基于拟群的伪随机序列周期研究

李妍芳，徐允庆*
（宁波大学 理学院，浙江 宁波 315211）

摘要：基于拟群的非线性伪随机序列在密码学中有着重要的应用，尤其是周期长的非线性伪随机序列，但该序列的拟群目前只能通过计算机做统计实验的方法得到. 笔者从理论上给出了周期增长率高的拟群的代数与组合特征以及其构造方法.

关键词：拟群；伪随机序列；置换群
中图分类号：O157.2; TP309.2　　文献标识码：A　　文章编号：1001-5132（2011）03-0041-04

伪随机序列在通讯、自动控制、计算机以及密码学等领域有着广泛的应用. 伪随机序列生成器是生成伪随机序列的算法，按照算法可分为线性伪随机序列生成器和非线性伪随机序列生成器. 非线性伪随机序列生成器由于具有其可任意长的周期和不可预测性而更适用于密码学领域.

基于拟群的伪随机序列生成器是非线性伪随机序列生成器[1]. 进入欧洲序列密码(eSTREAM)计划第 3 轮选拔的候选算法 Edon80[2]的密钥序列生成器是基于 4 阶拟群的伪随机序列生成器算法.

拟群的数量巨大，如 10 阶拟群就有 9.98×10^{36} 个[3]，而且随着拟群阶数的增大，其数量急剧增长，不同的 n 阶拟群的个数不小于 $(n!)^{2n}n^{-n^2}$ [4]. 但并不是每个拟群都能适用于伪随机序列生成器. 如 4 阶拟群一共有 576 个，Gligoroski 等[2]利用统计实验的方法得出最适用于产生密钥流的只有 64 个. 5 阶、6 阶、7 阶、8 阶、9 阶的拟群分别有 1.61×10^5 个、8.13×10^8 个、6.15×10^{13} 个、1.09×10^{20} 个、4.97×10^{29} 个[3]. 由于数量巨大，Dimitrova 等[1]只对以上阶数的拟群随机选取 $2^{16}=65536$ 个进行统计实验，分别得出了拟群周期增长率分布的一些结果，对于更高的阶数，其统计实验就更困难了.

各阶数的拟群都可能用于序列密码系统的伪随机密钥序列生成器算法，最方便的应是 256 阶. 但对阶数大的拟群用统计实验的方法测试几乎是不可能的，而且实验性的结果也并不十分准确可靠，这是因为实验结果与初始字符序列的选取有关. 基于以上原因，从理论上去确定一个拟群是否适用于伪随机序列生成器算法显得尤为必要.

1　概念与引理

定义 **1**　拟群 $(Q,\odot)$ 是一个广群(在集合 Q 上带有一个二元运算的代数结构)，并且对 $\forall a,b\in Q$，有以下 2 个方程:

$$a\odot x=b,\ y\odot a=b, \tag{1}$$

在集合 Q 上有唯一解.

在给定 Q 是一个集合 ($|Q|\geqslant 2$) 的情况下，我们用集合 $Q^+=\{x_1x_2...x_k\mid x_i\in Q,\quad k\geqslant 2\}$ 表示所有由集合 Q 中的元素组成的有限序列. 假定 $(Q,\odot)$ 是一个给定的拟群，对于一个确定的引导元 $\alpha\in Q$，可以定义一个 Q^+ 上基于该拟群运算“ $\odot$ ”的字符串变换 $E_\alpha:Q^+\to Q^+$，

$$E_\alpha(x_1x_2\cdots x_n)=y_1y_2\cdots y_n\Leftrightarrow \begin{cases} y_1=\alpha\odot x_1,\\ y_i=y_{i-1}\odot x_i,(i=2,\cdots,k). \end{cases} \tag{2}$$

由方程(1)有唯一解可得下面的引理.

引理 **1**　设 $\alpha,\alpha'\in Q$，$y_1y_2\cdots y_k=E_\alpha(x_1x_2\cdots x_k)$，$y'_1y'_2\cdots y'_k=E_{\alpha'}(x_1x_2\cdots x_k)$. 若 $\alpha'\neq\alpha$，则 $y_i\neq y'_i$ $(i=1,2,\cdots,k)$.

