通信情報保護學會誌
第2卷, 第2號, 1992. 6

그래프 동형문제와 군론(Group Theory)의 알고리즘

황규범* · 김 철**

1. 서 론

두 그래프에서 서로 이웃을 유지하는 정점들 사이에 1대 1대응이 있을때, 두 그래프를 동형(Isomorphic)이라 한다. n개의 정점을 갖는 주어진 두 그래프에는 n! 의 1대 1대응관계가 있을 수 있어서 두 그래프가 동형인지 아닌지를 결정하는 문제인 그래프의 동형문제를 풀기 위한 Polynomial-Time 알고리즘은 없다고 알려져 있다.

본 고는 암호화 프로토콜의 안전성 문제를 해결하기 위하여 제시된 모델인 영지식 증명 시스템등([한] 192쪽 참고)에서 사용되는 그래프의 동형 문제를 군론적인 관점에서 본 바를 조사한 것이며, 따라서 각각의 결과들에 대한 증명은 참고문헌의 제시로 대신한다. 군론의 기본적인 알고리즘을 언급한 후 그래프의 동형문제와의 관계를 논한다.

2. 기호 소개

집합 X에서 X 자신 위로의 1대 1대응 $\sigma : X \to X$를 X 위의 치환(permutation)이라 하고, 이 치환들 사이의 합성연산으로 이루는 군 S_X를 대칭군(symmetric group)이라 한다. 특히 집합 $X_n = \{1, 2, \cdots, n\}$ 위의 대칭군을 n차의 대칭군이라 하고 S_n으로 표시한다. 이 S_n의 위수(order), $|S_n|$, 는 n! 이다. S_n의 항등원(identity)으로 이루는 1원소 군을 1로 나타낸다. 군 G의 부분집합 H가 G의 연산에 관하여 군을 이룰때, H를 G의 부분군(subgroup)이라 하고 H<G로 나타낸다. 앞으로는 부분 집합 Γ에 의해 성성되는 S_n의 부분군을 $G = \langle \Gamma \rangle$라 표시한다.

다음의 세 기호는 일반적인 의미 그대로이다.

(1) Z(G)는 군 G의 중심(center), 즉 $Z(G) = \{x \in G \mid gx = xg \text{ for all } g \in G\}$이다.

(2) 군 G의 부분집합 $S(\neq\emptyset)$에 대하여, $N_G(S)$는 군 G의 부분군으로 G에서의 S의 정규화 부분군(normalizer), 즉 $N_G(S) = \{x \in G \mid xSx^{-1} = S\}$이다.

(3) 군 G의 부분집합 $S(\neq\emptyset)$에 대하여, $C_G(S)$는 군 G의 부분군으로 G에서의 S의 중심화 부분군(centralizer), 즉 $C_G(S) = \{x \in G \mid sx = xs \text{ for all } s \in S\}$이다.

군 G의 원소 g가 $g^2 = 1$을 만족하면 이 원소 g를 대합(involution)이라 한다.

3. 기본적인 Polynomial-Time 알고리즘

S_n의 부분군들 $H_1, H_2, \cdots, H_m$에 대하여 그 개수 m에 관한 다음 결과가 알려져 있다.

* 육군사관학교 수학과 부교수
** 광운대학교 이과대학 수학과 조교수

정리 3. 1 $1<H_1<H_2<\cdots<H_m\leq S_n$이라면, $m<2n$이다.
증명 Lagrange의 정리 ([Fr]의 101쪽 참고)를 이용하여 증명한다. [Ba]참고■

정리 3. 2 군 G의 모든 궤도(orbit)를 찾기 위한 Polynomial-Time 알고리즘이 존재한다.
증명 X_n을 정점들의 집합, 그리고, $g\in\Gamma$에 대하여 X_n의 $xg\neq x$인 $\{x, xg\}$를 연결선들의 집합으로 하는 그래프를 만든다. 이 그래프는 $O(n|\Gamma|)$로 결정될 수 있다. 이 그래프의 연결성분(connected components)이 바로 G의 궤적이다.■

또한 [At]에는 대칭군의 부분군에 관한 블럭(block)들을 찾는 Polynomial-Time 알고리즘이 존재함이 설명되어 있다.

