一类传递置换群阶的下界估计与实例

周琮伟,胡 斌,关 杰
(战略支援部队信息工程大学, 河南郑州 450001)

摘 要: 基于非交换群的抗量子密码体制是密码学的一个研究热点,其群的阶在一定程度上保证了求逆运算的困难性.本文对二元生成的传递置换群$< g_1, g_2 >$的阶这一代数命题进行了研究,给出了传递置换群的充分必要条件,以及二元生成的传递置换群阶的下界估计式.在实例化生成g_1, g_2使传递置换群$< g_1, g_2 >$的阶满足相应下界值的过程中,给出了一类特殊n阶轮换表成两个n元置换g_1, g_2乘积的方法,以及相应的二元生成的传递置换群$< g_1, g_2 >$的设计算法.最后,阐述了传递置换群在对称密码体制中的应用.

关键词: 抗量子密码体制; 有限群; 传递置换群; 群阶; 元的阶; 下界
中图分类号: O152.1 **文献标识码:** A **文章编号:** 0372-2112(2021)12-2366-06
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.12263/DZXB.20201412

The Lower Bound Estimation of Order of a Class of Transitive Permutation Groups and Instantiation

ZHOU Cong-wei, HU Bin, GUAN Jie
(*PLA SSF Information Engineering University*, *Zhengzhou*, *Henan* 450001, *China*)

Abstract: Post quantum cryptography based on non-commutative group is a hot topic in cryptography. The order of the group ensures the difficulty of inverse operation to some extent. We mainly study the algebraic proposition of order of transitive permutation groups $< g_1, g_2 >$ generated by two elements g_1, g_2, give a necessary and sufficient conditions of transitive permutation group, and get a lower bound estimation of order of transitive permutation groups generated by two elements. In the process of the instantiation for generating g_1, g_2 which enables the order of transitive permutation groups $< g_1, g_2 >$ to satisfy the corresponding lower bound value, we give a method expressing a class of special n-order cycles as the product of two n-ary permutations and a corresponding design algorithm on transitive permutation groups $< g_1, g_2 >$ generated by two elements. In the end, this paper describes the application of transitive permutation group in symmetric cryptography.

Key words: post quantum cryptography; finite group; transitive permutation group; order of group; element order; lower bound

1 引言

1994年,Shor提出了著名的大数因子分解的量子算法Shor算法,该算法借助量子计算机可以对基于有限交换群上的离散对数问题进行求解,因此设计基于非交换群上的密码体制具有现实意义.由于凯莱定理阐述了任一有限群与置换群同构,同时大多数置换群具有非交换性,对置换群的相关性质,特别是其生成元的分析就显得尤其重要.另外,在代数研究的角度上,有限群的生成元个数如何刻画群的性质一直以来也是群论的研究对象之一[1],针对置换群,例如传递置换群[2]与本原置换群[3],其最少生成元的个数上界均有渐进估计[4].设G是$\Omega = \{1, \cdots, n\}$上的一个置换群,记$n$次对称群为$S^{\Omega}$或$\mathrm{Sym}(n)$.令$d(G)$表示$G$的生成元集合的最小阶,则易知$d(\mathrm{Sym}(n)) = 2$.但$\forall g_1, g_2 \in S^{\Omega}$,其二元生成的置换群$< g_1, g_2 >$的相关性质却缺乏研究思路.本文主要利用传递置换群的充分必要条件,对传递置换群$< g_1, g_2 >$阶的下界进行估计,同时给定下界值,可以对g_1, g_2进行实例化生成.

2 基本概念

传递置换群的概念主要延伸于群在集合上的作用,这也是凯莱定理描述任一有限群同构置换群的内

收稿日期:2020-12-09;修回日期:2021-03-30;责任编辑:覃怀银
基金项目:国家自然科学基金(No. 61802437, No. 61802438)

在联系,本文的定义主要来自有限置换群的经典文献[5],为方便研究,对个别符号重新阐述说明和归纳. 特别地,本文一般用α,β,δ,a这些字母表示Ω中的元素、点或者符号,令α^g表示点α在置换g中的象.

定义1　若$\Omega=\{1,\cdots,n\}$上的一个子集Δ,且本文用Δ^G表示全部δ^g组成的集合,其中$\delta\in\Delta,g\in G$,则当满足$\Delta=\Delta^G$,就说Δ是G的一个不动区. 显然,Ω上的每个群G都有平凡不动区$\varnothing,\Omega$,如果G没有其他不动区,则称G是传递的,或者称为传递置换群.

定义2　当Δ是G的一个不动区时,每个$g\in G$诱导出Δ上的一个置换g^Δ,由所有$g\in G$诱导出的g^Δ的全体组成的集合G^Δ称为G在Δ上的成分. 显然G^Δ是Δ上的一个置换群,当$|G^\Delta|=|G|$时,称成分G^Δ是真实的. 当$\Delta(\Delta\neq\varnothing)$是一个极小不动区时,成分$G^\Delta$是传递的,此时称$\Delta$为$G$的一个轨道或者传递集. G的全部传递集是Ω上的一个划分.

