第9卷第4期 软 件 学 报 Vol. 9, No. 4
1998年4月 JOURNAL OF SOFTWARE Apr. 1998

一些非一次相关置换和对合的产生方法*

陶仁骥 陈世华

(中国科学院软件研究所 北京 100080)

摘要 本文讨论非一次相关置换和对合的产生问题.对于置换,首先给出了由给定置换进行仿射变换产生一类相关次数相同置换的方法,然后给出了由低维非一次相关置换递归产生高维非一次相关置换的方法,并估计了这些方法产生的置换个数.对于对合,给出了一个从特定非一次相关对合的不动点上构作不相交p-组产生非一次相关对合的方法,并估计出一个对合个数的松下界.

关键词 拉丁阵,相关,置换,对合.

中图法分类号 O157.2

密码学刺激了拉丁阵的研究.在文献[1,2]中,我们提出了拉丁阵概念,并研究了它们的计数问题.一个(n,k)-拉丁阵指一个$n\times nk$矩阵,每个元素在每列中恰出现1次,在每行中恰出现k次.拉丁阵是密码设计的有用工具.例如,m序列冠以模2加的流密码是可破的,但m序列冠以(4,4)-拉丁阵对应的置换则是安全的密码体制.[3]为了改进这种密码使其实现更容易,我们以阶数更高的非一次相关拉丁阵代替(4,4)-拉丁阵.这样就面临一个非一次相关拉丁阵的产生问题.在文献[4]中,我们使用一次独立可逆向量布尔函数,经过位移的方法构造非一次相关$(2^r,2^r)$-拉丁阵,并给出了一个基于真值表的产生全部一次独立可逆向量布尔函数的方法.尽管这种方法能枚举出全部这种函数,但它使用了穷举,而有的情形可能产生不出所要的函数.因此,研究产生一类一次独立可逆向量布尔函数的有效方法仍是有意义的.此外,从文献[4]第2节可以看出,基域$GF(2)$可改为$GF(q)$或有限环,可类似地定义相关性概念,并通过可逆向量函数加位移的办法构造相关次数相同的拉丁阵.因此,本文不限于$GF(2)$,而讨论一般情形$GF(q)$.

当加密为$y=w_1-\varphi(w_2-x)$时,解密为$x=w_2-\varphi^{-1}(w-y)$.因此,一般情形下,需要存储φ和φ^{-1}的表.如果只存储φ的表,则求$\varphi^{-1}(\cdot)$时用φ表需要查找,这是费时的.因此,将可逆φ限制到对合φ,即$\varphi^{-1}=\varphi$,是有实际需要的.

本文讨论非一次相关置换和对合的产生问题.首先,我们给出了由仿射变换产生一类相关次数相同置换的方法,然后给出了由低维非一次相关置换递归产生高维非一次相关置换的方法,并估计了这些方法产生的置换个数.对于对合,我们给出了一个从特定非一次相关对合的不动点上构作不相交p-组产生非一次相对对合的方法,并估计出一个对合个数的松下界.

1 产生一些相关次数>1的置换的方法

首先回顾一些基本概念[4],但已推广到$GF(q)$的情形.以R_q^r表示$GF(q)$上r维行向量空间.

定义. 设φ是R_q^r到自身的函数,分量函数为$\varphi_1,\ldots,\varphi_r$.任何非负整数$c$,如果存在$GF(q)$上$2r$元次数$\leqslant c$的多项式$h$,使得$h(x_1,\ldots,x_r,\varphi_1(x_1,\ldots,x_r),\ldots,\varphi_r(x_1,\ldots,x_r))=0$,其中$x_1,\ldots,x_r\in GF(q)$,则称$\varphi$ c次相关,h称为φ的一个相关多项式.如果φ不c次相关,则称$\varphi$$c$次独立.如果$\varphi$$c$次相关但$c-1$次独立,则称$c$为$\varphi$的相关次数,记作$c_\varphi$,称$c-1$为$\varphi$的独立次数,记作$I_\varphi$.

R_q^r中仿射变换指$xC+b$,C是r级矩阵,b是r维行向量.变换$xC+b$可逆当且仅当C非奇异.

