密码体制中的正形置换的构造与记数 [1]

亢保元

(中南大学铁道校区数力系 长沙 410075)

摘 要 正形置换在密码体制中有重要应用，该文在前人工作的基础上，利用有限群的理论对正形置换的构造和记数问题进行了讨论，特别在正形置换的记数方面得到了有价值的结果。

关键词 密码体制，置换，有限群

中图号 TN918.1

1 引 言

保密通信在信息时代日益显示出其重要性，而保密通信的实现则依赖于良好的密码体制。文献 [1] 中引进的一类特殊的置换——正形置换在密码体制中有重要应用，因此，近年来有多篇文献讨论正形置换的有关问题 [1−7]。文献 [2] 给出了正形置换的一个较好的构造方法，并由此给了正形置换的一个下界；文献 [4] 基于布尔函数给出了正形置换的一些构造方法；文献 [3] 基于布尔函数的级联运算，进一步增加了正形置换的构造方法。但总的来说，正形置换的理论还不成熟，正形置换的构造方法还不多见，正形置换的记数问题有待于讨论。

2 有关概念介绍

引进 m-bit 按位模二加法 $(\oplus)$，以 Z_2^m 记二元 m-维组的模二加法群，以二进制数 $(a_0, a_1, \cdots, a_{m-1})$ 表示一个整数 $i = \sum_{j=0}^{m-1} a_j 2^j$, $a_j \in \{0,1\}$。现定义正形置换：

定义 1[1] 一个 Z_2^m 上的正形置换是一个一一映射 $\sigma : Z_2^m \to Z_2^m$，它满足 $\{x \oplus \sigma(x)\} = Z_2^m$。将 Z_2^m 上的置换：$\sigma = \begin{pmatrix} 0 & 1 & \cdots & 2^m-1 \\ 0' & 1' & \cdots & (2^m-1)' \end{pmatrix}$ 简记为 $\{\sigma(0), \sigma(1), \cdots, \sigma(2^m-1)\}$，并记恒等置换为 $I = \{0, 1, \cdots, 2^m-1\}$。

下面给出正形置换的第二个定义：

定义 2 一个 2^m 阶正形置换是 S_{2^m} 中的一个置换，它满足 $P \oplus I \in S_{2^m}$。

正形置换的上述两个定义是一致的，只是出发点不同，可根据方便选择使用。

定义 3 设 σ 为 Z_2^m 上的一个置换，若对任意的 $x, y \in Z_2^m$，有 $\sigma(x \oplus y) = \sigma(x) \oplus \sigma(y)$，则称 σ 为一个线性置换，并设 G 为 Z_2^m 上全体线性置换做成的群。

3 主要结果

定理 1[7] 设 S 为正形置换，σ 为线性置换，则 $\sigma^{-1}S\sigma$ 仍为正形置换。

知道一个正形置换，由定理 1 指出的方法可构造多少正形置换呢？下面讨论这个问题。

设 s 为正形置换，σ, τ 均为线性置换，若 $\sigma^{-1}s\sigma = \tau^{-1}s\tau$，则 $(\tau\sigma^{-1})s = s(\tau\sigma^{-1})$，即 $\tau\sigma^{-1}$ 与 s 可换。又 $\tau\sigma^{-1}$ 为线性，故当设 H 为 G 中那些与 s 可交换的置换做成的群时 $\tau\sigma^{-1} \in H$，即 $\tau \in \sigma H$。而 σH 为 H 的一个陪集，于是 $\sigma^{-1}s\sigma = \tau^{-1}s\tau$，当且仅当 σ, τ 属于 H 的同一个陪集。这样就得到了下述定理：

定理 2 设 H 为 G 中那些与 s 可交换的置换做成的群，则知道一个正形置换，由定理 1 指出的方法可构造 $|G/H|$ 个正形置换。

为了进一步的讨论，下面引进正形置换间的一个等价关系——线性共轭关系：正形置换 s_1, s_2 等价，当且仅当存在线性置换 σ 使 $\sigma^{-1}s_1\sigma = s_2$。并设这一关系将 Z_2^m 上全体正形置换分成

[1] 2001-02-11 收到，2001-07-11 定稿

t 个类，$s_1, s_2, \cdots, s_t$ 分别是它们的代表，$H_1, H_2, \cdots, H_t$ 分别为与 $s_1, s_2, \cdots, s_t$ 可交换的线性置换做成的群。这时，由定理 2 可得下面的定理 3：

定理 3　设 $S(m)$ 为 Z_2^m 上正形置换的总数，则

(1) $S(m) = |G/H_1| + |G/H_2| + \cdots + |G/H_t|$;

(2) 当设 $|H_i| = \min\{|H_1|, \cdots, |H_t|\}$, $|H_j| = \max\{|H_1|, \cdots, |H_t|\}$ 时，有 $t|G/H_j| \le S(m) \le t|G/H_i|$。

下面基于正形置换的一个构造方法，再对正形置换的记数进行讨论。

定理 4　设 $P_1(m_1) = \{r(0), r(1), \cdots, r(2^{m_1}-1)\}$, $P_2(m_2) = \{t(0), t(1), \cdots, t(2^{m_2}-1)\}$ 分别为 2^{m_1}, 2^{m_2} 阶正形置换，则 $P(m_1+m_2) = \{\sigma(0), \sigma(1), \cdots, \sigma(2^{m_1+m_2}-1)\}$ 为 $2^{m_1+m_2}$ 阶正形置换。其中 $\sigma(j) = r(j_1) + t(j_2) \times 2^{m_1}$, $j_1 = 0, 1, \cdots, 2^{m_1}-1$, $j_2 = 0, 1, \cdots, 2^{m_2}-1$。

