Almost Optimal $\epsilon$ Bias

Abstract:

The question of finding an $\epsilon$-biased set with close to optimal support size, or, equivalently, finding an explicit binary code with distance $1/2-\epsilon$ and rate close to the Gilbert-Varshamov bound, attracted a lot of attention in recent decades. In this paper we solve the problem almost optimally and show an explicit $\epsilon$-biased set over $k$ bits with support size $O(k/\epsilon^{2+o(1)})$. This improves upon all previous explicit constructions which were in the order of $k^{2}/\epsilon^{2}$, $k/\epsilon^{3}$ or $(k/\epsilon^{2})^{5/4}$. The result is close to the Gilbert-Varshamov bound which is $O(k/\epsilon^{2})$ and the lower bound which is $\Omega(k/\epsilon^{2}\log(1/\epsilon))$. The main technical tool we use is bias amplification with the $s$-wide replacement product. Rozenman and Wigderson showed how to amplify the bias more economically by choosing two samples with an expander. Based on that they suggested a recursive construction that achieves sample size $O(k/\epsilon^{4})$. We show that amplification with a long random walk over the $s$-wide replacement product reduces the bias almost optimally.