文献[4]中定理1可照搬到$GF(q)$情形.

定理1. 设φ是R_q^r上变换,p和t是R_q^r上可逆仿射变换.又设$\psi(x)=p(\varphi(t(x)))$,$x\in R_q^r$.则有$c_\varphi=c_\psi$,从而$I_\varphi=I_\psi$.

以Ω_q^r表示所有R_q^r上变换的集合.任何R_q^r上可逆仿射变换p和t,令(p,t)为Ω_q^r上的一个变换,它将Ω_q^r中元素φ

---

* 本文研究得到国家自然科学基金资助.作者**陶仁骥**,1937年生,研究员,博士导师,主要研究领域为自动机理论,密码学,组合学.**陈世华**,女,1937年生,研究员,主要研究领域为自动机理论,密码学,组合学.

本文通讯联系人:陶仁骥,北京 100080,中国科学院软件研究所

本文1996-11-11收到原稿,1997-05-07收到修改稿

变到元素 $\varphi^{(p,t)}$，其中 $\varphi^{(p,t)}(x)=p(\varphi(t(x)))$，$x\in R_q^r$. 显然，$(p,t)$是可逆的，即它是 Ω_q^r 的一个置换. 定义积运算$(p,t)\cdot(p',t')=(p\cdot p',t'\cdot t)$，其中 $p\cdot p'(x)=p'(p(x))$，$t'\cdot t(x)=t(t'(x))$，$x\in R_q^r$. 容易验证，所有(p,t)，p 和 t 取遍 R_q^r 上可逆仿射变换，对上述积运算组成一群，记作 G_q^r，且对任何 $\varphi\in\Omega_q^r$ 和 G_q^r 中(p,t)和(p',t')，$\varphi^{(p,t)\cdot(p',t')}=(\varphi^{(p,t)})^{(p',t')}$.

用群论的术语[5]，定理 1 说，G_q^r 的一个传递集(轨道)中的变换有相同的相关次数. 因此，求出一个相关次数为 c 的置换 φ 后，再求含 φ 轨道即可求出 $|G_q^r|/|G_\varphi|$ 个相关次数仍为 c 的置换，其中 G_φ 为使 φ 不动的 G_q^r 中元素组成的子群.

关于 G_φ 的计算，可先计算出它的子群 $G'_\varphi=\{(p,e)|(p,e)\in G_\varphi\}$，其中 e 为恒同变换，然后计算 G'_φ 在 G_φ 中的陪集代表元素.

引理 1. 当 φ 是置换时，$G'_\varphi=\{(e,e)\}$.

证明：设$(p,e)\in G'_\varphi$ 由 G'_φ 和 G_φ 的定义，$\varphi^{(p,e)}=\varphi$. 因为 $\varphi^{(p,e)}=e\cdot\varphi\cdot p=\varphi\cdot p$，故 $\varphi\cdot p=\varphi$. 当 φ 是置换时，得 $p=e$.

引理 2. 如果 φ 为置换，则 G_φ 的阶不大于$(q^r-1)(q^r-q)\cdots(q^r-q^{r-1})q^r$.

证明：考虑 G'_φ 在 G_φ 中的陪集分解. 下面证明，若(p_1,t_1)和(p_2,t_2)不属同一陪集，则 $t_1\neq t_2$. 假如不然，有 $t_1=t_2$. 因为$(p_1^{-1},t_2^{-1})\in G_\varphi$，故$(p_1,t_1)\cdot(p_1^{-1},t_2^{-1})=(p_1\cdot p_2^{-1},e)\in G'_\varphi$. 由引理 1，得 $p_1\cdot p_2^{-1}=e$. 因此，$p_1=p_2$. 故$(p_1,t_1)=(p_2,t_2)$同属一陪集，矛盾. 故得 $t_1\neq t_2$. 由此易证，陪集个数至多为可逆仿射变换的个数. 因为 R_q^r 上可逆仿射变换的个数为$(q^r-1)(q^r-q)\cdots(q^r-q^{r-1})q^r$，且当 φ 为置换时 G'_φ 的阶为 1，故 G_φ 的阶至多为$(q^r-1)(q^r-q)\cdots(q^r-q^{r-1})q^r$.