由定义2可知,每个点$\alpha\in\Omega$恰属于G的一个传递集$\Delta=\alpha^G$. 两个点α,β属于同一个传递集当且仅当对某个$g\in G$,满足$\alpha^g=\beta$. 因此本文可以得到置换群G是传递的一个充分条件,即置换群G至少包含一个n阶轮换.

3　传递置换群的充分必要条件

以下本文通过研究置换的轮换形式给出置换群G是传递的充分必要条件,在证明之前本文需要给出G的稳定子群的定义.

定义3　G中那些使Δ中每个点都保持各自不动的置换组成G的一个子群G_Δ,称为G关于Δ的稳定子群,特别地,若Δ只包含一个点α,则记$G_\Delta=G_\alpha$.

关于G的稳定子群和传递集,有一个基本定理(轨道公式),即定理1.

定理1[5]　$|G_\alpha|\cdot|\alpha^G|=|G|$.

若记置换$g(g\in G)$的轮换形式中,单点轮换(1-轮换)的个数为$\sigma(g)$,则置换群G是传递的充分必要条件是G的所有元素的单点轮换的总数等于G的阶$|G|$,即定理2.

定理2　G是传递的充分必要条件是$\sum\limits_{g\in G}\sigma(g)=|G|$.

证明　先证必要性. 当G是传递的,由定义2可知,每个点$\alpha\in\Omega$所属的传递集$\Delta=\alpha^G$的阶$|\alpha^G|=n$,则根据定理1,G中关于点α保持不动的置换个数为$|G|/n$,则当点α遍历Ω时,G中所有元素的单点轮换的总数即为

$$\sum_{\alpha\in\Omega}|G_\alpha|=|G| \tag{1}$$

即在一个传递群中,每个元素平均保持一个点不动. 下证充分性.

令$h_i=|G_{\alpha_i}|,i=1,\cdots,n$,则由轨道公式可知$h_i=|G|/|\alpha_i^G|$. 记$D=\{(g,\alpha_i)\,|\,g\in G,\ \alpha_i\in\Omega,\alpha_i^g=\alpha_i\}$. 当分别从$G$中所有元素和$\Omega$中符号的角度去计算$|D|$时,就可得出等式

$$\sum_{g\in G}\sigma(g)=\sum_{i=1}^{n}h_i=\sum_{i=1}^{n}\frac{|G|}{|\alpha_i^G|} \tag{2}$$

由$\sum\limits_{g\in G}\sigma(g)=|G|$,约去因子$|G|$,得$\sum\limits_{i=1}^{n}\frac{1}{|\alpha_i^G|}=1$. 由基本不等式

$$\sqrt[n]{\frac{1}{|\alpha_1^G|}\frac{1}{|\alpha_2^G|}\cdots\frac{1}{|\alpha_n^G|}}\leqslant\frac{\sum\limits_{i=1}^{n}\frac{1}{|\alpha_i^G|}}{n} \tag{3}$$

可得

$$\frac{n}{\sum\limits_{i=1}^{n}\frac{1}{|\alpha_i^G|}}\leqslant\sqrt[n]{|\alpha_1^G||\alpha_2^G|\cdots|\alpha_n^G|} \tag{4}$$

又由式(3)、式(4)得

$$\sqrt[n]{|\alpha_1^G||\alpha_2^G|\cdots|\alpha_n^G|}\leqslant\frac{\sum\limits_{i=1}^{n}|\alpha_i^G|}{n} \tag{5}$$

从而

$$n=\frac{n}{\sum\limits_{i=1}^{n}\frac{1}{|\alpha_i^G|}}\leqslant\frac{\sum\limits_{i=1}^{n}|\alpha_i^G|}{n} \tag{6}$$

不妨设$|\alpha_1^G|$是$|\alpha_1^G|,|\alpha_2^G|,\cdots,|\alpha_n^G|$中的最大者,则立即由式(6)可得

$$n\leqslant\frac{\sum\limits_{i=1}^{n}|\alpha_i^G|}{n}\leqslant\frac{n\cdot|\alpha_1^G|}{n}=|\alpha_1^G| \tag{7}$$

但$|\alpha_1^G|\leqslant n$,故$|\alpha_1^G|=n$,因此点α_1可以传递到$\Omega=\{1,\cdots,n\}$上的其余点,从而G是传递的. 证毕.

□

定理2说明在一个传递置换群G中,每个元素平均保持一个点不动,故本文可以利用这个性质来估计G的阶.

4　传递置换群$<g_1,g_2>$阶的下界估计

应用定理2,当置换群$<g_1,g_2>$是传递的时,本文就可以对置换群$<g_1,g_2>$的阶做一个估计,具体的思路是分析$<g_1,g_2>$中一定存在的互异的置换,然后统计这些置换中单点轮换的个数. 记g_1的轮换形式中,所有i-轮换的集合为K_i;g_2的轮换形式中,所有i-轮换的集合为L_i,则g_1,g_2可以形式化表示为$1^{|K_1|}2^{|K_2|}\cdots n^{|K_n|}$,$1^{|L_1|}2^{|L_2|}\cdots n^{|L_n|}$,由置换乘积的定义,可得定理3.

