第25卷第3期 数 学 研 究 与 评 论 Vol.25, No.3
2005年8月 JOURNAL OF MATHEMATICAL RESEARCH AND EXPOSITION Aug., 2005

文章编号: 1000-341X(2005)03-0504-07 文献标识码: A

有限域上的逻辑函数与其 Chrestenson 谱的关系

滕吉红, 黄晓英, 李世取, 曾本胜
(解放军信息工程大学信息工程学院信息研究系, 河南 郑州 450002)
(E-mail: tengjihong@263.net)

摘 要: 本文首先给出了有限域上逻辑函数的 Chrestenson 线性谱的新定义 (不同于文献 [1] 所给出的), 如同 Chrestenson 循环谱 [1] 一样, 重新定义的 Chrestenson 线性谱也是有限域 F_q 到复数域的映射, 且证明了它们之间在实质意义下可以相互线性表出; 最后我们还用重新定义的 Chrestenson 线性谱给出了有限域上逻辑函数的反演公式.

关键词: Chrestenson 线性谱; Chrestenson 循环谱; 迹函数; 范得蒙矩阵.
MSC(2000): 94A60
中图分类: TN918.1

1 引 言

由于二元域上的布尔函数和其 Walsh 谱之间有一一对应的关系, 因此二元域上布尔函数的大多数性质可以通过其 Walsh 谱来刻画 [1],[2],[3]; 而素域和环 Z_m 上的逻辑函数与其 Chrestenson 谱之间也有一一对应的关系 [4], 因此研究素域和环 Z_m 上的逻辑函数的各种性质也可通过研究其 Chrestenson 谱的性质来达到, 且人们还发现布尔函数的 Walsh 线性谱和循环谱可以相互线性表出, 一般素域和环 Z_m 上逻辑函数的 Chrestenson 线性谱和循环谱也可以相互线性表出 [1],[5]. 有关结论能否推广到一般的有限域上是本文所要研究的主要问题. 文献 [1] 对有限域上的逻辑函数进行了专门的研究, 给出了有限域上逻辑函数的 Chrestenson 线性谱和循环谱的定义, 讨论了这两种谱的一些性质及其相互关系, 并利用这两种谱对有限域上的逻辑函数的平衡性、线性结构、相关免疫等性质进行了讨论, 得到了一些很好的结果, 对有限域上逻辑函数的研究是有指导意义的. 但文献 [1] 中所定义的 Chrestenson 线性谱只能理解为一种形式记号, 而无法做通常的数值解释, 因而它所给出的 Chrestenson 线性谱和循环谱的对应关系也只能理解为两种符号之间的对应, 为此我们对有限域上逻辑函数的 Chrestenson 线性谱重新给出了定义 (得到的是一组复数), 研究了我们新定义的 Chrestenson 线性谱和原有的 Chrestenson 循环谱的之间的关系 (特殊复数组之间的对应关系), 并利用有限域上迹 (trace) 函数的特殊性质, 给出了有限域上逻辑函数的反演公式的一般表示式, 特别地, 对有限域 F_4 上逻辑函数的反演公式给出了具体的表达式.

2 基本结论

下面有关有限域方面的结论见文献 [6].

以下总设 $q = p^l$, 其中 p 为素数, 有限域 F_q 为素域 F_p 的扩域, 由有限域的知识知, F_q 是 F_p 的单扩张, 即 $F_q = F_p(\alpha)$, 其中 α 是素域 F_p 上的某个代数次数为 l 的极小多项式的根, 易知 $1, \alpha, \alpha^2, \cdots, \alpha^{l-1}$ 是 F_q 在 F_p 上的一组基.

收稿日期: 2003-03-11

定义 1[6] 对任意的 $\beta \in F_q$, 称

$$\mathrm{tr}(\beta) = \beta + \beta^p + \beta^{p^2} + \cdots + \beta^{p^{l-1}}$$

为 β 在 F_p 上的迹 (trace), 并称 $\mathrm{tr}(\cdot)$ 为 F_q 在 F_p 上的迹函数.