证明　设 2^{m_1} 除 j 的商为 j_2，余数 j_1, $j = 0, 1, \cdots, 2^{m_1+m_2}-1$，则 $0 \le j_1 \le 2^{m_1}-1$, $0 \le j_2 \le 2^{m_2}-1$，故，由带余除法 [8] 知，$j = j_1 + j_2 \times 2^{m_1}$，且这种表示法是唯一的。又

$$\sigma(j) + j = (r(j_1) + t(j_2) \times 2^{m_1}) + (j_1 + j_2 \times 2^{m_2}) = (r(j_1) + j_1) + (t(j_2) + j_2) \times 2^{m_1}$$

而 $P_1(m_1)$, $P_2(m_2)$ 为正形置换，故 $r(j_k) + j_k (0 \le k \le 2^{m_1}-1)$, $t(j_k) + j_k (0 \le k \le 2^{m_1}-1)$ 互不相同，于是 $\sigma(j_k) + j_k (0 \le k \le 2^{m_1+m_2}-1)$ 亦互不相同，即 $P(m_1+m_2)$ 为正形置换。

易证下述引理：

引理　设 $\sigma(m_1) = \{\sigma(0), \sigma(1), \cdots, \sigma(2^{m_1}-1)\}$, $\tau(m_1) = \{\tau(0), \tau(1), \cdots, \tau(2^{m_1}-1)\}$ 均为 2^{m_1} 阶正形置换，且 $\sigma(m_1) \ne \tau(m_1)$。再设 $\rho(m_2) = \{\rho(0), \rho(1), \cdots, \rho(2^{m_2}-1)\}$ 为 2^{m_2} 阶正形置换，则 $s_1(m_1+m_2) = \{s_1(0), s_1(1), \cdots, s_1(2^{m_1+m_2}-1)\} \ne s_2(m_1+m_2) = \{s_2(0), s_2(1), \cdots, s_2(2^{m_1+m_2}-1)\}$ 其中 $s_1(j) = \sigma(j_1) + \rho(j_2) \times 2^{m_1}$, $s_2(j) = \tau(j_1) + \rho(j_2) \times 2^{m_1}$。

定理 5　设 $S(m)$ 为 Z_2^m 上正形置换的总数，则当 $n > m > 1$ 时，(1) $S(2n) \ge S(2m)$, (2) $S(2n+1) \ge S(2m+1)$。

证明　设 $n = m+h+1$，则 $2^{2n} = 2^{2m} \cdot 2^{2h} \cdot 2^2$，又 $S(m) \ge 1$ [2]，所以，利用定理 4 的方法可由 2^{2m} 阶正形置换构造 2^{2n} 阶正形置换，再注意到引理，则结论 (1) 成立。同理，$h = m+1$ 结论 (2) 成立。

因当 $n > m > 1$ 时是否有 $S(n) \ge S(m)$，是一个未知的问题，故定理 5 的结论是有价值的。

4 结束语

本文对正形置换的构造与记数提供了有益的思路，本文的有些方面作者将进一步深入讨论。正形置换的构造与记数两问题虽相互联系，又各有其特殊性，能否借助于正形置换的一些简单构造方法在正形置换的记数方面有所突破，本文做了一些尝试，望起到抛砖引玉的作用。

参　考　文　献

[1] L. Mittenthal, Block substitutions using orthomorphic mapping, Advances in Applied Mathematics, 1995, 16, 59–71.

[2] Z. Liu, C. Shu, D. Ye, A method for constructing orthomorphic Permutations of Degree 2^m, China Crypt'96, Zhengzhou, 1996, 4, 56–59.

[3] 邢育森，林晓东，杨义先，杨放春，密码体制中正形置换的构造与记数，通信学报，1999, 20(2), 27–30.

[4] 冯登国，刘振华，关于正形置换的构造，通信保密，1996, 66(2), 61–64.

[5] 廖勇，卢起骏，仿射正形置换的构造与记数，密码与信息，1996, (2), 23–25.

[6] 亢保元，王育民，正形置换与正形拉丁方的两个结果，西安电子科技大学学报，1997, 24(3), 421–424.

[7] 亢保元，王育民，线性置换与正形置换，西安电子科技大学学报， 1998, 25(2), 254–256.

[8] 高等代数 (第二版)，北京大学数学系几何与代数教研室代数小组编，北京，高等教育出版社， 1988.

CONSTRUCTIONS AND ENUMERATIONS OF ORTHOMORPHIC PERMUTATIONS IN CRYPTOSYSTEMS

Kang Baoyuan

(*Central Southern University of China, Changsha* 410075, *China*)

Abstract Orthomorphic permutations have good charateristic in cryptosystems.In this paper, by using of knowledge about finite group to investigate the constructions and enumerations of orthornophic permutations, several results are obtained.

Key words Crytosystems, Permutations, Finite group

亢保元： 男， 1965 年生，副教授，博士，主要研究方向为密码学中的代数问题.