# 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 $O(logN)$, 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 $O(logN)$, 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*.

G.C. Sirakoulis and S. Bandini (Eds.): ACRI 2012, LNCS 7495, pp. 52–62, 2012.

## 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 $\overline{S}$ 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 $\delta(S)$ is $\delta(S) = E(S, \overline{S})$ 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 $d - \mu_1 > \epsilon'$.

A graph $G_1$ has better expansion properties than graph $G_2$, implies that for any subset $S$, $|S| \leq n/2$ of the graph $G_1$ has a larger number of neighbouring elements outside the set $S$, compared to that in $G_2$. Mathematically, the value of $h(G_1) > h(G_2)$. Informally, it implies that the graph $G_1$ expands faster compared to graph $G_2$. A random regular graph has good expansion properties. However the problem of realizing such a graph is in its description which grows exponentially with the number of vertices.

For the proposed construction of expander graphs, we use graphs which are parameterized by a shorter *seed*. These pseudo-random graphs, posses properties like edge-density, identical to random graphs, if the seed is generated by a pseudo-random generator.

In the next section we present the construction of random $d$ regular graph using the properties of a special class of CA, known as the Two Predecessor Single Attractor Cellular Automaton (TPSA CA). The transition graphs of the CA is at the heart of the proposed construction.

## 3 Expander Graphs Using TPSA CA

TPSA CA are a special class of non-group CA in which the state transition graph forms a single inverted binary routed tree at all zero state (**Fig. 1**). Every reachable state in the state transition graph has exactly two predecessors. The only cyclic state is the all zero state (for a non-complemented TPSA CA), which is an attractor (or graveyard). If $T_n$ is the characteristic matrix of an $n$ cell automaton then the necessary and sufficient conditions to be satisfied by the Transition matrix for the CA to be TPSA CA are[3]:

1. Rank($T_n$)=$n-1$
2. Rank($T_n \oplus I_n$)=$n$, $I_n$ being an $n \times n$ identity matrix
3. Characteristic Polynomial = $x^n$
4. Minimal Polynomial = $x^n$

The following results [3] characterize the state transition of the non-complemented TPSA CA.

**Lemma 1.** *[3] For an n cell TPSA CA with characteristic polynomial $x^n$ and minimal polynomial $x^n$, (i) the number of attractors is 1, the all zero state, (ii) the number of states in the tree is $2^n$.*

**Lemma 2.** *For an n cell TPSA CA having $m(x) = x^n$ the depth of the tree is $n$.*

Next, we develop a method to recursively synthesize an $n$ cell TPSA. The state transition matrix of the $n$ cell TPSA is denoted by $T_n$ and is generated from an $n-1$ cell TPSA CA characterized by the matrix $T_{n-1}$. The following theorem describes the property exploited in the construction.

**Theorem 1.** *Given that $T_{n-1}$ is the characteristic matrix of an $(n-1)$ cell TPSA, the matrix $T_n$ denoted by:*

$$T_n = \begin{pmatrix} & & & & | & 0 \\ & & T_{n-1} & & | & \vdots \\ & & & & | & 0 \\ - & - & - & - & - & - \\ 0 & \dots & 0 & 1 & | & 0 \end{pmatrix}$$

*represents the characteristic matrix of an n cell TPSA.*

*Proof.* We prove the result using mathematical induction. Let us assume that the theorem holds for $n-1$. We have to prove that the result holds true for $n$ cell as well. Thus, $T_{n-1}$ represents the characteristic matrix of an $(n-1)$ cell TPSA CA. Thus, the four properties which $T_{n-1}$ satisfy are: i) Rank($T_{n-1}$)=$n-2$, ii) Rank($T_{n-1} \oplus I_{n-1}$)=$n-1$, $I_{n-1}$ being an $n-1 \times n-1$ identity matrix, iii) Characteristic Polynomial = $x^{n-1}$, iv) Minimal Polynomial = $x^{n-1}$.

It is evident that since the element at the $n^{th}$ row and $(n-1)^{th}$ column is 1 and by the construction methodology all the other rows have 0 in the $(n-1)^{th}$ columns the row added is linearly independent from the other rows of $T_n$. Hence it adds by 1 to the rank of $T_{n-1}$. Thus, $rank(T_n) = rank(T_{n-1})+1 = n-2+1 = n-1$.

