60/102 Null Boundary Cellular Automata based expander graphs

Sung-Jin Cho[1†] Un-Sook Choi[2] Han-Doo Kim[3]
Yoon-Hee Hwang[1] Jin-Gyoung Kim[1]

[1] *Department of Applied Mathematics, Pukyong National University, Busan 608-737, Korea*
[2] *Department of Media Engineering, Tongmyong University, Busan 626-847, Korea*
[3] *School of Computer Aided Science, Institute of Basic Science, Inje University, KimHae 621-749, Korea*

Expander graphs are useful in the design and analysis of communication networks. Mukhopadhyay et al. introduced a method to generate a family of expander graphs based on nongroup two predecessor single attractor Cellular Automata(CA). In this paper we propose a method to generate a family of expander graphs based on 60/102 Null Boundary CA(NBCA) which is a group CA. The spectral gap generated by our method is maximal. Moreover, the spectral gap is larger than that of Mukhopadhyay et al.

Keywords: Expander graphs, $60/102$ NBCA, Spectral gaps, Bipartite graphs, Eigenvalue.

1 Introduction

Expander graphs were first defined by Bassalygo and Pinsker and their existence first proved by Pinsker in the early 1970s [10]. Also expander graphs have utility in computational settings such as in the theory of error correcting codes and the theory of pseudorandomness as well as a tool for proving results in number theory and computational complexity [6, 8, 11]. Expander graphs are useful in the design and analysis of communication networks. Mukhopadhyay et al. introduced a method to generate a family of expander graphs based on nongroup two predecessor single attractor Cellular Automata(CA). In this paper we propose a method to generate a family of expander graphs based on 60/102 Null Boundary CA(NBCA) which is a group CA. The merit of our method is that it use regular, modular and cascadable structure of $60/102$ NBCA [1, 3, 4] to generate regular graphs of good expansion property with less storage. The spectral gap generated by our method is maximal. Moreover, the spectral gap is larger than that of Mukhopadhyay et al. [9].

2 Preliminaries

CA consist of a number of interconnected cells arranged spatially in a regular manner, where the state transition of each cell depends on the states of its neighbors. The CA structure investigated by Wolfram

†This work was supported by the Pukyong University Research Fund in 2009(PK-2009-26).

[12] can be viewed as a discrete lattice of sites (cells), where each cell can assume the value either 0 or 1. The next-state of a cell is assumed to depend on itself and on its two neighbors (3-neighborhood dependency). If the next-state function of a cell is expressed in the form of a truth table, then the decimal equivalent of the output is conventionally called the rule number for the cell.

Neighborhood state	111	110	101	100	011	010	001	000	
Next state	0	0	1	1	1	1	0	0	rule 60
Next state	0	1	1	0	0	1	1	0	rule 102

The top row gives all eight possible states of the three neighboring cells (the left neighbor of the ith cell, the ith cell itself, and its right neighbor) at the time of instant t. The second and third rows give the corresponding states of the ith cell at the time of instant $t+1$ for two illustrative CA rules.

Informally, expander graph is a graph $G = (V, E)$ 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.

Definition 2.1 ([8])**.** Suppose $G = (V, E)$ has n vertices. For a subset S of V define the *edge boundary* of S, ∂S, to be the set of edges connecting S to its complement $\overline{S}$. That is, ∂S consists of all those edges (v, w) such that $v \in S$ and $w \notin S$. The *expansion parameter for* G is defined by

$$h(G) \equiv \min_{S:|S|\leq n/2} \frac{|\partial S|}{|S|}$$

where $|X|$ denotes the size of a set X.