정리 3. 3 다음의 것들을 찾기 위한 Polynomial-Time 알고리즘이 존재한다.
(1) $|G|$, 즉, G의 원소의 개수
(2) G를 생성할 수 있는 원소의 개수가 n^2 보다 적은 집합
증명 [Si1], [Si2]참고■

위의 정리를 이용하여 다음의 따름정리를 얻을 수 있다.

따름정리 3. 4 S_n의 한 원소 σ가 G에 속하는지의 여부를 가리기 위한 Polynomial-Time 알고리즘이 존재한다.
증명 $\Gamma\cup\{\sigma\}$에 의해 생성되는 군의 위수가 G의 위수와 같은지를 보면 된다.■

정리 3. 5 군 G의 유도열(혹은, 교환자군열, derived series, [김]의 133쪽 참고)과 감소 중심열(descending central series, [Fr] 167쪽 참고)을 찾아내는 Polynomial-Time 알고리즘이 존재한다.
증명 [Fu]참고■

따라서 군 G의 가해성(solvability)을 Polynomial-Time으로 알 수 있다.

정리 3. 6 S_n의 두 부분군 A와 B에 대하여,
(1) A가 B를 정규화(normalizes)할 때, 혹은
(2) A의 모든 비순환 조성 인자(composition factor)의 위수가 주어진 정수 b보다 작거나 같을때, $A\cap B$를 찾는 Polynomial-Time 알고리즘이 존재한다.
증명 (1)은 [Fu], (2)는 [Lu1]참고■

위의 (2) 알고리즘은 $b\rightarrow\infty$일때 $f(b)\rightarrow\infty$인 $O(n^{f(b)})$이어서, 매우 큰 b에 대하여는 적합하지 않다. 이 외에도 군 G의 중심을 찾을 수 있는 Polynomial-Time 알고리즘과 군 G의 정규 부분군 A에 대하여 $C_G(A)$를 찾을 수 있는 Polynomial-Time 알고리즘이 있다.

정리 3. 7 군 G의 composition series(조성열)와 principal series를 찾는 Polynomial-Time 알고리즘이 존재한다.
증명 composition series는 [Lu2], principal series는 [Ro]참고■

위의 정리 결과로 군 G가 단순(simple) 한지의 여부를 Polynomial-Time으로 검사할 수 있으며, composition series의 인접한 A와 B(A<B)에 대하여 B/A가 충실하게(faithfully) 작용하는 집합을 Polynomial-Time으로 찾을 수 있다.([Lu1]참고) 이제 Sylow p-부분군에 대한 알고리즘을 알아보자.

정리 3. 8 군 G의 주어진 (소수) p-부분군에 대하여, 이 부분군을 포함하는 G의 Sylow p-부분군을 찾는 Polynomial-Time 알고리즘이 존재한다.
증명 [Ka1]참고■

위의 정리에 대한 따름정리로 다음을 얻을 수 있다.

따름정리 3. 9 가해군(solvable group) G의 정규 부분군 M과 M의 Sylow p-부분군 P에 대하여, $G=MD$인 $N_G(P)$의 부분군 D를 Polynomial-Time으로 찾을 수 있다.
증명 [Ta] 참고■

4. 그래프의 동형문제와의 관계

마지막으로 다음 정리를 통하여 군론의 알고리즘들과 그래프의 동형문제와의 관계를 알아보자.

정리 4. 1 다음 세 문제중의 어느 하나를 Polynomial-Time으로 찾을 수 있다면, 그래프의 동형문제도 Polynomial-Time으로 해결할 수 있다.

(1) S_n의 두 부분군 A와 B가 주어졌을 때, A∩B를 찾는 것.

(2) G의 p-부분군 P가 주어졌을 때, $N_G(P)$를 찾는 것.