定理 2. 设 φ 是 R_q^r 上置换，则 G_q^r 的含 φ 轨道的长不小于$(q^r-1)(q^r-q)\cdots(q^r-q^{r-1})q^r$.

证明：因 G_q^r 的阶为$((q^r-1)(q^r-q)\cdots(q^r-q^{r-1})q^r)^2$，且含 φ 轨道长为 $|G_q^r|/|G_\varphi|$，由引理 2 即得定理 2 中的结果.

定理 2 告诉我们，从一个置换出发，通过可逆仿射变换的方法可得出$(q^r-1)(q^r-q)\cdots(q^r-q^{r-1})q^r$ 以上置换，且由定理 1 知它们的相关次数相同.

定理 3. 设 φ 是 R_q^r 上置换，则有 $c_\varphi=c_{\varphi^{-1}}$.

证明：设 $h(x,y)$ 是 φ 的相关多项式. 令 $h'(x,y)=h(y,x)$，则 $h'(x,\varphi^{-1}(x))=h(\varphi^{-1}(x),x)=h(\varphi^{-1}(x),\varphi(\varphi^{-1}(x)))=0$，任 $x\in R_q^r$. 故 h' 是 φ^{-1} 的相关多项式. 因为 $\deg h'\leqslant\deg h$，故 $c_{\varphi^{-1}}\leqslant c_\varphi$ 由对称性，有 $c_\varphi\leqslant c_{\varphi^{-1}}$. 因此，$c_\varphi=c_{\varphi^{-1}}$.

引理 3. 设 φ 是 R_q^r 上置换，p 和 t 是 R_q^r 上可逆仿射变换，则$(p,t)\in G_\varphi$ 当且仅当$(t^{-1},p^{-1})\in G_{\varphi^{-1}}$.

证明：$(p,t)\in G_\varphi$ 当且仅当 $p(\varphi(t(x)))=\varphi(x)$任 $x\in R_q^r$，当且仅当 $t^{-1}(\varphi^{-1}(p^{-1}(y)))=\varphi^{-1}(y)$任意 $y\in R_q^r$，当且仅当$(t^{-1},p^{-1})\in G_{\varphi^{-1}}$.

引理 4. 设 $G''_\varphi=\{(e,t)|(e,t)\in G_\varphi\}$. 则当 φ 是置换时，$G''_\varphi=\{(e,e)\}$.

证明：设$(p,t)\in G''_\varphi$. 由 G''_φ 的定义知 $p=e$. 由引理 3，得$(t^{-1},e)\in G_{\varphi^{-1}}$. 由引理 1，有 $t^{-1}=e$. 故 $t=e$.

定理 4. 设 φ 是 R_q^r 上置换，p 是 R_q^r 上可逆仿射变换，则有：(a) $\varphi^{(t,p)}$，t 取遍 R_q^r 上可逆仿射变换，两两不同；(b) $\varphi^{(p,t)}$，t 取遍 R_q^r 上可逆仿射变换，两两不同.

证明：(a) 设 $\varphi^{(p,t)}=\varphi^{(p,t')}$，来证 $t=t'$. 记 $\varphi=\varphi^{(p,t)}$，则 $\varphi=\varphi^{(p^{-1},t^{-1})}$. 因此，$\varphi=\varphi^{(p,t)\cdot(p^{-1},t^{-1})}=\varphi^{(e,t^{-1}\cdot t)}$. 由引理 4，得 $t^{-1}\cdot t'=e$，故 $t'=t$.

(b) 证明与(a)类似，用引理 1.

定理 4 给出从一个置换出发经过可逆仿射变换得出相关次数相同的$(q^r-1)(q^r-q)\cdots(q^r-q^{r-1})q^r$ 个置换的方法.