设 $(Q,\odot_1)$，$(Q,\odot_2)$，$\cdots$，$(Q,\odot_t)$ 是 t 个 Q 上的

收稿日期：2010–08–16.　　宁波大学学报（理工版）网址: http://3xb.nbu.edu.cn
基金项目：国家自然科学基金（60873267）；浙江省自然科学基金（Y607026）.
第一作者：李妍芳（1985－），女，河南安阳人，在读硕士研究生，主要研究方向：组合设计和密码学. E-mail: liyanfang1002@163.com
*通讯作者：徐允庆（1959－），男，河南南阳人，博士/教授，主要研究方向：组合设计与密码学. E-mail: xuyunqing@nbu.edu.cn

拟群(不必不同). 选择引导元 $\alpha_1,\alpha_2,\cdots,\alpha_t\in Q$ (不必不同), 则可以按(2)式定义 $Q^+\to Q^+$ 的 t 个字符串变换 $E_{\alpha_1},E_{\alpha_2},\cdots,E_{\alpha_t}$, 并定义多重变换 $E^{(t)}$ 为:

$$E^{(t)}=E^{(t)}_{\alpha_1,\alpha_2,\cdots,\alpha_t}=E_{\alpha_t}\circ\cdots\circ E_{\alpha_2}\circ E_{\alpha_1}.$$

文献[2]中将初始序列 012301230123…经过 $t=80$ 重变换得到非线性伪随机序列 $y_{79,0}\ y_{79,1}\cdots$ (表 1)作为密钥序列, 其中“ $\odot_i$ ”$(i=0,1,\cdots,79)$ 都是基于集合 $Q=\{0,1,2,3\}$ 的拟群运算.

表 1 初始序列经过 t 重变换后的非线性伪随机序列

$\odot_i$	α	0	1	2	3	0	1	2	3	0	…
$\odot_0$	α_0	y_{00}	y_{01}	y_{02}	y_{03}	y_{04}	y_{05}	y_{06}	y_{07}	y_{08}	…
$\odot_1$	α_1	y_{10}	y_{11}	y_{12}	y_{13}	y_{14}	y_{15}	y_{16}	y_{17}	y_{18}	…
…	…	…	…	…	…	…	…	…	…	…	…
$\odot_{79}$	α_{79}	$y_{79.0}$	$y_{79.1}$	$y_{79.2}$	$y_{79.3}$	$y_{79.4}$	$y_{79.5}$	$y_{79.6}$	$y_{79.7}$	$y_{79.8}$	…

定义 **2** 设 $(Q,\odot)$ 为一拟群, $X\in Q^+$ 是集合 Q 上任一字符序列, $\alpha\in Q$. 记 $c(X)$ 为 X 的周期, $c(E_\alpha(X))$ 为字符序列 $E_\alpha(X)$ 的周期. 称

$$\sum_{\alpha\in Q}P(\alpha)c(E_\alpha(X))/c(X)$$

为拟群 $(Q,\odot)$ 对序列 X 的周期增长率,

$$C(Q,\odot)=\sum_{X\in Q^+}P(X)(\sum_{\alpha\in Q}P(\alpha)\frac{c(E_\alpha(X))}{c(X)})$$

为拟群 $(Q,\odot)$ 的周期增长率, 其中 $P(\alpha)$ 和 $P(X)$ 分别是 α 和 X 出现的概率.

每一个拟群都有一个周期增长率. 选择若干具有一定周期增长率的拟群对初始序列进行一系列的字符序列变换, 可以得到具有任意长周期的伪随机序列.

定义 **3** 设 $Q=\{1,2,\cdots,n\}$ (以下都如此假设), $(Q,\odot)$ 是集合 Q 上的拟群. 由方程(1)有唯一解知: $1\odot i$, $2\odot i,\cdots$, $n\odot i$ 是 Q 的一个全排列, 定义

$$\sigma_i=\begin{pmatrix}1 & 2 & \cdots & n\\ 1\odot i & 2\odot i & \cdots & n\odot i\end{pmatrix},$$

为拟群 $(Q,\odot)$ 的第 i 个列置换, 这里 $i=1,2,\cdots,n$.

设 $x_1x_2\cdots x_k$ 为 Q 上的字符序列, $y_1y_2\cdots y_k=E_\alpha(x_1x_2\cdots x_k)$, 则由(2)式可得:

$$\begin{cases}y_1=\sigma_{x_1}(\alpha),\\ y_i=\sigma_{x_i}(y_{i-1}),\quad i=2,3,\cdots,k,\end{cases}\tag{3}$$

其中 σ_{x_i} 为拟群 $(Q,\odot)$ 的第 x_i 个列置换.

