Crypto

Manan Vaswani

December 15, 2018

1 Introduction

The probabilistic method is perhaps one of the most powerful tools used mainly in, but not strictly limited to, the field of combinatorics. It uses concepts from probability theory but surprisingly, it can be applied in situations that are completely unrelated to probability. Most often, it is used to prove the existence of objects with a certain property.

The basic probabilistic method is as follows: Suppose we would like to prove the existence of a combinatorial object having certain properties. A naive approach would be to attempt a proof by construction, but in many cases, this is infeasible or even unnecessary if we don't need a specific example as part of our result. In order to solve this problem probabilistically, we construct an appropriate probability space corresponding to the object required. Then, we pick an object at random from this probability space and try to prove that it possesses the desired properties with a non-zero probability. Similarly, showing that the probability is strictly less than 1 proves the existence of an object without certain properties.

The main technique in applying the probabilistic method to the proof of a theorem is introducing randomness where there is none. This is usually the first and most important part of a probabilistic proof, as if we work with a model that is completely deterministic, there is no scope for us to utilise any general concepts from probability to obtain the required result.

One of the most important people to contribute to the study of the probabilistic method is undoubtedly Paul Erdös(1913-1996). Although their were others before him that employed this method, he made some of the most notable advancements in the field.

The aim of this paper is to explore the techniques used in the probabilistic method with a focus on how it is applied in the field of graph theory by using the concept of random graphs. The paper also demonstrates a deeply interesting phenomenon observed in the behaviour of random graphs.

2 Preliminaries

In this section, we shall look at some key tools in probability and analysis that will be used later in the paper.

2.1 Big-O Notation

Big-O notation is a symbolism used in mathematics and computer science to describe the asymptotic[1] behaviour of functions. Basically it tells us how fast a function grown or declines.
The first notation, denoted by the symbol $\mathcal{O}$, gives an asymptotic upper bound on functions.

Definition 2.1. *[?] For a given function $g(n)$, we call $\mathcal{O}(g(n))$ the set of functions*

$$\begin{aligned}\mathcal{O}(g(n)) = \{f(n) : &\textit{ there exist positive constants } c \textit{ and } n_0 \textit{ such that} \\ &0 \leq f(n) \leq cg(n) \textit{ for all } n \geq n_0\}\end{aligned} \tag{1}$$

Next, we introduce the stricter o-notation, to denote an upper bound that is not asymptotically tight.

Definition 2.2. *[?] For a given function $g(n)$, we define $o(g(n))$ to be the set of functions*

$$\begin{aligned}o(g(n)) = \{f(n) : &\textit{ for any positive constant } c > 0, \textit{ there exists a constant } n_0 > 0 \\ &\textit{such that } 0 \leq f(n) < cg(n) \textit{ for all } n \geq n_0\}\end{aligned} \tag{2}$$

Sometimes we are able to give an asymptotically tight upper and lower bound on a function for which we use the Θ-notation

Definition 2.3. *[?] For a given function $g(n)$, we denote $\Theta(g(n))$ to be the set of functions*

$$\begin{aligned}\Theta(g(n)) = \{f(n) : &\textit{ there exist positive constants } c_1, \textit{ } c_2 \textit{ and } n_0 \textit{ such that} \\ &0 \leq c_1 g(n) \leq f(n) < c_2 g(n) \textit{ for all } n \geq n_0\}\end{aligned} \tag{3}$$

[1] The asymptotic behaviour of a function refers to how a function $f(n)$ grows as $n \to \infty$