\alpha}$.

Finally we show the applicability of the new tests to PCPs. Starting with a 2-query PCP over an alphabet Σ and with soundness error $1 - \delta$, Rao [Rao08] (building on Raz's (k-fold) parallel repetition theorem [Raz98] and Holenstein's proof [Hol07]) obtains a new 2-query PCP over the alphabet Σ^k with soundness error $\exp(-\delta^2 k)$. Our techniques yield a 2-query PCP with soundness error $\exp(-\delta\sqrt{k})$; this is incomparable to Rao's result [Rao08] since our bound also applies when $k < 1/\delta$. Our PCP construction turns out to be essentially the same as the miss-match proof system defined and analyzed by Feige and Kilian [FK00], but with simpler analysis and exponentially better soundness error.

[*] U. C. San Diego and Institute for Advanced Study; russell@cs.ucsd.edu

[†] Simon Fraser University; kabanets@cs.sfu.ca

[‡] Institute for Advanced Study; avi@ias.edu