定义 **4** 设 Q 为一集合, G 为 Q 上的置换群, $\sigma\in G$, $\alpha\in Q$. 序列 $\alpha\ \sigma(\alpha)\cdots\sigma^k(\alpha)\cdots$ 的周期称为 σ 关于序列 $\alpha\ \alpha\ \alpha\cdots$ 的周期增长率, 记为 $C_\alpha(\sigma)$. 称 $C(\sigma)=\sum_{\alpha\in Q}P(\alpha)C_\alpha(\sigma)$ 为置换 σ 的周期增长率, 称

$$C(G)=\sum_{\sigma\in G}P(\sigma)C(\sigma)=\sum_{\sigma\in G}P(\sigma)(\sum_{\alpha\in Q}P(\alpha)C_\alpha(\sigma))$$

为置换群 G 的周期增长率, 其中 $P(\alpha)$ 和 $P(\sigma)$ 分别为 α 和 σ 出现的概率.

定理 **1** 设 G 是拟群 $(Q,\odot)$ 的 n 个列置换 $\sigma_1,\sigma_2,\cdots,\sigma_n$ 的生成子群, 即 $G=\langle\sigma_1,\sigma_2,\cdots,\sigma_n\rangle$. 则拟群 $(Q,\odot)$ 的周期增长率等于置换群 G 的周期增长率, 即 $C(Q,\odot)=C(G)$.

证明 设 $T=x_1x_2\cdots x_m\in Q^+$, 记 $\sigma_T=\sigma_{x_m}\cdots\sigma_{x_2}\sigma_{x_1}$. 令 $Q^+_\sigma=\{T\,|\,|T\|\cdots\|T\cdots\|\,c(T)=|T|,\sigma_T=\sigma\}$, 其中“ $\|$ ”表示字符序列的串联, $c(T)$ 表示 T 的周期, $|T|$ 表示 T 的长度, 则 $Q^+=\cup_{\sigma\in G}Q^+_\sigma$, 从而有:

$$C(Q,\odot)=\sum_{X\in Q^+}P(X)(\sum_{\alpha\in Q}P(\alpha)\frac{c(E_\alpha(X))}{c(X)})=$$
$$\sum_{\sigma\in G}\sum_{X\in Q^+_\sigma}P(X)(\sum_{\alpha\in Q}P(\alpha)\frac{c(E_\alpha(X))}{c(X)}).\tag{4}$$

设 $X=x_1x_2\cdots x_mx_1x_2\cdots x_m\cdots x_1x_2\cdots x_m\cdots$, 记 $E_\alpha(X)=y_1\cdots y_my_{m+1}\cdots y_{2m}\cdots y_{(k-1)m+1}\cdots y_{km}\cdots$ 则由(3)式可知:

$$y_m=\sigma_{x_m}(\cdots(\sigma_{x_2}(\sigma_{x_1}(\alpha)))\cdots).$$

由 $\sigma=\sigma_{x_m}\cdots\sigma_{x_2}\sigma_{x_1}$ 知, $y_{km}=\sigma^k(\alpha)$ $(k=1,2,\cdots)$. 因序列 $\alpha,\sigma(\alpha),\cdots,\sigma^k(\alpha),\cdots$ 的周期为 $C_\alpha(\sigma)$, 则由引理 1 可知道序列 $E_\alpha(X)=y_1\cdots y_my_{m+1}\cdots y_{2m}\cdots y_{(k-1)m+1}\cdots y_{km}\cdots$ 的周期 $c(E_\alpha(X))=c(X)C_\alpha(\sigma)$. 代入(4)式得:

$$C(Q,\odot)=\sum_{\sigma\in G}\sum_{X\in Q^+_\sigma}P(X)(\sum_{\alpha\in Q}P(\alpha)C_\alpha(\sigma))=$$
$$\sum_{\alpha\in Q}P(\alpha)(\sum_{\sigma\in G}C_\alpha(\sigma)\sum_{X\in Q^+_\sigma}P(X))=$$
$$\sum_{\alpha\in Q}P(\alpha)(\sum_{\sigma\in G}C_\alpha(\sigma)P(\sigma))=$$
$$\sum_{\sigma\in G}P(\sigma)(\sum_{\alpha\in Q}P(\alpha)C_\alpha(\sigma))=C(G).$$

2 主要结论

任一置换都可写成不相交轮换的乘积, 若 Q 上的置换 σ 是由 λ_1 个 1-轮换, λ_2 个 2-轮换, …, λ_n 个 n-轮换组成, 则称 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ 为置换 σ 的型, 这里 $\lambda_1+2\lambda_2+\cdots+n\lambda_n=n$.