下面我们给出有限域 F_q 上 q 值随机变量的定义：

设 $\Omega = F_q^n, \Omega$ 上的 σ- 代数取为：$F = \{A : A \subset \Omega\}$, 定义 $P(A) = \frac{|A|}{q^n}, A \subseteq F_q^n$, $|A|$ 表示 A 中所含元素的个数. 又定义 $F_q^n \to F_q$ 的 n 个映射： $X_i(x_1, x_2, \cdots, x_n) = x_i, (x_1, x_2, \cdots, x_n) \in F_q^n$, $1 \le i \le n$, 则得到概率空间 (Ω, F, P) 上的 n 个 q 值随机变量 $X_1, X_2, \cdots, X_n$. 容易验证：它们相互独立，且具有相同的分布： $P\{X_i = j\} = \frac{1}{q}, j \in F_q, 1 \le i \le n$. 对上面的 q 值随机变量 $X_1, X_2, \cdots, X_n$, 易知 $\mathrm{tr}(X_i), 1 \le i \le n$ 就是 (Ω, F, P) 上的 p 值随机变量，它们也相互独立且具有相同的分布：

$$P\{\mathrm{tr}(X_i) = j\} = \frac{1}{p}, \quad j \in F_p, \quad 1 \le i \le n.$$

文献 [1] 上给出的有限域上逻辑函数的 Chrestenson 线性谱和循环谱的定义如下：

定义 2[1] 设 $f(x), x \in F_q^n$ 为 n 元 q 值逻辑函数，则称

$$S_f(w) = \frac{1}{q^n} \sum_{x \in F_q^n} f(x) \cdot u^{-\mathrm{tr}(w \cdot x)}, \quad w \in F_q^n. \tag{1}$$

$$S_{(f)}(w) = \frac{1}{q^n} \sum_{x \in F_q^n} u^{\mathrm{tr}(f(x)) - \mathrm{tr}(w \cdot x)}, \quad w \in F_q^n \tag{2}$$

分别为 $f(x)$ 的 Chrestenson 线性谱和循环谱.

显然，对一般的有限域上的逻辑函数 $f(x)$, (1) 式所给出的 Chrestenson 线性谱只能理解为一种形式符号，因为 $f(x)$ 的取值在 F_q 中，而 u 是 p 次本原单位根， $u^{-\mathrm{tr}(wx)}$ 是在复数域中，它们之间并没有统一的运算法则. 文献 [1] 在考察有限域上 Chrestenson 线性谱和循环谱的关系时，还给出了下面的结论：

定理 1[1] 设 $f(x), x \in F_q^n$ 为 n 元 q 值逻辑函数，则由 (1) 式和 (2) 式定义的 $S_f(\cdot)$ 和 $S_{(f)}(\cdot)$ 有如下关系：

$$S_f(w) = \frac{1}{q} \sum_{i \in F_q} \sum_{k \in F_q} i \cdot u^{-\mathrm{tr}(ki)} S_{(kf)}(w), \quad w \in F_q^n; \tag{3}$$

$$S_{(f)}(w) = \sum_{k \in F_q} S_{f+k}(w)\, u^{-\mathrm{tr}(k)} / \sum_{i \in F_q} i u^{-\mathrm{tr}(i)}, \quad w \in F_q^n. \tag{4}$$

上面 (3) 式右边和式里是有限域 F_q 中元和复数在作 “运算”; 上面 (4) 式右边和式里是一些形式记号和复数在作 “运算”, “等式” 成立就意味着首先要在有限域和复数域之间以及由 (1) 式所得形式记号和复数之间 “默认” 有关的 “运算” 规则 $\cdots$, 这样做的合理性解释起来颇费周折且容易在有的情况下造成混乱，从而给研究带来不便.

基于此，我们对有限域上逻辑函数的 Chrestenson 线性谱重新定义如下：

定义 3 设 $f(x), x \in F_q^n$ 为 n 元 q 值逻辑函数，则称

$$S_f(w) = \frac{1}{q^n} \sum_{x \in F_q^n} \mathrm{tr}(f(x)) \cdot u^{-tr(w \cdot x)}, \quad w \in F_q^n \tag{5}$$

为 $f(x)$ 的 Chrestenson 线性谱.

本文中的 Chrestenson 循环谱仍采用文献 [1] 中的定义，即由上述 (2) 式定义.

易知我们定义的 Chrestenson 线性谱也具有反演公式如下：

$$\mathrm{tr}\left(f\left(x\right)\right)=\sum_{w\in F_q^n}S_f\left(w\right)\cdot u^{tr(w\cdot x)},\quad x\in F_q^n. \tag{6}$$

显然，这里新定义的 Chrestenson 线性谱和文献 [1] 所定义的 Chrestenson 循环谱都是有限域到复数域的映射，因此考察它们之间的关系是有实质意义的.