Similarly, using the fact that $rank(T_{n-1} \oplus I_{n-1}) = n-1$ (where $I_{n-1}$ is the identity matrix of order $n-1$), we have $rank(T_n \oplus I_n) = n$. The characteristic polynomial of the matrix $T_n$, denoted by $\phi_n(x)$ is evaluated as $det(T_n \oplus xI_n)$, where *det* denotes the determinant. Thus we have,

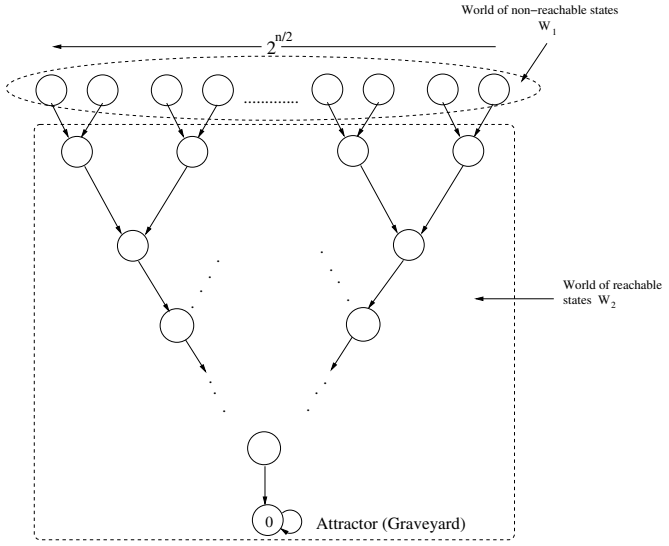


**Fig. 1.** The state transition graph of a non-complemented TPSA CA

$$\phi_n(x) = \det \left( \begin{array}{cccc|c} & & & & 0 \\ & & & & 0 \\ & & & & \vdots \\ & T_{n-1} \oplus & & xI_{n-1} & 0 \\ & & & & \vdots \\ & & & & 0 \\ & & & & 0 \\ \hline - & - & - & - & - \\ 0 & \ldots & 0 & 1 & x \end{array} \right)$$

$$= x\phi_{n-1}(x), (\phi_{n-1}(x) \text{ denotes the characteristic polynomial of } T_{n-1})$$

$$= x.x^{n-1} = x^n$$

In order to evaluate the minimal polynomial we make use of the following proposition.

**Lemma 3.** *Let $\phi_n(x)$ and $\psi_n(x)$ be the characteristic polynomial and the minimal polynomial of the matrix $T_n$, respectively. Let the greatest common divisor (gcd) of the matrix $(T_n \oplus I_n x)^\vee$ that is the matrix of algebraic complements of the elements of the matrix $(T_n \oplus I_n x)$ be $d(x)$. Then, $\phi_n(x) = d(x)\psi_n(x)$.*

From the matrix $(T_n \oplus I_n x)^\vee$ it may be observed that the element at the position $(0, n)$ is 1 and thus the gcd $d(x)$ is also 1. Thus the minimal polynomial is equal to the characteristic polynomial which is $x^n$. Thus, we observe that the construction follows all the four necessary and sufficient requirements of a TPSA CA. This completes the proof.

We have seen above that the state transition in the above class of TPSA CA is governed solely by the characteristic matrix. This class of CA is known as the *non-complemented* TPSA CA. On the contrary when the next state is obtained by the application of the characteristic matrix and then xoring with a vector $F$, the CA is known as the *complemented* TPSA CA.

The following results show how complementing the state transition function of the non-complemented CA generates a class of automaton with the same properties as the original TPSA CA.

**Lemma 4.** *Corresponding to a non-complemented TPSA CA $M_1$ and a state $Z$, there exists a complemented CA $M_2$ with state $Z$ as an attractor. If the characteristic matrix $M_1$ be indicated by $T_n$ and it is required to build a complemented TPSA CA such that $Z$ is the graveyard (attractor) then the characteristic matrix of the complemented CA, $\overline{T}_n$ is related to $T_n$ by*

$$\overline{T}_n(X) = T_n(X) \oplus (I_n \oplus T_n)Z$$

*where $X$ is the seed to the CA and $I_n$ is the identity matrix of order $n$.*

**Lemma 5.** *A complemented TPSA CA has the same structure as a non-complemented TPSA CA. To emphasize*

- *Number of attractors in the complemented CA is the same as that in the original non-complemented CA.*
- *Number of reachable states and non-reachable states are same as that in the original non-complemented CA.*

