

Kolmogorov Complexity, Pseudorandom Generators and Statistical Models Testing.

Jan Šindelář; Pavel Boček

Abstract: An attempt to formalize heuristic concepts like strings (sequences resp.) “typical” for a probability measure is stated in the paper. Both generating and testing of such strings is considered. Kolmogorov complexity theory is used as a tool.

Classes of strings “typical” for a given probability measure are introduced. It is shown that no pseudorandom generator can produce long strings from the classes. The time complexity of pseudorandom generators with oracles capable to recognize “typical” strings is shown to be at least exponential with respect to the length of the output.

Tests proclaiming some strings “typical” are introduced. We show that the problem of testing strings to be “typical” is undecidable. As a consequence, the problem of correspondence between probability measures and data is undecidable too. If the Lebesgue measure is considered, then the conditional probability of failure of a test is shown to exceed a positive lower bound almost surely.

Keywords:

AMS Subject Classification: 60B;