引理 **2** 设每个引导元出现的概率相等, 即

$\forall \alpha \in Q,\ P(\alpha)=1/n$．则 Q 上型为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ 的置换 σ 的周期增长率为：$C(\sigma)=(1/n)\sum_{i=1}^{n} i^2\lambda_i$.

证明　将置换 σ 写成不相交轮换乘积形式:

$$\sigma=(x_{11}^{(1)})\cdots(x_{\lambda_1 1}^{(1)})(x_{11}^{(2)}x_{12}^{(2)})\cdots(x_{\lambda_2 1}^{(2)}x_{\lambda_2 2}^{(2)})\cdots$$
$$(x_{11}^{(n)}x_{12}^{(n)}\cdots x_{1n}^{(n)})\cdots(x_{\lambda_n 1}^{(n)}x_{\lambda_n 2}^{(n)}\cdots x_{\lambda_n n}^{(n)}),$$

若 α 在上式的第 $\lambda_1+\lambda_2+\cdots+\lambda_{i-1}+j$ 个轮换中，即 $\alpha\in\{x_{j1}^{(i)},x_{j2}^{(i)},\cdots,x_{ji}^{(i)}\}\subseteq Q_{ij}$ $(1\leqslant i\leqslant n, 1\leqslant j\leqslant \lambda_i)$，不妨设 $\alpha=x_{j1}^{(i)}$，则字符序列

$$\alpha\sigma(\alpha)\sigma^2(\alpha)\cdots=x_{j1}^{(i)}x_{j2}^{(i)}\cdots x_{ji}^{(i)}x_{j1}^{(i)}\cdots.$$

由定义 4 可得 $C_\alpha(\sigma)=i$．再由 $Q=\bigcup_{i=1}^{n}\bigcup_{j=1}^{\lambda_i}Q_{ij}$ 得:

$$C(\sigma)=\sum_{\alpha\in Q}P(\alpha)C_\alpha(\sigma)=(1/n)\sum_{i=1}^{n}\sum_{j=1}^{\lambda_i}\sum_{\alpha\in Q_{ij}}C_\alpha(\sigma)=$$
$$(1/n)\sum_{i=1}^{n}\sum_{j=1}^{\lambda_i}\sum_{\alpha\in Q_{ij}} i=(1/n)\sum_{i=1}^{n} i^2\lambda_i.$$

引理**3**　设集合 Q 上的置换 σ 为 n 长轮换，即 σ 的型为 n^1．对 $1\leqslant i\leqslant n$，若 $(i,n)=d$，则置换 σ^i 的型为 $(n/d)^d$.

证明　当 $i=n$ 时定理显然成立. 下面设 $1\leqslant i\leqslant n-1$. 记 $j=n/d$, 则 $j\cdot i\equiv 0 \pmod n$，且当 $1\leqslant k\leqslant j-1$ 时 $ki\not\equiv 0 \pmod n$. 设 σ 的轮换分解式为: $\sigma=(a_0a_1\cdots a_{n-1})$，则

$$(a_m\sigma^i(a_m)\cdots\sigma^{(j-1)i}(a_m))=(a_m a_{m+i}\cdots a_{m+(j-1)i})$$

是 σ^i 的一个轮换. 取 $m=0,1,\cdots,d-1$ 可得 σ^i 的 d 个 j 长轮换:

$$\begin{cases}(a_0a_ia_{2i}\cdots a_{(j-1)i}),\\(a_1a_{1+i}a_{1+2i}\cdots a_{1+(j-1)i}),\\\vdots\\(a_{d-1}a_{d-1+i}a_{d-1+2i}\cdots a_{d-1+(j-1)i}).\end{cases}\tag{5}$$

若 $d=1$，即 i 与 n 互素，则 σ^i 的型为 n^1.

若 $d>1$，任给非负整数 p,q,r,s，设 $0\leqslant p<q\leqslant d-1$；$0\leqslant r,\ s\leqslant j-1$. 因 $(s-r)i \pmod n\in\{0,d,2d,\cdots,(j-1)d\}$，$0\leqslant q-p\leqslant d-1$，所以 $q-p+(s-r)i\not\equiv 0 \pmod n$，从而 $a_{p+ri}\neq a_{q+si}$.