**Lemma 6.** *If any state $Z$ in the non-reachable world of a non-complemented CA is made the graveyard in a complemented TPSA, then the non-reachable elements become elements of the reachable world in the complemented CA and viceversa. Thus the non-reachable world ($W_1$) and the reachable world ($W_2$) exchange themselves (***Fig. 2***).*

*Proof.* Let $X$ and $Z$ be two non-reachable elements in the $n$ cell non-complemented CA with characteristic matrix $T_n$. Let $X$ be the $l^{th}$ level sister of $Z$. In all cases $l < n$. Thus, we have:

$$T_n^l(X) = T_n^l(Z)$$

Let us consider the state transition diagram of the complemented CA with $Z$ as the graveyard. The state transition of the complemented CA is indicated by $\overline{T}_n$. We shall prove that in this state transition graph $X$ is a reachable state. Let, the depth of $X$ in the graph of the complemented CA be $t$. If $t$ is less than $n$ then $X$ is a reachable state. Since, $Z$ is the graveyard of this graph we have:

$$\begin{aligned} \overline{T}_n^t(X) &= Z \\ T_n^t(X) \oplus (I_n \oplus T_n^t)Z &= Z \\ T_n^t(X) &= T_n^t(Z) \end{aligned}$$

Thus, $X$ and $Z$ are $t^{th}$ level sisters in the state transition graph of the non-complemented CA. But we know that they are $l^{th}$ level sisters. Thus $t = l < n$. Thus, the depth of $X$ is lesser than $n$ and hence $X$ is a reachable state in the state transition graph of the complemented CA.

**Lemma 7.** *If the state $Z$ is chosen independently as the graveyard in a complemented TPSA from a uniform distribution, then the state transition graph is a pseudo-random graph.*

*Proof.* Given any input state $X$, the output $Y$ is governed by the equation: $Y = \overline{T}_n(X) = T_n(X) \oplus (I_n \oplus T_n)Z$.

Now, since $Z$ is chosen independently and randomly from a uniform distribution, the probability that $Z$ equals a particular $Z_1$ is given by $Pr[Z = Z_1] = \frac{1}{2^n}$. Here $n$ is the size of the TPSA CA.

Let, when $Z_1$ is the graveyard, the next state of a state $X_1$ is say $Y_1$. Thus, $Y_1 = T_n(X_1) \oplus (I_n \oplus T_n)Z_1$. We compute the probability that for any arbitrary graveyard, $Z$, the next state of $X_1$ is $Y_1$. That is we compute:

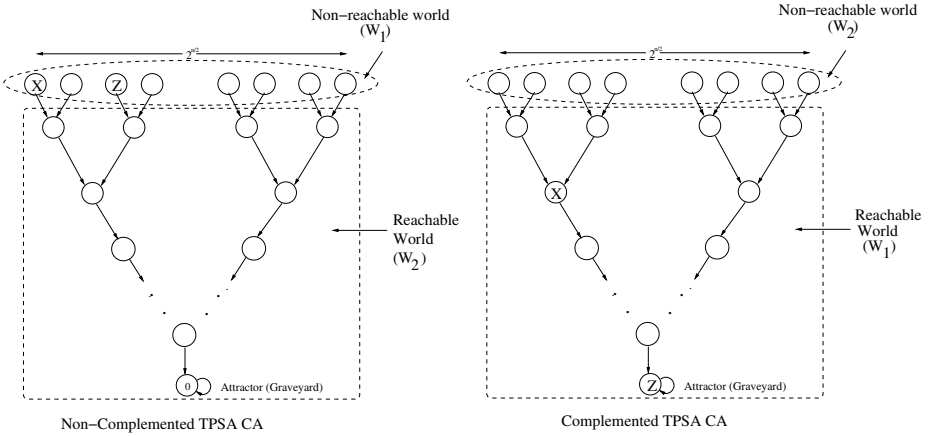


**Fig. 2.** The exchange of the worlds in a complemented TPSA CA

$$\begin{aligned} Pr[\overline{T_n}(X_1) = Y_1] &= Pr[T_n(X_1) \oplus (I_n \oplus T_n)Z = Y_1] \\ &= Pr[Z = Z_1] \\ &\quad (\text{ since, } rank(I_n \oplus T_n) = n) \\ &= \frac{1}{2^n} \end{aligned}$$

Thus the probability that there is an edge from $X_1$ to $Y_1$ is $Pr[X_1 \rightarrow Y_1] = \frac{1}{2^n} = \frac{1}{N}$, where $N$ is the number of vertices in the graph.