Example 2.2. Suppose G is the complete graph with n vertices, i.e., the graph in which every vertex is connected to every other vertex. Then for any vertex in S, each vertex in S is connected to all the vertices in $\overline{S}$, and thus $|\partial S| = |S| \times |\overline{S}| = |S|(n - |S|)$. It follows that the expansion parameter for G is given by

$$h(G) \equiv \min_{S:|S|\leq n/2} (n - |S|) = \lceil \frac{n}{2} \rceil$$

It is a marvellous fact that properties of the *eigenvalue spectrum* of the adjacency matrix $A(G)$ can be used to understand properties of the graph G. This occurs so frequently that we refer to the spectrum of $A(G)$ as *the spectrum of the graph* G. It is useful because the eigenvalue spectrum can be computed quickly, and certain properties, such as the largest and smallest eigenvalue, the determinant and trace, can be computed extremely quickly [8].

Let $G = (V, E)$ be an undirected graph and $A(G)$ be the adjacency matrix of the graph G. And let $\lambda_i(A(G))(1 \leq i \leq n)$ be eigenvalues of $A(G)$. Then $A(G)$ is a real symmetric matrix and thus diagonalized. Without loss of generality we can assume that $\lambda_1(A(G)) \geq \lambda_2(A(G)) \geq \cdots \geq \lambda_n(A(G))$.

Lemma 2.3. *[1] Let $\mathbb{C}$ be a CA where state transition matrix T and $\mathbb{C}'$ be the complemented CA derived from $\mathbb{C}$ where state transition operator $\overline{T}$. And let $\overline{T}^p$ denote p times application of the complemented CA operator $\overline{T}$. Then*

$$\overline{T}^p f(x) = [I \oplus T \oplus T^2 \oplus \cdots \oplus T^{p-1}]F(x) \oplus T^p f(x)$$

where T is the characteristic matrix of the corresponding noncomplemented rule vector and $F(x)$ is an n-dimensional vector (n=number of cells) responsible for inversion after XNORing. $F(x)$ has '1' entries (i.e., nonzero entries) for CA cell positions where XNOR function is employed and $f(x)$ is the current state assignment of the cells.

3 Properties of the eigenvalue spectrum

In this section, we give properties of the eigenvalue spectrum of the adjacency matrix $A(G)$ of an undirected graph G. The following three theorems are well-known.

Theorem 3.1. *Let G be an undirected d-regular graph whose adjacency matrix is $A(G)$. Then $\lambda_1(A(G)) = d$.*

Theorem 3.2. *Let G be an undirected d-regular graph. Then G is connected if and only if $\lambda_1(A(G)) > \lambda_2(A(G))$.*

Theorem 3.3. *Let G be an undirected d-regular graph. Then G is bipartite if and only if $\lambda_i(A(G)) = -\lambda_{n+1-i}(A(G)), i = 1, 2, \cdots, n$.*

Now we define the *gap for the d-regular graph G* to be the difference $\Delta(G) \equiv d - \lambda_2(A(G))$.

Theorem 3.4. *[2] Let G be a d-regular graph with spectrum $\lambda_1(A(G)) \geq \lambda_2(A(G)) \geq \cdots \geq \lambda_n(A(G))$. Then*

$$\frac{\Delta(G)}{2} \leq h(G) \leq \sqrt{2d\Delta(G)}$$

Example 3.5. Let G be an undirected graph with the adjacency matrix $A(G)$ as the following:

$$T = \begin{pmatrix}
0&1&0&0&0&0&0&1&2&0&0&0&0&0&0&0\\
1&0&1&0&0&0&0&0&0&0&0&1&0&0&0&1\\
0&1&0&0&0&0&0&1&0&0&0&0&0&0&2&0\\
0&0&0&0&1&0&1&0&0&1&0&0&0&1&0&0\\
0&0&0&1&0&1&0&0&0&0&0&0&2&0&0&0\\
0&0&0&0&1&0&1&0&0&0&0&1&0&0&0&1\\
0&0&0&1&0&1&0&0&0&0&2&0&0&0&0&0\\
1&0&1&0&0&0&0&0&0&1&0&0&0&1&0&0\\
2&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1\\
0&0&0&1&0&0&0&1&1&0&1&0&0&0&0&0\\
0&0&0&0&0&0&2&0&0&1&0&0&0&0&0&1\\
0&1&0&0&0&1&0&0&0&0&0&0&1&0&1&0\\
0&0&0&0&2&0&0&0&0&0&0&1&0&1&0&0\\
0&0&0&1&0&0&0&1&0&0&0&0&1&0&1&0\\
0&0&2&0&0&0&0&0&0&0&0&1&0&1&0&0\\
0&1&0&0&0&1&0&0&1&0&1&0&0&0&0&0
\end{pmatrix}$$

