60/102 NBCA에 기반을 둔 확장그래프들과 그 응용

김한두* · 조성진** · 최언숙***

Expander graphs based on 60/102 NBCA and its application

Han-Doo Kim* · Sung-Jin Cho** · Un-Sook Choi***

이 논문은 2010년도 정부재원(교육과학기술부 인문사회연구역량강화사업비)으로 한국연구재단의 지원을 받아 연구되었음(NRT-2010-B00008)

요 약

확장그래프는 통신망의 설계와 분석에 유용하다. Mukhopadhyay 등은 nongroup two predecessor single attractor CA(Cellular Automata; 이하 CA)에 기반을 둔 한 부류의 확장그래프들을 생성하는 방법을 소개했다. 본 논문에서는 group CA인 60/102 Null Boundary CA(NBCA)에 기반을 둔 한 부류의 확장그래프들을 생성하는 방법을 제안한다. 본 논문에서 제안된 방법에 의해 생성된 spectral gap은 Mukhopadhyay 등[12]에 의해 생성된 spectral gap보다 크다. 제안된 확장그래프들의 조합적 성질에 기반을 둔 일방향 함수들을 생성하는 알고리즘을 제안한다. 60/102 NBCA에 의해 생성된 d-정규 그래프를 이용한 일방향함수는 Goldreich의 방법[5]에 기반을 두고 있다.

ABSTRACT

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 CA(Cellular Automata). 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 larger than that of Mukhopadhyay et. al [12]. As an application we give an algorithm which generate one-way functions whose security lies on the combinatorial properties of our expander graphs. the one-way function using d-regular graph generated by the 60/102 NBCA is based on the Goldreich's construction [5].

키워드

확장그래프, 60/102 NBCA, 일방향함수, 인접행렬, 이분그래프, 보안

Key word

expander graph, 60/102 NBCA, one-way function, adjacency matrix, bipartite graph, security

* 정회원 : 인제대학교 (mathkhd@inje.ac.kr), 기초과학연구소
** 종신회원 : 부경대학교 (교신저자, sjcho@pknu.ac.kr)
*** 정회원 : 동명대학교

접수일자 : 2011. 05. 03
심사완료일자 : 2011. 06. 22

Ⅰ. 서 론

확장그래프들은 Pinsker[1]에 의해 처음 정의되었고, 1970년대 초 Pinsker에 의해 존재성이 처음으로 증명되었다. 또한 확장그래프들은 정수론과 계산복잡도의 여러 문제를 해결하는 도구로서 뿐만 아니라 오류정정부호이론, 의사소수이론 분야에서 유용하다([2]~[4]).

Goldreich[5]는 확장그래프와 같은 조합적 구성 방법을 이용한 일방향함수를 제안했다. 일방향함수는 안전한 통신에서 중요한 분야인 키 교환 알고리즘에서 중요하다. Diffie-Hellman 키 교환 알고리즘[6]은 안전한 키 분배 문제 방법을 제시하고 있다. 확장그래프는 통신 네트워크의 설계 및 분석에 유용하다. Mukhopadhyay 등은 직전자(predecessor)가 2개이고 끌개(attractor)가 1개인 nongroup CA에 기반을 둔 한 부류의 확장그래프를 생성하기 위한 한 방법을 제안했다. 본 논문에서 group CA인 60/102 Null Boundary CA(NBCA)에 기반을 둔 한 부류의 확장그래프를 생성하는 방법을 제안한다. 제안된 방법에 의해 생성된 확장그래프의 스펙트럴 갭(spectral gap)은 Mukhopadhyay 등에 의해 생성된 확장그래프의 스펙트럴 갭보다 크다. 본 논문에서 제안된 방법은 적은 저장공간으로 좋은 확장 성질을 갖는 정규그래프를 생성하기 위하여 60/102 NBCA([7]~[9])의 간단하고, 규칙적이며, 작은 단위로 확장 연결이 가능한 구조를 이용한다는 것이 장점이다. 한 가지 응용분야로 확장그래프의 조합적 성질들에 보안성이 의존하는 일방향함수들을 생성하는 알고리즘을 제안한다. 60/102 NBCA에 의해 생성된 d-정규그래프를 이용한 일방향함수는 Goldreich의 구성 방법[5]에 기반을 두고 있다.

