

1067-05-1120

Avraham Ben-Aroya and **Amnon Ta-Shma***, amnon@tau.ac.il. *Constructing Small-Bias Sets from Algebraic-Geometric Codes.*

We give an explicit construction of an ϵ -biased set over k bits of size $O\left(\frac{k}{\epsilon^2 \log(1/\epsilon)}\right)^{5/4}$. This improves upon previous explicit constructions when ϵ is roughly (ignoring logarithmic factors) in the range $[k^{-1.5}, k^{-0.5}]$. The construction builds on an algebraic-geometric code. However, unlike previous constructions we use low-degree divisors whose degree is significantly smaller than the genus. (Received September 19, 2010)