Then $\lambda_1(A(G)) = 4, \lambda_2(A(G)) = \lambda_3(A(G)) = 2\sqrt{2}, \lambda_4(A(G)) = \lambda_5(A(G)) = 2, \lambda_6(A(G)) = \cdots = \lambda_{11}(A(G)) = 0, \lambda_{12}(A(G)) = \lambda_{13}(A(G)) = -2, \lambda_{14}(A(G)) = \lambda_{15}(A(G)) = -2\sqrt{2}, \lambda_{16}(A(G)) = -4$. Moreover, $\Delta(G) = 4 - 2\sqrt{2}$. Thus $2 - \sqrt{2} \leq h(G) \leq 4\sqrt{2 - \sqrt{2}}$.

Since $\lambda_1(A(G)) > \lambda_2(A(G))$ and $\lambda_i(A(G)) = -\lambda_{17-i}(A(G))(i = 1, 2, \cdots, 16)$, G is connected and bipartite.

4 60/102 NBCA based expander graphs

In this section we show a construction of a family of random d-regular graphs using $60/102$ NBCA. Let $\mathbb{C}$ be the n-cell $60/102$ NBCA whose state transition matrix T is as the following:

$$T = \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{pmatrix}$$

Hereafter we write T by $T =< 60, 102, 102, \cdots, 102 >$.

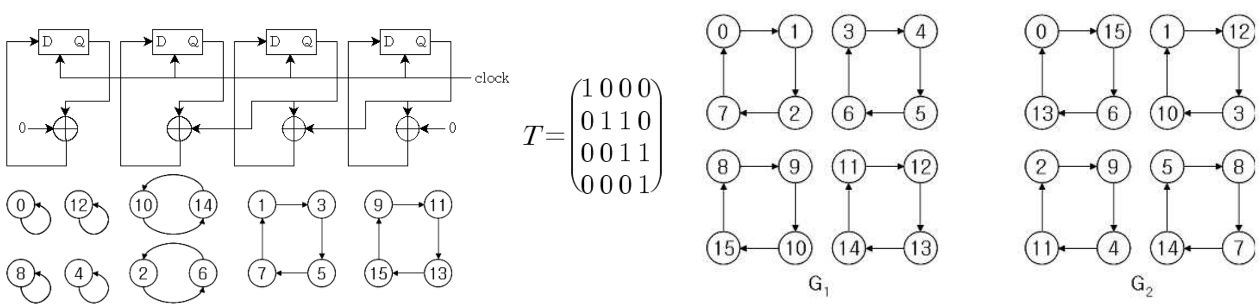
Clearly the characteristic (resp. minimal) polynomial $c(x)$ (resp. $m(x)$) of T is $c(x) = (x+1)^n$ (resp. $m(x) = (x+1)^{n-1}$). Since $m(x) = (x+1)^{n-1}$, we can obtain the following result. The proof of Theorem 4.1 is very similar to the proof of Theorem 3.4 in [3].

Theorem 4.1. *Let $\mathbb{C}$ be the n-cell $60/102$ NBCA with state transition matrix $T =< 60, 102, 102, \cdots, 102 >$. Let $\mathbb{C}'$ be the complemented CA derived from $\mathbb{C}$ with complement vector $(a_1, \cdots, a_{n-1}, 1)^t (a_i \in \{0, 1\}, i = 1, 2, \cdots, n-1$ where $\mathbf{x^t}$ is the transpose of the given vector $\mathbf{x}$) and state transition operator $\overline{T}$. If $ord(T) = 2^a$, then the following hold:*
(a) all the lengths of cycles in $\mathbb{C}'$ are the same.

