Abstract

A Boolean function on n variables is q-resilient if for any subset of at most q variables, the function is very likely to be determined by a uniformly random assignment to the remaining $n-q$ variables; in other words, no coalition of at most q variables has significant influence on the function. Resilient functions have been extensively studied with a variety of applications in cryptography, distributed computing, and pseudorandomness. The best known balanced resilient function on n variables due to Ajtai and Linial [AL93] is $\Omega(n/(\log^2 n))$-resilient. However, the construction of Ajtai and Linial is by the probabilistic method and does not give an efficiently computable function. In this work we give an explicit monotone depth three almost-balanced Boolean function on n bits that is $\Omega(n/(\log^2 n))$-resilient matching the work of Ajtai and Linial. The best previous explicit construction due to Meka [Meka09] (which only gives a logarithmic depth function) and Chattopadhyay and Zuckermman [CZ15] were only n^{1-c}-resilient for any constant $c < 1$. Our construction and analysis are motivated by (and simplifies parts of) the recent breakthrough of [CZ15] giving explicit two-sources extractors for polylogarithmic min-entropy; a key ingredient in their result was the construction of explicit constant-depth resilient functions. An important ingredient in our construction is a new randomness optimal oblivious sampler which preserves moment generating functions of sums of variables and could be useful elsewhere.