定理 2 设 $f(x),x\in F_q^n$ 为 n 元 q 值逻辑函数，则

$$S_f\left(w\right)=\frac{1}{p}\sum_{i\in F_p}\sum_{k\in F_p}i\cdot u^{-ki}S_{(kf)}\left(w\right), \tag{7}$$

$$S_{(j\cdot f)}\left(w\right)=\frac{u^{-j}-1}{p}\sum_{k\in F_p}S_{f+k\alpha^*}\left(w\right)u^{-j\cdot k},\quad j\in F_p\backslash\{0\}. \tag{8}$$

其中 $\alpha^*\in F_q$，且满足 $\mathrm{tr}(\alpha^*)=1$.

证明 对任意给定的 $w\in F_q^n$，$f(X)$ 和 $w\cdot X$ 都是上面所定义的概率空间 (Ω,F,P) 上的 q 值随机变量，易知 $S_f(w)$ 和 $S_{(f)}(w)$ 有概率表示式：

$$S_f\left(w\right)=\sum_{i\in F_p}i\sum_{j\in F_p}u^jP\left\{\mathrm{tr}\left(f\left(X\right)\right)=i,\ -\mathrm{tr}\left(w\cdot X\right)=j\right\},$$

$$S_{(f)}\left(w\right)=\sum_{i\in F_p}u^i\sum_{j\in F_p}u^jP\left\{\mathrm{tr}\left(f\left(X\right)\right)=i,\ -\mathrm{tr}\left(w\cdot X\right)=j\right\},$$

而 $\mathrm{tr}(f(X))$ 和 $\mathrm{tr}(w\cdot X)$ 都是概率空间 (Ω,F,P) 上的 p 值随机变量，所以由素域 F_p 上 Chrestenson 线性谱和循环谱的关系 [4] 可以得结论.

推论 1 设 $f(x),x\in F_q^n$ 为 n 元 q 值逻辑函数，则对任意的 $\beta\in F_q\backslash F_p$，

$$S_{\beta\cdot f}\left(w\right)=\frac{1}{p}\sum_{i\in F_p}\sum_{k\in F_p}i\cdot u^{-ki}S_{(k(\beta\cdot f))}\left(w\right), \tag{9}$$

$$S_{(\beta\cdot f)}\left(w\right)=\frac{u^{-1}-1}{p}\sum_{k\in F_p}S_{\beta\cdot f+k\alpha^*}\left(w\right)u^{-k}, \tag{10}$$

其中 $\alpha^*\in F_q$，且满足 $\mathrm{tr}(\alpha^*)=1$.

证明 只要在定理 2 中，取 $j=1$，用 $\beta f(x)$ 代替 $f(x)$ 即可得结论. □

注 (1) 在 (8) 式中，若 $q=p^l$，且 p 不整除 l，则由有限域上迹函数的性质知，$\mathrm{tr}(l^{-1})=l\cdot l^{-1}=1$，所以取 $\alpha^*=l^{-1}\in F_q$，有 $S_{(f)}\left(w\right)=\frac{u^{-j}-1}{p}\sum_{k\in F_p}S_{f+kl^{-1}}\left(w\right)u^{-k}$，这样 $f(x)$ 的 Chrestenson 循环谱可以由 $f(x)$ 与 F_p 中所有元素的 "和函数" 的 Chrestenson 线性谱来表示；

(2) 特别地，当 $l=1$ 时，(7) 式和 (8) 式就是文献 [4] 所给出环 Z_p 上的 Chrestenson 线性谱和循环谱的关系；而 $l=1,p=2$ 时就是文献 [3] 给出的 Walsh 循环谱和线性谱的关系；

(3) 对任意的 $\beta \in F_q \backslash F_p$, 由 (9) 式可以看出， $\beta f(x)$ 的线性谱可以由 $k(\beta f(x)), k \in F_q$ 的循环谱表出，且有例子表明，一般情况下 $\beta f(x)$ 的线性谱不能由 $kf(x), k \in F_p$ 的循环谱表出，对 $\beta f(x)$ 的循环谱也有类似的结论；

(4) 利用文献 [1] 中的结论，由逻辑函数的 Chrestenson 循环谱确定逻辑函数的 Chrestenson 线性谱需要 p^l 个函数的循环谱，而由我们的结果，只要 p 个函数的 Chrestenson 循环谱就可以确定出函数的 Chrestenson 线性谱，实现起来会更快；由逻辑函数的 Chrestenson 线性谱确定逻辑函数的 Chrestenson 循环谱也有同样的差别.

