最大距离置换的计数公式 [1]

吕述望 刘传东 范修斌

(中国科技大学研究生院 信息安全国家重点实验室 北京 100039)

摘 要 该文首次给出了置换距离和最大距离置换的定义，给出了具有良好密码学性质的最大距离置换的计数公式.

关键词 置换，置换距离，最大距离置换

中图号 TN918.1

1 引 言

由于某些置换具有良好的密码学性质，是一类重要的密码学资源，所以在分组密码和序列密码的设计中得到了广泛应用。人们针对不同的置换种类进行了分析，得到了一系列重要的研究成果 [1−4] 。随着置换理论在密码编码学中应用的日益广泛和深入，人们将对更多的具有某些密码学特征的置换种类进行研究。本文基于置换的密码学应用，首次给出了最大距离置换的概念，并给出了最大距离置换的一些基本性质和计数公式。由于最大距离置换具有良好的信息扩散和混乱作用，所以研究此类置换具有重要的意义。

2 基本概念和性质

定义 1 置换距离 设 S_n 为 n 元对称群，$T \in S_n$，称 $D(T)=\sum_{i=0}^{n-1}|T(i)-i|$ 为置换 T 的置换距离。

定义 2 最大置换距离 称 $M_n=\mathrm{Max}\{D(T)|T \in S_n\}$ 为最大置换距离。

定义 3 最大距离置换 $\forall T \in S_n$，若 $D(T)=M_n$，则称 T 为最大距离置换。

定义 4[5] 轮换 设 $T \in S_n$，$a_0,a_1,\cdots,a_{m-1} \in \alpha=\{0,1,\cdots,n-1\}$，满足：$T(a_0)=a_1$，$T(a_1)=a_2$，$\cdots$，$T(a_{m-2})=a_{m-1}$，$T(a_{m-1})=a_0$，而其余元素保持不变，则 T 称为一个轮换，用 $T=(a_0,a_1,\cdots,a_{m-1})$ 表示。

引理 1 $\forall$ 轮换 $L=(a_0,a_1,\cdots,a_{m-1})$，$\sum_{i=0}^{m-1}|L(a_i)-a_i|$ 为偶数.

证明 用数学归纳法。

$m=1$ 时，$|L(a_0)-a_0|=|a_0-a_0|=0$。 $m=2$ 时，$\sum_{i=0}^{1}|L(a_i)-a_i|=|a_1-a_0|+|a_0-a_1|=2|a_1-a_0|$。 $m=3$ 时，不妨设 $a_0=\min\{a_0,a_1,a_2\}$，则 $\sum_{i=0}^{2}|L(a_i)-a_i|=|a_1-a_0|+|a_2-a_1|+|a_0-a_2|=a_1-a_0+|a_2-a_1|+a_2-a_0=a_1+a_2-2a_0+|a_2-a_1|$。

若 $a_1>a_2$，$D(L)=a_1+a_2-2a_0+a_1-a_2=2(a_1-a_0)$，

若 $a_1<a_2$，$D(L)=a_1+a_2-2a_0+a_2-a_1=2(a_2-a_0)$。

假设当 $m<k(k>3)$ 时，$D(L)$ 为偶数。当 $m=k$ 时：

$$D(L)=\sum_{i=0}^{m-1}|L(a_i)-a_i|=\sum_{i=0}^{m-2}|a_{i+1}-a_i|+|a_0-a_{m-1}|=\left(\sum_{i=0}^{m-3}|a_{i+1}-a_i|+|a_0-a_{m-2}|\right)+(|a_{m-1}-a_{m-2}|+|a_{m-2}-a_0|+|a_0-a_{m-1}|)-2|a_0-a_{m-2}|.$$

由 $m=3$ 时结论成立和归纳假设，$D(L)$ 为偶数。 证毕

[1] 2002-03-18 收到，2002-07-29 改回

科技部 “973” 项目 (NO.G1999035808) 课题资助

性质 1　$\forall T$, $D(T)$ 均为偶数。

证明　$\forall T$, T 可唯一分解成一些互不相交的轮换的乘积，故由引理 1 可知，本命题成立。

3 计数公式

定理 1　最大置换距离 $M=\begin{cases} n^2/2, & n\equiv 0(\mathrm{mod}2); \\ (n^2-1)/2, & n\equiv 1(\mathrm{mod}2) \end{cases}$。