定理3　当置换群$<g_1,g_2>$是传递时,若g_1,g_2可

以形式化表示为 $1^{|K_1|}2^{|K_2|}\cdots n^{|K_n|}$, $1^{|L_1|}2^{|L_2|}\cdots n^{|L_n|}$. 而 g_1, g_2 是非幂等的且满足 $g_1g_2 \neq g_2g_1$,同时令

$$\mathrm{ord}(g_1) = \left[i_1, i_2, \cdots, i_k\right], \left|K_{i_j}\right| \geqslant 1, 1 \leqslant j \leqslant k \tag{8}$$

$$\mathrm{ord}(g_2) = \left[i_1, i_2, \cdots, i_l\right], \left|L_{i_j}\right| \geqslant 1, 1 \leqslant j \leqslant l \tag{9}$$

则

$$\left| < g_1, g_2 > \right| \geqslant \mathrm{ord}(g_1)\cdot\left(\left|K_1\right| + \sum_{j=1}^{k}\left|K_{i_j}\right|\right) + \mathrm{ord}(g_2)\cdot\left(\left|L_1\right| + \sum_{j=1}^{l}\left|L_{i_j}\right|\right) - n \tag{10}$$

证明 置换群 $< g_1, g_2 >$ 中,由于 g_1, g_2 是非幂等的,且满足 $g_1g_2 \neq g_2g_1$,故一定存在以下互不相同的元素 $\{I, g_1^1, g_1^2, \cdots, g_1^{\mathrm{ord}(g_1)-1}, g_2^1, g_2^2, \cdots, g_2^{\mathrm{ord}(g_2)-1}, g_1g_2, g_2g_1\}$.

以下我们依次分析这些置换中单点轮换的个数:

(1) 单位置换 I 的单点轮换个数为 n;

(2) $g_1^1, g_1^2, \cdots, g_1^{\mathrm{ord}(g_1)-1}, g_1^{\mathrm{ord}(g_1)} = I$ 中每个置换都包含 K_1 中的单点轮换,故个数为 $\mathrm{ord}(g_1)\cdot\left|K_1\right|$,同时

$$g_1^{i_j}, g_1^{2i_j}, \cdots, g_1^{\frac{\mathrm{ord}(g_1)}{i_j}\cdot i_j} = g_1^{\mathrm{ord}(g_1)} = I, 1 \leqslant j \leqslant k \tag{11}$$

式(11)中每个置换都包含 K_{i_j} 中出现的符号代表的单点轮换,故个数为

$$\sum_{j=1}^{k}\frac{\mathrm{ord}(g_1)}{i_j}\cdot\left|K_{i_j}\right|\cdot i_j = \sum_{j=1}^{k}\mathrm{ord}(g_1)\cdot\left|K_{i_j}\right|;$$

(3) $g_2^1, g_2^2, \cdots, g_2^{\mathrm{ord}(g_2)-1}, g_2^{\mathrm{ord}(g_2)} = I$ 中每个置换都包含 L_1 中的单点轮换,故个数为 $\mathrm{ord}(g_2)\cdot\left|L_1\right|$,同时

$$g_2^{i_j}, g_2^{2i_j}, \cdots, g_2^{\frac{\mathrm{ord}(g_2)}{i_j}\cdot i_j} = g_2^{\mathrm{ord}(g_2)} = I, 1 \leqslant j \leqslant l \tag{12}$$

式(12)中每个置换都包含 L_{i_j} 中出现的符号代表的单点轮换,故个数为

$$\sum_{j=1}^{l}\frac{\mathrm{ord}(g_2)}{i_j}\cdot\left|L_{i_j}\right|\cdot i_j = \sum_{j=1}^{l}\mathrm{ord}(g_2)\cdot\left|L_{i_j}\right|;$$

(4) g_1g_2, g_2g_1 一定包含 $K_1 \cap L_1, K_2 \cap L_2$ 中出现的符号代表的单点轮换,故个数为 $2(\left|K_1 \cap L_1\right| + 2\left|K_2 \cap L_2\right|)$.

但是考虑置换群 $< g_1, g_2 >$ 是传递时,若 $K_1 \cap L_1, K_2 \cap L_2 \neq \varnothing$,则 $< g_1, g_2 >$ 存在非平凡不动区,故 g_1g_2, g_2g_1 的单点轮换个数应为 0.