3 有限域上逻辑函数的反演公式

对于布尔函数和环 Z_m 上的逻辑函数而言，由于函数和谱之间有一一对应的关系，因此若知道了函数的谱值，即能通过反演公式直接求出相应的函数值. 而对于有限域上的逻辑函数 $f(x)$, 由于有限域上的迹函数具有下面的性质：

$$|T_i| = |\{x : x \in F_q, \mathrm{tr}(x) = i\}| = p^{l-1},$$

因此仅由 (6) 式右边的值无法唯一确定出 $f(x)$ 的值.

下面我们研究在什么条件下能由 Chrestenson 线性谱或循环谱唯一确定出 $f(x)$ 的值.

引理 1　设 $1, \alpha, \alpha^2, \cdots, \alpha^{l-1}$ 是 F_q 在 F_p 上的一组基，$x \in F_q$, 则对 F_p 上任一组取定的常数 $b_0, b_1, \cdots, b_{l-1}$, 方程组

$$\begin{cases} b_0 = x + x^p + x^{p^2} + \cdots + x^{p^{l-1}}, \\ b_1 = \alpha x + \alpha^p x^p + \alpha^{p^2} x^{p^2} + \cdots + \alpha^{p^{l-1}} x^{p^{l-1}}, \\ \quad \cdots \\ b_{l-1} = \alpha^{l-1} x + \alpha^{(l-1)p} x^p + \alpha^{(l-1)p^2} x^{p^2} \cdots + \alpha^{(l-1)p^{l-1}} x^{p^{l-1}}. \end{cases}$$

有唯一解，且存在 $c_i \in F_q$, 对任意的 $x \in F_q$, 使得

$$x = c_0 b_0 + c_1 b_1 + c_2 b_2 + \cdots + c_{l-1} b_{l-1}.$$

证明　由于上面方程组的系数矩阵是范得蒙 (Vandermonde) 矩阵

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha & \alpha^p & \alpha^{p^2} & \cdots & \alpha^{p^{l-1}} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \alpha^{l-1} & \alpha^{(l-1)p} & \alpha^{(l-1)p^2} & \cdots & \alpha^{(l-1)p^{l-1}} \end{bmatrix}$$

由有限域的知识 [6] 知，由于系数矩阵和增广矩阵的秩相同，因而上面的方程组有唯一解.

记行列式

$$\begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha & \alpha^p & \alpha^{p^2} & \cdots & \alpha^{p^{l-1}} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \alpha^{l-1} & \alpha^{(l-1)p} & \alpha^{(l-1)p^2} & \cdots & \alpha^{(l-1)p^{l-1}} \end{vmatrix} \triangleq d,$$

$$\begin{vmatrix} b_0 & 1 & 1 & \cdots & 1 \\ b_1 & \alpha^p & \alpha^{p^2} & \cdots & \alpha^{p^{l-1}} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ b_{l-1} & \alpha^{(l-1)p} & \alpha^{(l-1)p^2} & \cdots & \alpha^{(l-1)p^{l-1}} \end{vmatrix} \hat{=} d_1,$$

则 $x = \frac{d_1}{d}$, 而 d_1 可以按照第一列展开为:

$$d_1 = b_0 \cdot A_{01} + b_1 \cdot A_{11} + \cdots + b_{l-1} \cdot A_{l-1,1},$$

其中 $A_{i1}, 0 \le i \le l-1$, 为行列式 d_1 的第一列中的 b_i 所对应的代数余子式, 所以

$$x = \frac{d_1}{d} = \frac{b_0 \cdot A_{01} + b_1 A_{11} + \cdots + b_{l-1} \cdot A_{l-1,1}}{d},$$

再取 $c_i = \frac{A_{i1}}{d}$, $0 \le i \le l-1$, 由于代数余子式 A_{i1} 只和 F_q 在 F_p 中的基 $1, \alpha, \alpha^2, \cdots, \alpha^{l-1}$ 有关, 而与 x 无关, 所以对任意的 $x \in F_q$, 都有

$$x = c_0 b_0 + c_1 b_1 + c_2 b_2 + \cdots + c_{l-1} b_{l-1}.$$

注 从引理 1 可以看出, 由 x 可以唯一确定 $b_0, b_1, \cdots, b_{l-1}$ 中的任一个, 而由 $b_0, b_1, \cdots, b_{l-1}$ 中的一个却无法唯一确定 x, 但由全部 $b_0, b_1, \cdots, b_{l-1}$ 就可以唯一确定出 x.

