Spectral Distribution of Pseudo-random Matrices

Vahid Tarokh
Harvard University, USA

Abstract

In the previous century, much work has been done on the spectra of random matrices. However, not much is known about the spectra of matrices formed from pseudo-random sequences. In this talk, I will discuss some of our recent results (jointly with Behtash Babadi) in this direction.

First, we consider a binary linear block code C of length N, dimension k and minimum Hamming distance d over GF(2). Let $d^{\perp}$ denote the minimum Hamming distance of the dual code of C. Let $\epsilon : \mathrm{GF}(2)^N \rightarrow \{-1,1\}^N$ be the function induced by component-wise mapping $v_i \mapsto (-1)^{v_i}$ for $\mathbf{v} = (v_1, v_2, \cdots, v_N)$. Finally, for $p < N$, let A be a $p \times N$ random matrix whose rows are obtained by mapping a uniformly drawn set of size p of the codewords of C under ϵ. We will first show that for $d^{\perp}$ large enough and $y = p/N \in (0,1)$ fixed, as $N \rightarrow \infty$, the empirical spectral distribution of the Gram matrix of $\frac{1}{\sqrt{N}}A$ resembles that of a random i.i.d. Rademacher matrix (i.e., the Marchenko-Pastur distribution). We then present an explicit asymptotic uniform bound on the distance of the empirical spectral distribution of the aforementioned Gram matrix to the Marchenko-Pastur distribution as a function of y and $d^{\perp}$.

We then study the group randomness of pseudo-random sequences based on shortened first-order Reed- Muller codes and the Gold sequences. In particular, we characterize the empirical spectral distribution of random matrices from shortened first-order Reed-Muller codes. We show that although these sequences have very appealing randomness properties across individual codewords, they do not possess certain group randomness properties of i.i.d. sequences. In other words, the spectral distribution of random matrices from these sequences dramatically differs from that of the random i.i.d. generated matrices. In contrast, Gold sequences manifest the group randomness properties of random i.i.d. sequences. Upper bounds on the Kolmogorov complexity of these sequences are established, and it has been shown that these bounds are much lower than those of the random i.i.d. sequences, when the sequence length is large enough. We discuss the implications of these observations and motivate the need to develop novel randomness tests encompassing both individual and group randomness of sequences.

Finally, we study the spectral distribution of the product of two pseudo-random matrices based on binary block codes, and prove that if the dual distances of the underlying codes are large enough, the asymptotic spectral distribution will be close to a deterministic limit in the sense of Levy distance.