综上,扣除重复的两个单位置换 I,以上这些互不相同的置换中包含的单点轮换总个数为

$$\mathrm{ord}(g_1)\cdot\left(\left|K_1\right| + \sum_{j=1}^{k}\left|K_{i_j}\right|\right) + \mathrm{ord}(g_2)\cdot\left(\left|L_1\right| + \sum_{j=1}^{l}\left|L_{i_j}\right|\right) - n.$$

由定理 2 知置换群 $< g_1, g_2 >$ 的阶至少包含以上置换中单点轮换的个数,故定理即证. 证毕. □

在定理 3 中,若 $g_1g_2 = g_2g_1$,即 g_1, g_2 的轮换形式中所有 i-轮换都是不相交的,则立即推出置换群 $< g_1, g_2 >$ 的阶等于 $\mathrm{ord}(g_1)\cdot\mathrm{ord}(g_2) - 1$. 实际上,若设 n 次对称群 S^{Ω} 中元素的最大阶为 $S^{\Omega}(n)$,根据基本不等式,置换群 $< g_1, g_2 >$ 的阶将不超过 $(S^{\Omega}(\frac{n}{2}))^2 - 1$.

但以上这种情形时,置换群 $< g_1, g_2 >$ 就不是传递的,且其阶的值与定理 3 给出的下界值相比较小.

5 g_1, g_2 的实例化生成

由定义 2 可知,若 g_1g_2, g_2g_1 是一个 n 阶轮换,置换群 $< g_1, g_2 >$ 即是传递的. 因此当给定下界值,要找到两个生成元 g_1, g_2 使其生成的传递置换群 $< g_1, g_2 >$ 的阶大于该阈值的问题,就可以转化为将一个 n 阶轮换表成两个 n 元置换 g_1, g_2 的乘积,同时根据定理 3 相应调整 g_1, g_2 的阶. 以下本文给出一种两个同阶 n 元置换表成 n 阶轮换的特殊形式,首先本文给出引理 1.

引理 1 若 $\Omega = \{1, \cdots, n\}$ 上 n 元置换的轮换表示形式为 $g_1 = \tau_1\tau_2\cdots\tau_m = (a_1a_2\cdots a_{l_1})(a_{l_1+1}a_{l_1+2}\cdots a_{l_2})\cdots(a_{l_{m-1}+1}a_{l_{m-1}+2}\cdots a_{l_m}), l_m = n.$

此时,称 g_1 为 Ω 上的 m 型置换,则存在 Ω 上的 m 型置换 g_2 使 $g_2\cdot g_1$ 表成两个 Ω 上 n 阶轮换的乘积.

证明 由轮换的乘积等式 $(ka\cdots b)(lc\cdots d) = (kl)(ka\cdots blc\cdots d)$

其中,$a, \cdots, b, c, \cdots, d, k, l$ 为互不相同的 $\Omega = \{1, \cdots, n\}$ 上的元素,则可知

$$\begin{aligned}
g_1 &= (a_1a_2\cdots a_{l_1})(a_{l_1+1}a_{l_1+2}\cdots a_{l_2})\cdots(a_{l_{m-1}+1}a_{l_{m-1}+2}\cdots a_{l_m})\\
&= (a_1a_2\cdots a_{l_1})(a_{l_1+1}a_{l_1+2}\cdots a_{l_2})\cdots\\
&\quad [(a_{l_{m-2}+1}a_{l_{m-2}+2}\cdots a_{l_{m-1}})(a_{l_{m-1}+1}a_{l_{m-1}+2}\cdots a_{l_m})]\\
&= (a_1a_2\cdots a_{l_1})(a_{l_1+1}a_{l_1+2}\cdots a_{l_2})\cdots\\
&\quad (a_{l_{m-2}+1}a_{l_{m-1}+1})(a_{l_{m-2}+1}a_{l_{m-2}+2}\cdots a_{l_{m-1}}a_{l_{m-1}+1}a_{l_{m-1}+2}\cdots a_{l_m})\\
&= (a_1a_2\cdots a_{l_1})(a_{l_1+1}a_{l_1+2}\cdots a_{l_2})\cdots(a_{l_{m-2}+1}a_{l_{m-1}+1})\\
&\quad \cdot[(a_{l_{m-3}+1}a_{l_{m-3}+2}\cdots a_{l_{m-2}})\\
&\quad \cdot(a_{l_{m-2}+1}a_{l_{m-2}+2}\cdots a_{l_{m-1}}a_{l_{m-1}+1}a_{l_{m-1}+2}\cdots a_{l_m})]\\
&= (a_1a_2\cdots a_{l_1})(a_{l_1+1}a_{l_1+2}\cdots a_{l_2})\cdots(a_{l_{m-2}+1}a_{l_{m-1}+1})(a_{l_{m-3}+1}a_{l_{m-2}+1})\\
&\quad \cdot(a_{l_{m-3}+1}a_{l_{m-3}+2}\cdots a_{l_{m-2}}a_{l_{m-2}+1}a_{l_{m-2}+2}\cdots a_{l_{m-1}}a_{l_{m-1}+1}a_{l_{m-1}+2}\cdots a_{l_m})\\
&= \cdots = (a_{l_{m-2}+1}a_{l_{m-1}+1})(a_{l_{m-3}+1}a_{l_{m-2}+1})\cdots(a_{l_1+1}a_{l_2+1})(a_1a_{l_1+1})\\
&\quad \cdot(a_1a_2\cdots a_{l_1}a_{l_1+1}a_{l_1+2}\cdots a_{l_2}\cdots a_{l_{m-1}}a_{l_{m-1}+1}a_{l_{m-1}+2}\cdots a_{l_m})\\
&= (a_1a_{l_{m-1}+1}a_{l_{m-2}+1}\cdots a_{l_1+1})\\
&\quad \cdot(a_1a_2\cdots a_{l_1}a_{l_1+1}a_{l_1+2}\cdots a_{l_2}\cdots a_{l_{m-1}}a_{l_{m-1}+1}a_{l_{m-1}+2}\cdots a_{l_m})
\end{aligned}$$

