第 34 卷 第 3 期 应 用 数 学 学 报 Vol. 34 No. 3
2011 年 5 月 ACTA MATHEMATICAE APPLICATAE SINICA May, 2011

带共轭性质拟群的计数 *

沈幸炜 徐允庆

(宁波大学理学院, 宁波 315211)

(E-mail: xuyunqing@nbu.edu.cn)

摘 要 由一个拟群 $(Q,\otimes)$ 可以定义出 6 个共轭拟群, 这 6 个共轭拟群不一定互不相同, 其构成的集合 $C(Q,\otimes)$ 的基数 t 可能的取值是 1, 2, 3 或 6. 记 $q(n,t)$ 是所有满足 $|C(Q,\otimes)|=t$ 的 n 阶拟群的个数, 本文将给出 $q(n,2)$ 和 $q(n,6)$ 的计数问题.

关键词 拟群; 共轭; 置换

MR(2000) 主题分类 05B15

中图分类 O157.2

1 引言

一个广群 $(Q,\otimes)$ 如果满足对任意的 $a,b\in Q$, 方程 $a\otimes x=b$ 和 $y\otimes a=b$ 在 Q 上有唯一解, 则称 $(Q,\otimes)$ 是一个拟群, 集合 Q 的基数 $|Q|$ 称为拟群 $(Q,\otimes)$ 的阶数.

拟群 $(Q,\otimes)$ 可应用于序列密码的设计, 由拟群设计序列密码系统具有以下性质[1,2]:

1) 密文串的每一位仅与前一位有关, 即, 密文串是一个马尔可夫链;

2) 每一个密文字符在密文中出现的概率相等, 在一个 k 重的加密系统下, 每个长度不超过 k 的密文字符串在密文中出现的概率相等;

3) 在一个 k 重的加密系统下, 密文中的一个字符错误最多引起解密明文中不超过 k 个相邻的字符错误, 即不会引起错误的扩散;

4) 拟群的数量巨大, 已知不同的 10 阶拟群共有 $9982437658213039871725064756920320000$ 个. 随着拟群阶数的增大, 其数量则急剧增长, 不同的 n 阶拟群的个数至少是 $(n!)^{2n}n^{-n^2}$. 正是拟群如此巨大的数量, 在实践上为密码系统提供了几乎是无限的密钥空间.

近年来, 出现了很多基于拟群的加密算法, 消息认证算法和纠错码算法. 拟群加密算法有速度快的优点[3], Hassinen 和 Markovski[4] 设计了基于拟群的用于手机短信加密的密码系统. All-Or-Nothing 是 Rivest[5] 设计用于在分组密码中抵抗强力攻击 (brute-force

本文 2009 年 7 月 17 日收到. 2011 年 3 月 15 日收到修改稿.

* 国家自然科学基金 (60873267) 和浙江省自然科学基金 (Y607026) 资助项目.

attack) 的加密模式， Marnas[6] 等利用拟群设计了 All-Or-Nothing 模式的序列密码. Gligoroski[7] 结合拟群和 ElGamal 公钥密码算法设计了有公开密钥的序列密码系统. 进入欧洲序列密码计划第三轮选拔的候选算法 –Edon80 就是基于 4 阶拟群算法和拟群字符串变换的序列密码算法 [8,9].

对于一个拟群 $(Q,\otimes)$, 我们定义 Q 上的 6 个二元运算 $\otimes_{(1,2,3)}$, $\otimes_{(1,3,2)}$, $\otimes_{(2,1,3)}$, $\otimes_{(2,3,1)}$, $\otimes_{(3,1,2)}$, $\otimes_{(3,2,1)}$ 如下： $a\otimes b=c$ 当且仅当

$$a\otimes_{(1,2,3)} b=c,\quad a\otimes_{(1,3,2)} c=b,\quad b\otimes_{(2,1,3)} a=c,$$
$$b\otimes_{(2,3,1)} c=a,\quad c\otimes_{(3,1,2)} a=b,\quad c\otimes_{(3,2,1)} b=a.$$

显然集合 Q 关于这 6 个二元运算构成 6 个拟群 $(Q,\otimes_{(i,j,k)})$, $\{i,j,k\}=\{1,2,3\}$, 称为拟群 $(Q,\otimes)$ 的 *共轭*.

一个 n 阶拟群 $(Q,\otimes)$ 的 6 个共轭不一定互不相同. 记 $C(Q,\otimes)$ 为 $(Q,\otimes)$ 的所有共轭的集合, 设 $|\,C(Q,\otimes)\,|=t$, 则 t 的取值只能是 1, 2, 3 或 6[10]. t 的取值决定着由 $(Q,\otimes)$ 得到的 3 对加密 - 解密算法是否不同. 记 $q(n,t)$ 为 $|\,C(Q,\otimes)\,|=t$ 的所有 n 阶拟群 $(Q,\otimes)$ 的个数, 对 $q(n,t)$ 进行计算或估计, 进而得到 $|\,C(Q,\otimes)\,|=t$ 的 n 阶拟群在所有 n 阶拟群中所占的比例, 对拟群应用于信息加密有着基本的重要性.

记 $q(n)$ 为全体 n 阶拟群的数目, 计算 $q(n)$ 是一个比较困难的问题. 目前, 只有当 n 不超过 11 时， $q(n)$, $q(n,1)$, $q(n,3)$ 有准确的计数 [2,11], 如表 1.1 所示.

表 1.1

n	$q(n)$	$q(n,1)$	$q(n,3)$
1	1	1	0
2	2	2	0
3	12	3	9
4	576	16	240
5	161280	30	2070
6	812851200	480	1087200
7	61479419904000	1290	94344930
8	108776032459082956800	163200	1288586390400
9	497227634654120355827810304000	471240	1334200952647080
10	998243765821303987172506475692032000 0	386400000	1430106249252230726400
11	776966836171770144107444346734230682311065600000	2269270080	377407387362311667791337 60

本文将对 $n\le 11$, 给出 $q(n,2)$ 的计数, 并由此推出 $q(n,6)$, 以完成 11 阶以下, 有不同共轭性质的拟群计数问题.

