Minimax Study of Bias Correctors

Maciej Skorski

Abstract

Bias correctors are deterministic functions used to reduce the bias in physical random number generators; the most famous example is the xor function. In this talk we discuss how to construct such correctors under some prior assumptions on the input bias (for example, that the bias is bounded). We will see how to find the optimal construction by solving a min-max optimization over boolean functions. It turns out that the xor corrector is optimal when the bias is sufficiently small, but - interestingly - can be improved for certain bias values. We will also overview related results on the xor corrector, such as bias formulas due to Lacharme and Davies.