Thus for a given $X$, all the $Y$'s are equally probable and hence the distribution of $Y$ for a given $X$ is indistinguishable from a random distribution. Thus, the state transition graph of the TPSA CA *looks like* a random graph when the graveyard is chosen randomly and independently.

### 3.1 Construction of a Random *d* Regular Graph Using the TPSA CA

We have seen in the previous discussion that the TPSA CA is capable of generating pseudo-random graphs. In this section we present a method to generate pseudo-random $d$ regular graphs by composing the random graphs. It may be noted that the adjacency of the graph is stored in the graveyard state, thus leading to a very compact storage of the graph. This is because given the graveyard state, the entire transition graph can be obtained. If there are $N$ vertices in the graph, the graveyard state has a size $logN$ and thus the storage required to store the graph is $O(logN)$.

In order to construct the $d$ regular graph we proceed as follows. We first present the construction of a 4 regular graph. Let $Z_1 \in W_1$ (non-reachable world in the non-complemented TPSA CA) and $Z_2 \in W_2$ (reachable world in the

non-complemented TPSA CA). Let, $G_1$ and $G_2$ be the state transition graphs with $Z_1$ and $Z_2$ as the graveyards respectively.

Clearly, in $G_1$ if $X \in W_1$, $degree(X) = 3$ and if $X \in W_2$, $degree(X) = 1$. Similarly, in $G_2$ if $X \in W_1$, $degree(X) = 1$ and if $X \in W_2$, $degree(X) = 3$. Here *degree* is defined as the sum of the *indegree* and the *outdegree* in the corresponding graph.

Thus, in the graph $G$ obtained by a union operation in the graphs $G_1$ and $G_2$, allowing multiple edges and self loops, we have for $X \in G$, $degree(X) = 4$. If we continue the union operation in the above method we have $degree(X) = d = 2(t+1)$, where $t$ is an odd integer and represents the number of union operations. Thus we can construct a $d$ regular graph from the TPSA CA. In fact we argue that we have a pseudo-random $d$ regular graph, if the graveyards are properly chosen.

For each of the graphs, we choose the graveyard states independently in a random fashion. We have seen previously, that the probability than an edge exists from any $X$ to any $Y$ is $\frac{1}{N}$. After performing the union operation we obtain a $d$ regular graph, where there are $d$ neighbors of each vertex. If we divide the graveyards into two sets:

$$Z = \{Z_1, Z_3, \ldots, Z_{d/2-1}\} \in W_1$$
$$Z^* = \{Z_2, Z_4, \ldots, Z_{d/2}\} \in W_2$$

Thus the $d$ regular graph is formed by the union of $d/4$ graphs, each of which is the union of two graphs formed with the graveyards chosen as the pairs $(Z_1, Z_2), \ldots, (Z_{d/2-1}, Z_{d/2})$. Then in the final graph, if $X \in W_1$, there are $d/2$ incoming edges and $d/4$ outgoing edges belonging to graphs with graveyards from $Z$ and $d/4$ outgoing edges belonging to graphs with graveyards from $Z^*$. Similarly, if $X \in W_2$, there are $d/2$ incoming edges and $d/4$ outgoing edges belonging to graphs with graveyards from $Z^*$ and $d/4$ outgoing edges belonging to graphs with graveyards from $Z$.

We note that $Y$ cannot be on the other side of two edges $e$ and $e^*$ if:

1. $e$ and $e^*$ are both outgoing edges and $e$ belongs to a graph with graveyard from $Z$ and $e^*$ belongs to a graph with graveyard from $Z^*$ or both belongs to either $Z$ or $Z^*$.
2. $e$ and $e^*$ are both incoming edges and $e$ belongs to a graph with graveyard from $Z$ and $e^*$ belongs to a graph with graveyard from $Z^*$ or both belongs to either $Z$ or $Z^*$.

