Studying cutoff for card shuffling

Evita Nestoridi

In cryptography, in casinos, and in playing board games, many times people ask the same question: how is a person (not a computer) supposed to shuffle a deck of cards? We will discuss two specific card shuffles, the random-to-random and the Bernoulli–Laplace model. The first one is a very famous shuffle, not recommended for actual shuffling purposes. The latter is the first Markov chain introduced by Markov, it came to us from cryptography, and it is practiced by many casinos. Both card shuffles exhibit a sudden transition from an unmixed state to a random one, which we call cutoff. In joint work with M. Bernstein, we prove that random to random exhibits cutoff at $\frac{3}{4}n\log n$, answering a conjecture of Diaconis. In joint works with A. Eskenazis and G. White, we also prove cutoff for the Bernoulli–Laplace model, using a combination of algebraic and probabilistic techniques.