Ⅱ. 기본 개념

비형식적으로 확장그래프는 꼭지점의 모든 부분집합 S가 여집합 $\overline{S}=V-S$의 많은 꼭지점에 연결된다는 점에서 빠르게 확장되는 그래프 $G=(V,E)$이다.

<정의 2.1> ([10]) $G=(V,E)$는 꼭지점이 n개인 확장그래프이다. V의 부분집합 S에 대하여 S의 변경계(edge boundary) ∂S는 S의 꼭지점과 $\overline{S}$의 꼭지점을 연결하는 변들의 집합이다. G의 확장매개변수(expansion parameter) $h(G)$는 다음과 같다.

$$h(G)=\min\left\{\frac{|\partial S|}{|S|}\mid |S|\le\frac{n}{2}\right\}$$

단, $|X|$는 집합 X의 원소의 개수이다.

<예제 2.2> $G=(V,E)$는 꼭지점이 n개인 완전그래프이고 $S\subseteq V$라 하자. 그러면 S의 임의의 꼭지점은 $\overline{S}$의 모든 꼭지점과 연결되어 있으므로 $|\partial S|=|S|\times|\overline{S}|=|S|(n-|S|)$이다. 그러므로 G의 확장매개변수는 다음과 같다.

$$h(G)=\min\left\{n-|S|\mid |S|\le\frac{n}{2}\right\}=\lceil n/2\rceil$$

단, $\lceil x\rceil$는 x보다 작지 않은 최소 정수이다.

<예제 2.3> $G=(V,E)$는 꼭지점이 n개인 d-정규그래프이고 $S\subseteq V$라 하자. S의 꼭지점의 개수가 $\frac{n}{2}$ 이하라 하자. 그러면 S의 한 꼭지점은 $\overline{S}$의 $d\times|\overline{S}|/n$개 꼭지점과 연결되어 있으므로 $|\partial S|/|S|\approx d|\overline{S}|/n$ 이다. $|\overline{S}|$의 최소값은 대략 $n/2$이므로 꼭지점의 개수 n과 상관없이 $h(G)\approx d/2$가 성립한다.

<정의 2.4> 그래프 G의 인접행렬(adjacency matrix) $A(G)=(b_{ij})$는 $|V|\times|V|$ 행렬이고, b_{ij}는 다음과 같다.

$$b_{ij}=\begin{cases}1, i\text{번째 꼭지점과 }j\text{번째 꼭지점 사이에 변이 있다.}\\ 0, i\text{번째 꼭지점과 }j\text{번째 꼭지점 사이에 변이 없다.}\end{cases}$$

인접행렬 $A(G)$의 고유스펙트럼(eigenvalue spectrum)의 성질들을 이용하여 그래프 G의 성질들을 이해할 수 있다. $A(G)$의 고유스펙트럼을 그래프 G의 스펙트럼이라고 하겠다. 고유스펙트럼과 최대 고유값, 최소 고유값, 행렬식, 트레이스와 같은 성질들은 빠르게 계산이 가능하므로 유용하다[10].

$G=(V,E)$는 비방향그래프이고 $A(G)$는 G의 인접행렬이라고 한다. 그리고 $\lambda_i(A(G))\,(1\le i\le n)$는 $A(G)$

의 고유값이라 한다. 그러면 $A(G)$는 실대칭행렬이므로 대각화가 가능하다. 일반성을 잃지 않고 다음과 같이 가정할 수 있다.

$$\lambda_1(A(G)) \geq \lambda_2(A(G)) \geq \cdots \geq \lambda_n(A(G))$$

$\mathcal{C}$는 상태전이행렬이 T인 CA이고 $\mathcal{C}'$는 상태전이연산자가 $\overline{T}$인 $\mathcal{C}$로부터 유도된 여원(comple- mented) CA라 하자. 그리고 $\overline{T^p}$는 $\overline{T}$를 p번 적용한 연산자라 하자. XNOR 규칙이 적용되는 위치의 성분이 1이고 XNOR 규칙이 적용되지 않는 위치의 성분이 0인 벡터를 F라 하고 이를 여원벡터라 할 때, 여원 CA의 다음 상태를 구하는 식은 $\overline{T}x = Tx \oplus F$이고 $\overline{T^p}x = [I \oplus T \oplus T^2 \oplus \cdots \oplus T^{p-1}]F \oplus T^p(x)$이다.

