Vol. 28 (2018)
No. 1

数 学 杂 志
J. of Math. (PRC)

基于伪随机子集生成的 Boolean 函数

刘华宁, 陈晓林
(西北大学数学学院, 陕西 西安 710127)

摘 要: 本文基于有限域中的伪随机子集, 构造了大族 Boolean 函数并研究了其性质. 利用有限域中特征和估计的方法, 分析了 Boolean 函数的非线性, 平均灵敏度与稀疏性, 给出了估计式. 推广并改进了相关领域的已有结果.

关键词: Boolean 函数; 最大 Fourier 系数; 非线性; 平均灵敏度; 稀疏性

MR(2010) **主题分类号**: 94C10; 94A60; 11T71; 11T24 **中图分类号**: TN918.1; O156.4

文献标识码: A **文章编号**: 0255-7797(2018)01-0167-10

1 引言

Boolean 函数在流密码, 分组密码以及散列函数的研究中起着重要作用. 为了研究 Boolean 函数, 人们提出了许多有关 Boolean 函数的密码学指标.

设 $\mathbb{F}_2$ 是一个二元域, $\mathbb{F}_2^n$ 是 $\mathbb{F}_2$ 上的一个 n 维线性空间, 所谓 n 元 Boolean 函数 $B(x_1,\cdots,x_n)$ 是指从 $\mathbb{F}_2^n$ 到 $\mathbb{F}_2$ 的一个映射. 设 $\mathbf{x}=(x_1,\cdots,x_n)$, $\mathbf{a}=(a_1,\cdots,a_n)\in\mathbb{F}_2^n$, 则 $\langle\mathbf{a},\mathbf{x}\rangle=a_1x_1+\cdots+a_nx_n$ 表示通常的内积. Boolean 函数 $B(x_1,\cdots,x_n)$ 的最大 Fourier 系数 $\widehat{B}(\mathbf{a})$ 定义为

$$\widehat{B}(\mathbf{a})=\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{B(\mathbf{x})+\langle\mathbf{a},\mathbf{x}\rangle}.$$

Boolean 函数 $B(x_1,\cdots,x_n)$ 的非线性定义如下

$$nl(B)=2^{n-1}-\frac{1}{2}\max_{\mathbf{a}\in\mathbb{F}_2^n}\left|\widehat{B}(\mathbf{a})\right|.$$

每一个 Boolean 函数都可以唯一地表示成多项式的形式, 称为 Boolean 函数的代数正规型

$$B(x_1,\cdots,x_n)=\sum_{I\subseteq\{1,2,\cdots,n\}}a_I\prod_{i\in I}x_i,\qquad a_I\in\mathbb{F}_2.$$

Boolean 函数的稀疏性 $\mathrm{spr}(B)$ 是代数正规型中非零系数单项式的个数. 此外 Boolean 函数的平均灵敏度 $\sigma_{av}(B)$ 定义如下

$$\sigma_{av}(B)=2^{-n}\sum_{\mathbf{a}\in\mathbb{F}_2^n}\sum_{i=1}^{n}\left|B(\mathbf{a})-B(\mathbf{a}^{(i)})\right|,$$

*收稿日期: 2016-05-13 接收日期: 2016-10-27
基金项目: 国家自然科学基金资助 (11571277); 陕西省青年科技新星项目资助 (2014KJXX-61); 陕西省自然科学基金资助 (2014JM1007); 陕西省工业科技攻关项目资助 (2016GY-080; 2016GY-077).
作者简介: 刘华宁 (1979–), 男, 湖南永州, 教授, 主要研究方向: 数论及其应用.

其中 $\mathbf{a}^{(i)}$ 是 $\mathbf{a}$ 改变第 i 个坐标后所得的向量.

近几年来, 一些密码学研究者从数论的角度出发构造了许多具有 "好" 的密码学性质的 Boolean 函数. 例如, Coppersmith 与 Shparlinski [1] 利用模 p 的二次剩余构造了如下的 Boolean 函数.

命题 1.1 设 p 为奇素数, $s = \lfloor \log_2 p \rfloor$, 其中 $\lfloor x \rfloor$ 表示不超过 x 的最大整数. 定义 Boolean 函数为

$$B(u_1, \cdots, u_s) = \begin{cases} 0, & \text{如果 } u_1 + u_2 \cdot 2 + \cdots + u_s \cdot 2^{s-1} \text{ 是 } \mathbb{F}_p \text{ 上的二次剩余}, \\ 1, & \text{如果 } u_1 + u_2 \cdot 2 + \cdots + u_s \cdot 2^{s-1} \text{ 是 } \mathbb{F}_p \text{ 上的二次非剩余}, \end{cases} \tag{1.1}$$

其中 $u_j \in \{0, 1\}$ 且 $1 \le j \le s$. 则有

$$\mathrm{spr}(B) \ge 2^{-\frac{3}{2}} p^{\frac{1}{4}} (\log_2 p)^{-\frac{1}{2}} - 1, \ \ \sigma_{av}(B) \ge 0.5s + o(s).$$

Lange 与 Winterhof [2] 将上述命题进行了推广.