下面讨论相关次数>1 的 R_q^r 上置换的产生问题. 我们将给出一种产生一类这种置换的方法，它基于函数的多项式表示. 众所周知，$GF(q)$上全体 r 元函数构成一个 $GF(q)$上 q^r 维向量空间，且以 $x_1^{k_1}\cdots x_r^{k_r}$，记作 $P_{k_1\cdots k_r}(x_1,\cdots,x_r)$，$k_1,\cdots,k_r=0,1,\cdots,q-1$ 为一组基. 在文献[6]中我们称之为多项式基，在此基下的坐标称为多项式坐标. 将基元素确定一种次序，得到一个 q^r 维行向量 Γ. 将 f 的多项式坐标在这种次序下表示为 q^r 维列向量 b，则可形式地表示

$$f(x_1,\cdots,x_r)=\Gamma b.$$

在文献[6]中取定 $\Gamma=[P_{00\cdots00},P_{00\cdots01},\cdots,P_{(q-1)(q-1)\cdots(q-1)(q-2)},P_{(q-1)(q-1)\cdots(q-1)(q-1)}]$.

设 φ 是 R_q^r 上变换，它的分量函数为 $\varphi_1,\cdots,\varphi_r$. 设 φ_i 的多项式坐标为 b_i，$i=1,\cdots,r$，则称 $q^r\times r$ 矩阵$[b_1,\cdots,b_r]$为 φ 的多项式坐标阵，记作 B_φ. 去掉 B_φ 中第 $1,1+q^i,i=0,\cdots,r-1$ 行后所得的矩阵记作 H_φ^r.

定理 5. $c_\varphi>1$ 的充分必要条件为 B_φ^r 列线性无关.

证明：$c_\varphi=1$ 当且仅当存在 $c_0,\ldots,c_r,d_1,\ldots,d_r\in GF(q)$ 且 $d_1,\ldots,d_r$ 不全为 0，使得

$$c_0+\sum_{i=1}^{r}c_ix_i+\sum_{i=1}^{r}d_i\varphi_i(x_1,\ldots,x_r)=0,\qquad \text{任意 } x_1,\ldots,x_r\in GF(q),$$

当且仅当存在不全为 0 的 $d_1,\ldots,d_r\in GF(q)$ 使得 $d_1b_1^-+\ldots+d_rb_r^-=0$，其中 b_j^- 表示 B_φ^- 的第 j 列，当且仅当 B_φ^- 列线性相关.

设 $s<r$，φ 是 R_q^r 上变换，h_i 是 $GF(q)$ 上 $r-i$ 元函数，$i=1,2,\ldots,r-s$. 又设 $c_1,\ldots,c_{r-s}\in GF(q)$. 定义 R_q^r 上变换 φ 的分量函数为

$$\begin{aligned}
&\varphi_1(x_1,\ldots,x_r)=c_1x_1+h_1(x_2,\ldots,x_r)\\
&\varphi_2(x_1,\ldots,x_r)=c_2x_2+h_2(x_3,\ldots,x_r)\\
&\ldots\\
&\varphi_{r-s}(x_1,\ldots,x_r)=c_{r-s}x_{r-s}+h_{r-s}(x_{r-s+1},\ldots,x_r)\\
&\varphi_{r-s+1}(x_1,\ldots,x_r)=\varphi'_1(x_{r-s+1},\ldots,x_r)\\
&\ldots\\
&\varphi_r(x_1,\ldots,x_r)=\varphi'_s(x_{r-s+1},\ldots,x_r)\\
&x_1,\ldots,x_r\in GF(q)
\end{aligned}$$

其中 $\varphi'_1,\ldots,\varphi'_s$ 是 φ 的分量函数. 我们用 $\mathrm{Rec}(\varphi,h_1,\ldots,h_{r-s},c_1,\ldots,c_{r-s})$ 表示这样定义的 φ.

引理 5. 若 φ 是 R_q^s 上置换，且 $c_i\neq0,i=1,2,\ldots,r-s$，则 $\mathrm{Rec}(\varphi,h_1,\ldots,h_{r-s},c_1,\ldots,c_{r-s})$ 是 R_q^r 上置换.

定理 6. 设 $s<r$，φ 是 R_q^s 上置换，且 $c_\varphi>1$，则 $\Phi'=\{\varphi\mid\varphi=\mathrm{Rec}(\varphi,h_1,\ldots,h_{r-s},c_1,\ldots,c_{r-s})$ 某 $h_1,\ldots,h_{r-s},c_1,\ldots,c_{r-s},c_\varphi>1$ 且 $c_i\neq0,i=1,2,\ldots,r-s\}$ 中元素为 R_q^r 上置换，且 Φ' 中元素个数为

$$(q-1)^{r-s}q^{(r-s)(r+s+1)/2}\prod_{i=s}^{r-1}(q^{q^i-i-1}-q^i).$$

证明：由引理 5 知，Φ' 中元素为置换.

