Uniform Avoidance Coupling, Design of Anonymity Systems and Matching Theory

Ewa J. Infeld

Abstract

We start by introducing *avoidance coupling* of Markov chains, with an overview of existing results. We then introduce and motivate a new notion, *uniform coupling*. We show that the only Markovian avoidance coupling on a cycle is of this type, and that uniform avoidance coupling of simple random walks is impossible on trees, and prove that it is possible on several classes of graphs. We also derive a condition on the vertex neighborhoods in a graph equivalent to that graph admitting a uniform avoidance coupling of simple random walks, and an algorithm that tests this with run time polynomial in the number of vertices. We then discuss a conjecture that no Markovian avoidance coupling can be possible on a tree and propose how a proof might proceed.

In the second half of this work, we talk about the design of online communication systems that aim to guarantee anonymity for their users. A popular paradigm is k-anonymity. We notice that the scarcity of a typical social relation makes k-anonymity vulnerable to traffic analysis, and propose a way to use this scarcity to reduce the efficiency cost to exactly the amount of cover traffic we might need. Then we use Brègman's theorem to show that for a given infrastructure cost, modelled by the number of edges in a bipartite graph, k-anonymity offers the highest number of possible perfect matchings between users and observed behaviors.