The above properties hold because $rank(I_n \oplus T_n) = n$ and $Z \cap Z^* = \Phi$. Thus, the only possibility is if $e$ is say an incoming edge with graveyard from $Z$ and $e^*$ is an outgoing edge with graveyard from $Z^*$. Let the graveyards be respectively, $Z_i$ and $Z_j$, where $i$ is an odd integer such that $1 \leq i \leq d/2 - 1$ and $j$ is an even integer such that $2 \leq j \leq d/2$. Note that $Y$ cannot be opposite two pairs of edges, as then it implies that we also have two pairs of edges which have $Y$ and each pair belongs to the graphs with graveyard from $Z$ or $Z^*$. This is not permitted from our previous discussion. Thus, the node $Y$ can be opposite only one pair

of edges, in which one edge belongs to a graph with graveyard $Z_i \in Z$ and the other belongs to a graph with graveyard $Z_j \in Z^*$. Suppose, there is an edge from $Y$ to $X$ in the graph with graveyard $Z_i$. Thus, $X = T_n(Y) \oplus (I_n \oplus T_n)Z_i$. Also if there is an edge from $X$ to $Y$ in the graph with graveyard $Z_j$ we have, $Y = T_n(X) \oplus (I_n \oplus T_n)Z_j$. Thus, we have $Y = (I_n \oplus T_n)^{-1}(T_nZ_i \oplus Z_j)$. Thus for each pair of $Z_i$ and $Z_j$ we have one such $Y$ which may have two edges with an $X$. From the enumeration of $Z$ and $Z^*$ we can have $(d/4)^2$ pairs and thus $(d/4)^2$ values of $Y$ which may form 2 multiple edges with $X$. For these values of $Y$, using inclusion-exclusion principle, the probability that $Y$ is a neighbor of a given $X$ is $p = d/N - (d/4)^2(1/N)^2$. If we set $d = N/c$, for some integer $c > 0$ we have $p = \frac{1}{c}(\frac{16c-1}{16c}) \approx 1/c$, for $c > 4$. For some chosen values of $N = 128$ and $d = 16$, we have $p = 0.124$ which is almost equal to $1/8 = 0.125$.

For other cases of $Y$, $Y$ can be a neighbor of $X$ in only one of the $d$ edges, so the probability that $Y$ is the neighbor of $X$ is $\frac{d}{N}$. Thus, we can fairly state that for all cases the probability that $Y$ is a neighbor of $X$ has a probability of $d/N$. Thus we have indeed a $d$ regular graph which has its edge distributions like a random graph with $d$ regularity.

## 4 Experimental Observations on the Expansion Properties

We present some experimental results on the expansion properties of the constructed graph in **Table 1**. It measures the value of the two largest eigen values for the TPSA based graphs for degree $4, 8, 12$ and 16. The difference between the largest two eigen values is known as the spectral gap and should be large for good expansion of the graph. Results show that the spectral gap and hence the expansion increases proportionately with the number of union operations ($t$).

**Table 1.** Spectrum of a 4 cell TPSA based regular graph

| No. of Union (t) | Graveyards | Degree | First Eigen Value | Second Eigen Value | Spectral Gap (g) | g/t |
|---|---|---|---|---|---|---|
| 1 | {0},{4} | 4 | 4 | 3.2361 | 0.76 | 0.76 |
| 3 | {0,15},{4,8} | 8 | 8 | 4.899 | 3.10 | 1.03 |
| 5 | {0,15,3},{4,8,10} | 12 | 12 | 6.3440 | 5.66 | 1.14 |
| 7 | {0,15,3,2},{4,8,10,9} | 16 | 16 | 5.2263 | 10.77 | 1.54 |

The lower bound of the expansion of the generated graphs may be computed using Tanner's Theorem[8,9].

**Theorem 2.** *(***Tanner***) Let $M$ be the adjacency matrix of a $d$-regular graph $G$ with $N$ vertices and let $\lambda_2$ be its second largest eigenvalue. Then, for all sets $A$,*

$$N(A) \geq \frac{d^2 N}{d^2|A| + N\lambda_2^2(1 - |A|/N)}|A|$$

*,where $N(A)$ is the neighbourhood of $A$ outside $A$.*

Let, $G$ be the expander graph with $n$ nodes, generated by the TPSA based method. The expansion of the graph $G$ may be computed as follows:

$$\begin{aligned} E(G) &= max_{A\in[N]} min_{A\subseteq G;|A|=x}(|N(A)| - |A|) \\ &\geq max_{A\in[N]} \frac{d^2}{d^2 x/N + \lambda_2^2(1 - x/N)} x - x \\ &= max_{A\in[N]} \frac{Nx}{(1 - \frac{\lambda_2^2}{d^2})x + \frac{\lambda_2^2}{d^2} N} - x \\ &= max_{A\in[N]} \frac{Nx}{(1-c)x + cN} - x, \\ &\quad \text{where } c = \frac{\lambda_2^2}{d^2} \end{aligned}$$