Ⅲ. 고유 스펙트럼의 성질

이 절에서 비방향그래프 G의 인접행렬 $A(G)$의 고유 스펙트럼의 성질들을 조사한다. 다음 정리들은 잘 알려져 있다.

<정리 3.1> G가 비방향 d-정규그래프일 때 $\lambda_1(A(G)) = d$이다.

<정리 3.2> G가 비방향 d-정규그래프일 때 G가 연결그래프일 필요충분조건은 $\lambda_1(A(G)) > \lambda_2(A(G))$이다.

<정리 3.3> G가 비방향 d-정규그래프일 때 G가 이분그래프(bipartite graph)일 필요충분조건은 $\lambda_i(A(G)) = -\lambda_{n+1-i}(A(G))$ $(i = 1,2,\cdots,n)$이다.

<정의 3.4> d-정규그래프 G의 갭(gap) $\Delta(G)$을 $\Delta(G) = d - \lambda_2(A(G))$ 로 정의한다.

<정리 3.5[11]> G가 $\lambda_1(A(G)) \geq \lambda_2(A(G)) \geq \cdots \geq \lambda_n(A(G))$을 만족하는 d-정규그래프라 하자. 그러면 $\Delta(G)/2 \leq h(G) \leq \sqrt{2d\Delta(G)}$ 이다.

<예제 3.6> 비방향그래프 G의 인접행렬 $A(G)$이 다음과 같다고 하자.

$$A(G) = \begin{pmatrix} 0\,1\,0\,1\,2\,0\,0\,0 \\ 1\,0\,1\,0\,0\,0\,0\,2 \\ 0\,1\,0\,1\,0\,0\,2\,0 \\ 1\,0\,1\,0\,0\,2\,0\,0 \\ 2\,0\,0\,0\,0\,1\,0\,1 \\ 0\,0\,2\,1\,0\,1\,0\,1 \\ 0\,0\,2\,0\,0\,1\,0\,1 \\ 0\,2\,0\,0\,1\,0\,1\,0 \end{pmatrix}$$

그러면 다음이 성립한다.

$\lambda_1(A(G)) = 4, \lambda_2(A(G)) = \lambda_3(A(G)) = 2, \lambda_4(A(G)) = \lambda_5(A(G)) = 0, \lambda_6(A(G)) = \lambda_7(A(G)) = -2,$

$\lambda_8(A(G)) = -4$. 더욱이 $\Delta(G) = 4-2 = 2$이므로 $1 \leq h(G) \leq 4$이다. $\lambda_1(A(G)) > \lambda_2(A(G))$이고 $\lambda_i(A(G)) = -\lambda_{9-i}(A(G))$ $(i = 1,2,\cdots,8)$이므로 G는 연결그래프이고 이분그래프이다.

Ⅳ. 60/102 NBCA에 기반을 둔 확장그래프

이 절에서 60/102 NBCA를 이용하여 한 부류의 임의의 d-정규그래프들을 구성한다. $\mathcal{C}$는 상태전이행렬 T가 다음과 같은 n-셀 60/102 NBCA라 하자. 이후로 상태전이행렬 T는 $T = < 60,102,\cdots,102 >$를 나타낸다.

<정리 4.1[7]> T의 특성다항식 $c(x)$는 $c(x) = (x+1)^n$이다.

<정리 4.2[7]> T의 최소다항식 $m(x)$는 $m(x) = (x+1)^{n-1}$이다.

$m(x) = (x+1)^{n-1}$이므로 다음 정리가 성립한다. 정리 4.3의 증명은 [7]의 정리 3.4의 증명과 유사하다.

<정리 4.3> $\mathcal{C}$는 상태전이행렬이 T인 n-셀 60/102 NBCA라 하자. $\mathcal{C}'$은 여원벡터(complemented vector)가 $(a_1,\cdots,a_{n-1},1)^t$ $(a_i \in \{0,1\}, i = 1,2,\cdots,n-1)$이고 상태전이연산자가 $\overline{T}$인 $\mathcal{C}$로부터 유도된 여원 CA라고 하자. 단, $\boldsymbol{x}^t$는 벡터 $\boldsymbol{x}$의 전치행렬이다.

$\mathrm{ord}(T) = 2^a$이면 다음이 성립한다.

