김일성종합대학학보
(자연과학)
주체106(2017)년 제63권 제2호

JOURNAL OF **KIM IL SUNG** UNIVERSITY
(NATURAL SCIENCE)
Vol. 63 No. 2 JUCHE106(2017).

극대평면그라프에서의 비밀분배도식구성과 정보비평가

김현정, 김광천

우리는 정보보안체계구성에 널리 리용되고있는 비밀분배도식과 정보비평가에 관한 몇가지 연구결과를 제기하였다.

선행연구[1]에서는 임의의 그라프 G에 대하여 정보비 $\tilde{\rho}(G)$는 적어도 $\frac{1}{d}$이라는것과 G를 매 정점이 평균 λ번 피복되는 완전2조그라프들에 의하여 피복되는 그라프라고 할 때 $\tilde{\rho}(G)\geq\frac{1}{\lambda}$이 성립된다는것을 밝혔다. 여기서 d는 정점의 평균차수이다.

또한 평균차수가 d인 임의의 그라프 G에 대하여 $\tilde{\rho}(G)\geq\frac{2}{d+1}$가 성립되며 임의의 그라프 G에 관하여 $\tilde{\rho}(G)\geq\frac{c\log n}{n}$인 상수 $c>0$이 존재한다는것을 밝혔다.

선행연구[3]에서는 매 그라프를 완전2조그라프들에 의하여 피복하되 매 정점이 그 2조그라프들중의 최대로 $\frac{cn}{\log_2 n}$개에 포함되게 할수 있다는것을 증명하였다.

선행연구[4]에서는 길이가 5보다 큰 임의의 륜체의 평균정보비가 꼭 2/3라는것을 증명하였으며 선행연구[2]에서는 특별하게 구성된 그라프 G_n에 대하여 그것의 정보비의 아래, 웃한계를 평가하였다.

론문에서는 극대평면그라프우에서의 비밀분배도식들을 새로 구성하고 평균정보비를 평가하였다.

1. 극대평면그라프우에서의 비밀분배도식의 구성

G를 정점의 개수가 n인 그라프라고 하고 정점모임을 V로 표시하자.

정점부분모임 $A\subseteq V$에 대하여 A를 G의 독립모임 혹은 안정모임이라고 부른다.

주어진 그라프 G에 대하여 정점의 개수가 제일 큰 독립모임을 G의 최대독립모임이라고 부르며 최대독립모임의 원소수를 G의 내부안정수라고 부르고 $\alpha(G)$로 표시한다.

정의 다음의 조건을 만족시키는 우연량 $\xi_v, v\in V$와 ξ_s들의 모임을 그라프 G의 완전비밀공유도식이라고 부른다.

① ξ_s는 비밀이고 ξ_v는 v의 비밀분배몫이다.

② 정점 v, w사이에 릉이 존재하면 ξ_v와 ξ_w는 ξ_s를 완전히 결정한다.

③ $A\subseteq V$가 독립이면 ξ_s와 모임 $\{\xi_v, v\in V\}$는 통계적으로 독립이다.

$H(\xi)$를 우연량 ξ의 엔트로피 혹은 정보량이라고 하면 $\sum_{v\in V}H(\xi_v)/n$는 비밀분배몫의

평균크기이고 이때 $\tilde{\rho}_s = \dfrac{n \cdot H(\xi_s)}{\sum_{v \in V} H(\xi_v)}$ 를 비밀공유도식 s 의 평균정보비라고 부른다. 그리고 G 우에서 정의된 가능한 완전비밀공유도식 s 에 관한 $\tilde{\rho}_s$ 의 상한을 G 의 평균정보비라고 부르고 $\bar{\rho} = \bar{\rho}(G)$ 로 표시한다.

그라프를 평면우에 그릴 때 모든 릉들이 정점이 아닌데서 서로 사귀지 않게 그릴수 있다면 그 그라프를 평면그라프라고 부르며 G 를 평면그라프라고 할 때 여기에 하나의 릉을 보충하여도 평면그라프가 되지 않으면 G 를 극대평면그라프라고 부른다.

G 가 n 개의 정점을 가진 극대평면그라프라고 할 때 G 의 릉의 수가 $3n-6$ 개라는것은 알려져있다.