The expression in the variable $x$ becomes maximum at $x = x_{max}$, where

$$\begin{aligned} \frac{x_{max}}{N} &= \frac{\sqrt{c} - c}{1 - c} \\ &= \frac{\lambda - \lambda^2}{1 - \lambda^2}, \text{ where } \lambda = \sqrt{c} \end{aligned}$$

Thus the lower bound of the expansion of the graph $G$ is

$$E(G) \geq \frac{\lambda(1 + \lambda^2) - 2\lambda^2}{\lambda(1 - \lambda^2)} N$$

Using the above result we obtain lower bounds of the expansion of the generated expander graphs and tabulate them in **Table 2**.

**Table 2.** Expansion of the expander graphs generated by 4 cell TPSA CA

| No. of nodes ($N$) | Degree ($d$) | First Eigenvalue ($\lambda_1$) | Second Eigenvalue ($\lambda_2$) | $\lambda = \frac{\lambda_2}{\lambda_1}$ | Expansion Bound ($E(G)$) |
|---|---|---|---|---|---|
| 16 | 4 | 4 | 3.2361 | 0.809 | 1.688 |
| 16 | 8 | 8 | 4.899 | 0.6124 | 3.85 |
| 16 | 12 | 12 | 6.3440 | 0.5287 | 7.84 |
| 16 | 16 | 16 | 5.2263 | 0.3266 | 8.12 |

As expected the expansion increases with the increase in the degree of the graphs. The results may be compared with the expansion rates of other constructions of expander graphs, with similar parameters as mentioned in [8]. It

is mentioned in [1], that the best results are from the random construction of the expander graphs. A typical value of the expansion bound of the random expander constructions mentioned in [8,1] is $N = 20, d = 8$ and $E(G) = 6.49$. This is quite similar to the expansion bound of the proposed construction. The storage required to store the $d$ graphs is that of storing $d$ graveyard states, and is thus $O(logN)$, and is thus possible to be realized by efficient implementations.

## 5 Conclusion

We have proposed a new construction method of expander graphs using a special class of Cellular Automata, called TPSA-CA. We have characterized the CA and have theoretically explained its various properties. Finally, we show that the transition graphs of the CA can be composed to realize random regular graphs which also has good expansion properties. The storage required to store the expander graph of $N$ vertices is $O(logN)$.

## References

1. Goldreich, O.: Candidate One-Way Functions Based on Expander Graphs. Cryptology ePrint Archive, Report 2000/063 (2000)
2. Charles, D.X., Lauter, K.E., Goren, E.Z.: Cryptographic Hash Functions from Expander Graphs. Journal of Cryptology (2007)
3. Chaudhuri, P.P., Chowdhury, D.R., Nandi, S., Chattopadhyay, S.: Additive Cellular Automata Theory and its Application, vol. 1. IEEE Computer Society Press (1997)
4. Linial, N., Wigderson, A.: Expander graphs and their applications, (2003), `http://www.math.ias.edu/boaz/ExpanderCourse/`
5. Lubotzky, A., Phillips, R., Sarnak, P.: Ramanujan graphs. Combinatorica 8(3), 261–277 (1988)
6. Margulis, G.A.: Explicit constructions of expanders. Problemy Peredači Informacii 9(4), 71–80 (1973)
7. Margulis, G.A.: Explicit group-theoretic constructions of combinatorial schemes and their applications in the construction of expanders and concentrators. Problemy Peredachi Informatsii 24(1), 51–60 (1988)
8. Panjwani, S.K.: An Experimental Evaluation of Goldreich's One-Way Function, Cryptology ePrint Archive, Report 2000/063 (2001)
9. Alon, N.: Eigen Values, Geometric Expanders, Sorting in Rounds and Ramsey Theorem. Combinatorica 6, 207–219 (1986)