2 主要定理

Lindner 和 Steedley 在 [10] 中给出了拟群的共轭数 t 与拟群的运算性质之间的关系：

引理 2.1 (见 [10, Corollary 5]) 设 $(Q,\otimes)$ 为任一拟群, 变量 $x,y,x\in Q$, 记 5 个恒等式构成的集合 $I=\{x(xy)=y,\ xy=yx,\ x(yx)=y,\ (xy)x=y,\ (yx)x=y\}$, 则

(1) $|C(Q,\otimes)|=1$ 当且仅当 $(Q,\otimes)$ 满足 I 中的所有恒等式;

(2) $|C(Q,\otimes)|=2$ 当且仅当 $(Q,\otimes)$ 恰好满足恒等式 $x(yx)=y$ 和 $(xy)x=y$;

(3) $|C(Q,\otimes)|=3$ 当且仅当 $(Q,\otimes)$ 恰好满足 3 个恒等式 $xy=yx$, $x(xy)=y$ 和 $(yx)x=y$ 中的一个;

(4) $|C(Q,\otimes)|=6$ 当且仅当 $(Q,\otimes)$ 不满足 I 中的任何一个恒等式.

设 $(Q,\otimes)$ 是一个 n 阶拟群，以下我们总是假设 $Q=\{1,2,3,\cdots,n\}$. 设 $1\otimes i=x_i$ $(1\leq i\leq n)$, 由拟群的定义可知，当 $i\neq j$ 时， $x_i\neq x_j$ $(1\leq i,j\leq n)$, 即 $(x_1,x_2,\cdots,x_n)$ 是 $1,2,\cdots,n$ 的一个排列. 因此，我们可以引进以下概念.

定义 2.1 设 $(Q,\otimes)$ 是一个 n 阶拟群，记 $x_i=1\otimes i$ $(1\leq i\leq n)$, 则称置换

$$\alpha=\begin{pmatrix}1 & 2 & \cdots & n\\ x_1 & x_2 & \cdots & x_n\end{pmatrix}$$

为 $(Q,\otimes)$ 的 *首行置换*.

设 σ 是集合 $Q=\{1,2,\cdots,n\}$ 上的一个 n 阶置换， $1\leq l\leq n$. 如果

(1) $\sigma(x_1)=x_2,\sigma(x_2)=x_3,\cdots,\sigma(x_l)=x_1$,

(2) $\sigma(x)=x$, 当 $x\neq x_i$ $(i=1,2,\cdots,l)$,

则称 σ 是一个长度为 l 的 *轮换*, 并记为 $\sigma=(x_1,x_2,\cdots,x_l)$. 任一置换可以写成不相交轮换乘积的形式 [12,p.48−49]:

$$\sigma=(x_{11}^{(1)})\cdots(x_{r_11}^{(1)})(x_{11}^{(2)}x_{12}^{(2)})\cdots(x_{r_21}^{(2)}x_{r_22}^{(2)})\cdots(x_{11}^{(k)}x_{12}^{(k)}\cdots x_{1k}^{(k)})\cdots(x_{r_k1}^{(k)}x_{r_k2}^{(k)}\cdots x_{r_kk}^{(k)}),$$

其中 $k\leq n$, r_i $(1\leq i\leq k)$ 代表长度为 i 的轮换个数， $\sum\limits_{i=1}^{k}i\cdot r_i=n$. 我们将指数形式的符号 $1^{r_1}2^{r_2}\cdots k^{r_k}$ 称为置换 σ 的 *型*.

记 $\mathcal{Q}(n,2)$ 为满足 $|C(Q,\otimes)|=2$ 的所有 n 阶拟群 $(Q,\otimes)$ 组成的集合，则 $q(n,2)=|\mathcal{Q}(n,2)|$. 我们将集合 $\mathcal{Q}(n,2)$ 中的拟群按首行置换进行划分，记 $\mathcal{Q}(\alpha,2)$ 为 $\mathcal{Q}(n,2)$ 中所有以 α 为首行置换的拟群集合. 则我们可以得到以下定理.

引理 2.2 设 α 是一个 n 阶置换且 $\mathcal{Q}(\alpha,2)$ 非空. 将 α 写成不相交轮换乘积，则元素 1 所在轮换的长度必为 1 或 2.

证　$\forall(Q,\otimes)\in\mathcal{Q}(\alpha,2)$, 设 $1\otimes 1=x_1$, 若 $x_1=1$, 则显然 (1) 是 α 的一个轮换; 若 $x_1\neq 1$, 则由引理 2.1 (2) 可知 $1\otimes x_1=1$. 所以有 $\alpha(1)=x_1$, $\alpha(x_1)=1$. 因此 $(1\ x_1)$ 是 α 的一个轮换. 证毕.

定理 2.1 设 α,β 是两个 n 阶置换， α,β 有相同的型且元素 1 所在的轮换有相同的长度，则 $|\mathcal{Q}(\alpha,2)|=|\mathcal{Q}(\beta,2)|$.