(b) $ord(\overline{T}) = \begin{cases} 2^a, & \text{if } 2^{a-1} < n-1 < 2^a, \\ 2^{a+1}, & \text{if } n-1 = 2^{a+1}. \end{cases}$

Remark A. *By Theorem 4.1, the state transition diagram of $\mathbb{C}'$ does not have any attractor.*

Example 4.2. Let $\mathbb{C}$ be the 4-cell $60/102$ NBCA whose state transition matrix is $T =< 60, 102, 102, 102 >$. Then the structure and the state transition diagram of $\mathbb{C}$ are as in Figs. 1(a) and 1(b).



(a) The structure and the state transition diagram of $\mathbb{C}$

(b) The state transition diagram G_1 (resp. G_2) of the complemented CA with $F_1 = (0,0,0,1)^t$ (resp. $F_2 = (1,1,1,1)^t$)

Fig. 1:

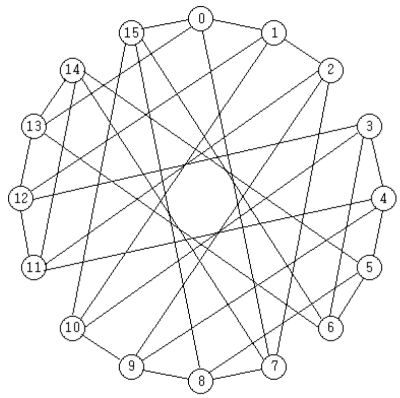


Fig. 2: The graph G

Let $F_1 = (0,0,0,1)^t$. Then by Lemma 2.3 $\overline{T}0 = 1$, $\overline{T}1 = 2$, $\overline{T}2 = 7$, $\overline{T}3 = 4$, $\overline{T}4 = 5$, $\cdots$, $\overline{T}14 = 11$ and $\overline{T}15 = 8$. Thus we obtain the state transition diagram G_1 of the state transition operator $\overline{T}$ of the complemented CA $\mathbb{C}_1'$ with complement vector $F_1 = (0,0,0,1)^t$ of $\mathbb{C}$. Also we see that $ord(\overline{T}) = ord(T) = 4$ and all lengths of cycles in $\mathbb{C}$ are all the same by Theorem 4.1.

Fig. 1(b) shows the state transition diagram G_1 and G_2 of the complemented CA with $F_1 = (0,0,0,1)^t$ and $F_2 = (1,1,1,1)^t$ respectively whose two adjacency 8×8 matrices $A(G_1)$ and $A(G_2)$ respectively using Example 4.2 are as the following.

$$A(G_1) = \begin{pmatrix}
0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&1&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&0\\
0&0&0&0&0&0&0&0&1&0&1&0&0&0&0&0
\end{pmatrix}
\qquad
A(G_2) = \begin{pmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1\\
0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0\\
0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0\\
0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0
\end{pmatrix}$$

Let G be the graph obtained by the union of the graphs G_1 and G_2. Then $A(G)$ is as the following:

$$A(G) = \begin{pmatrix}
0&1&0&0&0&0&0&1&0&0&0&0&0&1&0&1\\
1&0&1&0&0&0&0&0&0&0&1&0&1&0&0&0\\
0&1&0&0&0&0&0&1&0&1&0&1&0&0&0&0\\
0&0&0&0&1&0&1&0&0&0&1&0&1&0&0&0\\
0&0&0&1&0&1&0&0&0&1&0&1&0&0&0&0\\
0&0&0&0&1&0&1&0&1&0&0&0&0&0&1&0\\
0&0&0&1&0&1&0&0&0&0&0&0&0&1&0&1\\
1&0&1&0&0&0&0&0&1&0&0&0&0&0&1&0\\
0&0&0&0&0&1&0&1&0&1&0&0&0&0&0&1\\
0&0&1&0&1&0&0&0&1&0&1&0&0&0&0&0\\
0&1&0&1&0&0&0&0&0&1&0&0&0&0&0&1\\
0&0&1&0&1&0&0&0&0&0&0&0&1&0&1&0\\
0&1&0&1&0&0&0&0&0&0&0&1&0&1&0&0\\
1&0&0&0&0&0&1&0&0&0&0&0&1&0&1&0\\
0&0&0&0&0&1&0&1&0&0&0&0&1&0&1&0\\
1&0&0&0&0&0&1&0&1&0&1&0&0&0&0&0
\end{pmatrix}$$

