Title : Combinatorial properties of pseudo-random graphs.

Co-Encadrants : Andrei ROMASHCHENKO and Alexander SHEN (LIRMM)
contact for more detail : `{andrei.romashchenko,alexander.shen}@lirmm.fr`

Keywords : pseudo-random generators, expander graphs

Prerequisites : The candidate should have programming skills as well as a suitable theoretical background (in linear algebra, graph theory, and probability).

Abstract : The study of random graphs is a large and a well developed branch of graph theory. It deals with the typical properties that hold with high probability for a randomly chosen graph. For example, it is known that the vast majority of graphs of fixed degree satisfy the definition of an expander. The expander graphs posses several interesting properties : high vertex expansion, strong connectivity, fast mixing, etc. Graphs of this type have many important applications in computer science and in coding theory.

Thus, for several practical applications we need expander graphs. But though almost any randomly chosen graph is an expander, it is rather hard to produce such a graph explicitly, in a deterministic way. On the other hand, generating and storing a large random graph is a an expensive procedure, which consumes much resources.

We propose to study an intermediate approach that combines the usual deterministic and probabilistic paradigms : we propose to produce graphs using (classical) pseudo-random number generators. The idea is to compare the properties of pseudo-random graphs with the typical properties of truly random graphs. More technically, we propose to estimate theoretically some specific combinatorial properties of truly random graphs (expansion rate, spectral gap) and then compare them with the properties of pseudo-random graphs by numerical experiments. Both positive and negative results would be interesting : either we obtain efficient constructions that produces pseudo-random graphs with interesting combinatorial properties (useful for applications), or we discover new tests to distinguish truly random sequences from pseudo-random ones.

Some more detail : The notion of an expander graph was introduced in 1970s in the context of coding theory. The expanders form a class of graphs that combine sparseness (degree of vertices in an expander is very small) with extremely high connectivity. Expanders have many interesting combinatorial properties : vertex and edges expansion, fast mixing, etc. Expanders are widely employed in many areas of computer science, e.g., they are used to construct error correcting codes and data structures, to organize reliable computations, to improve the performance of randomized algorithms, etc.

For standard (and useful in applications) values of parameters, the existence of expanders can be easily proven in a non constructive manner. Moreover, it can be shown that most graphs (most graphs in some natural classes) are expanders. The same time, it is rather hard to construct an expander explicitly. In some settings (uniform expanders, Ramanujan graphs) the problem of effective constructions of expanders was ultimately resolved, though the solution is based on highly nontrivial mathematical technique. In other settings (e.g., for bipartite graphs) the known explicit constructions still cannot achieve the optimal values of parameters.

We propose an approach that lies between the classic deterministic paradigm (explicit and algorithmically effective constructions of expanders) and the probabilistic method (the implicit arguments, which show that a randomly chosen graph is typically an expander). We propose to study the graphs whose description can be represented as an output of a pseudo-random numbers generator. In this case a graph has a very concise description (a graph is determined by the value of the seed of the chosen generator), though it cannot be described purely deterministically.

The random number generators are used in a wide range of application, from Monte-Carlo algorithms to cryptography. The computer science community worked out many types of pseudo-random generators known to be efficient in one or another type of applications. The quality of a pseudo-random generator is a classic issue, and there exist standard benchmarks that compare the performance of generators. However, most of the randomness tests in use are focused on statistical properties of a pseudo-random sequence ; subtle combinatorial properties of the output (like the second eigenvalue of a pseudo-random graph) are studied much less. We suggest to close this gap and investigate the 'pseudo-random' graphs produced by different generators, comparing the properties of pseudo-random objects with the properties of truly random graphs. More specifically, we suppose to compare the expander-like parameters (vertex expansion, the eigenvalues, etc.)

for random and pseudo-random graph. We expect that the results will substantially depend on the type of the generator in use and on the parameters (number of vertices, degree) of the generated graphs. In this research both positive and negative answers would be interesting and promising. Indeed, if we show that a pseudo-random graphs is typically a good expander, then we obtain a cheap and effective tool to construct good expanders. Otherwise we obtain a non-conventional test that can distinguish random and pseudorandom sequences of bits, so we get a new technique to measure the quality of pseudo-random generators.

Bibliography :

[1] S. Hoory, N. Linial, and A. Wigderson. Expander graphs and their applications. Bulletin of the American Mathematical Society 43.4 (2006) : 439-561.

[2] N. Alon, J.H. Spencer. The Probabilistic Method. Wiley-Interscience Publication. 2nd ed. 2004.

[3] D. Knuth. The Art of Computer Programming, Volume 2 : Seminumerical Algorithms, 3rd edition (Addison-Wesley, Boston, 1998).

[4] Alexander Shen. Randomness tests : theory and practice. Report (2021). `http://www.lirmm.fr/ ashen/racaf/final-detailed.pdf`