设 $\varphi=\mathrm{Rec}(\varphi,h_1,\ldots,h_{r-s},c_1,\ldots,c_{r-s}),c_i\neq0,i=1,2,\ldots,r-s$. 由 φ 的构造，容易证明 φ 的多项式坐标阵 B_φ 具有下述性质：B_φ 的后 s 列后 q^r-q^s 行中元素皆为 0；任何 $j,1\leqslant j\leqslant r-s$，$B_\varphi$ 的第 j 列中，行 $q^{r-j}+1$ 元素为 c_j，后 $q^r-q^{r-j}-1$ 行中元素为 0；B_φ 的前 q^s 行后 s 列矩阵为 φ 的多项式坐标阵 B_φ. 由定理 5，因为 $c_\varphi>1$，故 B_φ^- 列线性无关. 因此 B_φ 后 s 列线性无关. 应用定理 5，我们有 $c_\varphi>1$ 当且仅当 B_φ^- 的第 j 列不属于 B_φ^- 的第 $j+1$ 列至 r 列生成的列空间，$j=1,\ldots,r-s$. 由于 B_φ 具有上述性质，使 $c_\varphi>1$ 的 B_φ^- 的第 j 列当第 $j+1$ 至 r 列取定一种值时只能有 $q^{q^{r-j}-r+j-1}-q^{r-j}$ 种取法，$1\leqslant j\leqslant r-s$. 又因 B_φ 的第 $1,q^0+1,\ldots,q^{r-1}+1$ 行各有 q^{r-s} 种取法，B_φ 的第 q^i+1 行共有 $q^{r-i-1}(q-1)$ 种取法，$s\leqslant i\leqslant r-1$，故使 $c_\varphi>1$ 的 B_φ 的取法共有 $\prod_{j=1}^{r-s}(q^{q^{r-j}-r+j-1}-q^{r-j})\cdot(q^{r-s})^{s+1}\cdot\prod_{i=s}^{r-1}(q^{r-i-1}(q-1))=(q-1)^{r-s}q^{(r-s)(r+s+1)/2}\prod_{i=s}^{r-1}(q^{q^i-i-1}-q^i)$ 种，它为 Φ' 中元素的个数.

由定理 6 的证明，我们有

推论 1. 设 $s<r$，φ 是 R_q^s 上置换，且 $c_\varphi>1$. 设 B 是 $GF(q)$ 上 $q^r\times r$ 矩阵，满足条件：B 的前 q^s 行后 s 列矩阵为 B_φ，B 的后 q^r-q^s 行后 s 列全为 0；任何 $j,1\leqslant j\leqslant r-s$，$B$ 的第 j 列中，行 $q^{r-j}+1$ 元素非 0，后 $q^r-q^{r-j}-1$ 行元素全为 0；任何 $j,1\leqslant j\leqslant r-s-1$，$B$ 的第 j 列中行 $q^{r-j-1}+2$ 至行 q^{r-j} 中元素不全为 0；B 的前 q^s 行后 $s+1$ 列矩阵中第 1 列不能由其余列线性表示. 如果 B 为 φ 的多项式坐标阵，则 φ 是 R_q^s 上置换，且 $c_\varphi>1$. 进一步，由这种 B 得出的相关次数 >1，R_q^s 上置换的个数为

$$(q-1)^{r-s}(q^{q^s}-q^s)\prod_{i=s+1}^{r-1}(q^{q^i}-q^{q^{i-1}+1}).$$

2　产生一些相关次数 >1 的对合的方法

任何 $a_1,\ldots,a_r\in GF(q),r\geqslant1$，以 $Q_{a_1\ldots a_r}(x_1,\ldots,x_r)$ 表示 $GF(q)$ 上 r 元函数，它在点 $(a_1,\ldots,a_r)$ 上取值 1，在其它点上取值 0. 易知，$Q_{a_1\ldots a_r}(x_1\ldots x_r)=\prod_{i=1}^{r}Q_{a_i}(x_i)$. 容易验证，$Q_a(x)=1-(x-a)^{q-1}$.