The characteristic polynomial of $A(G)$ is $x^6(x-4)(x+4)(x-2)^4(x+2)^4$. Hence the eigenvalues of

$A(G)$ are $\lambda_1 = 4$, $\lambda_2 = \cdots = \lambda_5 = 2$, $\lambda_6 = \cdots = \lambda_{11} = 0$, $\lambda_{12} = \cdots = \lambda_{15} = -2$, $\lambda_{16} = -4$. Therefore by Theorem 3.2 and Theorem 3.3 G is connected and bipartite. Fig. 2 shows the graph G with the adjacency matrix $A(G)$.

Theorem 4.3. *Let $\mathbb{C}$ be the 60/102 NBCA whose state transition matrix is T. Let $\mathbb{C}'_1$ (resp. $\mathbb{C}'_2$) be the complemented CA derived from $\mathbb{C}$ with the complement vector $F_1 = (0, *, \cdots, *, 1)^t$ (resp. $F_2 = (1, *, \cdots, *, 1)^t$). Also let $\overline{T}_1 X = TX \oplus F_1$ and $\overline{T}_2 X = TX \oplus F_2$. Let G_1 (resp. G_2) be the graph obtained from $\mathbb{C}'_1$ (resp. $\mathbb{C}'_2$). And let G be the union of two graphs G_1 and G_2 whose adjacency matrix is $A(G_1)$ and $A(G_2)$ respectively. Then G is a bipartite 4-regular graph.*

Table 1 shows the eigenvalue spectrum of $A(G)$ which is the union of G_1 and G_2. In Table 1 let $F_1 = (0, 1, 1, 1)^t$ and $F_2 = (1, 1, 0, 1)^t$. Then the eigenvalue spectrum of $A(G)$ is $\lambda_1 = 4, \lambda_2 = \cdots = \lambda_5 = 2, \lambda_6 = \cdots = \lambda_{11} = 0, \lambda_{12} = \cdots = \lambda_{15} = -2, \lambda_{16} = -4$. Therefore in this case the graph G is a bipartite 4-regular graph.

Table 2 shows the result of an experimentation performed with the $60/102$ NBCA based regular graph. It measures the value of the two largest eigenvalues for random $60/102$ NBCA based graphs for degree $4, 8, 12$ and 16. Our results show that the spectral gap and hence the expansion increases proportionately with the number of union operations (t). Table 3 shows that the spectral gap by the our method is larger than the spectral gap by Mukhopadhyay's method [9].

Theorem 4.4. *Let $\mathbb{C}$ be the n-cell $60/102$ NBCA. Also let $\mathbf{x} = (x_1, x_2, \cdots, x_n)^t$ be a state of the state transition diagram of the state transition matrix T of $\mathbb{C}$. Then the immediate predecessor $\mathbf{y} = (y_1, y_2, \cdots, y_n)^t$ of $\mathbf{x}$ satisfies the following:*

$$y_1 = x_1, y_n = x_n, y_k = x_k \oplus y_{k+1} \;\; (k = 2, \cdots, n-1)$$

Remark B. *It is easy to see that the inverse matrix T^{-1} of T is of the following form.*

$$T^{-1} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 1 & \cdots & 1 & 1 & 1 \\ 0 & 0 & 1 & \cdots & 1 & 1 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{pmatrix}$$

So the required time to get the immediate predecessors is $O(n)$. For the given n-cell 60/102 NBCA, the construction of d-regular graphs which have the maximum spectral gaps depend on the relationship between F_1 and F_2. For example, in Table 1 let $F_1 = (0, 0, 0, 1)^t$ and $F_2 = (1, 1, 1, 1)^t$. Then the spectral gap is 2 which is the maximum value in the 4-regular graph.