此时,可令

$$g_2=(a_1a_2\cdots a_{l_1}a_{l_1+1}a_{l_1+2}\cdots a_{l_2}\cdots a_{l_{m-1}}a_{l_{m-1}+1}a_{l_{m-1}+2}\cdots a_{l_m})\cdot(a_1a_{l_{m-1}+1}a_{l_{m-2}+1}\cdots a_{l_1+1})$$

则由置换的乘积知

$$g_2=(a_1a_{l_{m-1}+2}\cdots a_{l_m})(a_{l_{m-1}+1}a_{l_{m-2}+2}\cdots a_{l_{m-1}})\cdots(a_{l_1+1}a_2\cdots a_{l_1})$$

从而

$$g_2\cdot g_1=(a_1a_2\cdots a_{l_1}a_{l_1+1}a_{l_1+2}\cdots a_{l_2}\cdots a_{l_{m-1}}a_{l_{m-1}+1}a_{l_{m-1}+2}\cdots a_{l_m})(a_1a_{l_{m-1}+1}a_{l_{m-2}+1}\cdots a_{l_1+1})(a_1a_2\cdots a_{l_1})\cdot(a_{l_1+1}a_{l_1+2}\cdots a_{l_2})\cdots(a_{l_{m-1}+1}a_{l_{m-1}+2}\cdots a_{l_m})$$

$$\Leftrightarrow g_2\cdot g_1=(a_1a_2\cdots a_{l_1}a_{l_1+1}a_{l_1+2}\cdots a_{l_2}\cdots a_{l_{m-1}}a_{l_{m-1}+1}a_{l_{m-1}+2}\cdots a_{l_m})\{(a_1a_{l_{m-1}+1}a_{l_{m-2}+1}\cdots a_{l_1+1})(a_1a_2\cdots a_{l_1})\cdot(a_{l_1+1}a_{l_1+2}\cdots a_{l_2})\cdots(a_{l_{m-1}+1}a_{l_{m-1}+2}\cdots a_{l_m})]$$

$$\Leftrightarrow g_2\cdot g_1=(a_1a_2\cdots a_{l_1}a_{l_1+1}a_{l_1+2}\cdots a_{l_2}\cdots a_{l_{m-1}}a_{l_{m-1}+1}a_{l_{m-1}+2}\cdots a_{l_m})(a_1a_2\cdots a_{l_1}a_{l_{m-1}+1}a_{l_{m-1}+2}\cdots a_{l_m}a_{l_{m-2}+1}a_{l_{m-2}+2}\cdots a_{l_{m-1}}\cdots a_{l_1+1}a_{l_1+2}\cdots a_{l_2})$$

此时,$g_2\cdot g_1$表成了两个n阶轮换的乘积,引理即证. 证毕.

□

上述引理1中,若考察$g_2\cdot g_1$表成两个Ω上n阶轮换的乘积

$$\begin{pmatrix}1 & \cdots & l_1-1 & l_1 & l_2+1 & \cdots & n-1 & n & l_1+1 & \cdots & l_2-1 & l_2\\ 3 & \cdots & l_1+1 & l_2+2 & l_2+3 & \cdots & 1 & l_1+2 & l_1+3 & \cdots & l_2+1 & 2\end{pmatrix}$$

其中,除了点l_1,n,l_2外,其余点x的对应关系都是$x+2 \bmod n$. 以下本文要将上述点的对应关系依次链接成一条传递链. 当n为奇数时,首先考虑这两条自然数传递链,即奇数链和偶数链,结合点l_1,n,l_2的对应关系,可表示为

$$\begin{cases}1\to 3\to 5\to\cdots\to n\to l_1+2\\ l_2\to 2\to 4\to\cdots\to n-1\to 1\\ l_1\to l_2+2\end{cases}$$

以下分情况讨论:

(1) 当l_1,l_2同为奇数时,考虑以下传递链

$$1\to\cdots\to l_1\to l_2+2\to\cdots\to n\to l_1+2\to\cdots\to l_2\downarrow\\ 1\leftarrow n-1\leftarrow\cdots\leftarrow 4\leftarrow 2$$

其中所有偶数存在的传递链可由第二行链表示,且第一行链也恰好遍历所有的奇数.