(a) C'의 사이클들의 모든 길이는 같다.

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

참고 A. 정리 4.3에 의하면 C의 상태전이는 어떤 끌개도 없다.

<예제 4.4> C가 상태전이행렬이 $T = < 60, 102, 102 >$인 3-셀 60/102 NBCA라 하자. 그러면 C의 상태전이는 다음과 같다.

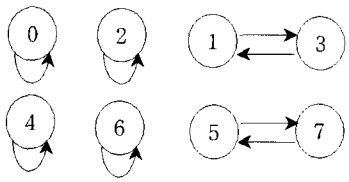

그림 1. C의 상태전이

Fig. 1. The state transition diagram of C

$F_1 = (0,0,1)^t$라 하면 보조정리 2.5에 의하여 $\overline{T}0 = 1, \overline{T}1 = 2, \overline{T}2 = 3, \overline{T}3 = 0, \overline{T}4 = 5, \overline{T}5 = 6, \overline{T}6 = 7, \overline{T}7 = 4$이다. 그러면 C의 여원벡터가 $F_1 = (0,0,1)^t$인 여원 CA C_1'의 상태전이연산자 $\overline{T}$의 상태전이도표 G_1을 얻는다. $\mathrm{ord}(\overline{T}) = 2 \cdot \mathrm{ord}(T) = 2 \cdot 2 = 4$이고, 정리 4.3에 의해 C의 사이클들의 모든 길이가 똑같다.

그림 2는 여원벡터가 각각 $F_1 = (0,0,1)^t$, $F_2 = (1,1,1)^t$인 여원 CA의 상태전이도표 G_1, G_2를 보여준다. 8×8 인접행렬 $A(G_1), A(G_2)$은 예제 4.4에서와 같이 다음과 같다.

$$A(G_1) = \begin{pmatrix} 01010000 \\ 10100000 \\ 01010000 \\ 10100000 \\ 00000101 \\ 00001010 \\ 00000101 \\ 00001010 \end{pmatrix}, A(G_2) = \begin{pmatrix} 00000101 \\ 00001010 \\ 00000101 \\ 00001010 \\ 01010000 \\ 10100000 \\ 0101000 \end{pmatrix}$$

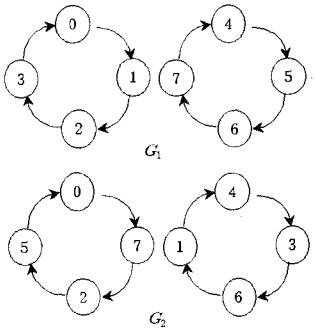

그림 2. $F_1 = (0,0,1)^t$ $(F_2 = (1,1,1)^t)$인 여원 CA의 상태전이 G_1 (또는 G_2)

Fig. 2. The state transition diagram G_1 (resp. G_2) of the complemented CA with $F_1 = (0,0,1)^t$ (resp. $F_2 = (1,1,1)^t$)

G는 두 그래프 G_1과 G_2의 합그래프이다. 그러면 $A(G)$는 다음과 같다.

$$A(G) = \begin{pmatrix} 01010101 \\ 10101010 \\ 01010101 \\ 10101010 \\ 01010101 \\ 10101010 \\ 01010101 \\ 10101010 \end{pmatrix}$$

$A(G)$의 특성다항식은 $x^6(x-4)(x+4)$이다. 그러므로 $A(G)$의 고유값은 $\lambda_1 = 4, \lambda_2 = \cdots = \lambda_5 = 0, \lambda_6 = -4$이다. 그러므로 정리 3.2와 정리 3.3에 의하여 G는 연결 이분그래프이다. 그림 3은 인접행렬이 $A(G)$인 그래프 G이다.

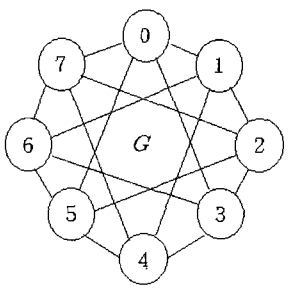

그림 3. 그래프 G

Fig. 3. The graph G

<정리 4.5> $\boldsymbol{C}$는 상태전이행렬이 T인 60/102 NBCA이고 $\boldsymbol{C}_1'$(또는 $\boldsymbol{C}_2'$)은 여원벡터가 $F_1=(0,*,\cdots,*,1)^t$, $(F_2=(1,*,\cdots,*,1)^t)$인 $\boldsymbol{C}$로부터 유도된 여원 CA라 하자. 또한 $\overline{T_1}X=TX\oplus F_1$, $\overline{T_2}X=TX\oplus F_2$라 하자.