命题 1.2 设 p 为奇素数, $\mathbb{F}_q$ 是阶为 $q = p^r (r \ge 1)$ 的有限域, $\beta_0, \cdots, \beta_{r-1}$ 是 $\mathbb{F}_q$ 在 $\mathbb{F}_p$ 上的一组基, $s = \lfloor \log_2 p \rfloor$. 定义 Boolean 函数如下

$$\begin{aligned} & B(u_{11}, \cdots, u_{1s}, \cdots, u_{r1}, \cdots, u_{rs}) \\ = & \begin{cases} 0, & \text{如果} k_0\beta_0 + \cdots + k_{r-1}\beta_{r-1} \text{ 是}\mathbb{F}_q \text{ 上的平方}, \\ 1, & \text{如果} k_0\beta_0 + \cdots + k_{r-1}\beta_{r-1} \text{ 是 } \mathbb{F}_q \text{ 上的非平方}, \end{cases} \end{aligned} \tag{1.2}$$

其中 $k_{i-1} = u_{i1} + u_{i2} \cdot 2 + \cdots + u_{is} \cdot 2^{s-1}$, $u_{ij} \in \{0, 1\}$ 且 $1 \le j \le s$, $1 \le i \le r$. 则有

$$\mathrm{spr}(B) \ge \left(2^{-\frac{3}{2}} \left(3^{\frac{1}{r}} + r \right)^{-\frac{1}{2}} p^{\frac{1}{4}} \right)^r - 1.$$

随后文献 [3] 进一步研究了命题 1.2 中 Boolean 函数的性质, 得到了以下结果.

命题 1.3 设 p, r, s, B 如以上命题所定义. 则有

$$\begin{aligned} & \max_{\mathbf{a} \in \mathbb{F}_2^{rs}} \left| \widehat{B}(\mathbf{a}) \right| \le 2^{\frac{2r+3}{4}} q^{\frac{7}{8}} (\log p + 1)^{\frac{r}{4}} + 1, \\ & \sigma_{av}(B) \ge 0.5rs + o(rs). \end{aligned}$$

最近几十年来, 随着数论、组合以及相关学科的发展, 伪随机子集得到了深入的研究和广泛的应用. 许多论文都是关于这一领域的, 这些论文中提出了大量的思想、方法和工具. 1992 年, Chung 与 Graham [4] 发现整数环的子集具有一类令人惊奇的互相等价的性质, 并且如果一个子集满足这类性质中的任何一条, 则满足其余性质. Gowers [5] 对整数环的伪随机子集进行了具体的数量分析, 利用所定义的 Gowers 范数, 在整数环的子集引入了新的伪随机测度, 进而给出了 Szemerédi 定理的新证明.

伪随机子集不仅有着深刻的理论意义, 还在网络安全、密码学等领域中具有广泛的应用. 研究者发现伪随机子集可以提高密钥预分配过程的效率和安全性, 进而改善密钥管理、广播认证协议、无线传感网络的过程 (参阅文献 [6]), 另外还可用于构造匿名路径以避免路径信息被窃听 (参阅文献 [7] 与 [8]).

本文将利用伪随机子集构造大族的 Boolean 函数, 并在第 2 节到第 4 节中证明下面的结论.

定理 1.1 设 p 为奇素数, $q=p^r$, $\mathbb{F}_q$ 为有限域, $A\subset\mathbb{F}_q$ 是 $\mathbb{F}_q$ 的子集, 满足

$$0\notin A,\qquad |A|=\frac{q-1}{2}\quad 与\quad \sum_{\chi\neq\chi^0}\left|\sum_{b\in A}\chi(b)\right|=\frac{q-1}{2},$$

其中 $\sum\limits_{\chi\neq\chi^0}$ 表示对 $\mathbb{F}_q$ 的所有非平凡乘法特征求和. 设 $\beta_0,\cdots,\beta_{r-1}$ 是 $\mathbb{F}_q$ 在 $\mathbb{F}_p$ 上的一组基. 定义 $s=\lfloor\log_2 p\rfloor$, 并设 $u_{ij}\in\{0,1\}$, $1\le j\le s$, $1\le i\le r$. 记 $k_{i-1}=u_{i1}+u_{i2}\cdot 2+\cdots+u_{is}\cdot 2^{s-1}$, $1\le i\le r$. 定义

$$\begin{aligned}&B(u_{11},\cdots,u_{1s},\cdots,u_{r1},\cdots,u_{rs})\\ =&\begin{cases}0, & 如果 k_0\beta_0+\cdots+k_{r-1}\beta_{r-1}\in A,\\ 1, & 如果 k_0\beta_0+\cdots+k_{r-1}\beta_{r-1}\notin A.\end{cases}\end{aligned}\tag{1.3}$$