证明　设置换 T 将 $\alpha=\{0,1,2,\cdots,n-1\}$ 分成两部分：$\alpha=\alpha_1\cup\alpha_2$, $\forall i\in\alpha$, $i\le T(i)\Leftrightarrow i\in\alpha_1$, $\forall j\in\alpha$, $j>T(j)\Leftrightarrow j\in\alpha_2$。易知 $\alpha_1\cap\alpha_2=\phi$。设 $\sum_{i\in\alpha_1} i=a$, $\sum_{j\in\alpha_2} j=b$, $\sum_{i\in\alpha_1} T(i)=c$, $\sum_{j\in\alpha_2} T(j)=d$, 则

$$D(T)=\sum_{i\in\alpha_1}|T(i)-i|+\sum_{j\in\alpha_2}|T(j)-j|=\sum_{i\in\alpha_1}(T(i)-i)+\sum_{j\in\alpha_2}(j-T(j))$$

$$=\left(\sum_{i\in\alpha_1}T(i)+\sum_{j\in\alpha_2}j\right)-\left(\sum_{i\in\alpha_1}i+\sum_{j\in\alpha_2}T(j)\right)=(c+b)-(a+d)$$

易知 $a+b+c+d=2Q$, 其中 $Q=0+1+2+\cdots+(n-1)=(1/2)(n-1)n$。故 $D(T)=2Q-2(a+d)=2[Q-(a+d)]$。

(1) 设 $\#\{\alpha_1\}=k$, 则易知 $\#\{T\alpha_2\}=n-k$, $a\ge 0+1+2+\cdots+(k-1)=(1/2)k(k-1)$, $d\ge 0+1+2+\cdots+(n-k-1)=(1/2)(n-k)(n-k-1)$, $a+d\ge(1/2)k(k-1)+(1/2)(n-k)(n-k-1)=(1/2)(n^2-n)+(k^2-nk)$。

(2) 设 $f(x)=x^2-nx$, $x\in R$, 易知 $f(x)$ 是具有最小值的抛物线，故

$$\min\{f(k),k\in Z\}=\begin{cases} -n^2/4, & k=n/2, \quad n\equiv 0(\mathrm{mod}2) \\ -(n^2-1)/4, & k=(n\pm 1)/2, n\equiv 1(\mathrm{mod}2) \end{cases}$$

由 (1) 和 (2) 易知命题成立。

由定理 1 易得如下推论：

推论 1　最大距离置换 T，将 $\alpha=\{0,1,\cdots,n-1\}$ 分成了前后两部分 α_1, α_2, $\forall i\in\alpha_1$, $T(i)\ge i$, $\forall j\in\alpha_2$, $T(j)<j$。

当 n 为偶数时，$\alpha_1=\{0,1,\cdots,n/2-1\}$, $\alpha_2=\{n/2,n/2+1,\cdots,n-1\}$。

当 n 为奇数时，$\alpha_1=\{0,1,\cdots,(n-1)/2\}$, $\alpha_2=\{(n+1)/2,\cdots,n-1\}$ 或 $\alpha_1=\{0,1,\cdots,(n-3)/2\}$, $\alpha_2=\{(n-1)/2,\cdots,n-1\}$。

推论 2　如果 $D(T)=M_n$，

当 n 为偶数时，$\alpha_1=\{0,1,\cdots,n/2-1\}$, $\alpha_2=\{n/2,n/2+1,\cdots,n-1\}$；

当 n 为奇数时，$\alpha_1=\{0,1,\cdots,(n-1)/2\}$, $\alpha_2=\{(n+1)/2,\cdots,n-1\}$, $\forall T'\in S_n$, 若 $T'\alpha_1=\alpha_1$, $T'\alpha_2=\alpha_2$, 则 $D(T'T)=M_n$。

推论 3　如果 $D(T)=M_n$, 当 n 为奇数时，若 $\alpha_1=\{0,1,\cdots,(n-3)/2\}$，$\alpha_2=\{(n-1)/2,\cdots,n-1\}$, $\forall T'\in S_n$, 若 $T'\alpha_1=\alpha_1$, $T'\alpha_2=\alpha_2$, 且 $T'((n-1)/2)\ne(n-1)/2$, 则 $D(T'T)=M_n$。

