文章编号: 0583-1431(2021)01-0145-06 **文献标识码: A**

基于有限域中的二次特征生成的伪随机二进制格点

刘华宁 李柯瑶

西北大学数学学院 西安 710127
E-mail: hnliu@nwu.edu.cn; likeyao@stumail.nwu.edu.cn

摘 要 本文利用有限域的二次特征与乘法逆构造了大族的伪随机格点, 并研究了其密码学性质: 伪随机性、碰撞和雪崩效应.

关键词 有限域; 二次特征; 伪随机格点; 特征和
MR(2010) 主题分类 11K45, 11K38, 11T24
中图分类 O156.4

Large Family of Pseudorandom Binary Lattices by Using the Quadratic Character in Finite Fields

Hua Ning LIU Ke Yao LI

School of Mathematics, Northwest University, Xi'an 710127, *P. R. China*
E-mail: *hnliu@nwu.edu.cn*; *likeyao@stumail.nwu.edu.cn*

Abstract In this paper, we construct a large family of pseudorandom binary lattices by using the quadratic character in finite fields, and study the cryptography properties: pseudorandom measure, collision and avalanche effect.

Keywords finite field; quadratic character; pseudorandom lattice; character sum
MR(2010) Subject Classification 11K45, 11K38, 11T24
Chinese Library Classification O156.4

1 引言

Hubert, Mauduit 与 Sárközy [5] 于 2006 年开始了对伪随机二进制格点的研究. 具体来说, 设

$$I_N^n = \{\mathbf{x} = (x_1, \ldots, x_n) : x_1, \ldots, x_n \in \{0, 1, \ldots, N-1\}\}.$$

函数 $\eta(\mathbf{x}) : I_N^n \to \{-1, +1\}$ 称为 n 维二进制 N 格点, 或者简称为二进制格点. 设 $k \in \mathbb{N}$,

收稿日期: 2019-02-26; 接受日期: 2020-04-30
基金项目: 国家自然科学基金资助项目 (11571277); 陕西省自然科学基础研究计划项目 (2020JM-026)

$\mathbf{u}_i\,(i=1,\dots,n)$ 为 n 维单位向量, 其中第 i 个分量为 1 而其他分量均为 0. 定义

$$\mathbb{Q}_k(\eta)=\max_{\mathbf{B},\mathbf{d}_1,\dots,\mathbf{d}_k,\mathbf{T}}\Bigg|\sum_{j_1=0}^{t_1}\cdots\sum_{j_n=0}^{t_n}\eta\left(j_1b_1\mathbf{u}_1+\cdots+j_nb_n\mathbf{u}_n+\mathbf{d}_1\right)\times\cdots\times\eta\left(j_1b_1\mathbf{u}_1+\cdots+j_nb_n\mathbf{u}_n+\mathbf{d}_k\right)\Bigg|,$$

其中最大值取遍所有的 n 维向量 $\mathbf{B}=(b_1,\dots,b_n)$, $\mathbf{d}_1,\dots,\mathbf{d}_k$, $\mathbf{T}=(t_1,\dots,t_n)$, 此处 $t_1,\dots,t_n$ 都为非负整数, $b_1,\dots,b_n$ 为正整数, $\mathbf{d}_1,\dots,\mathbf{d}_k$ 为互不相同的整数向量, 并且所有的点 $j_1b_1\mathbf{u}_1+\cdots+j_nb_n\mathbf{u}_n+\mathbf{d}_i$ 都属于 I_N^n. 函数 $\mathbb{Q}_k(\eta)$ 称为格点 η 的 k 阶伪随机测度. 对于 n 维二进制 N 格点 η, 如果 $\mathbb{Q}_k(\eta)$ 对于较小的 k 都是 N^n 的无穷小量, 则称 η 是一个伪随机二进制格点.