证　将置换 α,β 写成不相交轮换的乘积，若 1 所在轮换的长度大于 2, 则由引理 2.2 可知 $\mathcal{Q}(\alpha,2)$ 和 $\mathcal{Q}(\beta,2)$ 都是空集，即 $|\mathcal{Q}(\alpha,2)|=|\mathcal{Q}(\beta,2)|=0$. 以下设 1 所在轮换的长

度不大于 2. 设 α, β 的型为 $1^{r_1}2^{r_2}\cdots k^{r_k}$, 且

$$\alpha=(a_{11}^{(1)})\cdots(a_{1r_1}^{(1)})(a_{11}^{(2)}a_{21}^{(2)})\cdots(a_{1r_2}^{(2)}a_{2r_2}^{(2)})\cdots(a_{11}^{(k)}a_{21}^{(k)}\cdots a_{k1}^{(k)})\cdots(a_{1r_k}^{(k)}a_{2r_k}^{(k)}\cdots a_{kr_k}^{(k)}), \tag{1}$$

$$\beta=(b_{11}^{(1)})\cdots(b_{1r_1}^{(1)})(b_{11}^{(2)}b_{21}^{(2)})\cdots(b_{1r_2}^{(2)}b_{2r_2}^{(2)})\cdots(b_{11}^{(k)}b_{21}^{(k)}\cdots b_{k1}^{(k)})\cdots(b_{1r_k}^{(k)}b_{2r_k}^{(k)}\cdots a_{kr_k}^{(k)}), \tag{2}$$

其中

$$\begin{cases} a_{1j}^{(i)}=\min\{a_{1j}^{(i)},a_{2j}^{(i)},\cdots,a_{ij}^{(i)}\}\ \text{且}\ a_{11}^{(i)}<a_{12}^{(i)}<\cdots<a_{1r_i}^{(i)},\ \ 1\le i\le k;\\ b_{1j}^{(i)}=\min\{b_{1j}^{(i)},b_{2j}^{(i)},\cdots,b_{ij}^{(i)}\}\ \text{且}\ b_{11}^{(i)}<b_{12}^{(i)}<\cdots<b_{1r_i}^{(i)},\ \ 1\le i\le k, \end{cases}$$

即, 每个轮换的第一个元素是轮换中各元素中最小的; 同一长度的轮换按第一个元素的大小排列. 做置换

$$\sigma=\begin{pmatrix} a_{11}^{(1)}&\cdots&a_{1r_1}^{(1)}&a_{11}^{(2)}&a_{12}^{(2)}&\cdots&a_{\lambda_21}^{(2)}&a_{\lambda_22}^{(2)}&\cdots&a_{11}^{(k)}&a_{12}^{(k)}&\cdots&a_{1k}^{(k)}&\cdots&a_{\lambda_k1}^{(k)}&a_{\lambda_k2}^{(k)}&\cdots&a_{\lambda_kk}^{(k)}\\ b_{11}^{(1)}&\cdots&b_{1r_1}^{(1)}&b_{11}^{(2)}&b_{12}^{(2)}&\cdots&b_{\lambda_21}^{(2)}&b_{\lambda_22}^{(2)}&\cdots&b_{11}^{(k)}&b_{12}^{(k)}&\cdots&b_{1k}^{(k)}&\cdots&b_{\lambda_k1}^{(k)}&b_{\lambda_k2}^{(k)}&\cdots&b_{\lambda_kk}^{(k)} \end{pmatrix}, \tag{3}$$

则由 α, β 中元素 1 所在的轮换有相同的长度可知 $\sigma(1)=1$.

$\forall\,(Q,\otimes)\in\mathcal{Q}(\alpha,2)$, 定义 Q 上一个新的二元运算 $\odot$ 如下:

$$a\odot b=\sigma\big(\sigma^{-1}(a)\otimes\sigma^{-1}(b)\big),\qquad \forall\,a,b\in Q.$$

不难验证集合 Q 关于运算 $\odot$ 构成拟群且置换 σ 是 $(Q,\otimes)$ 到 $(Q,\odot)$ 的同构映射. 下面证明 $(Q,\odot)\in\mathcal{Q}(\beta,2)$.

由引理 2.1 可知 $(Q,\otimes)$ 满足且只满足恒等式集合

$$I=\{x(xy)=y,\ xy=yx,\ x(yx)=y,\ (xy)x=y,\ (yx)x=y\}$$

中的 $x(yx)=y$ 和 $(xy)x=y$ 这两个恒等式. 由同构关系可知拟群 $(Q,\odot)$ 也满足这两个恒等式, 所以 $|C(Q,\odot)|=2$.

设 α 的表达式 (1) 中有轮换 $(x_1x_2\cdots x_l)$, 则

$$\begin{cases} 1\otimes x_i=x_{i+1}, & 1\le i\le l-1,\\ 1\otimes x_l=x_1. \end{cases}$$

设 $\sigma(x_i)=y_i\ \ (1\le i\le l)$, 即置换 β 的表达式中有轮换 $(y_1y_2\cdots y_l)$, 则

$$\begin{cases} 1\odot y_i=\sigma\big(\sigma^{-1}(1)\otimes\sigma^{-1}y_i\big)=\sigma\big(1\otimes x_i\big)=\sigma\big(x_{i+1}\big)=y_{i+1}, & 1\le i\le l-1,\\ 1\odot y_l=\sigma\big(\sigma^{-1}(1)\otimes\sigma^{-1}y_l\big)=\sigma\big(1\otimes x_l\big)=\sigma\big(x_1\big)=y_1. \end{cases}$$

所以 β 是拟群 $(Q,\odot)$ 的首行置换. 综上所述, $(Q,\odot)\in\mathcal{Q}(\beta,2)$.

由以上叙述可知 $\forall\,(Q,\otimes)\in\mathcal{Q}(\alpha,2)$, 存在唯一的 $(Q,\odot)\in\mathcal{Q}(\beta,2)$ 与之对应, 其中 α 与 β, $(Q,\odot)$ 与 $(Q,\otimes)$ 的关系如前所述. 因此, 我们作集合 $\mathcal{Q}(\alpha,2)$ 到集合 $\mathcal{Q}(\beta,2)$ 的映射 φ 如下:

$$\varphi\big((Q,\otimes)\big)=(Q,\odot),\qquad \forall\,(Q,\otimes)\in\mathcal{Q}(\alpha,2).$$