극대평면그라프의 내부안정수는 다음과 같이 계산된다.

$$\frac{2\left[\log_2 n - \log_2\left(\dfrac{2\log_2 \dfrac{r}{n\log_2 n}}{-\log_2\left(1-\dfrac{2r}{n(n-1)}\right)} - \dfrac{\log_2\log_2 n}{2\log_2 n}\left(\log_2\left(\dfrac{3}{e}\right) - \dfrac{\log_2(3\log_2 n)^2}{2}\right) + \log_2 e\right)\right]}{-\log_2\left(1-\dfrac{2r}{n(n-1)}\right)} - 3$$

다음과 같은 두가지 비밀분배도식에 대하여 보자.

비밀분배도식 1 $G=(V,\ E)$ 는 극대평면그라프이고 $V=\{v_1,\ v_2,\ \cdots,\ v_n\}$ 이라고 하자.

① 극대평면그라프 G 의 비밀을 S 로 한다.

② 정점 v_1 과 이웃인 모든 정점들에 S 와 독립인 우연비트 r_1 을 대응시키고 v_1 에는 $r_1 \oplus S$ 를 대응시킨다.

③ $G-v_1$ 에서 정점 v_2 와 이웃인 모든 정점들에 S, r_1 과 독립적으로 우연비트 r_2 를 대응시키고 v_2 에는 $r_2 \oplus S$ 를 대응시킨다.

④ $G-\{v_1, v_2\}$ 에서 정점 v_3 과 이웃인 모든 정점들에 S, r_1, r_2 와 독립적으로 우연비트 r_3 을 대응시키고 v_3 에는 $r_3 \oplus S$ 를 대응시킨다.

⑤ 우의 과정을 정점 v_{n-2} 에 이를 때까지 반복한다.

⑥ 마지막으로 $G-\{v_1, v_2, \cdots, v_{n-2}\}$ 에서 v_{n-1} 과 이웃인 정점에 S, $r_1, r_2, \cdots, r_{n-2}$ 와 독립적으로 우연비트 r_{n-1} 을 대응시키고 v_{n-1} 에는 $r_{n-1} \oplus S$ 를 대응시킨다.

비밀분배도식 2 극대평면그라프는 모든 면이 3각형으로 되여있다.

① 극대평면그라프 G 의 비밀을 S 로 한다.

② G 의 임의의 i 째 3각형의 세 정점 v_1, v_2, v_3 에 대하여 v_1 에는 비밀 S 와 비트수가 같고 S 와 독립적인 우연수 t_i 를 대응시키고 v_2 에는 $\log_2(t_i/S)$ 를, v_3 에는 $\log_2(t_i/S)+\log_2 t_i$ 를 대응시킨다.

③ G 의 매 3각형에 대하여 ②를 반복한다.

정리 1 비밀분배도식 1은 완전비밀분배도식이다.

증명 우선 G 의 매 릉은 비밀을 결정할수 있다.

$\{v_i, v_j\}$ 를 G 의 임의의 릉이라고 하고 $i<j$ 라고 하면 v_i 에는 $r_i \oplus S$ 가 대응되고 정

점 v_j에는 우연비트 r_i가 대응된다. 따라서 그것들의 배타적론리합은 $r_i \oplus r_i \oplus S = S$이므로 릉 $\{v_i, v_j\}$는 비밀을 완전히 결정한다.

한편 독립인 정점부분모임은 비밀 S와 독립이고 또 서로 독립인 우연량들의 모임이므로 비밀 S와 통계적으로 독립이라는것은 분명하다.(증명끝)

정리 2 비밀분배도식 2는 완전비밀도식이다.

2. 극대평면그라프우에서의 평균정보비평가

정리 3 극대평면그라프 G의 평균정보비는 $\tilde{\rho}(G) \geq \dfrac{1}{4-7/n}$을 만족시킨다.

증명 G의 평균정보비가 $\dfrac{1}{4-7/n}$인 완전비밀분배도식을 구성하면 정리는 증명된다.

여기서는 비밀분배도식 1에 대하여 평균정보비를 평가한다.