(2) 当l_1,l_2同为偶数时,考虑以下传递链

$$1\to 3\to 5\to\cdots\to n\downarrow\\ \cdots\leftarrow 2\leftarrow l_2\leftarrow\cdots\leftarrow l_1+2\downarrow\\ l_1\to l_2+2\to\cdots\to n-1\to 1$$

$$(a_1a_2\cdots a_{l_1}a_{l_1+1}a_{l_1+2}\cdots a_{l_2}\cdots a_{l_{m-1}}a_{l_{m-1}+1}a_{l_{m-1}+2}\cdots a_{l_m})(a_1a_2\cdots a_{l_1}a_{l_{m-1}+1}a_{l_{m-1}+2}\cdots a_{l_m}a_{l_{m-2}+1}a_{l_{m-2}+2}\cdots a_{l_{m-1}}\cdots a_{l_1+1}a_{l_1+2}\cdots a_{l_2})$$

仍是一个n阶轮换时,对应的$l_1,l_2,\cdots,l_{m-1},l_m=n$应该满足什么条件. 此时不妨假设引理1中的置换乘积中诸$a_i=i$,即

$$g_2\cdot g_1=(12\cdots n)(12\cdots l_1(l_{m-1}+1)(l_{m-1}+2)\cdots l_m(l_{m-2}+1)(l_{m-2}+2)\cdots l_{m-1}\cdots(l_1+1)(l_1+2)\cdots l_2).$$

当$m=2,3$时,有定理4和定理5存在.

定理4 当n为奇数时,置换$(12\cdots n)(12\cdots n)$一定是n阶轮换;当n为偶数时,该置换一定不是n阶轮换.

证明 当n为奇数时,定理中的置换满足下面的传递链

$$1\to 3\to\cdots\to n\to 2\to 4\cdots\to n-1$$

因此,该置换一定是n阶轮换;当n为偶数时,该置换容易证明是2型置换,故定理即证. 证毕.

□

定理5 当n为奇数,且l_1,l_2的奇偶性相同或者l_1为偶数,l_2为奇数时,置换$(12\cdots n)(12\cdots l_1(l_2+1)(l_2+2)\cdots n(l_1+1)(l_1+2)\cdots l_2)$一定是$n$阶轮换;当$n$为偶数时,该置换一定不是$n$阶轮换.

证明 由置换的乘积可知,$(12\cdots n)(12\cdots l_1(l_2+1)(l_2+2)\cdots n(l_1+1)(l_1+2)\cdots l_2)$的对应形式为

$$\begin{pmatrix}1 & \cdots & l_1-1 & l_1 & l_2+1 & \cdots & n-1 & n & l_1+1 & \cdots & l_2-1 & l_2\\ 3 & \cdots & l_1+1 & l_2+2 & l_2+3 & \cdots & 1 & l_1+2 & l_1+3 & \cdots & l_2+1 & 2\end{pmatrix}$$

其中,所有奇数存在的传递链可由第一行链表示,且第二行链也恰好遍历所有的偶数.

(3) 当l_1为偶数,l_2为奇数时,考虑以下传递链

$$(1\to\cdots\to l_2)\to 2\to\cdots\to l_1\to\\ (l_2+2\to\cdots\to n)\to l_1+2\to\cdots\to n-1\to 1$$

可以看出括号内的传递链包含所有的奇数,括号外的传递链包含所有的偶数.

(4) 当l_1为偶数,l_2为奇数时,存在以下一条短的传递链

$$1\to\cdots\to l_1\to l_2+2\to\cdots\to n-1\to 1$$

因此,无法将上述所有点的关系链接成一条传递链,即定理中的置换就不是n阶轮换.

当n为偶数时,考虑这两条自然数传递链

$$\begin{cases}1\to 3\to 5\to\cdots\to n-1\to 1\\ l_2\to 2\to 4\to\cdots\to n\to l_1+2\end{cases}$$

本文考虑l_1为奇数,l_2为偶数的情况,则存在以下一条短的传递链

$$1\to\cdots\to l_1\to l_2+2\to\cdots\to\\ n\to l_1+2\to\cdots\to n-1\to 1$$

该传递链并没有遍历2到l_2间的所有偶数,故此时定理中的置换就不是n阶轮换. 同理其余情形的l_1,l_2都无法使第二行链中的所有偶数链接到第一行的闭链中,故定理即证. 证毕.

□

实际上当m是任意数时,根据定理5的证明过程有以下定理6存在.

定理6 当n为奇数,且$l_1,l_2,\cdots,l_{m-1}$的奇偶性相同时,置换$(12\cdots n)(12\cdots l_1(l_{m-1}+1)(l_{m-1}+2)\cdots l_m(l_{m-2}+1)(l_{m-2}+2)\cdots l_{m-1}\cdots(l_1+1)(l_1+2)\cdots l_2)$一定是$n$阶轮换.