任给两个不同的拟群 $(Q,\otimes_1)$, $(Q,\otimes_2)\in\mathcal{Q}(\alpha,2)$, 定义

$$x\odot_1 y=\sigma\big(\sigma^{-1}(x)\otimes_1\sigma^{-1}(y)\big),\qquad \forall\, x,y\in Q,$$
$$x\odot_2 y=\sigma\big(\sigma^{-1}(x)\otimes_2\sigma^{-1}(y)\big),\qquad \forall\, x,y\in Q,$$

则 $\varphi\big((Q,\otimes_i)\big)=(Q,\odot_i)$ $(i=1,2)$. 因 $(Q,\otimes_1)$ 和 $(Q,\otimes_2)$ 是两个不同的拟群，所以存在 $a,b\in Q$, 使 $a\otimes_1 b\neq a\otimes_2 b$. 从而有

$$\sigma(a)\odot_1\sigma(b)=\sigma(a\otimes_1 b)\neq\sigma(a\otimes_2 b)=\sigma(a)\odot_2\sigma(b).$$

所以 $(Q,\odot_1)$ 和 $(Q,\odot_2)$ 是两个不同的拟群，即 φ 是单射.

$\forall\,(Q,\odot)\in\mathcal{Q}(\beta,2)$, 定义 Q 上的二元运算 $\otimes$ 如下：

$$a\otimes b=\sigma^{-1}\big(\sigma(a)\odot\sigma(b)\big),\qquad \forall\, a,b\in Q.$$

则容易验证 Q 关于运算 $\otimes$ 构成拟群，且有 $(Q,\otimes)\in\mathcal{Q}(\alpha,2)$ 和 $\varphi\big((Q,\otimes)\big)=(Q,\odot)$.

综上所述可知 φ 是集合 $\mathcal{Q}(\alpha,2)$ 到集合 $\mathcal{Q}(\beta,2)$ 的双射，因此 $|\mathcal{Q}(\alpha,2)|=|\mathcal{Q}(\beta,2)|$. 证毕.

记 $\mathcal{Q}^{(i)}(n,2)$ $(i=1,2,\cdots,n)$ 为 $\mathcal{Q}(n,2)$ 中满足 $1\otimes 1=i$ 的拟群 $(Q,\otimes)$ 组成的集合，则 $\{\mathcal{Q}^{(1)}\ (n,2),\ \mathcal{Q}^{(2)}(n,2),\ \cdots,\ \mathcal{Q}^{(n)}(n,2)\}$ 为集合 $\mathcal{Q}(n,2)$ 的一个划分. 我们可以得到以下定理.

定理 2.2　当 $i,j\in\{2,3,\cdots,n\}$ 时，$|\mathcal{Q}^{(i)}(n,2)|=|\mathcal{Q}^{(j)}(n,2)|$.

证　令 $\sigma=(i\ j)$, $\forall\,(Q,\otimes)\in\mathcal{Q}^{(i)}(n,2)$, 定义 Q 上新的二元运算 $\odot$ 如下：

$$a\odot b=\sigma\big(\sigma^{-1}(a)\otimes\sigma^{-1}(b)\big),\qquad \forall\, a,b\in Q.$$

利用与定理 2.1 证明的类似方法可得集合 Q 关于运算 $\odot$ 构成拟群且 $(Q,\odot)\in\mathcal{Q}(n,2)$. 又

$$1\odot 1=\sigma(\sigma^{-1}(1)\otimes\sigma^{-1}(1))=\sigma(1\otimes 1)=\sigma(i)=j,$$

所以有 $(Q,\odot)\in\mathcal{Q}^{(j)}(n,2)$.

作集合 $\mathcal{Q}^{(i)}(n,2)$ 到集合 $\mathcal{Q}^{(j)}(n,2)$ 的映射 ψ 如下：

$$\psi\big((Q,\otimes)\big)=(Q,\odot),\qquad \forall\,(Q,\otimes)\in\mathcal{Q}^{(i)}(n,2),$$

其中 $(Q,\odot)$ 与 $(Q,\otimes)$ 的关系如前所述. 利用与定理 2.1 证明的类似方法同样可证得 ψ 是 $\mathcal{Q}^{(i)}(n,2)$ 到 $\mathcal{Q}^{(j)}(n,2)$ 的双射. 因此 $|\mathcal{Q}^{(i)}(n,2)|=|\mathcal{Q}^{(j)}(n,2)|$. 证毕.

3　计数公式

记 $\mathcal{T}_i$ 为满足 $\alpha(1)=i$ 的 n 阶置换的型的全体构成的集合，即 $\mathcal{T}_i=\{T(\alpha)\mid \alpha$ 为 n 阶置换，且 $\alpha(1)=i\}$, 其中 $1\le i\le n$, $\forall\, T\in\mathcal{T}_i$, 记 $P_n^{(i)}(T)$ 为型为 T 的全体 n 阶首行置

换组成的集合. 则根据定理 2.1 可知

$$q(n,2)=\sum_{i=1}^{n}\sum_{T\in\mathcal{T}_i}|P_n^{(i)}(T)|\cdot|\mathcal{Q}(\alpha,2)|,$$

其中 $T(\alpha)\in P_n^{(i)}(T)$.

设 $i,j\in\{2,3,\cdots,n\}$, $\forall T\in\mathcal{T}_i$, $T'\in\mathcal{T}_j$, 若 T 与 T' 有相同的型, 则显然有 $|P_n^{(i)}(T)|=|P_n^{(j)}(T')|$. 所以由定理 2.2 可知, 当 $j\in\{3,\cdots,n\}$ 时, $\sum\limits_{T\in\mathcal{T}_2}|P_n^{(2)}(T)|\cdot|\mathcal{Q}(\alpha,2)|=\sum\limits_{T\in\mathcal{T}_j}|P_n^{(j)}(T)|\cdot|\mathcal{Q}(\alpha,2)|$. 因此我们有以下定理.