由此可知(5)式中的 d 个长轮换是不交的. 这 d 个轮换的元素个数为 $dj=n$，所以 σ^i 是这 d 个轮换的乘积，σ^i 的型为 $(n/d)^d$.

定理 **2**　设 S_n 为集合 $Q=\{1,2,\cdots,n\}$ 上的 n 次对称群，$\sigma\in S_n$ 是 n 长轮换. 设 $k_1k_2\cdots k_n$ 是 Q 中元素的一个全排列. 定义 Q 上的二元运算“ $*$ ”为:

$$i*j=\sigma^{k_j}(i),\forall i,j\in Q,\tag{6}$$

则 $(Q,*)$ 是一个拟群.

证明　$\forall a,b\in Q$，显然 2 个方程 $a*x=b, y*a=b$ 在集合 Q 上有唯一解.

$(Q,*)$ 的列置换依次是 σ^{k_1}，σ^{k_2}，$\cdots$，σ^{k_n}，且 $(Q,*)$ 列置换的生成群 $C_n=\langle\sigma\rangle=\{e,\sigma,\sigma^2,\cdots,\sigma^{n-1}\}$，这里 e 表示恒等置换. 我们称拟群 $(Q,*)$ 为 n 长轮换 σ 的生成拟群.

定理 **3**　设集合 Q 上的置换 σ 为 n 长轮换，$C_n=\langle\sigma\rangle=\{e,\sigma,\cdots,\sigma^{n-1}\}$ 为 σ 的生成子群. 设 $\forall\alpha\in Q$ $P(\alpha)=1/n$；$P(\sigma^i)=1/n$ $(i=0,1,\cdots,n-1)$. 则置换群 C_n 的周期增长率为:

$$C(C_n)=\sum_{d|n}(1/d)\phi(n/d),$$

其中 ϕ 是欧拉函数，且由 n 长轮换生成的不同拟群共有 $n!(n-2)!$ 个.

证明　记 $Q_d=\{i\mid 0\leqslant i\leqslant n-1,(i,n)=d\}$，则 $\{0,1,\cdots,n-1\}=\cup_{d|n}Q_d$，$Q_d$ 中元素个数为:

$$|Q_d|=|\{i\mid 0\leqslant i\leqslant n-1,(i,n)=d\}|=$$
$$|\{(i/d)\mid (i/d,n/d)=1,\ 0\leqslant i/d\leqslant n/d-1\}|=$$
$$\phi(n/d),$$

其中 $\phi(m)=m(1-1/p_1)(1-1/p_2)\cdots(1-1/p_q)$, $(m=p_1^{i_1}p_2^{i_2}\cdots p_q^{i_q}$，$p_i$ 是素数，$1\leqslant i\leqslant q)$ 为 $1,2,\cdots,m$ 中与 m 互素的数的个数. $\forall i\in Q_d$，由引理 3 知置换 σ^i 的型为 $(n/d)^d$. 由引理 2 知其周期增长率为: $C(\sigma^i)=(1/n)(n/d)^2d=n/d$. 因

$$C(C_n)=\sum_{i=0}^{n-1}P(\sigma^i)C(\sigma^i)=(1/n)\sum_{d|n}\sum_{i\in Q_d}C(\sigma^i)=$$
$$\frac{1}{n}\sum_{d|n}\frac{n}{d}\phi(\frac{n}{d})=\sum_{d|n}\frac{1}{d}\phi(\frac{n}{d}).$$

在(6)式中，$k_1k_2\cdots k_n$ 是 Q 中元素的任意一个全排列，Q 上的任一个 n 长轮换都可生成 $n!$ 个不同的拟群. 在 n 次置换群中，n 长轮换共有 $(n-1)!$ 个. 每个 n 长轮换生成的拟群有 $n-1$ 个 n 长轮换和一个恒等置换. 所以由 n 长轮换生成的不同 n 阶拟群共有 $n!(n-1)!/(n-1)=n!(n-2)!$ 个.

推论 **1**　设 n 是素数，σ 是 Q 上的 n 轮换. 设 $\forall\alpha\in Q$，$P(\alpha)=1/n$，$P(\sigma^i)=1/n$ $(i=0,1,\cdots,n-1)$. $(Q,*)$ 是 σ 的生成拟群，则拟群 $(Q,*)$ 的周期增长率为 $(n^2-n+1)/n$.