则有

$$\max_{\mathbf{a}\in\mathbb{F}_2^{rs}}\left|\widehat{B}(\mathbf{a})\right|\le 2^{\frac{2r+3}{4}}q^{\frac{7}{8}}(\log p+1)^{\frac{r}{4}}-\frac{1}{2^{\frac{8r+3}{4}}}q^{\frac{5}{8}}(\log p+1)^{\frac{3r}{4}},\tag{1.4}$$

$$nl(B)\ge\frac{q}{2^{r+1}}-2^{\frac{2r-1}{4}}q^{\frac{7}{8}}(\log p+1)^{\frac{r}{4}}+\frac{1}{2^{\frac{8r+7}{4}}}q^{\frac{5}{8}}(\log p+1)^{\frac{3r}{4}},\tag{1.5}$$

$$\mathrm{spr}(B)\ge 2^{-\frac{3}{2}r}q^{\frac{1}{4}}(\log p+1)^{-\frac{r}{2}}-1,\tag{1.6}$$

$$\sigma_{av}(B)\ge 0.5rs+o(rs).\tag{1.7}$$

注 设 p 为奇素数, $q=p^r$, $\mathbb{F}_q$ 为有限域. 定义 $A=\{a:\ a\in\mathbb{F}_q,\ a\ 是\ \mathbb{F}_q\ 上的平方\}$. 不难证明

$$0\notin A,\qquad |A|=\frac{q-1}{2}\quad 与\quad \sum_{\chi\neq\chi^0}\left|\sum_{b\in A}\chi(b)\right|=\frac{q-1}{2}.$$

因此本文是对文献 [2] 与 [3] 的推广.

2 最大 Fourier 系数与非线性

首先介绍下面的引理.

引理 2.1 设 p 为奇素数, $q=p^n$, χ 为有限域 $\mathbb{F}_q$ 上的 $d\,(d>1)$ 阶乘法特征, $v_1,\cdots,v_n$ 是 $\mathbb{F}_q$ 在 $\mathbb{F}_p$ 上的一组基. 设 $f(x)\in\mathbb{F}_q[x]$ 不能表为 $\mathbb{F}_q$ 上任何多项式的 d 次幂的常数倍, 且在它的分裂域中有 m 个不同的根. 定义

$$B=\left\{\sum_{i=1}^{n}j_iv_i:0\le j_i\le t_i,\ i=1,2,\cdots,n\right\},$$

其中 $t_1,\cdots,t_n$ 是非负整数且 $t_1<p,\cdots,t_n<p$. 则有

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

证 参阅文献 [9] 中的定理 2.

现在考虑 Boolean 函数的最大 Fourier 系数. 设 $z \in \mathbb{F}_q^*$, 易证

$$\frac{2}{q-1}\sum_{b\in A}\sum_{\chi}\chi(z)\chi\left(b^{-1}\right)-1=\begin{cases}1, & \text{当 } z\in A,\\ -1, & \text{当 } z\notin A.\end{cases}$$

记 $k_{i-1}=u_{i1}+u_{i2}\cdot 2+\cdots+u_{is}\cdot 2^{s-1}$, 其中 $u_{ij}\in\{0,1\}$, $1\le j\le s$, $1\le i\le r$. 定义

$$\mathcal{H}_{2^s}=\left\{k_0\beta_0+\cdots+k_{r-1}\beta_{r-1}:0\le k_{i-1}\le 2^s-1,\ i=1,\cdots,r\right\}.$$

对于任意 $\mathbf{a}\in\mathbb{F}_2^{rs}$, 可得

$$\begin{aligned}\widehat{B}(\mathbf{a}) &= \sum_{\mathbf{x}\in\mathbb{F}_2^{rs}}(-1)^{B(\mathbf{x})+\langle\mathbf{a},\mathbf{x}\rangle}=\sum_{z\in\mathcal{H}_{2^s}^*}\left(\frac{2}{q-1}\sum_{b\in A}\sum_{\chi}\chi(z)\chi\left(b^{-1}\right)-1\right)\cdot(-1)^{\langle z,\mathbf{a}\rangle}-1\\ &= \sum_{z\in\mathcal{H}_{2^s}^*}\left(\frac{2}{q-1}\sum_{b\in A}\sum_{\chi\neq\chi^0}\chi(z)\chi\left(b^{-1}\right)\right)\cdot(-1)^{\langle z,\mathbf{a}\rangle}-1\\ &= \frac{2}{q-1}\sum_{\chi\neq\chi^0}\left(\sum_{b\in A}\chi\left(b^{-1}\right)\right)\sum_{z\in\mathcal{H}_{2^s}^*}\chi(z)(-1)^{\langle z,\mathbf{a}\rangle}-1,\end{aligned}$$

其中 $z=k_0\beta_0+\cdots+k_{r-1}\beta_{r-1}$, $k_{i-1}=u_{i1}+u_{i2}\cdot 2+\cdots+u_{is}\cdot 2^{s-1}$, $1\le i\le r$, 且

$$\langle z,\mathbf{a}\rangle=\langle(u_{11},\cdots,u_{1s},\cdots,u_{r1},\cdots,u_{rs}),\mathbf{a}\rangle.$$

令 $S(\mathbf{a})=\sum\limits_{z\in\mathcal{H}_{2^s}}\chi(z)(-1)^{\langle z,\mathbf{a}\rangle}$, 可得

$$\left|\widehat{B}(\mathbf{a})\right| \le \frac{2}{q-1}\sum_{\chi\neq\chi^0}\left|\sum_{b\in A}\chi\left(b^{-1}\right)\right|\cdot|S(\mathbf{a})|+1. \tag{2.1}$$