定理 3.1 设 $\alpha\in P_n^{(1)}(T)$, $\beta\in P_n^{(2)}(T)$, 则

$$q(n,2)=\sum_{T\in\mathcal{T}_1}|P_n^{(1)}(T)|\cdot|\mathcal{Q}(\alpha,2)|+(n-1)\sum_{T\in\mathcal{T}_2}|P_n^{(2)}(T)|\cdot|\mathcal{Q}(\beta,2)|.$$

引理 3.1 (见 [13, Example 13.3]) 设 $b_1+2b_2+\cdots+kb_k=n$. 型为 $1^{b_1}2^{b_2}\cdots k^{b_k}$ 的 n 阶置换的个数为

$$\frac{n!}{b_1!b_2!\cdots b_k!1^{b_1}2^{b_2}\cdots k^{b_k}}.$$

由此我们就可以得到下面的定理.

定理 3.2 设 $T=1^{r_1}2^{r_2}\cdots k^{r_k}$ 为 n 阶置换的型,

(1) 若 $T\in\mathcal{T}_1$, 则 $|P_n^{(1)}(T)|=\dfrac{r_1\cdot(n-1)!}{\prod\limits_{i=1}^{k}(i^{r_i}\cdot r_i!)}$;

(2) 若 $T\in\mathcal{T}_2$, 则 $|P_n^{(2)}(T)|=\dfrac{2r_2\cdot(n-2)!}{\prod\limits_{i=1}^{k}(i^{r_i}\cdot r_i!)}$.

证 若 $T\in\mathcal{T}_1$ 则由引理 2.2 可知以 T 为型的置换必有轮换 (1), 所以 $r_1\geq1$, 且集合 $P_n^{(1)}(T)$ 中的元素个数等于型为 $1^{r_1-1}2^{r_2}\cdots k^{r_k}$ 的 $n-1$ 阶置换的个数, 所以由引理 3.1 可知,

$$|P_n^{(1)}(T)|=\frac{(n-1)!}{(r_1-1)!r_2!\cdots r_k!1^{r_1-1}2^{r_2}\cdots k^{r_k}}=\frac{r_1\cdot(n-1)!}{\prod\limits_{i=1}^{k}(i^{r_i}\cdot r_i!)}.$$

若 $T\in\mathcal{T}_2$ 则由引理 2.2 可知以 T 为型的置换必有轮换 (1 2), 所以 $r_2\geq1$, 且集合 $P_n^{(2)}(T)$ 中的元素个数就等于型为 $1^{r_1}2^{r_2-1}\cdots k^{r_k}$ 的 $n-2$ 阶置换的个数, 所以由引理 3.1 可知

$$|P_n^{(2)}(T)|=\frac{(n-2)!}{(r_1)!(r_2-1)!\cdots r_k!1^{r_1}2^{r_2-1}\cdots k^{r_k}}=\frac{2r_2\cdot(n-2)!}{\prod\limits_{i=1}^{k}(i^{r_i}\cdot r_i!)}.$$

证毕.

对于任一个型 T, 利用定理 3.2 可以计算 $|P_n^{(1)}(T)|$ 和 $|P_n^{(2)}(T)|$. 当 $n\leq11$ 时, 对于一个型为 T 的首行置换 α 和 β, 利用计算机搜索可计算 $|\mathcal{Q}(\alpha,\in)|$ 和 $|\mathcal{Q}(\beta,\in)|$. 其结果如附录所示 (这里我们略去了 $n\leq3$ 的情况). 由此我们得到当 $n\leq11$ 时 $q(n,2)$ 的计数, 并

根据表 1.1 和公式 $q(n)=q(n,1)+q(n,2)+q(n,3)+q(n,6)$ 算得 $q(n,6)$. $q(n,2)$ 和 $q(n,6)$ 的数值如表 3-1 所示.

表 3.1

n	$q(n,2)$	$q(n,6)$
1	0	0
2	0	0
3	0	0
4	2	318
5	90	159090
6	2400	811761120
7	138966	61479325557760
8	20618880	10877603117047578432 0
9	9569061432	4972276346541190216172881242 48
10	13300960425216	9982437658213038441618802203342768384
11	74559785905598400	7769668361717701441074066059954198913561115977 60

4　附录

表 4.1 $|P_4^{(1)}(T)|$ 与 $|\mathcal{Q}(\alpha,\in)|$ 相关数据

T	$\lvert P_4(T)^{(1)}\rvert$	$\lvert\mathcal{Q}(\alpha,2)\rvert$	T	$\lvert P_4^{(1)}(T)\rvert$	$\lvert\mathcal{Q}(\alpha,2)\rvert$	T	$\lvert P_4^{(1)}(T)\rvert$	$\lvert\mathcal{Q}(\alpha,2)\rvert$
1^4	1	0	$1^2 2^1$	3	0	$1^1 3^1$	2	1

表 4.2 $|P_4^{(2)}(T)|$ 与 $|\mathcal{Q}(\beta,2)|$ 相关数据

T	$\lvert P_4^{(2)}(T)\rvert$	$\lvert\mathcal{Q}(\beta,2)\rvert$	T	$\lvert P_4^{(2)}(T)\rvert$	$\lvert\mathcal{Q}(\beta,2)\rvert$
$1^2 2^1$	1	0	2^2	1	0

表 4.3 $|P_5^{(1)}(T)|$ 与 $|\mathcal{Q}(\alpha,2)|$ 相关数据

T	$\lvert P_5^{(1)}(T)\rvert$	$\lvert\mathcal{Q}(\alpha,2)\rvert$	T	$\lvert P_5^{(1)}(T)\rvert$	$\lvert\mathcal{Q}(\alpha,2)\rvert$	T	$\lvert P_5^{(1)}(T)\rvert$	$\lvert\mathcal{Q}(\alpha,2)\rvert$
1^5	1	2	$1^3 2^1$	6	0	$1^1 2^2$	3	0
$1^2 3^1$	8	2	$1^1 4^1$	6	4			