证明 当n为奇数,各点l_i的对应关系为$l_i\to l_{i-2}+2(i>2),l_1\to l_{m-1}+2,l_2\to 2$,则根据定理5的证明过程,当$l_1,l_2,\cdots,l_{m-1}$同为奇数时,考虑以下传递链

$$\begin{array}{c}1\to\cdots\to l_1\to l_{m-1}+2\to\cdots\to n\\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\downarrow\\ l_{i-1}\leftarrow\cdots\leftarrow l_{i-2}+2\leftarrow l_i\leftarrow\cdots\leftarrow l_{m-2}+2\\ \downarrow\\ \cdots\to l_2\to 2\to 4\to\cdots\to n-1\to 1\end{array}$$

其中,所有偶数存在的传递链可由第二行链表示,且第一行链也恰好遍历所有的奇数;当$l_1,l_2,\cdots,l_{m-1}$同为偶数时,考虑以下传递链

$$\begin{array}{c}1\to 3\to 5\to\cdots\to n\to l_{m-2}+2\\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\downarrow\\ \cdots\leftarrow l_{i-1}\leftarrow\cdots\leftarrow l_{i-2}+2\leftarrow l_i\leftarrow\cdots\\ \downarrow\\ l_2\to 2\to\cdots\to l_1\to l_{m-1}+2\to\cdots\to n-1\to 1\end{array}$$

其中,所有奇数存在的传递链可由第一行链表示,且第二行链也恰好遍历所有的偶数,故定理即证. 证毕.

□

可以看出,当n为奇数,且$l_1,l_2,\cdots,l_{m-1}$的奇偶性相同时,定理6中$g_2\cdot g_1$即是一个n阶轮换. 而当本文在实际需求中遇到n为偶数时,本文可以先考虑两个$n-1/(n+1)$元置换的乘积表成$n-1/(n+1)$阶轮换,然后乘以一个对换扩展到n阶轮换,以下举一个例子.

例 当$n=16$时,使置换群$<g_1,g_2>$的阶大于500.

由文献[6]可知,$S^{\Omega}(15)=105$,各轮换长分别为3,5,7,此时无法将l_1,l_2满足定理5的情形,又根据文献[6],本文考虑$S^{\Omega}(17)=2\times3\times5\times7$,此时无法将$l_1,l_2,l_3$满足定理6的情形. 故只能取$n=15$的次大阶60,各轮换长分别为4,5,6,即相应的步骤如下:

$$\begin{aligned}&g_1=(1\ \ 2\ \ 3\ \ 4)(5\ \ 6\ \ 7\ \ 8\ \ 9)(10\ \ 11\ \ 12\ \ 13\ \ 14\ \ 15),\\&g_2'=(1\ \ 11\ \ 12\ \ 13\ \ 14\ \ 15)(10\ \ 6\ \ 7\ \ 8\ \ 9)(5\ \ 2\ \ 3\ \ 4),\\&g_2'\cdot g_1=(1\ \ 3\ \ 5\ \ 7\ \ 9\ \ 2\ \ 4\ \ 11\ \ 13\ \ 15\ \ 6\ \ 8\ \ 10\ \ 12\ \ 14),\\&(1\ \ 16)\cdot g_2'\cdot g_1\\&=(1\ \ 16)(1\ \ 3\ \ 5\ \ 7\ \ 9\ \ 2\ \ 4\ \ 11\ \ 13\ \ 15\ \ 6\ \ 8\ \ 10\ \ 12\ \ 14)\\&=(1\ \ 3\ \ 5\ \ 7\ \ 9\ \ 2\ \ 4\ \ 11\ \ 13\ \ 15\ \ 6\ \ 8\ \ 10\ \ 12\ \ 14\ \ 16),\\&g_2=(1\ \ 16)\cdot g_2'\\&=(1\ \ 11\ \ 12\ \ 13\ \ 14\ \ 15\ \ 16)(10\ \ 6\ \ 7\ \ 8\ \ 9)(5\ \ 2\ \ 3\ \ 4).\end{aligned}$$

故本文给出了一组g_1,g_2的设计,其中$\mathrm{ord}(g_1)=60,\mathrm{ord}(g_2)=140$,根据定理3,置换群$<g_1,g_2>$的阶大于$60\times(1+3)+140\times3=660$.

从以上例子,结合二元生成的传递置换群$<g_1,g_2>$阶的下界估计式分析知,$S^{\Omega}(n)$的值直接影响其下界值以及设计g_1,g_2. 文献[6,7]均指出n次对称群中元素的最大阶$S^{\Omega}(n)$满足一个近似关系

$$\lim_{n\to\infty}(\log S^{\Omega}(n)/\sqrt{n\log n})=1$$

其中log是自然对数,据此文献[7]给出了$S^{\Omega}(n)$的一个上下界,即当$n\geqslant2$时,$S^{\Omega}(n)\leqslant e^{\sqrt{n\log n}\left(1+\frac{\log\log n}{2\log n}\right)}$;当$n>906$时,$S^{\Omega}(n)\geqslant e^{\sqrt{n\log n}}=K$.