(3) G의 대합(involution)들의 집합 Δ가 주어져을때, $C_G(\Delta)$를 찾는것.

증명 [Ho]참고■

[Ki]에는 (3)의 경우를 환(ring)에서 사용하여 $C_G(\Delta)$와 관련된 것들을 찾는 예들이 있다. 또한 3절에서 살펴본 바와 같이 G가 가해군(solvable group)이면, (1)과 (3)의 경우는 Polynomial-Time 알고리즘이 있으나, (2)의 경우는 G가 가해군(solvable group)이라도 Polynomial-Time 알고리즘이 있는지는 알려지고 있지 않다. 다만 (2)에서 P가 Sylow군이라면, 그때는 $N_G(P)$를 찾는 Polynomial-Time 알고리즘이 존재함이 알려져 있다.([Ka2] 참고)

참 고 문 헌

[김] 김응태, 박승안, 현대대수학－제 3 판, 경문사, 1991.

[한] 한국전자통신연구소, 현대 암호학, 한국전자통신연구소, 1991.

[At] M. D. Atkinson, *An algorithm for finding the blocks of a permutation group*, Math. Comput. 29 (1975), 911-913.

[Ba] L. Babai, *On the length of subgroup chains in the symmetric group*, Comm. Algebra 14(1986), 1729-1736.

[Ho] C. M. Hoffman, *Group-theoretic algorithms and graph isomorphism*, *LNCS 136*, Springer, Berlin, 1982.

[Fr] J. B. Fraleigh, *A first course in abstract algebra*, Addison Wesley, Reading, Massachusetts, 1989.

[Fu] M. Furst, J. Hopcroft, and E. Lukes, *Polynomial-time algorithms for permutation groups*, Proc. 21st IEEE Symposium Foundations of Computer Science(1980), 36-41.

[Kal] W. M. Kantor, *Sylow's theorem in polynomial-time*, J. Comp. Syst. 30(1985), 359-394.

[Ka2] W. M. Kantor, *Finding Sylow normalizers in polynomial-time*, J. Algorithms, To appear.

[Ki] C. Kim, *A classification of the finite rings with unity by computable means*, Ph. D. Thesis, NCSU, 1989.

[Lu1] E. Lukes, *Isomorphism of graphs of bounded valence can be tested in polynomial-time*, J. Comp. Syst. Sci. 25(1982), 42-65.

[Lu2] E. Lukes, *Computing the composition of a permutation group in polynomial time*, Combinatorica 7(1987), 87-99.

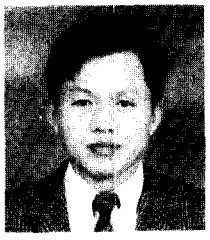
[Ro] L. Ronyai, *Zero divisors and invariant subspaces*, To appear.

[Si1] C. C. Sims, *computational methods in the study of permutation groups*, *Computational methods in Abstruct Algebra*, *J. Leech(ed.)*, Pergamon, Elmsford, N. Y., 1978, pp. 169-183.

[Si2] C. C. Simes, *Group-theoretical algorithms*, *Lecture Notes in Math.*, *697*, Springer, Berlin, 1978, pp. 108-124.

[Ta] W. M. Kantor and D. E. Taylor, *Polynomial-time versions of Sylow's theorem*, J. Algoithms 9(1988), 1-17.

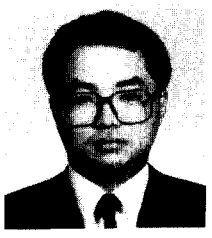
□ 著者紹介



황 규 범

1976년 육군 사관학교 졸업
1980년 서울대학교 수학과 졸업
1983년 고려대학교 수학과(이학석사)
1989년 고려대학교 수학과(이학박사)
1990년 미국 Michigan State Univ.(Post Dr.)
현재 육군사관학교 수학과 부교수
관심분야 : 암호학의 수학적 이론, DB의 보안

□ 著者紹介



김 철

본지 30P 참조