表 4.4 $|P_5^{(2)}(T)|$ 与 $|\mathcal{Q}(\beta,2)|$ 相关数据

T	$\lvert P_5^{(2)}(T)\rvert$	$\lvert\mathcal{Q}(\beta,2)\rvert$	T	$\lvert P_5^{(2)}(T)\rvert$	$\lvert\mathcal{Q}(\beta,2)\rvert$	T	$\lvert P_5^{(2)}(T)\rvert$	$\lvert\mathcal{Q}(\beta,2)\rvert$
$1^3 2^1$	1	2	$1^1 2^2$	3	0	$2^1 3^1$	2	5

表 4.5 $|P_6^{(1)}(T)|$ 与 $|\mathcal{Q}(\alpha,2)|$ 相关数据

T	$\lvert P_6^{(1)}(T)\rvert$	$\lvert\mathcal{Q}(\alpha,2)\rvert$	T	$\lvert P_6^{(1)}(T)\rvert$	$\lvert\mathcal{Q}(\alpha,2)\rvert$	T	$\lvert P_6^{(1)}(T)\rvert$	$\lvert\mathcal{Q}(\alpha,2)\rvert$
1^6	1	0	1^42^1	10	2	1^22^2	15	0
1^33^1	20	6	1^24^1	30	10	1^15^1	24	20
$1^12^13^1$	20	8						

表 4.6 $|P_6^{(2)}(T)|$ 与 $|\mathcal{Q}(\beta,2)|$ 相关数据

T	$\lvert P_6^{(2)}(T)\rvert$	$\lvert\mathcal{Q}(\beta,2)\rvert$	T	$\lvert P_6^{(2)}(T)\rvert$	$\lvert\mathcal{Q}(\beta,2)\rvert$	T	$\lvert P_6^{(2)}(T)\rvert$	$\lvert\mathcal{Q}(\beta,2)\rvert$
1^42^1	1	8	1^22^2	6	2	2^3	3	0
$1^12^13^1$	8	11	2^14^1	6	26			

表 4.7 $|P_7^{(1)}(T)|$ 与 $|\mathcal{Q}(\alpha,2)|$ 相关数据

T	$\lvert P_7^{(1)}(T)\rvert$	$\lvert\mathcal{Q}(\alpha,2)\rvert$	T	$\lvert P_7^{(1)}(T)\rvert$	$\lvert\mathcal{Q}(\alpha,2)\rvert$	T	$\lvert P_7^{(1)}(T)\rvert$	$\lvert\mathcal{Q}(\alpha,2)\rvert$
1^7	1	0	1^52^1	15	24	1^32^2	45	32
1^12^3	15	2	1^43^1	40	12	1^13^2	40	96
1^34^1	90	40	1^25^1	144	72	1^16^1	120	106
$1^12^13^1$	120	60	$1^12^14^1$	90	98			

表 4.8 $|P_7^{(2)}(T)|$ 与 $|\mathcal{Q}(\beta,2)|$ 相关数据

T	$\lvert P_7^{(2)}(T)\rvert$	$\lvert\mathcal{Q}(\beta,2)\rvert$	T	$\lvert P_7^{(2)}(T)\rvert$	$\lvert\mathcal{Q}(\beta,2)\rvert$	T	$\lvert P_7^{(2)}(T)\rvert$	$\lvert\mathcal{Q}(\beta,2)\rvert$
1^52^1	1	0	1^32^2	10	72	1^12^3	15	74
$1^22^13^1$	20	72	2^23^1	20	156	$1^12^14^1$	30	126
2^15^1	24	202						

表 4.9 $|P_8^{(1)}(T)|$ 与 $|\mathcal{Q}(\alpha,2)|$ 相关数据

T	$\lvert P_8^{(1)}(T)\rvert$	$\lvert\mathcal{Q}(\alpha,2)\rvert$	T	$\lvert P_8^{(1)}(T)\rvert$	$\lvert\mathcal{Q}(\alpha,2)\rvert$	T	$\lvert P_8^{(1)}(T)\rvert$	$\lvert\mathcal{Q}(\alpha,2)\rvert$
1^8	1	450	1^62^1	21	450	1^42^2	105	438
1^22^3	105	758	1^53^1	70	384	1^23^2	280	1233
1^44^1	210	480	1^35^1	504	840	1^26^1	840	1513
1^17^1	720	2226	$1^32^13^1$	420	672	$1^12^23^1$	210	1296
$1^22^14^1$	630	1356	$1^12^15^1$	504	1760	$1^13^14^1$	420	2208

表 4.10 $|P_8^{(2)}(T)|$ 与 $|\mathcal{Q}(\beta,2)|$ 相关数据

T	$\lvert P_8^{(2)}(T)\rvert$	$\lvert\mathcal{Q}(\beta,2)\rvert$	T	$\lvert P_8^{(2)}(T)\rvert$	$\lvert\mathcal{Q}(\beta,2)\rvert$	T	$\lvert P_8^{(2)}(T)\rvert$	$\lvert\mathcal{Q}(\beta,2)\rvert$
1^62^1	1	450	1^42^2	15	1014	1^22^3	45	1502
2^4	15	1850	$1^32^13^1$	40	1176	2^13^2	40	3303
$1^22^14^1$	90	1696	$1^12^15^1$	144	2620	2^16^1	120	4279
2^23^1	120	2112	2^24^1	90	3780			

表 4.11 $|P_9^{(1)}(T)|$ 与 $|\mathcal{Q}(\alpha,2)|$ 相关数据

T	$\lvert P_9^{(1)}(T)\rvert$	$\lvert\mathcal{Q}(\alpha,2)\rvert$	T	$\lvert P_9^{(1)}(T)\rvert$	$\lvert\mathcal{Q}(\alpha,2)\rvert$	T	$\lvert P_9^{(1)}(T)\rvert$	$\lvert\mathcal{Q}(\alpha,2)\rvert$
1^9	1	0	1^72^1	28	3840	1^52^2	210	18432
1^32^3	420	45504	1^12^4	105	85144	1^63^1	112	11520
1^33^2	1120	44136	1^54^1	420	23040	1^14^2	1260	127064
1^45^1	1344	36576	1^36^1	3360	57192	1^27^1	5760	85148
1^18^1	5040	124736	$1^42^13^1$	1120	30144	$1^22^23^1$	1680	59424
$1^12^13^2$	1120	84996	$1^32^14^1$	2520	52064	$1^12^24^1$	1260	95264
$1^22^15^1$	4032	74816	$1^12^16^1$	3360	109288	$1^23^14^1$	3360	75456
$1^13^15^1$	2688	108966						