当n较大时,本文其实无法利用计算机搜索得到$S^{\Omega}(n)$的精确值,也无法判断其对应的m型置换中$l_1,l_2,\cdots,l_{m-1}$的各部分值,但是本文可以根据$S^{\Omega}(n)$的下界值K反解出一个阈值情况下n的对应值,同时根据定理6给出一个二元生成的传递置换群$<g_1,g_2>$的设计见算法1.

以上设计算法还可以根据n的大小在第3步设置跳变值加快寻找满足$X\cdot(k_0,2k_1,\cdots,2k_{m-1})\geqslant K$的一组$m,k_0,k_1,\cdots,k_{m-1}$,其中,$X\cdot(k_0,2k_1,\cdots,2k_{m-1})$是定理3给出的真正下界值.

算法 1　一个二元生成的传递置换群$< g_1, g_2 >$的设计算法

输入:一个阶的下界值K(足够大);

输出:二元生成的传递置换群$< g_1, g_2 >$的g_1, g_2,即

$$g_1 = (a_1 a_2 \cdots a_{l_1})(a_{l_1+1} a_{l_1+2} \cdots a_{l_2}) \cdots (a_{l_{m-1}+1} a_{l_{m-1}+2} \cdots a_{l_m}),$$

$$g_2 = (a_1 a_{l_{m-1}+2} \cdots a_{l_m})(a_{l_{m-1}+1} a_{l_{m-2}+2} \cdots a_{l_{m-1}}) \cdots (a_{l_1+1} a_2 \cdots a_{l_1}).$$

步骤:

1. 找到$e^{\sqrt{n \log n}} \geqslant K$的最小奇整数$n$,若$n \leqslant 905$,则返回error;
2. 置$m, k_0, k_1, \cdots, k_{m-1}$为0,令$m++$且满足$k_0 + 2(k_1 + \cdots + k_{m-1}) = n$;
3. 判断$2 \cdot (k_0, 2k_1, \cdots, 2k_{m-1}) \geqslant K$,若否则返回2;
4. 置$l_1 = k_0, l_i = l_{i-1} + 2k_{i-1} (m - 1 \geqslant i \geqslant 2), l_m = n$,令$a_1, \cdots, a_{l_m}$为$1, \cdots, n$的任意一组置换.

6　在密码体制的应用

在对称密码体制中,非线性模块的设计至关重要. 在多数非线性模块的设计中,例如采用S盒和非线性移位寄存器的部件都可以等价于一个置换. 因此基于多个非线性部件设计的密码模块的安全周期就可以用多个置换生成的置换群的阶衡量. 特别地,对于某些情况下,还要考虑该置换群即非线性模块的传递性. 本文的密码体制应用便基于此进行展开.

7　结论

本文给出了二元生成的传递置换群$< g_1, g_2 >$阶的下界估计,但实际上本文给出的下界值过于宽泛,同时如何更快更好地设计g_1, g_2,且使其不但满足阶最大,又能使其乘积是n阶轮换,这些问题依然亟待解决且也是本文下一步的研究方向.

参考文献

[1] AL MENEGAZZO F. The number of generators of a finite group[J]. Archiv Der Mathematik, 1989, 53(6): 521 – 523.

[2] BRYANT R M, KOVÁCS L G, ROBINSON G R. Transitive permutation groups and irreducible linear groups[J]. Quarterly Journal of Mathematics, 1995, 46(184): 9 – 22.

[3] LUCCHINI A, MENEGAZZO F, MORIGI M. Asymptotic results for primitive permutation groups and irreducible linear groups[J]. Journal of Algebra, 2000, 223(1): 154 – 170.

[4] LUCCHINI A, MENEGAZZO F, MORIGI M. Asymptotic results for transitive permutation groups[J]. Bulletin of the London Mathematical Society, 2000, (2): 191 – 195.

[5] WIELANDT H . 有限置换群[M]. 王萼芳, 译. 北京: 科学出版社, 1984. 1 – 6.

[6] MILLER W. The maximum order of an element of a finite symmetric group[J]. The American Mathematical Monthly, 1987, 94(6): 497 – 506.

[7] MASSIAS J P, ROBIN N G. Effective bounds for the maximal order of an element in the symmetric group[J]. Mathematics of Computation, 1989, 53(188): 665 – 678.

作者简介

周琮伟　男,1994年3月出生于四川眉山. 现为战略支援部队信息工程大学博士研究生. 主要研究方向为移位寄存器中的数学理论. E-mail: zhoucongwei@qq.com

胡　斌　男,1972年11月出生于河南信阳. 现为战略支援部队信息工程大学教授、博士生导师. 主要研究方向为密码设计与分析. E-mail: hb2110@126.com

关　杰　女,1974年9月出生于河南郑州. 现为战略支援部队信息工程大学教授、博士生导师. 主要研究方向为密码设计与分析. E-mail: guanjie007@163.com