基于有限域 $\mathbb{F}_p$ 上的多元多项式 $f(x_1,x_2,\dots,x_n)\in\mathbb{F}_p\,[x_1,x_2,\dots,x_n]$, 人们已经构造了一些伪随机二进制格点 [3, 4, 6]. 该领域的研究需要使用多变量多项式的特征和与指数和的估计, 这在数论中是很困难的领域, 因此这方面进展缓慢. 另一方面, 利用有限域的二次特征也可构造伪随机二进制格点. 例如令 $p>2$ 为素数, $q=p^n$ 且 $\mathbb{F}_q$ 为有限域, $v_1,\dots,v_n$ 为 $\mathbb{F}_q$ 到 $\mathbb{F}_p$ 的一组基. Mauduit 与 Sárközy [7] 证明了如下结论.

命题 1.1 设 γ 为 $\mathbb{F}_q$ 的二次特征, $f(x)\in\mathbb{F}_q[x]$, $0<\deg(f)<p$ 且 $f(x)$ 在 $\overline{\mathbb{F}}_q$ 中没有重根. 定义

$$\eta(x_1,\dots,x_n)=\begin{cases}\gamma(f(x_1v_1+\cdots+x_nv_n)), & \text{如果 } f(x_1v_1+\cdots+x_nv_n)\neq 0,\\ +1, & \text{如果 } f(x_1v_1+\cdots+x_nv_n)=0.\end{cases}$$

当 $k=2$ 或者 $4^{n(\deg(f)+k)}<p$ 时, 有

$$\mathbb{Q}_k(\eta)<k\deg(f)(q^{\frac12}\,(\log p+1)^n+2).$$

Mérai [10] 利用一般的乘法特征推广了上面的格点. 此外基于有限域中的特殊子集, 文 [2] 和 [8] 中分别给出了大族的伪随机二进制格点. 本文将利用有限域的二次特征和乘法逆进一步构造大族的伪随机格点, 并研究其伪随机性、碰撞和雪崩效应.

定理 1.2 设 γ 为 $\mathbb{F}_q$ 的二次特征, $f(x)\in\mathbb{F}_q[x]$. 定义

$$\eta(\mathbf{x})=\eta\left(x_1,x_2,\dots,x_n\right)=\begin{cases}\gamma((x_1v_1+\cdots+x_nv_n)^2f(x_1v_1+\cdots+x_nv_n)+(x_1v_1+\cdots+x_nv_n)),\\ \quad\text{若 } (x_1v_1+\cdots+x_nv_n)^2f(x_1v_1+\cdots+x_nv_n)+(x_1v_1+\cdots+x_nv_n)\neq 0,\\ 1,\quad\text{若 } (x_1v_1+\cdots+x_nv_n)^2f(x_1v_1+\cdots+x_nv_n)+(x_1v_1+\cdots+x_nv_n)=0.\end{cases}$$

假设多项式 $xf(x)+1$ 在 $\mathbb{F}_q$ 没有零点, 则有

$$\mathbb{Q}_k(\eta)\ll k(\deg(f)+2)q^{\frac12}(1+\log p)^n.$$

注意到当 $q\equiv 3\pmod 4$ 时, -1 是 $\mathbb{F}_q$ 中的非平凡元. 由定理 1.2 可得下面的推论.

推论 1.3 设 $q\equiv 3\pmod 4$, γ 为 $\mathbb{F}_q$ 的二次特征, $f(x)=xg^2(x)$, 其中 $g(x)\in\mathbb{F}_q[x]$ 是任意多项式. 定义

$$\eta(\mathbf{x})=\eta\left(x_1,x_2,\dots,x_n\right)=\begin{cases}\gamma((x_1v_1+\cdots+x_nv_n)^2f(x_1v_1+\cdots+x_nv_n)+(x_1v_1+\cdots+x_nv_n)),\\ \quad\text{若 } (x_1v_1+\cdots+x_nv_n)^2f(x_1v_1+\cdots+x_nv_n)+(x_1v_1+\cdots+x_nv_n)\neq 0,\\ 1,\quad\text{若 } (x_1v_1+\cdots+x_nv_n)^2f(x_1v_1+\cdots+x_nv_n)+(x_1v_1+\cdots+x_nv_n)=0,\end{cases}$$

则有 $\mathbb{Q}_k(\eta)\ll k(\deg(f)+2)q^{\frac12}\,(1+\log p)^n$.