表 4.12 $|P_9^{(2)}(T)|$ 与 $|\mathcal{Q}(\beta,2)|$ 相关数据

T	$\lvert P_9^{(2)}(T)\rvert$	$\lvert\mathcal{Q}(\beta,2)\rvert$	T	$\lvert P_9^{(2)}(T)\rvert$	$\lvert\mathcal{Q}(\beta,2)\rvert$	T	$\lvert P_9^{(2)}(T)\rvert$	$\lvert\mathcal{Q}(\beta,2)\rvert$
1^72^1	1	26880	1^52^2	21	26880	1^32^3	105	51456
1^12^4	105	118840	$1^42^13^1$	70	34176	$1^12^13^2$	280	121536
$1^32^14^1$	210	60672	$1^22^15^1$	504	98496	$1^12^16^1$	840	159424
2^17^1	720	243404	$1^22^23^1$	420	78720	2^33^1	210	166176
$1^12^24^1$	630	142592	2^25^1	504	213418	$2^13^14^1$	420	216096

表 4.13 $|P_{10}^{(1)}(T)|$ 与 $|\mathcal{Q}(\alpha,2)|$ 相关数据

T	$\lvert P_{10}^{(1)}(T)\rvert$	$\lvert\mathcal{Q}(\alpha,2)\rvert$	T	$\lvert P_{10}^{(1)}(T)\rvert$	$\lvert\mathcal{Q}(\alpha,2)\rvert$	T	$\lvert P_{10}^{(1)}(T)\rvert$	$\lvert\mathcal{Q}(\alpha,2)\rvert$
1^{10}	1	2273208	1^82^1	36	1531320	1^62^2	378	2042088
1^42^3	1260	4415496	1^22^4	945	9668472	1^73^1	168	1513728
1^43^2	3360	4431096	1^13^3	2240	13637592	1^64^1	756	2317056
1^24^2	11340	13090368	1^55^1	3024	3577728	1^46^1	10080	5595768
1^37^1	25920	8630104	1^28^1	45360	13076928	1^19^1	40320	19477944
$1^42^13^1$	2520	2935296	$1^32^23^1$	7560	6501696	$1^12^33^1$	2520	13607424
$1^22^13^2$	10080	9457272	$1^42^14^1$	7560	5146272	$1^22^24^1$	11340	11131712
$1^32^15^1$	18144	7917280	$1^12^25^1$	9072	16421888	$1^22^16^1$	30240	11982744
$1^12^17^1$	25920	17863976	$1^33^14^1$	15120	7682496	$1^23^15^1$	24192	11619708
$1^13^16^1$	20160	17248992	$1^14^15^1$	18144	19494096	$1^12^13^14^1$	15120	15865632

表 4.14 $|P_{10}^{(2)}(T)|$ 与 $|\mathcal{Q}(\beta,2)|$ 相关数据

T	$\lvert P_{10}^{(2)}(T)\rvert$	$\lvert\mathcal{Q}(\beta,2)\rvert$	T	$\lvert P_{10}^{(2)}(T)\rvert$	$\lvert\mathcal{Q}(\beta,2)\rvert$	T	$\lvert P_{10}^{(2)}(T)\rvert$	$\lvert\mathcal{Q}(\beta,2)\rvert$
1^82^1	1	2273208	1^62^2	28	4623048	1^42^3	210	7627656
1^22^4	420	14231832	2^5	105	28288952	$1^52^13^1$	112	5656320
$1^22^13^2$	1120	13877064	$1^22^14^1$	420	8353536	2^14^2	1260	39484864
$1^32^15^1$	1344	11828448	$1^22^23^1$	420	78720	$1^12^17^1$	5760	26243340
2^18^1	5040	39418432	2^23^2	1120	28344888	$1^12^33^1$	1680	19828896
$1^32^23^1$	1120	9959616	$1^22^24^1$	2520	16240480	2^34^1	1260	33257792
$1^12^25^1$	4032	0	2^26^1	3360	35965464	$1^12^13^14^1$	3360	23359584
$2^13^15^1$	2688	34969500						

表 4.15 $|P_{11}^{(1)}(T)|$ 与 $|\mathcal{Q}(\alpha,2)|$ 相关数据

T	$\lvert P_{11}^{(1)}(T)\rvert$	$\lvert\mathcal{Q}(\alpha,2)\rvert$	T	$\lvert P_{11}^{(1)}(T)\rvert$	$\lvert\mathcal{Q}(\alpha,2)\rvert$	T	$\lvert P_{11}^{(1)}(T)\rvert$	$\lvert\mathcal{Q}(\alpha,2)\rvert$
1^{11}	1	757555200	1^92^1	45	596275200	1^72^2	630	784281600
1^52^3	3150	1607208960	1^32^4	4725	3431000064	1^12^5	945	7136000832
1^83^1	240	567244800	1^53^2	8400	1607448960	1^23^3	22400	4856404032
1^74^1	1260	857733120	1^34^2	56700	4494239744	1^65^1	6048	1297267200
1^15^2	72576	9803204160	1^56^1	25200	1986046848	1^47^1	86400	3006434208
1^38^1	226800	4492632576	1^29^1	403200	6654950592	1^110^1	362880	9794434240
$1^62^13^1$	5040	1089607680	$1^42^23^1$	25200	2343879936	$1^22^33^1$	25200	4900575744
$1^12^23^2$	50400	3389181120	$1^32^13^2$	25200	6934385664	$1^52^14^1$	18900	1844060160
$1^32^24^1$	56700	3905079808	$1^12^34^1$	18900	8025383424	$1^12^15^1$	60480	2794053120
$1^12^25^1$	90720	5801834240	$1^32^16^1$	151200	4178635968	$1^12^26^1$	75600	8543095296
$1^22^17^1$	259200	6202218688	$1^12^18^1$	226800	9136122112	$1^43^14^1$	50400	2705718528
$1^13^24^1$	50400	7943718528	$1^33^15^1$	120960	4045569600	$1^23^16^1$	201600	5989337088
$1^13^17^1$	172800	8822460480	$1^24^15^1$	181440	6658560640	$1^14^16^1$	151200	9786456192
$1^22^13^14^1$	151200	5585455872	$1^12^13^15^1$	120960	8231326080			