G_1(또는 G_2)는 $\boldsymbol{C}_1'$(또는 $\boldsymbol{C}_2'$)로부터 만들어진 그래프라 하고 G는 두 그래프 G_1, G_2의 합그래프라고 하자.

그러면 G는 이분 4-정규그래프이다.

$S=\{(x_1,x_2,\cdots,x_n)^t|x_i\in\{0,1\}\}$,

$A_1=\{(0,x_2,\cdots,x_{n-1},0)^t|x_i\in\{0,1\}\}$,

$A_2=\{(1,x_2,\cdots,x_{n-1},0)^t|x_i\in\{0,1\}\}$,

$B_1=\{(0,x_2,\cdots,x_{n-1},1)^t|x_i\in\{0,1\}\}$,

$B_2=\{(1,x_2,\cdots,x_{n-1},1)^t|x_i\in\{0,1\}\}$라 하고

$A=A_1\cup A_2$, $B=B_1\cup B_2$라 하면 $A\cup B=S$이다.

임의의 $X\in A_1$에 대하여

$\overline{T_1}X=TX\oplus F_1$

$=(0,*,\cdots,*,0)^t\oplus(0,*,\cdots,*,1)^t$

$=(0,*,\cdots,*,1)^t\in B_1$

$\overline{T_2}X=TX\oplus F_2$

$=(0,*,\cdots,*,0)^t\oplus(1,*,\cdots,*,1)^t$

$=(1,*,\cdots,*,1)^t\in B_2$

임의의 $X\in A_2$에 대하여

$\overline{T_1}X=TX\oplus F_1$

$=(1,*,\cdots,*,0)^t\oplus(0,*,\cdots,*,1)^t$

$=(1,*,\cdots,*,1)^t\in B_2$

$\overline{T_2}X=TX\oplus F_2$

$=(1,*,\cdots,*,0)^t\oplus(1,*,\cdots,*,1)^t$

$=(0,*,\cdots,*,1)^t\in B_1$

이와 유사하게 임의의 $Y\in B_1$에 대하여 $\overline{T_1}Y\in A_1$, $\overline{T_2}Y\in A_2$임을 보일 수 있다. 또한 임의의 $Y\in B_2$에 대하여 $\overline{T_1}Y\in A_2$, $\overline{T_2}Y\in A_1$임을 보일 수 있다.

표1은 G_1과 G_2의 합 그래프인 G의 고유 스펙트럼이다. 표1에서 $F_1=(0,0,0,0)^t$, $F_2=(1,1,0,0)^t$라 하자. 그러면 $A(G)$의 확장 스펙트럼은 $\lambda_1=\lambda_2=\lambda_3=\lambda_4=4, \lambda_5=\cdots=\lambda_{14}=0, \lambda_{15}=\lambda_{16}=-4$이다. 그러므로 이 경우 그래프 G는 이분그래프가 아니고 비연결 그래프이다. 또한 $F_1=(0,0,1,1)^t$, $F_2=(1,0,0,1)^t$라 하면 G는 이분그래프이다.

표 1. $A(G)$의 고유 스펙트럼
Table 1. The eigenvalue spectrum of $A(G)$

첫 행(열)의 8개 벡터는 여원벡터 F_1(또는 F_2)

	0000	0010	0100	0110
1000	-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)
1100				
1010	-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)
1110				
1001	-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)
1101				
1011				
1111				

	0001	0011	0101	0111
1000	-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)
1100				
1010				
1110				
1001	-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)
1101				
1011	-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)
1111				

<정리 4.6> $\boldsymbol{C}$는 상태전이행렬이 T인 n셀 60/102 NBCA이고 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)^t$는 T의 한 상태라 하자. 그러면 $\boldsymbol{x}$의 직전자 $\boldsymbol{y}=(y_1,y_2,\cdots,y_n)^t$는 다음 식을 만족한다:

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

(증명) C의 상태전이행렬 $T=(t_{ij})$는 다음과 같다.