引理 6. 设 φ' 是 R_q^r 上变换，且 φ' 在点 $(a_1,\ldots,a_r)$ 和 $(b_1,\ldots,b_r)$ 上不动. 设 φ 是 φ' 和对换 $(a_1\ldots a_r,b_1\ldots b_r)$ 的乘积.

则有 $\varphi(x_1,\ldots,x_r)=\varphi'_i(x_1,\ldots,x_r)+(b_i-a_i)Q_{a_1\ldots a_r}(x_1,\ldots,x_r)+(a_i-b_i)Q_{b_1\ldots b_r}(x_1,\ldots,x_r)$，$i=1,\ldots,r$，其中 φ 和 φ'_i 分别为 φ 和 φ' 的第 i 分量函数.

引理 7. $(b_i-a_i)Q_{a_1\ldots a_r}(x_1,\ldots,x_r)+(a_i-b_i)Q_{b_1\ldots b_r}(x_1,\ldots,x_r)$ 的多项式表示中，项 $\prod_{h=1}^{r}x_h^{q-1}$ 的系数为 0，项 $\left(\prod_{h=1}^{r}x_h^{q-1}\right)/x_j$ 的系数为 $(-1)^r(q-1)(b_i-a_i)(b_j-a_j)$，$i,j=1,\ldots,r$.

证明：利用

$$Q_{d_1\ldots d_r}(x_1,\ldots,x_r)=(-1)^r\prod_{h=1}^{r}((x_h-d_h)^{q-1}-1)=(-1)^r\prod_{h=1}^{r}(x_h^{q-1}-(q-1)d_hx_h^{q-2}+\ldots)$$

$$=(-1)^r\prod_{h=1}^{r}x_h^{q-1}-(-1)^r(q-1)d_1\left(\prod_{h=1}^{r}x_h^{q-1}\right)/x_1-\ldots-$$

$$(-1)^r(q-1)d_r\left(\prod_{h=1}^{r}x_h^{q-1}\right)/x_r+\ldots$$

即得引理中结果.

引理 8. 设 φ 是 R_q^r 上对合且可分解为不相交对换 $(a_1\ldots a_r,b_1\ldots b_r),\ldots,(c_1\ldots c_r,d_1\ldots d_r)$ 的乘积，则 φ 的分量函数可表示为

$$\varphi_i(x_1,\ldots,x_r)=x_i+(b_i-a_i)Q_{a_1\ldots a_r}(x_1,\ldots,x_r)+(a_i-b_i)Q_{b_1\ldots b_r}(x_1,\ldots,x_r)+\ldots+$$

$$(d_i-c_i)Q_{c_1\ldots c_r}(x_1,\ldots,x_r)+(c_i-d_i)Q_{d_1\ldots d_r}(x_1,\ldots,x_r),\quad \text{其中 } i=1,\ldots,r.$$

证明：显然，φ 可经恒同变换逐步添加对换而得. 由引理 6 即得.

任何 R_q^r 上变换 φ，以 L_φ 表示 φ 的多项式系数阵 B_φ 的末行，以 H_φ 表示 B_φ 中对应基元素 $\left(\prod_{j=1}^{r}x_j^{q-1}\right)/x_i$，$i=1,\ldots,r$ 的行所组成的子矩阵.

任何 R_q^r 上对换 $\alpha=(a_1\ldots a_r,b_1\ldots b_r)$，记 $r\times r$ 矩阵

$$D_\alpha=(-1)^r(q-1)\begin{bmatrix}b_1-a_1\\ \ldots\\ b_r-a_r\end{bmatrix}[b_1-a_1,\ldots,b_r-a_r].$$

引理 9. 设 $r(q-1)\geqslant 3$，φ 是 R_q^r 上对合且可分解为不相交对换 $\alpha_1,\ldots,\alpha_t$ 的乘积，则有 $H_\varphi=\sum_{i=1}^{t}D_{\alpha_i}$.

证明：由引理 7 和引理 8 即得.