定理 2　最大距离置换个数 $K_n=\begin{cases} [(n/2)!]^2, & n\equiv 0(\mathrm{mod}2); \\ [((n-1)/2)!]^2\cdot n, & n\equiv 1(\mathrm{mod}2) \end{cases}$

证明　由定理 1 的证明过程可知：

(1) 当 n 为偶数时，再由推论 2 易知：

$D(T)=M_n \Leftrightarrow k=n/2,\ \alpha_1=\{0,1,\cdots,n/2-1\},\ \alpha_2=\{n/2,n/2+1,\cdots,n-1\},$

$T\alpha_1=\{n/2,n/2+1,\cdots,n-1\},\ T\alpha_2=\{0,1,\cdots,n/2-1\}$

故 $K_n=[(n/2)!]^2$ 。

(2) 当 n 为奇数时，$D(T)=M_n \Leftrightarrow k=(n+1)/2$ 或者 $k=(n-1)/2$，$\alpha_1=\{0,1,\cdots,k-1\}$，$T\alpha_2=\{0,1,\cdots,n-k-1\}$ 。

(a) $k=(n+1)/2$ 时：$\alpha_1=\{0,1,\cdots,(n-1)/2\}$, $T\alpha_2=\{(n-1)/2,(n+1)/2,\cdots,n-1\}$, $\alpha_2=\{(n+1)/2,(n+3)/2,\cdots,n-1\}$, $T\alpha_2=\{0,1,\cdots,(n-3)/2\}$ 。易知 $K_n^1=((n-1)/2+1)!(n-1-(n+1)/2+1)!=((n+1)/2)!((n-1)/2)!$ 。

(b) $k=(n-1)/2$ 时：$\alpha_1=\{0,1,\cdots,(n-3)/2\}$, $T\alpha_1=\{(n+1)/2,(n+3)/2,\cdots,n-1\}$, $\alpha_2=\{(n-1)/2,(n+1)/2,\cdots,n-1\}$, $T\alpha_2=\{0,1,\cdots,(n-1)/2\}$ 。

再由推论 3 可知，只要满足 $T((n-1)/2)\neq(n-1)/2$ 的 T 即为最大距离置换。

故可知 $K_n^2=((n-1)/2)![((n+1)/2)!-((n-1)/2)!]=[((n-1)/2)!]^2(n-1)/2$ 。

由上述分析可知：$K_n=K_n^1+K_n^2=((n+1)/2)!((n-1)/2)!+[((n-1)/2)!]^2(n-1)/2=[((n-1)/2)!]^2\cdot n$ 。

故本定理得证。 证毕

4 结 束 语

本文给出了最大距离置换的计数公式，由计数公式可知此类置换具有可观的数量，在密码编码中，可作为信息扩散的一类重要的密码学资源。

参 考 文 献

[1] 亢保元，田建波，王育民，全距置换，密码学进展— Chinacrypt'98, 北京，科学出版社， 1998, 207-211.

[2] 张保东，正形置换与分组密码设计，北京，中国科学院研究生院博士后研究工作报告， 1999.7

[3] 刘振华，舒畅，正形置换的研究和应用，第五届通信保密现状研讨会论文集，四川省电子学会， 1995, 39-43.

[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] 聂灵沼，丁石孙，代数学引论，北京，高等教育出版社， 2000, 28.

COUNTING FORMULA OF THE PERMUTATION WITH THE MAXIMUM DISTANCE

Lü Shuwang Liu Chuandong Fan Xiubin

(*State Key Lab. of Info. Security, Graduate School of Sci. and Tech. of China, Beijing* 100039, *China*)

Abstract In this paper, the new concepts of the permutation distance and the permutation with the maximum distance are given. The formula counting the number of the permutation with the maximum distance is also given.

Key words Permutation, Permutation distance, The permutation with the maximum distance

吕述望： 男， 1941 年生，教授，博士生导师，国家 973 项目负责人，主要从事密码理论的研究和芯片集成.

刘传东： 男， 1966 年生，硕士生，主要从事信号与信息处理.

范修斌： 男， 1966 年生，副教授，博士后，主要从事概率论在信息安全中的应用.