证明　令 $C_n=\langle\sigma\rangle$. 由定理 2 和定理 3 可知拟群 $(Q,*)$ 的周期增长率 $C(Q,*)=C(Q,*)=\phi(n)+$

$(1/n)\phi(1)=n-1+1/n=(n^2-n+1)/n$.

3 注记

由于引导元 α 的选取是随机的, 所以在引理 2, 定理 3 和推论 1 中假设 $P(\alpha)=1/n$. Markovski 等[5]给出了以下定理.

定理 4 设 $1\leqslant l\leqslant t$, $X=x_1x_2\cdots x_k\in Q^+$, $Y=E^{(t)}(X)$, 则 Y 中长度为 l 的子串(子序列)的分布是均匀的.

据此在定理 3 和推论 1 中假设置换群中每个置换的概率 $P(\sigma^i)$ 相等. 由引理 2 知任何 n 次置换的周期增长率都小于 n, 由定理 1 知, 任何 n 阶拟群的周期增长率都小于 n.

Dimitrova 等[1]对 5 至 9 阶拟群实验结果如下:

5 阶拟群: 周期增长率不小于 4.2 的有 1343 个, 约占 $2^{16}=65536$ 个的 2.05%.

6 阶拟群: 周期增长率不小于 3.5 的有 35142 个, 约占 $2^{16}=65536$ 个的 53.6%.

7 阶拟群: 周期增长率不小于 6.1 的有 272 个, 占 $2^{16}=65536$ 个的 0.42%.

8 阶拟群: 周期增长率不小于 5.2 的有 14895 个, 约占 $2^{16}=65536$ 个的 22.7%.

9 阶拟群: 周期增长率不小于 6.6 的 3712 个, 约占 $2^{16}=65536$ 个的 5.66%.

由定理 3 和推论 1 可得具有较大周期增长率的 n 阶拟群 $n!(n-2)!$ 个, $5\leqslant n\leqslant 11$ 的情形见表 2.

随着拟群阶数的增加, 定理 3 越来越显示出其相对于实验方法的优越性. 特别是当 n 为素数时, 周期增长率不小于 $n-1$. 对于 256 阶的拟群可以用型为 256^1 的置换生成 周期增长率为 $43691/256=170.668$ 的拟群 $256!254!>10^{1009}$ 个.

表 2 $5\leqslant n\leqslant 11$ 时具有较大周期增长率的 n 阶拟群个数

阶数	周期增长率	个数
5	4.2	720
6	3.5	17280
7	$6^{1/7}$	604800
8	$5^{3/8}$	2.90×10^7
9	$6^{7/9}$	1.83×10^9
10	6.3	1.46×10^{11}
11	$10^{1/11}$	1.45×10^{13}

参考文献:

[1] Dimitrova V, Markovski J. On quasigroup pseudo random sequence generator[C]//Manolopoulos Y, Spirakis P. Proc of the 1st Balkan Conference in Informatics. Thessaloniki: 2004:393-401.

[2] Gligoroski D, Markovski S, Knapskog S J. The stream cipher edon80[J]. Lecture Notes in Computer Science, 2008, 4986:152-169.

[3] 徐允庆. 图分解与带共轭性质拟群的计数[J]. 应用数学学报, 2008, 31(4):608-614.

[4] Van Lint J H, Wilson R M. A course in combinatorics[M]. Cambridge: Cambridge University Press, 1992:182-187.

[5] Markovski S, Gligoroski D, Bakeva V. Quasigroup String Processing: Part 1[C]//Proc of Maced Acad of Sci and Arts for Math and Tech Sci, 1999, 1/2:13-28.

Quasigroups Based Periodicity of Pseudo Random Sequence

LI Yan-fang, XU Yun-qing*

(Faculty of Sciences, Ningbo University, Ningbo 315211, China)

Abstract: Nonlinear pseudo random sequences based on quasigroups play an important role in cryptography. Nonlinear pseudo random sequences with large periods have more extensive applications. However, until present, the quasigroups, which generate nonlinear pseudo random sequences with large periods, can be only found by means of computerized statistical search. In this paper, we give the algebraic and combinatorial characteristics as well as the construction of quasigroups with large period growth rate.

Key words: quasigroups; pseudo random sequence; permutation group

（责任编辑 史小丽）