下面我们给出有限域上逻辑函数 $f(x)$ 和一组逻辑函数的 Chrestenson 线性谱

$$\{S_{\alpha^j f}(w) : w \in F_q^n, j = 0, 1, \cdots, l-1\}$$

之间的关系:

定理 3 设 $f(x), x \in F_q^n$ 为 n 元 q 值逻辑函数, 则存在 $c_i \in F_q$, $0 \le i \le l-1$, 使得对任意给定的 $x_0 \in F_q^n$, 有

$$f(x_0) = \sum_{i=0}^{l-1} c_i \sum_{w \in F_q^n} S_{\alpha^i f}(w) \cdot u^{\mathrm{tr}(w \cdot x_0)}. \tag{11}$$

证明 对任意 $x_0 \in F_q^n$, 在引理 1 中用 $f(x_0)$ 代替 x, 用 $\mathrm{tr}(f(x_0)), \cdots, \mathrm{tr}(\alpha^{l-1} f(x_0))$ 代替 $b_0, b_1, \cdots, b_{l-1}$, 即有

$$f(x_0) = c_0 \mathrm{tr}(f(x_0)) + c_1 \mathrm{tr}(\alpha f(x_0)) + \cdots + c_{l-1} \mathrm{tr}\left(\alpha^{l-1} f(x_0)\right),$$

而由反演公式

$$\mathrm{tr}(f(x_0)) = \sum_{w \in F_q^n} S_f(w) \cdot u^{tr(w \cdot x_0)},$$

所以

$$f(x_0) = \sum_{i=0}^{l-1} c_i \sum_{w \in F_q^n} S_{\alpha^i f}(w) \cdot u^{\mathrm{tr}(w \cdot x_0)}.$$

定理 4 设 $f(x)$ 和 $g(x), x \in F_q^n$ 都是 n 元 q 值逻辑函数, 则

(1) $\mathrm{tr}(f(x)) \equiv \mathrm{tr}(g(x)), x \in F_q^n$ 的充分必要条件是对任意的 $w \in F_q^n$, 都有 $S_{(f)}(w) = S_{(g)}(w)$;

(2) $f(x)\equiv g(x), x\in F_q^n$ 的充分必要条件是对任意的 $0\le j\le l-1$, 以及任意的 $w\in F_q^n$, 都有 $S_{(\alpha^j f)}(w)=S_{(\alpha^j g)}(w)$.

证明 (1) 充分性由 (6) 式可知，必要性由 (2) 式可证;

(2) 充分性由 (11) 可以证明;

必要性. 由有限域上的迹函数的性质可知，$f(x)\equiv g(x), x\in F_q^n$ 的充要条件是对任意的 $0\le j\le l-1, \mathrm{tr}(\alpha^j f(x))\equiv \mathrm{tr}(\alpha^j g(x)), x\in F_q^n$. 再由

$$\begin{aligned} S_{(\alpha^j f)}(w) &= \frac{1}{q^n}\sum_{x\in F_q^n} u^{\mathrm{tr}(f(x))-\mathrm{tr}(w\cdot x)} = \frac{1}{q^n}\sum_{x\in F_q^n} u^{\mathrm{tr}\left(\alpha^j g(x)\right)-\mathrm{tr}(w\cdot x)} \\ &= S_{(\alpha^j g)}(w) \end{aligned}$$

即得必要性的证明. □

从定理 4 很容易看出，一般有限域上逻辑函数的反演公式和二元域以及素域上的反演公式是不同的，二元域 (素域) 上的逻辑函数与其 Walsh 谱 (Chrestenson 谱) 是一一对应的，但有限域上则没有此性质，一般只能说有限域上逻辑函数的迹函数与其 Chrestenson 谱是一一对应的.

对具体的有限域, 定理 3 中的 $c_i, 0\le i\le l-1$ 都可以求出, 如下面我们可以给出用 Chrestenson 线性谱反演 F_4 上逻辑函数的具体表示式:

取 $q=2^2$, 周知 F_4 为二元域 GF(2) 的二次扩域，且 x^2+x+1 是 GF(2) 上的不可约多项式, 设 α 是 $x^2+x+1=0$ 的根，则 $1,\alpha$ 是 F_4 在 GF(2) 中的一组基，F_4 即可表示为 $\{0,1,\alpha,\alpha^2\}$ 或 $\{0,1,\alpha,1+\alpha\}$.