表 4.16 $|P_{11}^{(2)}(T)|$ 与 $|\mathcal{Q}(\beta,2)|$ 相关数据

T	$\lvert P_{11}^{(2)}(T)\rvert$	$\lvert\mathcal{Q}(\beta,2)\rvert$	T	$\lvert P_{11}^{(2)}(T)\rvert$	$\lvert\mathcal{Q}(\beta,2)\rvert$	T	$\lvert P_{11}^{(2)}(T)\rvert$	$\lvert\mathcal{Q}(\beta,2)\rvert$
1^{11}	1	757555200	1^92^1	36	1833984000	1^72^2	378	2967874560
1^52^3	1260	5359941120	1^32^4	945	10674662208	1^83^1	168	2238151680
1^53^2	3360	5190628032	1^23^3	2240	14970100320	1^74^1	756	3232135680
1^34^2	11340	13891439104	1^65^1	3024	4450122240	1^56^1	10080	6384500928
1^47^1	25920	9376302720	1^38^1	45360	13886907904	1^29^1	40320	20583466368
$1^62^13^1$	2520	3815663616	$1^42^23^1$	7560	7396546560	$1^22^33^1$	2520	15071708160
$1^32^13^2$	10080	10469014848	$1^52^14^1$	7560	6002928384	$1^32^24^1$	11340	12091194368
$1^42^15^1$	18144	8756686080	$1^22^25^1$	9072	17881434880	$1^32^16^1$	30240	12922056768
$1^22^17^1$	25920	19150512608	$1^43^14^1$	15120	8444665344	$1^33^15^1$	24192	12496615680
$1^23^16^1$	20160	18502060128	$1^24^15^1$	18144	20591254400	$1^22^13^14^1$	15120	17228484480

参 考 文 献

[1] Markovski S, Kusakatov V. Quasigroup String Processing: Part 2. *Proc. of Maced. Acad. of Sci. and Arts for Math. and Tech. Sci*, 2000, XXI: 15–32

[2] McKay B D, Meynert A, Myrvold W. Small Latin Squares, Quasigroups and Loops. *Journal of Combinatorial Designs*, 2007, 15(2): 98–119

[3] Markovski S, Gligoroski D, Andova A. Using Quasigroups for One-one Secure Encoding. *Proceedings of 8-th Conference for Logic and Computing*, Novi Sad, Yugoslavia, 1997, 157–162

[4] Hassinen M, Markovski S. Secure SMS Messaging Using Quasigroup Encryption and Java SMS API. *Proc. of the Eighth Symposium on Programming Languages and Software Tools*, 2003, 187–199

[5] Rivest R L. All-or-nothing Encryption and the Package Transform. Lecture Notes In Computer Science, Vol.1267, Springer-Verlag, 1997, 210–218

[6] Marnas S I, Angelis L, Bleris G L. All-or-Nothing Transforms Using Quasigroups. *Proc. 1st Balkan Conference in Informatics*, 2003, 183–191

[7] Gligoroski D. Stream Cipher Based on Quasigroup String Transformations in Z_p^*. CoRRcs. CR/0403043v2, 2004

[8] Gligoroski D, Markovski S, Kocarev L, Gusev M. Edon80 eSTREAM. ECRYPT Stream Cipher Project Report 2005/007, 2005

[9] Gligoroski D, Markovski S, Kocarev L, Gusev M. Edon80—Hardware Synchronous Stream Cipher. Symmetric Key Encryption Workshop (SKEW), Scandinavian Congress Center, Aarhus, Denmark, 26–27, May, 2005

[10] Lindner C C, Steedley D. On the Number of Conjugates of a Quasigroup. *Algebra Univ.*, 1975, 5(1): 191–196

[11] 徐允庆. 图分解与带共轭性质拟群的计数. 应用数学学报, 2008, 31(4): 608–614
(Xu Y. Counting of Quasigroups with Conjugate Properties Using Graph Decomposition. *Acta Mathematicae Applicatae Sinica*, 2008, 31(4): 608–614)

[12] Jacbson N. Basic Algebra(2nd). New York: W. H. Freeman and Company, 1985

[13] van Lint J H, Wilson R M. A Course in Combinatorics (2nd). London: Cambridge University Press, 2001

Counting of Quasigroups with Conjugate Properties

SHEN Xingwei XU Yunqing

(*Faculty of Science, Ningbo University, Ningbo* 315211)

(*E-mail: xuyunqing@nbu.edu.cn*)

Abstract With a quasigroup, we can define six conjugate quasigroups which are not necessarily distinct. The number of distinct conjugates of a quasigroup is always 1, 2, 3 or 6. Denote the set of the conjugates of a quasigroup $(Q, \otimes)$ by $C(Q, \otimes)$, and the number of all quasigroups of order n satify $|C(Q, \otimes)| = t$ by $q(n, t)$. In this paper, we get the calculators to count the $q(n, 2)$ and $q(n, 6)$.

Key words quasigroup; conjugation; permutation

MR(2000) Subject Classification 05B15

Chinese Library Classification O157.2