Imitation Games

Abstract

One of Alan Turing's most influential papers is his 1950 *Computing machinery and intelligence*, in which he introduces the famous "Turing test" for probing the nature of *intelligence* by evaluating the abilities of machines to behave as humans. In this test, which he calls the "Imitation Game," a (human) referee has to distinguish between two (remote and separate) entities, a human and a computer, only by observing answers to a sequence of arbitrary questions to each entity. Mountains of words have been written on support, critique, variants of and experimentation with this idea and its value. It is not the purpose of this lecture to discuss this body of work.

Instead, this lecture will exposit, through examples from a surprisingly diverse array of settings, the remarkable power of this idea, as revealed in the past few decades of work in the theory of computation and discrete mathematics. Wigderson will discuss variations of the Imitation Game in which we change the nature of the referee, and of the objects to be distinguished, to yield analogs of the Turing test (often called "the simulation paradigm" or "computational indistinguishability" among others in different contexts). These new Imitation Games lead to novel, precise, and operative definitions of classical notions, including *secret, knowledge, privacy, randomness, proof, fairness,* and others. These definitions have in turn led to numerous results, applications, and understanding.

Some, among many consequences of this fundamental idea, are the foundations of cryptography (from online shopping to digital elections), the surprising discoveries on the power and limits of randomness, the recent influential notion of differential privacy, and breakthrough results on patterns in the prime numbers and navigation in networks. Central to each of these settings are computational and information theoretic limitations placed on the referee in the relevant Imitation Game.

This lecture will survey some of these developments and speculate on future uses of this paradigm in science and society, in a way which is hopefully accessible without any specific background knowledge.