注 1.4 本文构造的大族格点, 所基于的多项式集合与命题 1.1 中是不相同的, 并且定理 1.2 对于伪随机测度的阶 k 没有限制条件. 因此本文是对文献 [7] 以及相关领域的进一步发展.

2 特征和的估计与格点的伪随机性

首先引入下面的两个引理.

引理 2.1 设 χ 是有限域 $\mathbb{F}_q$ 的非平凡 d 阶乘法特征, $f(x)\in\mathbb{F}_q[x]$ 有 m 个不同的根, 且不能表为某个多项式的 d 次幂的常数倍, 则有

$$\left|\sum_{z\in\mathbb{F}_q}\chi(f(z))\right|\le(m-1)q^{\frac{1}{2}}.$$

证明 参阅文献 [11, 定理 $2C'$]. 证毕.

引理 2.2 设 $q=p^n$, $\mathbb{F}_q$ 为有限域, $v_1,\dots,v_n$ 是 $\mathbb{F}_q$ 在 $\mathbb{F}_p$ 上的一组基. 定义 $\mathbb{F}_q$ 的子集 B 为

$$B=\left\{\sum_{j=1}^{n}j_iv_i:0\le j_i\le t_i,\,0\le t_i\le p-1,\,i=1,2,\dots,n\right\}.$$

设 χ 是 $\mathbb{F}_q$ 的非平凡 d 阶乘法特征, $f(x)\in\mathbb{F}_q[x]$ 有 m 个不同的根, 且不能表为某个多项式的 d 次幂的常数倍, 则有

$$\left|\sum_{z\in B}\chi(f(z))\right|<mq^{\frac{1}{2}}(1+\log p)^n.$$

证明 这是文献 [12, 定理 2]. 证毕.

现在证明定理 1.2. 设 $b_1,\dots,b_n$ 为正整数, $\mathbf{d}_1,\dots,\mathbf{d}_k$ 为互不相同的整数向量, 并记

$$\mathbf{d}_i=(d_{i1},\dots,d_{in}),\quad i=1,2,\dots,k.$$

由 η 的定义可得

$$\begin{aligned}
&\sum_{j_1=0}^{t_1}\cdots\sum_{j_n=0}^{t_n}\eta\left(j_1b_1\mathbf{u}_1+\cdots+j_nb_n\mathbf{u}_n+\mathbf{d}_1\right)\cdots\eta\left(j_1b_1\mathbf{u}_1+\cdots+j_nb_n\mathbf{u}_n+\mathbf{d}_k\right)\\
&=\sum_{j_1=0}^{t_1}\cdots\sum_{j_n=0}^{t_n}\eta\left(j_1b_1+d_{11},\dots,j_nb_n+d_{1n}\right)\cdots\eta\left(j_1b_1+d_{k1},\dots,j_nb_n+d_{kn}\right)\\
&=\sum_{j_1=0}^{t_1}\cdots\sum_{j_n=0}^{t_n}\gamma(((j_1b_1+d_{11})v_1+\cdots+(j_nb_n+d_{1n})v_n)^2f((j_1b_1+d_{11})v_1+\cdots\\
&\qquad+(j_nb_n+d_{1n})v_n)+((j_1b_1+d_{11})v_1+\cdots+(j_nb_n+d_{1n})v_n))\\
&\times\cdots\times\gamma(((j_1b_1+d_{k1})v_1+\cdots+(j_nb_n+d_{kn})v_n)^2f((j_1b_1+d_{k1})v_1+\cdots\\
&\qquad+(j_nb_n+d_{kn})v_n)+((j_1b_1+d_{k1})v_1+\cdots+(j_nb_n+d_{kn})v_n))+O(k(\deg(f)+2)).
\end{aligned}$$

令

$$\begin{aligned}
&B=\left\{\sum_{l=1}^{n}j_l(b_lv_l):0\le j_l\le t_l,\,l=1,\dots,n\right\},\\
&z=j_1(b_1v_1)+\cdots+j_n(b_nv_n),\\
&z_i=d_{i1}v_1+\cdots+d_{in}v_n,\quad i=1,\dots,k,
\end{aligned}$$