定理 7. 设 $r(q-1)\geqslant 2$，φ 是 R_q^r 上对合，则有 $L_\varphi=0$.

证明：注意到对合可分解为不相交对换的乘积，由引理 7 和引理 8 即得.

定理 8. 设 $r(q-1)\geqslant 3$，则存在 R_q^r 上对合 φ，使得 $c_\varphi>1$.

证明：令 φ 是 R_q^r 上对合，它是下列 r 个对换的乘积：

$$(111\ldots110,111\ldots100),$$
$$(111\ldots101,111\ldots001),$$
$$\ldots\ldots$$
$$(101\ldots111,001\ldots111),$$
$$(011\ldots111,011\ldots110).$$

由引理 9，容易证明 $H_\varphi=(-1)^r(q-1)E$，其中 E 为 r 级单位矩阵. 又因 $r(q-1)\geqslant 2$，故 H_φ 属于 B_φ^-. 因此 B_φ^- 列线性无关. 由定理 5，得 $c_\varphi>1$.

定理 9. 设 $r(q-1)\geqslant 3$，φ 是 R_q^r 上对合且可分解为不相交对换 $\alpha_1,\ldots,\alpha_t$ 的乘积. 如果 $\sum_{i=1}^{t}D_{\alpha_i}$ 非奇异，则 $c_\varphi>1$.

证明：由引理 9，H_φ 非奇异. 因为 $r(q-1)-1\geqslant 2$，故 H_φ 属于 B_φ^-. 因此，B_φ^- 列线性无关. 由定理 5，得 $c_\varphi>1$.

推论 2. 设 $r(q-1)\geqslant 3$，φ 是 R_q^r 上对合且 H_φ 非奇异. 又设 $\alpha_1,\ldots,\alpha_s$ 是 R_q^r 上不相交对换，且 α_i 的动点为 φ 的不动点，$i=1,\ldots,s$. 如果 $\sum_{i=1}^{s}D_{\alpha_i}-0$，则 $\alpha_1,\ldots,\alpha_s$ 和 φ 的乘积是 R_q^r 上对合，且相关次数 >1.

记 $GF(q)$的特征为 p. 设 $\alpha_i=(a_{i1},\ldots a_{ri},b_{i1},\ldots b_{ri})$, $i=1,\ldots,p$, 是 p 个两两不交的 R_q^r 上的对换. 如果$(b_{1i}-a_{1i},\ldots,b_{ri}-a_{ri})$和$(b_{1j}-a_{1j},\ldots,b_{rj}-a_{rj})$至多相差一个负号，任何 $i,j=1,\ldots,p$, 则称 $\alpha_1,\ldots,\alpha_p$ 为一个 p-组.

推论 3. 设 $r(q-1)\geqslant 3$, φ 是 R_q^r 上对合且 H_φ 非奇异. 又设 $\alpha_1,\ldots,\alpha_{tp}$是两两不相交的 R_q^r 上对换，且 α_i 的动点为 φ 的不动点，$i=1,\ldots,tp$. 如果 $\alpha_1,\ldots,\alpha_{tp}$可划分为 t 个 p-组，则 $\alpha_1,\ldots,\alpha_{tp}$和 φ 的乘积是 R_q^r 上对合且相关次数>1.

证明：因为任何 p-组 $\beta_1,\ldots,\beta_p$ 都有 $D_{\beta_i}=D_{\beta_j}$, $i,j=1,\ldots,p$, 故 $\sum_{i=1}^{p}D_{\beta_i}=0$. 由推论 1 即得.

推论 2 给出产生一类相关次数>1 的对合的方法，即从一个 H_φ 非奇异对合 φ 出发，添加不动点上的 p-组.