根据文献 [3] 中的方法, 设 x 是一个整数且 $1<x<s$, 则有

$$\begin{aligned}k_{i-1} &= u_{i1}+u_{i2}\cdot 2+\cdots+u_{is}\cdot 2^{s-1}\\ &= u_{i1}+u_{i2}\cdot 2+\cdots+u_{ix}\cdot 2^{x-1}+u_{i(x+1)}\cdot 2^x+u_{i(x+2)}\cdot 2^{x+1}+\cdots+u_{is}\cdot 2^{s-1}\\ &= u_{i1}+u_{i2}\cdot 2+\cdots+u_{ix}\cdot 2^{x-1}+2^x\left(u_{i(x+1)}+u_{i(x+2)}\cdot 2+\cdots+u_{is}\cdot 2^{s-x-1}\right).\end{aligned}$$

显然任意 $z\in\mathcal{H}_{2^s}$ 都能唯一地表为 $z=y+w$, 其中 $y\in\mathcal{H}_{2^x}$, 且

$$w\in 2^x\mathcal{H}_{2^{s-x}} = \left\{2^x\left(k_0\beta_0+\cdots+k_{r-1}\beta_{r-1}\right):0\le k_{i-1}\le 2^{s-x}-1, i=1,\cdots,r\right\}.$$

定义

$$\begin{aligned}\mathbf{a} &= (a_{11},\cdots,a_{1s},\cdots,a_{r1},\cdots,a_{rs}),\\ \mathbf{b} &= (a_{11},\cdots,a_{1x},\cdots,a_{r1},\cdots,a_{rx}),\\ \mathbf{c} &= \left(a_{1(x+1)},\cdots,a_{1s},\cdots,a_{r(x+1)},\cdots,a_{rs}\right).\end{aligned}$$

易知 $\langle z,\mathbf{a}\rangle=\langle y,\mathbf{b}\rangle+\langle w,\mathbf{c}\rangle$. 由 Cauchy-Schwarz 不等式有

$$\begin{aligned}
|S(\mathbf{a})|^2 &= \left|\sum_{y\in\mathcal{H}_{2^x}}\sum_{w\in 2^x\mathcal{H}_{2^{s-x}}}\chi(y+w)(-1)^{\langle y,\mathbf{b}\rangle+\langle w,\mathbf{c}\rangle}\right|^2\\
&\le \left(\sum_{y\in\mathcal{H}_{2^x}}\left|\sum_{w\in 2^x\mathcal{H}_{2^{s-x}}}\chi(y+w)(-1)^{\langle w,\mathbf{c}\rangle}\right|\right)^2\\
&\le 2^{rx}\sum_{y\in\mathcal{H}_{2^x}}\left|\sum_{w\in 2^x\mathcal{H}_{2^{s-x}}}\chi(y+w)(-1)^{\langle w,\mathbf{c}\rangle}\right|^2\\
&= 2^{rx}\sum_{y\in\mathcal{H}_{2^x}}\sum_{w_1\in 2^x\mathcal{H}_{2^{s-x}}}\sum_{w_2\in 2^x\mathcal{H}_{2^{s-x}}}\chi\left((y+w_1)(y+w_2)\right)\cdot(-1)^{\langle w_1,\mathbf{c}\rangle+\langle w_2,\mathbf{c}\rangle}\\
&\le 2^{rx}\sum_{w_1\in 2^x\mathcal{H}_{2^{s-x}}}\sum_{w_2\in 2^x\mathcal{H}_{2^{s-x}}}\left|\sum_{y\in\mathcal{H}_{2^x}}\chi\left((y+w_1)(y+w_2)\right)\right|\\
&\le 2^{rx+rs}+2^{rx}\sum_{\substack{w_1\in 2^x\mathcal{H}_{2^{s-x}}\\ w_1\ne w_2}}\sum_{w_2\in 2^x\mathcal{H}_{2^{s-x}}}\left|\sum_{y\in\mathcal{H}_{2^x}}\chi\left((y+w_1)(y+w_2)\right)\right|.
\end{aligned}$$

再由引理 2.1 可得

$$\begin{aligned}
|S(\mathbf{a})|^2 &< 2^{rx+rs}+2^{rx}\cdot 2^{r(s-x)}\left(2^{r(s-x)}-1\right)\cdot 2q^{\frac{1}{2}}\left(1+\log p\right)^r\\
&= 2^{rx+rs}+2^{2rs-rx}\cdot 2q^{\frac{1}{2}}\left(1+\log p\right)^r-2^{rs}\cdot 2q^{\frac{1}{2}}\left(1+\log p\right)^r.
\end{aligned}$$

设实数 x_0 满足

$$2^{rx_0+rs}=2^{2rs-rx_0}\cdot 2q^{\frac{1}{2}}\left(1+\log p\right)^r. \quad \text{即} \quad 2^{rx_0}=2^{\frac{rs}{2}}2^{\frac{1}{2}}q^{\frac{1}{4}}\left(1+\log p\right)^{\frac{r}{2}}.$$