$$t_{ij}=\begin{cases}1 & ,i=j\\ 1 & ,i=j-1\ (j=3,\cdots,n)\\ 0 & ,\text{그밖의 경우}\end{cases}$$

그러면 $T^{-1}=\begin{pmatrix}I_1 & O\\ OA\end{pmatrix}$, 단 $A=(a_{ij})$는 $a_{ij}=\begin{cases}1, & i\le j\\ 0, & \text{그밖의 경우}\end{cases}$ 이므로

$$y=T^{-1}x=\begin{pmatrix}1&0&0&\cdots&0&0&0\\0&1&1&\cdots&1&1&1\\0&0&1&\cdots&1&1&1\\\vdots&\vdots&\vdots&\ddots&\vdots&\vdots&\vdots\\0&0&0&\cdots&1&1&1\\0&0&0&\cdots&0&1&1\\0&0&0&\cdots&0&0&1\end{pmatrix}\begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix}$$

$$=\begin{pmatrix}x_1\\x_2\oplus x_3\oplus\cdots\oplus x_n\\\vdots\\x_{n-1}\oplus x_n\\x_n\end{pmatrix}$$

이다. 따라서 $y_1=x_1, y_n=x_n, y_k=x_k\oplus y_{k+1}$ $(k=2,\cdots,n-1)$이 성립한다.

표2는 정규그래프에 기반을 둔 60/102 NBCA로 수행한 실험결과이다. 임의의 4차, 8차. 12차. 16차 60/102 NBCA에 기반을 둔 그래프들에 대한 두 가지 최대 고유값을 보여주고 있다. 실험결과에 의하면 스펙트럴 갭과 그리고 확장 매개변수가 합 연산자(t)의 개수에 비례하여 증가한다는 것을 보여준다. 표3은 우리 방법에 의한 스펙트럴 갭이 Mukhopadhyay의 방법에 의한 스펙트럴 갭보다 크다는 것을 보여준다[12].

표 2. 4-셀 60/102 NBCA에 기반을 둔 정규그래프의 스펙트럼
Table 2. Spectrum of the 4-cell 60/102 NBCA based regular graph

합의 개수 (t)	여원 벡터	차수	첫째 고유값	둘째 고유값	스펙트럴 갭(g)	g/t
1	1,15	4	4	2	2	2
3	1,3,9,15	8	8	4	1	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

표 3. Mukhopadhyay의 스펙트럴 갭과 우리 방법에 의한 스펙트럴 갭의 비교
Table 3. Comparison of Mukhopadhyay's spectral gaps with our spectral gaps

합의 개수 (t)	g/t(Mukhopadhyay의 방법)	g/t (우리 방법)
1	0.76	2
3	1.03	1.33
5	1.14	2
7	1.54	2.2857

참고 B. T의 역행렬

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

을 구하기는 쉽다. 그러므로 직전자들을 얻는데 걸리는 시간은 $O(n)$이다. 주어진 n-셀 60/102 NBCA에 대하여 최대 스펙트럴 갭들을 갖는 d-정규그래프들의 구성은 F_1과 F_2 사이의 관계에 의존한다. 예를 들어 표1에서 $F_1=(0,0,0,1)^t$, $F_2=(1,1,1,1)^t$라 하면 스펙트럴 갭은 4-정규그래프에서 최대값인 2이다.

이제

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

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

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

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

이고 $K=(F_{11}\times F_{21})\cup(F_{12}\times F_{22})$라 하자.

$(F_1,F_2)\in K$인 여원벡터 F_1,F_2를 선택하고 G_1 (또는 G_2)를 여원벡터가 F_1(또는 F_2)인 그래프라 하자. 그러면 스펙트럴 갭이 최대인 확장그래프를 구성할 수 있다.

다음 표4의 알고리즘 A는 그래프 G_1과 G_2의 합그래프인 G의 한 꼭지점의 네 이웃 꼭지점을 계산하는 방법을 제시한다.

표 4. 알고리즘 A.
Table 4. Algorithm A.

