Конференція молодих учених «Підстригачівські читання – 2017», 23–25 травня 2017 р., Львів

УДК 512.543

МІНІМАЛЬНІ СИСТЕМИ ТВІРНИХ І СТРУКТУРА СИЛОВСЬКИХ 2-ПІДГРУПП ЗНАКОЗМІННИХ ГРУП A_{2^k}, A_n І СИМЕТРИЧНОЇ ГРУПИ І ЇХ ЗАСТОСУВАННЯ В КРИПТОГРАФІЇ

Руслан Скуратовський, Павло Радчук

Міжрегіональна Академія управління персоналом, pradchuk@ukr.net

Мета нашого дослідження – вивчити структуру силовських 2-підгруп і побудувати мінімальну систему твірних для таких підгруп. Підмножина $X^n \subset X^*$ називається n-тим рівнем дерева X^*, при цьому $X^0 = \{v_0\}$. Підмножину X^*, утворену множиною вершин $\cup_{i=0}^{k} X^i$, позначено так: $X^{[k]}$. Позначимо кожну вершину з X^l, $0 \le l < k$, символом 0, чи 1, залежно від стану вершинної перестановки в ній. Отримане так вершинно-розмічене регулярне дерево є елементом з $AutX^{[k]}$. Перестановка, що діє на ребрах у вершині з $X^{[k]}$і зберігає відношення інцидентності графа, називається вершинною перестановкою (в.п.). Індексом l-го рівня автоморфізму α з $AutX^{[k]}$ назвемо кількість нетривіальних в.п., що є на X^l. Нехай τ автоморфізм, що має нетривіальні в.п. лише у вершинах $v_{k-1,i}$ і $v_{k-1,j}$, де $i \le 2^{k-2}$, $j > 2^{k-2}$ α_l – такий, що має одну нетривіальну в.п., яка розташована у $v_{l,1}$.

Твердження. *Порядки груп* $G_k = \langle \alpha_0, \alpha_1, \alpha_2, ..., \alpha_{k-2}, \tau \rangle$, $Syl_2 A_{2^k}$ *рівні* 2^{2^k-2}.

Теорема. *Максимальна 2-підгрупа групи* $AutX^{[k]}$, *що діє парними перестановками на* X^k *має структуру напівпрямого добутку* $G_k \square B_{k-1} \leftthreetimes W_{k-1}$ *і ізоморфна* $Syl_2 A_{2^k}$, *де* $B_{k-1} = \wr_{i=1}^{k-1} C_2$, $W_{k-1} = (C_2)^{2^{k-1}-1}$, *а порядок підгрупи* W_{k-1} *рівний* $2^{2^{k-1}-1}$, $k > 1$.

Теорема. *Група* A_{2^k} *має мінімальну систему твірних з* k *елементів.*

Приклад мінімальної системи твірних для $Syl_2 A_{2^3}$. Розглянемо підгрупу $G_3 = \langle \alpha_0, \alpha_1, \tau_{14} \rangle$ автоморфізмів вершинно-поміченого дерева $X^{[3]}$, де портрети породжуючих автоморфізмів зображено на рис. 1.; C_2 розглядається як група S_2.

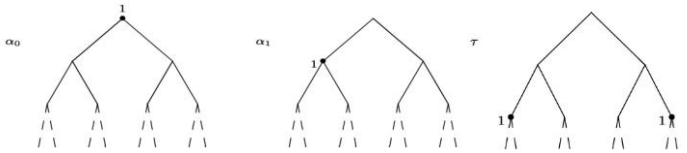

Рис.1 Портрети породжуючих автоморфізмів

Нехай $n = 2^{k_0} + 2^{k_1} + ... + 2^{k_m}$, де $0 \le k_0 < k_1 < ... < k_m$. Діагональною системою твірних $S_d = \langle \alpha_0, \alpha_1, ..., \alpha_{k-1} \rangle$ для $AutX^{[k]}$ назвемо таку, яка має нетривіальні індекси лише на i-му рівні. Такий рівень назвемо активним: на ньому є непарна кількість активних в.п. Кількість нетривіальних в.п. в α_l на рівні X^l є непарною, і рівна 2^{l-1}.

Твердження. *Загальна кількість систем твірних S_d для $Syl_2S_{2^k}$ рівна* $2^{1+2+4+...+2^{k-1}-k} = 2^{2^k-k-1}$.

Дійсно кількість базисів для фактор групи $G_k / G_k^2 \cong (C_2)^k$ рівна порядку $GL(k, \mathbb{F}_2)$, тобто $(2^k-1)(2^k-2)...(2^k-2^{k-1})$. Оскільки у кожної системи твірних групи $(C_2)^k$ є $2^{k(2^k-k-1)} = (|G_k|/2^k)^k$ прообразів, де $|G_k|/2^k$ – кількість прообразів одного елемента з $(C_2)^k$, то всього систем твірних є $(2^k-1)(2^k-2)(2^k-2^2)...(2^k-2^{k-1})2^{k(2^k-k-1)}$.

Таким чином ріст кількості систем S_d виражається експоненційною функцією від k. Це дозволяє побудувати криптосистему, що має множину алфавітів Y, що співпадає з одною з усіх 2^{2^k-k-1} різних систем твірних, секретним ключем в якій, є обраний алфавіт. Нехай $n_m = 2^{k_0} + 2^{k_1} + ... + 2^{k_m}$, де $k_0 < k_1 < ... < k_m$. Відомо, що $Syl_2S_n \cong Syl_2S_{2^{k_0}} \times Syl_2S_{2^{k_2}} \times Syl_2S_{2^{k_2}} \times ... \times Syl_2S_{2^{k_m}}$.

Теорема. *Централізатор 2-підгрупи $Syl_2S_{2^{k_i}}$, $i \le m$ в силовській 2-підгрупі Syl_2S_n ізоморфний підгрупі $C_{AutS_n}(Syl_2S_{2^{k_i}}) \cong Syl_2S_n / Syl_2S_{2^{k_i}}$.*

Теорема. *Якщо $m > 0$, то довільна мінімальна система твірних для Syl_2A_n має $\sum_{i=0}^{m} k_i - 1$ твірних.*

Теорема. Якщо $n_m = 4k+2$, то мінімальна система твірних для $Syl_2A_{n_m}$ має $\sum_{i=1}^{m} k_i$ елементів.

1. *Skuratovskii R. V., Drozd Y. A.* Generators and and relations for wreath products // Ukr Math J. – 2008. – Vol. 60, Issue 7. – pp. 1168–1171.
2. *Skuratovskii R. V.* Structure and minimal generating sets of sylow 2-subgroups of alternating groups, source: https://arxiv.org/pdf/1702.05784.pdf
3. *Skuratovskii R. V.* Corepresentation of a Sylow p-subgroup of a group S_n" // Cybernetics and systems analysis. – 2009. – N. 1. – pp. 27-41.

MINIMAL GENERATING SETS AND STRUCTURE OF SYLOW 2-SUBGROUPS OF ALTERNATING AND SYMMETRIC GROUPS

In this article the research of Sylows p-subgroups of A_n and S_n, which was started by Dmitruk and V. I. Suschanskii is continued. Let $Syl_2A_{2^k}$ and Syl_2A_n be Sylow 2-subgroups of corresponding alternating groups A_{2^k} and A_n. The purpose of this paper is to research the structure of a Sylow 2-subgroups and to construct a minimal generating set for such subgroups.