定理 5 设 $f(x), x\in F_4^n$ 是 n 元 4 值逻辑函数，则 $f(x)$ 与其 Chrestenson 线性谱有如下的关系：对任意的 $x\in F_4^n$, 都成立

$$f(x)=\alpha^2\sum_{w\in F_4^n} S_f(w)(-1)^{\mathrm{tr}(w\cdot x)}+\sum_{w\in F_4^n} S_{\alpha f}(w)(-1)^{\mathrm{tr}(w\cdot x)}.$$

证明 因为

$$f(x)+f(x)^2=\mathrm{tr}(f(x)),\quad \alpha f(x)+\alpha^2 f(x)^2=\mathrm{tr}(\alpha f(x)),$$

所以在引理 1 中

$$d=\alpha+\alpha^2=1,\quad A_{01}=\alpha^2,\quad A_{11}=1,$$

再由定理 3 以及 (6) 式可知

$$\begin{aligned} f(x) &= \alpha^2\mathrm{tr}(f(x))+\mathrm{tr}(\alpha f(x)) \\ &= \alpha^2\sum_{w\in F_4^n} S_f(w)(-1)^{\mathrm{tr}(w\cdot x)}+\sum_{w\in F_4^n} S_{\alpha f}(w)(-1)^{\mathrm{tr}(w\cdot x)}. \end{aligned}$$

4 结束语

本文对有限域上逻辑函数的 Chrestenson 线性谱重新给出了定义，重新考查了有限域上逻辑函数新定义的线性谱和原循环谱的关系与相应素域上两种谱的关系之间的联系和区别. 定理

3 虽然只是给出了有限域上逻辑函数的 Chrestenson 线性谱和函数自身的关系，但由于这样定义的有限域上逻辑函数的 Chrestenson 线性谱和循环谱也可以相互线性表出，因此相应的结果对有限域上的逻辑函数的 Chrestenson 循环谱也成立，在这里不作详细讨论. 由于有限域上逻辑函数的许多密码学性质都可以通过其 Chrestenson 谱予以刻画，故逻辑函数谱值的计算是重要的，根据本文中 Chrestenson 线性谱的定义自然可进一步考虑其快速计算的实现问题.

参考文献:

[1] 冯登国. 频谱理论及其在密码学中的应用 [M]. 北京：科学出版社， 2000.
FENG Deng-guo. *The Application of Spectral Theory in Cryptology* [M]. Beijing: Science Publishing Company, 2000. (in Chinese)

[2] 冯登国，裴定一. 密码学导引 [M]. 北京：科学出版社， 1999.
FENG Deng-guo, PEI Ding-yi. *An Introduction to Cryptology* [M]. Beijing: Science Publishing Company, 1999. (in Chinese)

[3] 丁存生，肖国镇. 流密码学及其应用 [M]. 北京：国防工业出版社， 1994.
DING Cun-sheng, XIAO Guo-zhen. *The Application of Streanm Chipers* [M]. Beijing: National Defense Publishing Company, 1994. (in Chinese)

[4] 赵亚群，李世取. p 值逻辑函数最佳仿射逼近的谱特征谱 [J]. 工程数学学报， 1997, 4: 73–79.
ZHAO Ya-qun, LI Shi-qu. *The Spectral characteristic of BAA attack for p-valued logical functions* [J]. J. Engrg. Math., 1997, 4: 73–79. (in Chinese)

[5] 李世取，曾本胜，廉玉忠，等. 密码学中的逻辑函数 [M]. 北京中软出版公司， 2003.
LI Shi-qu, ZENG Ben-sheng, LIAN Yu-zhong. et al. *The Logical Functions in Cryptology* [M]. The Publishing Company of Software, 2003.

[6] LIDL R, NIEDERREITER H. *Finite Fields* [M]. Addison-Wesley Publishing Company, 1984.

Relations between Logical Functions and Their Chrestenson Spectrum over Finite Fields

TENG Ji-hong, HUANG Xiao-ying, LI Shi-qu, ZENG Ben-sheng
(Department of Information Research, Information Engineering University, Zhengzhou 450002, China)

Abstract: We firstly redefine the Chrestenson linear spectrum of logical functions over Finite Fields, which was ever offered in [1]. The linear spectrum proposed in this paper, as well as Chrestenson cyclic spectrum, is a mapping from Finite Fields into Complex Fields, so it is reasonable to study the relation between Chrestenson linear spectrum and Chrestenson cyclic spectrum. Finally, we show that any logical functions over finite fields can be deduced by a group of Chrestenson linear spectrum.

Key words: Chrestenson linear spectrum; Chrestenson cyclic spectrum; trace function; Vandermonde matrix.