알고리즘 A. G의 한 꼭지점의 네 이웃 꼭지점을 계산하는 방법
INPUT : 여원벡터 $(F_1, F_2) \in K$와 한 상태 $x \in G$
OUTPUT : x의 네 이웃 꼭지점들(S_1, S_2, P_1, P_2)
Step1: 연산자 $\overline{T_1}$(또는 $\overline{T_2}$)를 이용한 x의 다음 상태 S_1 (또는 S_2)를 구한다.
$S_1 = \overline{T_1}x = Tx \oplus F_1$, $S_2 = \overline{T_2}x = Tx \oplus F_2$
/* Step2와 Step3에서 정리 4.6을 이용하여 직전자 P_1(또는 P_2)를 구한다. */
Step2: $W = x \oplus F_1$와 $V = x \oplus F_2$를 계산한다.
Step3: $W = (w_1, w_2, \cdots, w_n)$와 $V = (v_1, v_2, \cdots, v_n)$에 대하여
$P_1 = (p_{11}, p_{12}, \cdots, p_{1n})$과 $P_2 = (p_{21}, p_{22}, \cdots, p_{2n})$을 구한다.
$p_{11} = w_1, p_{1n} = w_n, p_{1k} = w_k \oplus p_{1,k+1}$
$p_{21} = v_1, p_{2n} = v_n, p_{2k} = v_k \oplus p_{2,k-1} (k = 2, \cdots, n-1)$

일반적으로 확장 d-정규그래프의 상태는 60/102 NBCA의 크기가 증가함에 따라 꼭지점의 개수에 지수적으로 비례하여 증가한다. 하지만 단지 두 여원벡터 F_1과 F_2만을 저장하면 되므로 이 문제는 알고리즘 A에 의해 해결된다. 다음 표5의 알고리즘 B는 알고리즘 A를 이용하여 생성된 일방향함수의 구성 방법을 보여준다. (60/102 NBCA에 의해 생성된 d-정규그래프를 이용한) 일방향함수는 [5]에서 제안된 구성 방법에 기반을 두고 있다.

표 5. 알고리즘 B.
Table 5. Algorithm B.

알고리즘 B. 60/102 NBCA를 이용한 일방향함수 H
INPUT : l비트 벡터 $x = (x_1, x_2, \cdots, x_l)$
OUTPUT : 2^n비트 벡터 $y = (y_1, y_2, \cdots, y_{2^n})$, 단 $y = H(x)$
Step1: $n = \lceil \log_2 l \rceil$ 을 계산한다. 단 $n > 3$
Step2: $x' = (x_1', x_2', \cdots, x_{2^n}') = R \| x$
단, $x_1' = 0, \cdots, x_{2^n-l}' = 0, x_{2^n-l+1}' = x_1, x_{2^n-l+2}' = x_2, \cdots, x_{2^n}' = x_l$ 이고
$R = (0, \cdots, 0)$은 길이가 $2^n - l$인 벡터이다.
Step3: $(F_1, F_2) \in K$인 두 n비트 벡터 F_1, F_2를 선택한다.
Step4: 알고리즘 A에 의해 $2^n \times d$배열 $S = (s_{ij})$를 구성한다. 단 $s_{i1}, \cdots, s_{id}$는 꼭지점 i의 d개 이웃 꼭지점들이다. 배열 S는 다음과 같은 형태이다.

$$\begin{matrix} s_{11} & s_{12} & \cdots & s_{1d} \\ s_{21} & s_{22} & \cdots & s_{2d} \\ \vdots & \vdots & \ddots & \vdots \\ s_{2^n,1} & s_{2^n,2} & \cdots & s_{2^n,d} \end{matrix}$$

Step 5: $y = (y_1, y_2, \cdots, y_{2^n})$를 계산한다.
단, $y_i = (X(s_{i1}) \wedge X(s_{i2})) \vee (X(s_{i3}) \wedge X(s_{i4})) \vee \cdots \vee (X(s_{i,d-1}) \wedge X(s_{id}))$
이고 x'에서 $X(k) = x_k'$이다.