Now let

$$F_{11} = \{(0, a_2, a_3, \cdots, a_{n-2}, 0, 1) | a_i \in \{0, 1\}, i = 2, \cdots, n-2\}$$

$$F_{12} = \{(0, a_2, a_3, \cdots, a_{n-2}, 1, 1) | a_i \in \{0, 1\}, i = 2, \cdots, n-2\}$$

$$F_{21} = \{(1, a_2, a_3, \cdots, a_{n-2}, 1, 1) | a_i \in \{0, 1\}, i = 2, \cdots, n-2\}$$

$$F_{22} = \{(1, a_2, a_3, \cdots, a_{n-2}, 0, 1) | a_i \in \{0, 1\}, i = 2, \cdots, n-2\}$$

and let $U = (F_{11} \times F_{21}) \cup (F_{12} \times F_{22})$.

Tab. 1: The eigenvalue spectrum of $A(G)$. The eight vectors on the first row(resp. column) are the complement vectors F_1(resp. F_2)

	0000	0010	0100	0110	0001	0011	0101	0111
1000 1100	-4(2) 0(10) 4(4)	-4(1) -2(4) 0(4) 2(4) 4(3)	-4(2) 0(10) 4(4)	-4(1) -2(4) 0(4) 2(4) 4(3)	-4(1) -2.8284(2) -2(2) 0(6) 2(2) 2.8284(2) 4(1)	-4(1) -2.8284(2) -2(2) 0(6) 2(2) 2.8284(2) 4(1)	-4(1) -2.8284(2) -2(2) 0(6) 2(2) 2.8284(2) 4(1)	-4(1) -2.8284(2) -2(2) 0(6) 2(2) 2.8284(2) 4(1)
1010 1110	-4(1) -2(4) 0(4) 2(4) 4(3)	-4(2) 0(10) 4(4)	-4(1) -2(4) 0(4) 2(4) 4(3)	-4(2) 0(10) 4(4)				
1001 1101	-2.8284(2) -2(2) 0(6) 2(2) 2.8284(2) 4(2)	-2.8284(2) -2(2) 0(6) 2(2) 2.8284(2) 4(2)	-2.8284(2) -2(2) 0(6) 2(2) 2.8284(2) 4(2)	-2.8284(2) -2(2) 0(6) 2(2) 2.8284(2) 4(2)	-4(2) 0(12) 4(2)	-4(1) -2(4) 0(6) 2(4) 4(1)	-4(2) 0(12) 4(2)	-4(1) -2(4) 0(6) 2(4) 4(1)
1011 1111					-4(1) -2(4) 0(6) 2(4) 4(1)	-4(2) 0(12) 4(2)	-4(1) -2(4) 0(6) 2(4) 4(1)	-4(2) 0(12) 4(2)

Tab. 2: Spectrum of the 4-cell 60/102 NBCA based regular graph

No. of Union (t)	Complement vector	Degree	First Eigenvalue	Second Eigenvalue	Spectral Gap (g)	g/t
1	1,15	4	4	2	2	2
3	1,3,9,15	8	8	4	4	1.33
5	1,3,5,9,11,15	12	12	2	10	2
7	1,3,5,7,9,11,13,15	16	16	0	16	2.2857

Tab. 3: Comparison of Mukhopadhyay's spectral gaps with our spectral gaps

No. of Union (t)	g/t(Mukhopadhyay's method)	g/t(Our method)
1	0.76	2
3	1.03	1.33
5	1.14	2
7	1.54	2.2857

Choose the complement vectors F_1, F_2 such that $(F_1, F_2) \in U$. Let G_1 (resp. G_2) be the graph with F_1 (resp. F_2). Then we can construct an expander graph where spectral gap is maximal.

The following algorithm shows computing the four neighbors of a vertex in G which is the union of G_1 and G_2.