并取 $x=\lfloor x_0\rfloor+1$, 有

$$\begin{aligned}
|S(\mathbf{a})|^2 &< 2\cdot 2^{rx+rs}-2^{rs}\cdot 2q^{\frac{1}{2}}\left(1+\log p\right)^r<2\cdot 2^{r(x_0+1)+rs}-2^{rs}\cdot 2q^{\frac{1}{2}}\left(1+\log p\right)^r\\
&= 2^{r+\frac{3}{2}}2^{\frac{3rs}{2}}q^{\frac{1}{4}}\left(1+\log p\right)^{\frac{r}{2}}-2^{rs+1}q^{\frac{1}{2}}\left(1+\log p\right)^r\\
&\le 2^{r+\frac{3}{2}}q^{\frac{7}{4}}\left(1+\log p\right)^{\frac{r}{2}}-\frac{1}{2^{r-1}}q^{\frac{3}{2}}\left(1+\log p\right)^r. \qquad (2.2)
\end{aligned}$$

结合 (2.1) 与 (2.2) 式可得

$$\left|\widehat{B}(\mathbf{a})\right| \le \sqrt{2^{r+\frac{3}{2}}q^{\frac{7}{4}}\left(1+\log p\right)^{\frac{r}{2}}-\frac{1}{2^{r-1}}q^{\frac{3}{2}}\left(1+\log p\right)^r}+1.$$

注意到

$$\begin{aligned}
&2^{\frac{2r+3}{4}}q^{\frac{7}{8}}\left(\log p+1\right)^{\frac{r}{4}}-\sqrt{2^{\frac{2r+3}{2}}q^{\frac{7}{4}}\left(\log p+1\right)^{\frac{r}{2}}-\frac{1}{2^{r-1}}q^{\frac{3}{2}}\left(1+\log p\right)^r}-1\\
\ge\ &\frac{1}{2^{\frac{8r+3}{4}}}q^{\frac{5}{8}}\left(\log p+1\right)^{\frac{3r}{4}},
\end{aligned}$$

因此

$$\begin{aligned}\left|\widehat{B}(\mathbf{a})\right| &\leq \sqrt{2^{r+\frac{3}{2}}q^{\frac{7}{4}}\left(1+\log p\right)^{\frac{r}{2}}-\frac{1}{2^{r-1}}q^{\frac{3}{2}}\left(1+\log p\right)^{r}}+1\\ &\leq 2^{\frac{2r+3}{4}}q^{\frac{7}{8}}\left(\log p+1\right)^{\frac{r}{4}}-\frac{1}{2^{\frac{8r+3}{4}}}q^{\frac{5}{8}}\left(\log p+1\right)^{\frac{3r}{4}}.\end{aligned}$$

这就证明了 (1.4) 式. 又由于 $s=\lfloor\log_2 p\rfloor>\log_2 p-1$, 则有

$$\begin{aligned}nl(B) &= 2^{rs-1}-\frac{1}{2}\max_{\mathbf{a}\in\mathbb{F}_2^{rs}}\left|\widehat{B}(\mathbf{a})\right|\\ &> 2^{r\log_2 p-r-1}-2^{\frac{2r-1}{4}}q^{\frac{7}{8}}\left(\log p+1\right)^{\frac{r}{4}}+\frac{1}{2^{\frac{8r+7}{4}}}q^{\frac{5}{8}}\left(\log p+1\right)^{\frac{3r}{4}}\\ &= \frac{q}{2^{r+1}}-2^{\frac{2r-1}{4}}q^{\frac{7}{8}}\left(\log p+1\right)^{\frac{r}{4}}+\frac{1}{2^{\frac{8r+7}{4}}}q^{\frac{5}{8}}\left(\log p+1\right)^{\frac{3r}{4}}.\end{aligned}$$

从而可得 (1.5) 式.

3 稀疏性

设整数 a 满足 $2^a>(\mathrm{spr}(B)+1)^{\frac{1}{r}}\geq 2^{a-1}$. 令 $\mathcal{M}=\{0,\cdots,2^a-1\}^r\setminus\{(0,\cdots,0)\}$, 对每一个 $\underline{m}=(m_1,\cdots,m_r)\in\mathcal{M}$, 定义函数

$$\begin{aligned}&B_{\underline{m}}(u_{11},\cdots,u_{1(s-a)},\cdots,u_{r1},\cdots,u_{r(s-a)})\\ =\ &B(u_{11},\cdots,u_{1(s-a)},m_{11},\cdots,m_{1a},\cdots,u_{r1},\cdots,u_{r(s-a)},m_{r1},\cdots,m_{ra}),\end{aligned}$$

其中 $m_i=m_{i1}+\cdots+m_{ia}2^{a-1}$, $m_{ij}\in\{0,1\}$, $1\leq j\leq a$, $1\leq i\leq r$. 对于定义在 $u_{11},\cdots,u_{1(s-a)},\cdots,u_{r1},\cdots,u_{r(s-a)}$ 的所有 $B_{\underline{m}}$ 中, 不同单项式的个数不超过 $\mathrm{spr}(B)$. 注意到 $|\mathcal{M}|=2^{ar}-1>\mathrm{spr}(B)$, 则可以找到非平凡的线性组合, 使得

$$\sum_{\underline{m}\in\mathcal{M}}c_{\underline{m}}B_{\underline{m}}(u_{11},\cdots,u_{1(s-a)},\cdots,u_{r1},\cdots,u_{r(s-a)})=0,\qquad c_{\underline{m}}\in\mathbb{F}_2.$$