则有

$$\sum_{j_1=0}^{t_1}\cdots\sum_{j_n=0}^{t_n}\eta(j_1b_1\mathbf{u}_1+\cdots+j_nb_n\mathbf{u}_n+\mathbf{d}_1)\cdots\eta(j_1b_1\mathbf{u}_1+\cdots+j_nb_n\mathbf{u}_n+\mathbf{d}_k)$$
$$=\sum_{z\in B}\gamma(((z+z_1)^2f(z+z_1)+(z+z_1))\cdots((z+z_k)^2f(z+z_k)+(z+z_k)))+O(k(\deg(f)+2)).$$

由于多项式 $xf(x)+1$ 在 $\mathbb{F}_q$ 没有零点, 因此 $-z_1,\ldots,-z_k$ 都是多项式 $((z+z_1)^2 f(z+z_1)+(z+z_1))\cdots((z+z_k)^2 f(z+z_k)+(z+z_k))$ 的简单零点. 再由引理 2.2 可得

$$\sum_{j_1=0}^{t_1}\cdots\sum_{j_n=0}^{t_n}\eta(j_1b_1\mathbf{u}_1+\cdots+j_nb_n\mathbf{u}_n+\mathbf{d}_1)\cdots\eta(j_1b_1\mathbf{u}_1+\cdots+j_nb_n\mathbf{u}_n+\mathbf{d}_k)$$
$$\ll k(\deg(f)+2)q^{\frac{1}{2}}(1+\log p)^n.$$

因此

$$\mathbb{Q}_k(\eta)\ll k(\deg(f)+2)q^{\frac{1}{2}}(1+\log p)^n.$$

这就证明了定理 1.2.

3 碰撞与雪崩效应

碰撞与雪崩效应是密码学中重要的概念 [9], 并在文 [1] 中以下面的方式推广到二进制格点上.

设 $N\in\mathbb{N}$, $n\in\mathbb{N}$, $\mathscr{S}$ 是给定的集合. 对任意 $s\in\mathscr{S}$ 可确定一个二进制格点

$$\eta=\eta_s:I_N^n\to\{-1,+1\},$$

并定义如下的二进制格点族:

$$\mathscr{F}=\mathscr{F}(\mathscr{S})=\{\eta_s:s\in\mathscr{S}\}.$$

定义 3.1 如果对于 $s\in\mathscr{S}$, $s'\in\mathscr{S}$, $s\neq s'$, 有 $\eta_s=\eta_{s'}$, 则称在 $\mathscr{F}=\mathscr{F}(\mathscr{S})$ 中有一个碰撞. 如果在 $\mathscr{F}=\mathscr{F}(\mathscr{S})$ 中没有碰撞, 就称 $\mathscr{F}$ 是无碰撞的.

定义 3.2 如果对于 $s\in S$, $s'\in S$, $s\neq s'$, η_s 与 $\eta_{s'}$ 至少有 $\left(\frac{1}{2}-o(1)\right)N^n$ 个元素不相同, 则称 $\mathscr{F}$ 具有强雪崩效应.

下面引入的测度有助于研究碰撞和雪崩效应.

定义 3.3 设 $N\in\mathbb{N}$, $n\in\mathbb{N}$, $\eta:I_N^n\to\{-1,+1\}$ 以及 $\eta':I_N^n\to\{-1,+1\}$, 则 η 与 η' 之间的距离 $d(\eta,\eta')$ 定义为

$$d(\eta,\eta')=|\{(x_1,\ldots,x_n):(x_1,\ldots,x_n)\in I_N^n,\,\eta(x_1,\ldots,x_n)\neq\eta'(x_1,\ldots,x_n)\}|.$$

此外 $\mathscr{F}$ 上的最小距离 $m(\mathscr{F})$ 的定义为

$$m(\mathscr{F})=\min_{\substack{s,s'\in\mathscr{S}\\ s\neq s'}}d(\eta_s,\eta_{s'}).$$

本文将进一步研究定理 1.2 中的格点族的碰撞与雪崩效应. 结论如下:

定理 3.4 设 $1\le D\le\frac{1}{2}q^{\frac{1}{2}}$, 以及

$$\mathscr{S}=\left\{f(x):f(x)\in\mathbb{F}_q[x],\,f(x)\text{的首项系数为 1 且 }1\le\deg(f)\le D\right\}.$$

定义

$$\eta_f(\mathbf{x}) = \eta_f(x_1, x_2, \ldots, x_n) = \begin{cases} \gamma\big((x_1v_1+\cdots+x_nv_n)^2 f(x_1v_1+\cdots+x_nv_n)+(x_1v_1+\cdots+x_nv_n)\big), \\ \quad \text{若 } (x_1v_1+\cdots+x_nv_n)^2 f(x_1v_1+\cdots+x_nv_n)+(x_1v_1+\cdots+x_nv_n)\neq 0, \\ 1, \quad \text{若 } (x_1v_1+\cdots+x_nv_n)^2 f(x_1v_1+\cdots+x_nv_n)+(x_1v_1+\cdots+x_nv_n)=0, \end{cases}$$

以及

$$\mathscr{F} = \mathscr{F}(\mathscr{S}) = \{\eta_f : f \in \mathscr{S}\},$$

则有

$$m(\mathscr{F}) > \frac{q}{2} - \frac{3D}{2}q^{\frac{1}{2}}.$$

显然 $\mathscr{F}$ 无碰撞的充分必要条件是 $m(\mathscr{F})>0$, 并且当

$$m(\mathscr{F}) \geq \left(\frac{1}{2} - o(1)\right)N^n$$

时, $\mathscr{F}$ 具有强雪崩效应. 由定理 3.4 可得下面的推论.

推论 3.5 当 $1 \leq D < \frac{1}{3}q^{\frac{1}{2}}$ 时, 定理 3.4 中的格点族 $\mathscr{F}$ 是无碰撞的. 此外当 $D = o(q^{\frac{1}{2}})$ 时, $\mathscr{F}$ 具有强雪崩效应.

现在证明定理 3.4. 设 $f_1, f_2 \in \mathscr{S}$ 且 $f_1 \neq f_2$, 有

$$\begin{aligned} d(\eta_{f_1}, \eta_{f_2}) &= \sum_{\substack{x_1=1 \\ \eta_{f_1}(x_1,\ldots,x_n)\neq\eta_{f_2}(x_1,\ldots,x_n)}}^{p} \cdots \sum_{x_n=1}^{p} 1 \\ &= \frac{1}{2}\sum_{x_1=1}^{p}\cdots\sum_{x_n=1}^{p}(1-\eta_{f_1}(x_1,\ldots,x_n)\eta_{f_2}(x_1,\ldots,x_n)) \\ &= \frac{q}{2} - \frac{1}{2}\sum_{x_1=1}^{p}\cdots\sum_{x_n=1}^{p}\eta_{f_1}(x_1,\ldots,x_n)\eta_{f_2}(x_1,\ldots,x_n). \end{aligned} \tag{3.1}$$

由格点的定义可得

$$\begin{aligned} &\left|\sum_{x_1=1}^{p}\cdots\sum_{x_n=1}^{p}\eta_{f_1}(x_1,\ldots,x_n)\eta_{f_2}(x_1,\ldots,x_n)\right| \\ &\leq \Bigg|\sum_{x_1=1}^{p}\cdots\sum_{x_n=1}^{p}\gamma\big((x_1v_1+\cdots+x_nv_n)^2 f_1(x_1v_1+\cdots+x_nv_n)+(x_1v_1+\cdots+x_nv_n)\big) \\ &\quad \times\gamma\big((x_1v_1+\cdots+x_nv_n)^2 f_2(x_1v_1+\cdots+x_nv_n)+(x_1v_1+\cdots+x_nv_n)\big)\Bigg| \\ &\quad + \deg(f_1)+\deg(f_2)+4 \\ &= \left|\sum_{z\in\mathbb{F}_q}\gamma\left(z^2f_1(z)+z\right)\gamma\left(z^2f_2(z)+z\right)\right| + \deg(f_1)+\deg(f_2)+4 \\ &\leq \left|\sum_{z\in\mathbb{F}_q}\gamma\left((zf_1(z)+1)(zf_2(z)+1)\right)\right| + \deg(f_1)+\deg(f_2)+4. \end{aligned} \tag{3.2}$$