定理 10. 设 $r(q-1)\geqslant 3$, p 为 $GF(q)$的特征. 则 R_q^r 上相关次数>1 的对合至少有$(n_p)^{q^r/p-2r-2}$个，其中 $n_2=2$，当 $p>2$时，

$$n_p=1+\sum_{i=1}^{(p-1)/2}\left[\binom{p-i}{i}+\binom{p-i-1}{i-1}\right].$$

证明：设 $0\neq e\in R_q^r$. 称 R_q^r 中 p 个不同元素 $a,a+e,\ldots,a+(p-1)e$ 为一个 e-圈，其中 $a+ie=b_1\ldots b_r,b_j=a_j+ie_j$, $a=a_1\ldots a_r,e=e_1\ldots e_r$. 容易证明，$R_q^r$ 可划分为 q^r/p 个不相交的 e 圈. 不难证明，从一个 e-圈中挑选出若干形如$(a+ie,a+(i+1)e)$的不相交对换的取法(包括 0 个对换)有 n_p 种. 考虑定理 8 证明中所构造的 φ. 去掉含 φ 的动点的 e-圈，至多 $2r$ 个. 从其余的 e-圈中挑选出 p 的倍数个形如$(a+ie,a+(i+1)e)$的不相交对换. 由于 e-圈个数$\geqslant q^r/p-2r$，从一个 e-圈中可挑选出不相交对换的个数可达到$(p-1)/2$(当 $p>2$)，故上述取法数$\geqslant(n_p)^{q^r/p-2r-2}$. 由定理 9 中推论 2，由 φ 和这些对换的乘积产生的对合的相关次数>1.

推论 4. 设 $r(q-1)\geqslant 3$ 且 $GF(q)$的特征 α. 则 R_q^r 上相关次数>1 的对合至少有 $\alpha^{q^r/2-2r-1}$个.

致谢　感谢刘木兰教授提出的许多意见，特别是对引理 1 证明的简化.

参考文献

1 陶仁骥，陈世华. 拉丁阵的枚举和计数(I)，情形 $n\leqslant 3$. 中国科学(A 辑)，1990，33(8)：803～809；1990，33(12)：1430～1438
(Tao Ren-ji, Chen Shi-hua. Enumeration of Latin arrays (I)——case $n\leqslant 3$. Science in China (Chinese Edition), series A, 1990, 33(8): 803～809; 1990, 33(12): 1430～1438)

2 陶仁骥，陈世华. 拉丁阵的枚举和计数(II)，情形 $n=4,k\leqslant 4$. 中国科学(A 辑)，1990，33(9)：930～937；1991，34(1)：20～29
(Tao Ren-ji, Chen Shi-hua. Enumeration of Latin arrays (II)——case $n=4,k\leqslant 4$. Science in China (Chinese Edition), series A. 1990, 34(9): 930～937; 1991, 34(1): 20～29)

3 陶仁骥. (4,4)-拉丁阵在密码设计上的一种应用. 计算机学报，1991，14(6)：423～431
(Tao Ren-ji. An application of (4,4)-Latin arrays to cryptography. Chinese Journal of Computers, 1991, 14(6): 423～431)

4 陶仁骥，陈世华. 一类一次独立拉丁阵的产生方法. 中国科学(A 辑)，1995，25(6)：650～658；1995，38(7)：884～896
(Tao Ren-ji, Chen Shi-hua. A generation method for a kind of Latin arrays with degree 1 of independence. Science in China (Chinese Edition), series A, 1995, 25(6): 650～658; 1995, 38(7): 884～896)

5 维兰特(王萼芳译). 有限置换群. 北京：科学出版社，1984
(Wielandt H. Finite permutation group. Beijing: Academic Press Inc., 1964)

6 陶仁骥. 有限自动机的可逆性. 北京：科学出版社，1979. 283～288
(Tao Ren-ji. Invertibility of finite automata. Beijing: Science Press, 1979. 283～288)

Generation of Some Permutations and Involutions with Dependence Degree >1

TAO Ren-ji　CHEN Shi-hua

(Institute of Software　The Chinese Academy of Sciences　Beijing　100080)

Abstract　In this paper, the authors deal with the generation of permutations and involutions with dependence degree >1. For permutation, they first give a method of generating a kind of permutations with the same dependence degree by affine transformations to a given permutation, then a recursive method of generating higher dimensional permutations from lower ones, and numbers of permutations generated by these methods are evaluated. For involution, the authors give a method of generating involutions with dependence degree >1 by making p disjoint transpositions with the same distance from fixed points of a given involution, and a loose lower bound of numbers of such generated involutions.

Key words　Latin square, dependence, permutation, involution.