Algorithm (Computing neighbors of a vertex in G)**.**

Input: Complement vectors $(F_1, F_2) \in K$ and a state $\mathbf{x} \in G$.

Output: The four neighbors (S_1, S_2, P_1, P_2) of **x**.

Step 1: Find the next state S_1 (resp. S_2) of $\mathbf{x}$ using the operator $\overline{T}_1$ (resp. $\overline{T}_2$).

$$S_1 = \overline{T}_1\mathbf{x} = T\mathbf{x} \oplus F_1$$
$$S_2 = \overline{T}_2\mathbf{x} = T\mathbf{x} \oplus F_2$$

/* Find the immediate predecessor P_1 (resp. P_2) by using Theorem 4.4 in Step 2 and Step 3 */

Step 2: Compute $W := \mathbf{x} \oplus F_1$ and $V := \mathbf{x} \oplus F_2$.

Step 3: For $W = (w_1, w_2, \cdots, w_n)$, $V = (v_1, v_2, \cdots, v_n)$ and $k = 2, \cdots, n-1$ find $P_1 := (p_{11}, p_{12}, \cdots, p_{1n})$ and $P_2 := (p_{21}, p_{22}, \cdots, p_{2n})$

$$\begin{aligned} p_{11} &= w_1, \;\; p_{1n} = w_n, \;\; p_{1k} = w_k \oplus p_{1k+1} \\ p_{21} &= v_1, \;\; p_{2n} = v_n, \;\; p_{2k} = v_k \oplus p_{2k+1} \end{aligned}$$

In general the description of an expander d-regular graph grows exponentially with the number of vertices as the increase of the size of 60/102 NBCA. However as we require to store only two complement vectors F_1 and F_2, this problem is solved by the above algorithm.

5 Conclusion

In this paper, we proposed a method to generate expander graphs with good expansion properties based on group $60/102$ NBCA. The expansion properties by our method is better than the expansion properties proposed by Mukhopadhyay et al.

References

[1] P. Pal Chaudhuri, D. Roy Chowdhury, S. Nandi, and S. Chattopadhyay. Additive cellular automata theory and its application i, ieee computer society press, california. *IEEE Computer Society Press, California*, 2000.

[2] J. Cheeger. A lower bound for the smallest eigenvalue of the laplacian. in problems in analysis(papers dedicated to solomon bochner, 1969, 195-199). *Princeton Univ. Press*, 1970.

[3] S.J. Cho, U.S. Choi, H.D. Kim, and Y.H. Hwang. Analysis of complemented ca derived from linear hybrid group ca, computers and mathematics with applications. *Computers and Mathematics with Applications*, 53:54–63, 2007.

[4] S.J. Cho, U.S. Choi, H.D. Kim, Y.H. Hwang, J.G. Kim, and S.H. Heo. New synthesis of one-dimensional 90/150 linear hybrid group cellular automata. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 26:1720–1724, 2007.

[5] W. Diffie and M. Hellman. New direction in cryptography. *IEEE Transaction on Information Theory*, pages 644–654, 1976.

[6] D.Peleg and E.Upfal. Constructing disjoint paths on expander graphs. *Combinatorica*, pages 289–313, 1989.

[7] O. Goldreich. Candidate one-way functions based on expander graphs. *Cryptology ePrint Archieve, Report 200/063*, pages 1–9, 2000.

[8] S. Hoory, N. Lindal, and A. Wigderson. Expander graphs and their applications. *Bull. AMS*, 2006.

[9] D. Mukhopadhyay and D.R. Chowdhury. Generation of expander graphs using cellular automata and its applications to cryptography. *LNCS*, 4173:636–645, 2006.

[10] M.S. Pinsker. On the complexity of a concentrator. *In 7th International Telegraffic Conference*, pages 1–4, 1973.

[11] M. Sipser and D. Spielman. Expander codes. *IEEE Transactions on Information Theory*, 42:1710–1722, 1996.

[12] S. Wolfram. Statistical mechanics of cellular automata. *Rev. Mod. Phys.*, 55:601–644, 1983.