注意到 f_1, f_2 都是首项系数为 1 的多项式. 假设 $(zf_1(z)+1)(zf_2(z)+1)$ 可表为某个多项式的平方, 例如

$$(zf_1(z)+1)(zf_2(z)+1) = g^2(z),$$

则必有 $g(z) = zh(z) \pm 1$, 从而

$$z^2 f_1(z) f_2(z) + z(f_1(z) + f_2(z)) = z^2 h^2(z) \pm 2zh(z),$$

可得

$$\begin{cases} f_1(z) f_2(z) = h^2(z), \\ f_1(z) + f_2(z) = \pm 2h(z). \end{cases}$$

那么有 $(f_1(z) - f_2(z))^2 = 0$, 即 $f_1(z) = f_2(z)$, 从而矛盾. 因此 $(zf_1(z)+1)(zf_2(z)+1)$ 不可能表为某个多项式的平方. 再由引理 2.1 和 (3.2) 可得

$$\begin{aligned} &\left| \sum_{x_1=1}^{p} \cdots \sum_{x_n=1}^{p} \eta_{f_1}(x_1, \ldots, x_n) \eta_{f_2}(x_1, \ldots, x_n) \right| \\ &\quad \le (\deg(f_1) + \deg(f_2) + 1)\, q^{\frac{1}{2}} + \deg(f_1) + \deg(f_2) + 4 < 3Dq^{\frac{1}{2}}. \end{aligned} \tag{3.3}$$

结合 (3.1) 和 (3.3) 有

$$d(\eta_{f_1}, \eta_{f_2}) > \frac{q}{2} - \frac{3D}{2} q^{\frac{1}{2}}.$$

因此

$$m(\mathscr{F}) > \frac{q}{2} - \frac{3D}{2} q^{\frac{1}{2}}.$$

定理 3.4 证毕.

参 考 文 献

[1] Gyarmati K., Mauduit C., Sárközy A., Measures of pseudorandomness of families of binary lattices, I (Definitions, a construction using quadratic characters), *Publ. Math. Debrecen*, 2011, **79**(3–4): 445–460.

[2] Gyarmati K., Mauduit C., Sárközy A., Measures of pseudorandomness of families of binary lattices, II (A further construction), *Publ. Math. Debrecen*, 2012, **80**(3–4): 479–502.

[3] Gyarmati K., Sárközy A., Stewart C. L., On Legendre symbol lattices, *Unif. Distrib. Theory*, 2009, **4**(1): 81–95.

[4] Gyarmati K., Sárközy A., Stewart C. L., On Legendre symbol lattices, II, *Unif. Distrib. Theory*, 2013, **8**(1): 47–65.

[5] Hubert P., Mauduit C., Sárközy A., On pseudorandom binary lattices, *Acta Arith.*, 2006, **125**(1): 51–62.

[6] Liu H., Large families of pseudorandom binary lattices by using the multiplicative inverse modulo p, *Int. J. Number Theory*, 2019, **15**(3): 527–546.

[7] Mauduit C., Sárközy A., On large families of pseudorandom binary lattices, *Unif. Distrib. Theory*, 2007, **2**(1): 23–37.

[8] Mauduit C., Sárközy A., Construction of pseudorandom binary lattices by using the multiplicative inverse, *Monatsh. Math.*, 2008, **153**(3): 217–231.

[9] Menezes A. J., van Oorschot P. C., Vanstone S. A., Handbook of Applied Cryptography, CRC Press, Boca Raton, 1996.

[10] Mérai L., Construction of pseudorandom binary lattices based on multiplicative characters, *Period. Math. Hungar.*, 2009, **59**(1): 43–51.

[11] Schmidt W. M., Equations over Finite Fields, Lecture Notes in Mathematics, Vol. 536, Springer, Berlin, 1976.

[12] Winterhof A., Some estimates for character sums and applications, *Des. Codes Cryptogr.*, 2001, **22**(2): 123–131.