定义

$$\begin{aligned}&\mathcal{H}_{2^{s-a}}=\left\{k_0\beta_0+\cdots+k_{r-1}\beta_{r-1}:0\leq k_{i-1}\leq 2^{s-a}-1,i=1,\cdots,r\right\},\\ &2^{s-a}\mathcal{H}_{2^a}=\left\{2^{s-a}\left(k_0\beta_0+\cdots+k_{r-1}\beta_{r-1}\right):0\leq k_{i-1}\leq 2^a-1,i=1,\cdots,r\right\}.\end{aligned}$$

容易证明

$$\begin{aligned}&c_{\underline{m}}B_{\underline{m}}(u_{11},\cdots,u_{1(s-a)},\cdots,u_{r1},\cdots,u_{r(s-a)})\\ =\ &c_{\underline{m}}B(u_{11},\cdots,u_{1(s-a)},m_{11},\cdots,m_{1a},\cdots,u_{r1},\cdots,u_{r(s-a)},m_{r1},\cdots,m_{ra})\\ =\ &c_wB\left(y+w\right),\end{aligned}$$

其中 $y\in\mathcal{H}_{2^{s-a}}$, $w\in 2^{s-a}\mathcal{H}_{2^a}\setminus\{0\}$, 且 $\underline{m}\in\mathcal{M}$ 与 $w\in 2^{s-a}\mathcal{H}_{2^a}\setminus\{0\}$ 是一一对应的.

定义

$$\mathcal{N}=\left\{w\in 2^{s-a}\mathcal{H}_{2^a}\setminus\{0\}:\text{与 }w\text{ 对应的 }\underline{m}\text{ 满足 }c_{\underline{m}}=1\right\},$$

以及 $L=|\mathcal{N}|$. 则有

$$\begin{aligned}
2^{(s-a)r} &= \sum_{u_{11}=0}^{1}\cdots\sum_{u_{1(s-a)}=0}^{1}\cdots\sum_{u_{r1}=0}^{1}\cdots\sum_{u_{r(s-a)}=0}^{1}1\\
&= \sum_{u_{11}=0}^{1}\cdots\sum_{u_{1(s-a)}=0}^{1}\cdots\sum_{u_{r1}=0}^{1}\cdots\sum_{u_{r(s-a)}=0}^{1}(-1)^{\sum\limits_{\underline{m}\in\mathcal{M}}c_{\underline{m}}B_{\underline{m}}(u_{11},\cdots,u_{1(s-a)},\cdots,u_{r1},\cdots,u_{r(s-a)})}\\
&= \sum_{y\in\mathcal{H}_{2^{s-a}}}(-1)^{\sum\limits_{w\in\mathcal{N}}B(y+w)}=\sum_{y\in\mathcal{H}_{2^{s-a}}}\prod_{w\in\mathcal{N}}(-1)^{B(y+w)}\\
&= \sum_{y\in\mathcal{H}_{2^{s-a}}}\prod_{w\in\mathcal{N}}\left(\frac{2}{q-1}\sum_{b\in A}\sum_{\chi}\chi(y+w)\chi\left(b^{-1}\right)-1\right)\\
&= \sum_{y\in\mathcal{H}_{2^{s-a}}}\prod_{w\in\mathcal{N}}\left(\frac{2}{q-1}\sum_{b\in A}\sum_{\chi\neq\chi^0}\chi\left(b^{-1}\right)\chi(y+w)\right).
\end{aligned}$$

为方便起见, 记 $\mathcal{N}=\{w_1,w_2,\cdots,w_L\}$. 可得

$$\begin{aligned}
2^{(s-a)r} &= \sum_{y\in\mathcal{H}_{2^{s-a}}}\left(\frac{2}{q-1}\sum_{b_1\in A}\sum_{\chi_1\neq\chi^0}\chi_1\left(b_1^{-1}\right)\chi_1(y+w_1)\right)\\
&\quad\times\cdots\times\left(\frac{2}{q-1}\sum_{b_L\in A}\sum_{\chi_L\neq\chi^0}\chi_L\left(b_L^{-1}\right)\chi_L(y+w_L)\right)\\
&= \frac{2^L}{(q-1)^L}\sum_{\chi_1\neq\chi^0}\sum_{b_1\in A}\chi_1\left(b_1^{-1}\right)\cdots\sum_{\chi_L\neq\chi^0}\sum_{b_L\in A}\chi_L\left(b_L^{-1}\right)\\
&\quad\times\sum_{y\in\mathcal{H}_{2^{s-a}}}\chi_1(y+w_1)\cdots\chi_L(y+w_L).
\end{aligned}$$

设 χ' 是 $\mathbb{F}_q$ 的乘法特征群的生成元, 其阶为 $q-1$, 则可把 $\chi_1,\cdots,\chi_L$ 分别写成

$$\chi_1=(\chi')^{a_1},\cdots,\chi_L=(\chi')^{a_L},$$

其中 $1\le a_1,\cdots,a_L\le q-2$. 定义

$$\chi^*=(\chi')^{(a_1,\cdots,a_L)},\quad \delta_1=\frac{a_1}{(a_1,\cdots,a_L)},\quad\cdots,\quad \delta_L=\frac{a_L}{(a_1,\cdots,a_L)},$$