계의 총 비밀 S의 크기는 1bit이다. 그리고 매 정점에 배당되는 비밀분배몫들의 총량은 릉의 총 개수에 G의 정점의 개수에서 하나를 던 량을 합한것과 같다.

따라서 정점이 n개인 극대평면그라프의 릉의 개수가 $3n-6$이라는것을 고려하면 매 정점에 배당되는 비밀분배몫들의 총 량은 $4n-7$이고 이로부터 매 정점에 배당되는 비밀분배몫의 평균크기는 $\dfrac{4n-7}{n}$이다.

이리하여 비밀분배도식의 평균정보비는 $\tilde{\rho}_s = \dfrac{1}{4-7/n}$이며 따라서 극대평면그라프 G의 평균정보비는 $\tilde{\rho}(G) \geq \dfrac{1}{4-7/n}$이다.(증명끝)

정리 4 극대평면그라프 G의 평균정보비는 $\tilde{\rho}(G) \geq \dfrac{1}{4-10/n}$을 만족시킨다.

증명 여기서는 비밀분배도식 2에 대하여 평균정보비를 평가한다.

하나의 3각형을 이루는 3개의 정점들에 배당되는 비밀분배몫의 총합의 크기는 다음과 같다.

$$\log_2 t_v + \log_2\left(\frac{t_v}{S}\right) + \log_2 t_v + \log_2\left(\frac{S}{t_v}\right) =$$

$$= \log_2 t_v + \log_2 t_v - \log_2 S + \log_2 t_v + \log_2 S - \log_2 t_v = 2\log_2 t_v$$

다음 오일레르공식을 리용하여 극대평면그라프 G의 3각형개수를 구하면 다음과 같다.

$$f = m - n + 2$$

여기서 f는 면의 개수, m은 릉의 개수, n은 정점의 개수이다.

릉의 개수 m이 $m = 3n-6$으로 표시되므로 3각형의 개수는 $f = 3n-6-n+2 = 2n-4$이다. 그런데 여기서는 그라프의 내면만이 필요하므로 극대평면그라프 G의 내면을 이루는 3각형의 개수는 $2n-5$이다.

따라서 G의 정점들에 배당되는 비밀분배몫의 총 크기는 $(2n-5)\cdot 2\log_2 t_v$이고 G의 매 정점들에 배당되는 비밀분배몫의 평균크기는 다음과 같다.

$$\frac{(2n-5)\cdot 2\log_2 t_v}{n}$$

결국 G의 비밀분배도식 2의 평균정보비는 다음과 같다.

$$\widetilde{\rho}_s = \frac{\log_2 S}{\dfrac{(2n-5)\cdot 2\log_2 t_v}{n}} = \frac{n\log_2 S}{(2n-5)\cdot 2\log_2 t_v}$$

그런데 비밀 S와 우연수 t_v는 비트수가 같으므로 $\log_2 S$와 $\log_2 t_v$의 크기는 같다.

따라서 평균정보비 $\widetilde{\rho}_s$는 다음과 같이 계산된다.

$$\widetilde{\rho}_s = \frac{n\log_2 S}{(2n-5)\cdot 2\log_2 t_v} = \frac{n}{(2n-5)\cdot 2} = \frac{1}{4-10/n}$$

따라서 G의 평균정보비 $\widetilde{\rho}(G)$는 관계식 $\widetilde{\rho}(G) \geq \dfrac{1}{4-10/n}$을 만족시킨다.(증명끝)

참 고 문 헌

[1] L. Csirmaz; Cryptology ePrint Archive:Report, 2005/059.

[2] L. Csirmaz; Cryptology ePrint Archive:Report, 2010/058.

[3] L. Pyber et al.; Covering a Graph by Complete Bipartite Graph, Preprint, 34～85, 1995.

[4] D. R. Stinson; IEEE Trans. Inform. Theory, 40, 118, 1994.

주체105(2016)년 10월 5일 원고접수

Diagram Construction of the Secret Allocation and Evaluation of the Information Rate in the Maximum Planar Graphs

Kim Hyon Jong, Kim Kwang Chon

We propose several studying results on the diagram of the secret allocation and the evaluation of the information rate that are widely used in the construction of the information security system.

We carry out two evaluations for average information rate of maximum planar graphs.

Key word: maximum planar graph