<예제 4.7> 주어진 15비트 $x = 100000101111$ $(= 2095)$에 대하여 Step1에 의해 $n = \lceil \log_2 15 \rceil = 4$이다. 그러므로 $x' = 0000 \| 100000101111$이다. $F_1 = (0,0,0,1)^t$, $F_2 = (1,1,1,1)^t$라 하자. 그러면 다음과 같이 $2^4 \times 4$ 배열 $S = (s_{ij})$을 구성할 수 있다.

$$\begin{matrix} 2 & 8 & 14 & 16 \\ 1 & 3 & 11 & 13 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & 7 & 9 & 11 \end{matrix}$$

Step4에 의해
$y_1 = (X(2) \wedge X(8)) \vee (X(14) \wedge X(16))$
$= (0 \wedge 0) \vee (1 \wedge 1) = 1,$
$y_2 = (X(1) \wedge X(3)) \vee (X(11) \wedge X(13))$
$= (0 \wedge 0) \vee (1 \wedge 1) = 1, \cdots,$
$y_{16} = (X(1) \wedge X(7)) \vee (X(9) \wedge X(11))$
$= (0 \wedge 0) \vee (0 \wedge 1) = 0$ 이다.
그러므로 $y = H(x) = 1101001000010100 (= 53780)$

V. 결 론

본 논문에서는 group CA인 60/102 NBCA에 기반을 둔 좋은 확장 성질들을 갖는 한 부류의 확장그래프들을 생성하는 방법을 제안했다. 본 논문에서 제안된 방법에 의해 생성된 확장그래프의 성질들은 Mukhopadhyay 등에 의해 생성된 확장 성질들보다 우수하다. 제안된 확장그래프들은 확장그래프들의 조합적 성질에 기반을 둔 보안성 때문에 효율적인 일방향함수들을 생성하는 데 사용할 수 있다.

참고문헌

[1] M.S. Pinker, On the complexity of a concentrator, In 7th International Telegraffic Conference, 1973.
[2] S. Hoory, N. Lindal, and A. Wigderson, Expander graphs and their applications, Bull. AMS, Vol. 43, pp. 439-561, 2006.

[3] D. Peleg and E. Upfal, Constructing disjoint paths on expander graphs, Combinatorica, Vol. 9, pp. 289-313, 1989.

[4] M. Sipser and D. Spielman, Expander codes, IEEE Transactions on Information Theory, Vol. 42, pp. 1710-1722, 1996.

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

[6] W. Diffie and M. Hellman, New directions in cryptography, in IEEE Transaction on Information Theory, Vol. 22, pp. 644-654, 1976.

[7] 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, Vol. 53, pp. 54-63, 2007.

[8] P. Pal Chaudhuri, D. Roy Chowdhury, S. Nandi, and S. Chattopadhyay, Additive Cellular Automata Theory and its Applications Vol. 1, IEEE Computer Society Press, 1997.

[9] 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, Vol. 26, pp. 1720-1724, 2007.

[10] M.A. Nielsen, Introduction to expander graphs, www.ginfo.org/people/nielsen/blog/archive/notes/expander-graphs.pdf, 2005.

[11] J. Cheeger, A lower bound for the smallest eigenvalue of the Laplacian, In Problems in analysis (Papers dedicated to Solomon Bochner, 1969, pp. 195-199), Princeton Univ. Press, Princeton, N.J., 1970.

[12] D. Mukhopadhyay and D.R. Chowdhury, Generation of expander graphs using cellular automata and its applications to cryptography, ACRI 2006, LNCS Vol. 4173, pp. 636-645, 2006.

저자소개

김한두(Han-Doo Kim)

1982년 2월 : 고려대학교 수학과 학사
1984년 2월 : 고려대학교 수학과 석사
1988년 2월 : 고려대학교 수학과 박사
1989년 ~ 현재 : 인제대학교 컴퓨터 응용과학부 정교수, 기초과학연구소
※관심분야 : 전산수학, 셀룰라 오토마타론

조성진(Sung-Jin Cho)

1979년 2월: 강원대학교 수학교육과 학사
1981년 2월: 고려대학교 수학과 석사
1988년 2월: 고려대학교 수학과 박사
1988년 ~ 현재 : 부경대학교 응용수학과 정교수
※관심분야 : 셀룰라 오토마타론, 정보보호, 부호이론

최언숙(Un-Sook Choi)

1992년 2월 : 성균관대학교 산업공학과 학사
2000년 2월 : 부경대학교 응용수학과 석사
2004년 2월 : 부경대학교 응용수학과 박사
2004년 3월~2006년 2월 : 영산대학교 자유전공학부 단임교수
2006년 3월~현재 : 동명대학교 자율전공학부 전임강사
※관심분야 : 셀룰라 오토마타론, 정보보호, 부호이론