Generating Expander Graphs Using Cellular Automata

Debdeep Mukhopadhyay

Department of Computer Science and Engineering,
Indian Institute of Technology Kharagpur, India
debdeep@cse.iitkgp.ernet.in

Abstract. The paper characterizes a special class of Cellular Automaton (CA) called Two Predecessor Single Attractor CA (TPSA-CA). We show that the transition graphs of the TPSA-CA can be used to realize pseudo-random regular graphs with good expansion properties. The elegance of the scheme lies in the fact that the storage required to capture the graph is \(O(\log N)\), where \(N\) is the total number of vertices in the graph.

Keywords: expander graphs, Cellular Automata (CA), Two-Predecessor Single Attractor CA (TPSA-CA).

1 Introduction

Expander Graphs have been a significant tool both in theory and practice. It has been used in solving problems in communication and construction of error correcting codes as well as a tool for proving results in number theory and computational complexity. The combinatorial properties of the expander graphs can also lead to the construction of one-way functions \([1]\) and hash functions \([2]\) for cryptography.

The present work characterizes a special class of Cellular Automata (CA) \([3]\), known as the Two Predecessor Single Attractor Cellular Automata (TPSA-CA). Next the work shows that the transition graphs generated by the TPSA-CA can be composed to realize pseudo-random regular graphs with expansion properties. Informally, a pseudo-random graph \(G = (V, E)\) is a graph that behaves like a truly random graph. The paper shows that the CA based transition graphs have uniform edge distributions, if the graveyard states are chosen uniformly and independently. We provide both theoretical and experimental evidence to show that the pseudo-randomness of the generated graphs can be utilized to demonstrate good expansion properties. The elegance in the scheme lies in the fact that the storage required for the generation of the graphs is \(O(\log N)\), where \(N\) is the number of vertices in the graph.

The outline of the paper is as follows: Section \([2]\) describes some of the preliminaries of expander graphs. The TPSA-CA is characterized in section \([3]\) and the state transitions of the machine is employed to generate pseudo-random regular graphs. In section \([4]\) we present experimental evidence of the expansion properties of the generated graphs. The work is concluded in section \([5]\).
2 Preliminaries on Expander Graphs

Informally expander graphs are a class of graphs \( G = (V, E) \) in which every subset \( S \) of vertices expands quickly, in the sense that it is connected to many vertices in the set \( S \) of complementary vertices. It may be noted that the graph may have self loops and multiple edges. The following definition states formally the expansion property of these class of graphs [4].

**Definition 1.** The edge boundary of a set \( S \in G \) denoted \( \delta(S) = E(S, \overline{S}) \) is the set of outgoing edges from \( S \). The expansion parameter of \( G \) is defined as:

\[
h(G) = \min_{S: |S| \leq N/2} \frac{|\delta(S)|}{|S|}
\]

where \(|S|\) denotes the size of a set \( S \) and \( N \) is the total number of vertices in the graph.

There are other notions of expansion, the most popular being counting the number of neighbouring vertices of any small set, rather than the number of outgoing edges.

Random graphs have been utilized to develop expander graphs. A random graph \( G(N, p) \) is a probability distribution of all the labeled graphs on \( N \)-vertices where for each pair \( 1 \leq i, j \neq N, (i, j) \) is an edge of \( G(N, p) \) with probability \( p = p(N) \), independently of any other edges.

Although \( d \)-regular random graphs on \( N \) vertices define an expander, for real life applications it is necessary to have more explicit constructions on \( O(2^n) \) vertices, where \( n \) is the parameter defining the problem size. This is because to store a description of a random graph on so many vertices requires exponential time and space. Two well known constructions are found in [5,6,7].

The properties of the eigenvalue spectrum of the adjacency matrix \( A(G) \) can also be used to understand properties of the graph \( G \).

The adjacency matrix of a graph \( G \), denoted by \( A(G) \) is an \( n \times n \) matrix such that each element \((u, v)\) denotes the number of edges in \( G \) between vertex \( u \) and vertex \( v \) [4]. For a \( d \)-regular graph, the sum of each row and column in \( A(G) \) is \( d \). By definition the matrix \( A(G) \) is symmetric and therefore has an orthonormal base \( v_0, v_1, \ldots, v_{n-1} \), with eigenvalues \( \mu_0, \mu_1, \ldots, \mu_{n-1} \) such that for all \( i \) we have \( Av_i = \mu_i v_i \). Without loss of generality we assume the eigenvalues sorted in descending order \( \mu_0 \geq \mu_1 \geq \ldots \geq \mu_{n-1} \). The eigenvalues of \( A(G) \) are called the spectrum of \( G \). The following two results are important in estimating the expansion properties of the graph.

1. \( \mu_0 = d \)
2. \( \frac{d - \mu_1}{2} \leq h(G) \leq \sqrt{2d(d - \mu_1)} \)

Thus, the parameter \( d - \mu_1 \), also known as the Spectral Gap gives a good estimate on the expansion of the graph \( G \). The graph is an expander if the spectral gap has a lower bound \( \epsilon' \) such that \( d - \mu_1 > \epsilon' \).