则 χ^* 的阶为 $q-1$ 的大于 1 的因数, $1\le\delta_1,\cdots,\delta_L\le q-2$, 且 $(\delta_1,\cdots,\delta_L)=1$, 从而

$$\sum_{y\in\mathcal{H}_{2^{s-a}}}\chi_1(y+w_1)\cdots\chi_L(y+w_L)=\sum_{y\in\mathcal{H}_{2^{s-a}}}\chi^*\left((y+w_1)^{\delta_1}\cdots(y+w_L)^{\delta_L}\right).$$

注意到 $w_1,\cdots,w_L$ 互不相同, 且 $(\delta_1,\cdots,\delta_L)=1$. 则 $(y+w_1)^{\delta_1}\cdots(y+w_L)^{\delta_L}$ 不可能表

为某个多项式的 $d>1$ 次幂. 由引理 2.1 可得

$$\begin{aligned}\left|\sum_{y\in\mathcal{H}_{2^{s-a}}}\chi_1(y+w_1)\cdots\chi_L(y+w_L)\right| &= \left|\sum_{y\in\mathcal{H}_{2^{s-a}}}\chi^*\left((y+w_1)^{\delta_1}\cdots(y+w_L)^{\delta_L}\right)\right| \\ &< Lq^{\frac{1}{2}}\left(\log p+1\right)^r.\end{aligned}$$

因此

$$2^{(s-a)r}<Lq^{\frac{1}{2}}\left(\log p+1\right)^r\le\left(2^{ar}-1\right)q^{\frac{1}{2}}\left(\log p+1\right)^r.$$

注意到 $s=\lfloor\log_2 p\rfloor>\log_2 p-1$, 有 $2^{ar}>2^{-\frac{r}{2}}q^{\frac{1}{4}}\left(\log p+1\right)^{-\frac{r}{2}}$. 从而 $\mathrm{spr}(B)\ge\left(2^{a-1}\right)^r-1>2^{-\frac{3}{2}r}q^{\frac{1}{4}}\left(\log p+1\right)^{-\frac{r}{2}}-1$. 这就证明了 (1.6) 式.

4 平均灵敏度

令

$$M=\lfloor s^{\frac{1}{2}}\rfloor,\quad H=2M+1,\quad J=\lfloor s-s^{\frac{1}{2}}\rfloor,\quad K=2^s-H2^J.$$

并记 $B'(k)=B(u_{11},\cdots,u_{1s},\cdots,u_{r1},\cdots,u_{rs})$, 其中

$$k=k_0+k_1p+\cdots+k_{r-1}p^{r-1},\quad 0\le k_{i-1}\le p-1,\quad 1\le i\le r,$$

且

$$k_{i-1}=u_{i1}+u_{i2}\cdot 2+\cdots+u_{is}\cdot 2^{s-1},\quad u_{ij}\in\{0,1\},\quad 1\le j\le s,\quad 1\le i\le r.$$

定义

$$\mathcal{H}'_K=\left\{k_0+k_1p+\cdots+k_{r-1}p^{r-1}:0\le k_{i-1}\le K-1,i=1,\cdots,r\right\}.$$

根据文献 [3] 中的方法, 以及引理 2.1 可得

$$\begin{aligned}\sigma_{av}(B) &= 2^{-rs}\sum_{i=1}^{r}\sum_{j=1}^{s}\sum_{\substack{k\in\mathcal{H}'_{2^s}\\ B'(k)\neq B'(k^{(ij)})}}1\ge 2^{-rs}\sum_{i=1}^{r}\sum_{j=1}^{J}\sum_{\substack{k\in\mathcal{H}'_{2^s}\\ B'(k)\neq B'(k^{(ij)})}}1 \\ &= 2^{-rs}M^{-1}\left(\sum_{i=1}^{r}\sum_{j=1}^{J}\sum_{h=1}^{M}\left|\sum_{\substack{k\in\mathcal{H}'_K\\ B'(k+h2^jp^{i-1})\neq B'((k+h2^jp^{i-1})^{(ij)})}}1-\sum_{\substack{k\in\mathcal{H}'_{2^s}\\ B'(k)\neq B'(k^{(ij)})}}1\right|\right. \\ &\qquad \left.+\sum_{i=1}^{r}\sum_{j=1}^{J}\sum_{k\in\mathcal{H}'_K}\sum_{\substack{h=1\\ B'(k+h2^jp^{i-1})\neq B'((k+h2^jp^{i-1})^{(ij)})}}^{M}1\right) \\ &\ge 2^{-rs}M^{-1}(o(rJM2^{rs})+0.5JK^rrM+o(JK^rrM)) \\ &\ge 0.5rs+o(rs).\end{aligned}$$

这就证明了 (1.7) 式.

5 进一步的讨论

利用相同的方法, 还可构造范围更大的 Boolean 函数族, 并证明下面的结论.

定理 5.1 设 p 为奇素数, $q=p^r$, $\mathbb{F}_q$ 为有限域, $A\subset\mathbb{F}_q$ 是 $\mathbb{F}_q$ 的子集, 满足

$$0\notin A,\qquad |A|=\frac{q-1}{2}\quad 与\quad \sum_{\chi\neq\chi^0}\left|\sum_{b\in A}\chi(b)\right|\leq c(q-1).$$

设 $\beta_0,\cdots,\beta_{r-1}$ 是 $\mathbb{F}_q$ 在 $\mathbb{F}_p$ 上的一组基. 定义 $s=\lfloor\log_2 p\rfloor$, 并设 $u_{ij}\in\{0,1\}$, $1\leq j\leq s$, $1\leq i\leq r$. 记 $k_{i-1}=u_{i1}+u_{i2}\cdot 2+\cdots+u_{is}\cdot 2^{s-1}$, $1\leq i\leq r$. 定义

$$\begin{aligned}&B(u_{11},\cdots,u_{1s},\cdots,u_{r1},\cdots,u_{rs})\\ =&\begin{cases}0, & 如果\ k_0\beta_0+\cdots+k_{r-1}\beta_{r-1}\in A,\\ 1, & 如果\ k_0\beta_0+\cdots+k_{r-1}\beta_{r-1}\notin A.\end{cases}\end{aligned}$$

则有

$$\max_{\mathbf{a}\in\mathbb{F}_2^{rs}}\left|\widehat{B}(\mathbf{a})\right|\leq 2c\left(2^{\frac{2r+3}{4}}q^{\frac{7}{8}}(\log p+1)^{\frac{r}{4}}-\frac{1}{2^{\frac{8r+3}{4}}}q^{\frac{5}{8}}(\log p+1)^{\frac{3r}{4}}\right),\tag{5.1}$$

$$nl(B)\geq\frac{q}{2^{r+1}}-c\left(2^{\frac{2r+3}{4}}q^{\frac{7}{8}}(\log p+1)^{\frac{r}{4}}-\frac{1}{2^{\frac{8r+3}{4}}}q^{\frac{5}{8}}(\log p+1)^{\frac{3r}{4}}\right),\tag{5.2}$$

$$\mathrm{spr}(B)\gg\frac{\log q}{2^r},\tag{5.3}$$

$$\sigma_{av}(B)\geq 0.5rs+o(rs).\tag{5.4}$$

注 满足定理 5.1 中的条件的子集有很多个. 例如, 设 g 是 $\mathbb{F}_q^*$ 的生成元, 则下列子集

$$\begin{aligned}A_1&=\{g^n:1\leq n\leq q-1,n\equiv 0(\mathrm{mod}\ 2)\},\\ A_2&=\{g^n:1\leq n\leq q-1,n\equiv 1(\mathrm{mod}\ 2)\},\\ A_3&=\{g^n:1\leq n\leq q-1,n\equiv 1,2(\mathrm{mod}\ 4)\},\quad 当\ q\equiv 1(\mathrm{mod}\ 4),\\ A_4&=\{g^n:1\leq n\leq q-1,n\equiv 1,3,7,8(\mathrm{mod}\ 8)\},\quad 当\ q\equiv 1(\mathrm{mod}\ 8)\end{aligned}$$

都满足定理 5.1 的要求.

参 考 文 献

[1] Coppersmith D, Shparlinski I E. On polynominal approximation of the discrete logarithm and the Diffie-Hellman mapping[J]. J. Cryp., 2000, 13(3): 339–360.

[2] Lange T, Winterhof A. Incomplete character sums over finite fields and their application to the interpolation of the discrete logarithm by Boolean functions[J]. Acta Arith., 2002, 101(3): 223–229.

[3] Lange T, Winterhof A. Interpolation of the discrete logarithm in $\mathbb{F}_q$ by Boolean functions and by polynomials in several variables modulo a divisor of $q-1$[J]. Disc. Appl. Math., 2003, 128(1): 193–206.

[4] Chung F R K, Graham R L. Quasi-random subsets of $\mathbb{Z}_n$[J]. J. Combin. The. Ser. A, 1992, 61(1): 64–86.

[5] Gowers W T. A new proof of Szemerédi's theorem[J]. Geom. Funct. Anal., 2001, 11(3): 465–588.

[6] 苏忠, 林闯, 任丰原. 无线传感器网络中基于散列链的随机密钥预分发方案 [J]. 计算机学报, 2009, 32(1): 30–41.

[7] 夏永波. Bent 序列的构造及其相关值分布 [J]. 数学杂志, 2010, 30(4): 663–670.

[8] Xu L, Chen S, Huang X, Mu Y. Pseudonym and bloom filter based secure and anonymouse DSR protocol in wireless ad hoc network[J]. Int. J. Comput. Netw. Commun. Secur., 2010, 5(1): 35–44.

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

LARGE FAMILY OF BOOLEAN FUNCTIONS CONSTRUCTED BY USING PSEUDORANDOM SUBSETS

LIU Hua-ning, CHEN Xiao-lin

(*School of Mathematics, Northwest University, Xi'an 710127, China*)

Abstract: In this paper, we study the cryptography properties of large families of Boolean functions constructed by the pseudorandom subsets in finite fields. Using bounds on character sums over finite fields, we obtain lower bounds on the nonlinearity, average sensitivity and sparsity, which generalizes the previous results.

Keywords: Boolean function; maximum Fourier coefficient; nonlinearity; average sensitivity; sparsity

2010 MR Subject Classification: 94C10; 94A60; 11T71; 11T24