相关免疫函数的性质和构造*)

肖 鸿[1,2] 张卫国[1] 周 宇[1] 肖国镇[1]
(西安电子科技大学综合业务网国家重点实验室 西安 710071)[1]
(空军工程大学电讯工程学院 西安 710077)[2]

摘 要 利用Walsh频谱方法给出了一个布尔函数是m阶相关免疫函数的一个充要条件，给出了几种由已知相关免疫函数构造新的相关免疫函数的方法。

关键词 布尔函数，相关免疫，Walsh谱

On the Properties and Constructions of Correlation-immune Boolean Functions

XIAO Hong[1,2] ZHANG Wei-Guo[1] ZHOU Yu[1] XIAO Guo-Zhen[1]
(State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071)[1]
(Telecommunication Engineering Institute, Air Force Engineering, Xi'an 710077)[2]

Abstract A sufficient and necessary condition that a Boolean function is m th-order correlation immune is presented by using the Walsh spectral method. We also propose some ways on constructing new correlation immune Boolean functions from old ones.

Keywords Boolean function, Correlation immune, Walsh spectral

1 引言

布尔函数及其Walsh谱，特别是其Walsh谱在密码学研究中具有重要的地位[1~3]，而相关免疫性是流密码系统抗相关分析能力的重要指标[4]，人们对其进行了大量研究，取得了一系列重要成果[3,5~7]。本文通过分析一般布尔函数的Walsh谱，得到了布尔函数相关免疫性的一个判定条件，并给出了一些相关免疫布尔函数的性质。

2 预备知识

为了叙述方便，我们记样本空间

$B=GF^n(2)=\{(\alpha_1,\alpha_2,\cdots,\alpha_n):\alpha_i=0 \text{ 或 } 1,\ 1\leqslant i\leqslant n\}$

B 上的代数取为

$F=\{A:A\subseteq B\}$

定义

$P\{A\}=|A|/2^n, A\subseteq B$

则$(GF^n(2), F, P)$成为一个概率空间。定义 $GF^n(2)$到 $GF(2)$的 n 个映射：

$X_i(x_1,x_2,\cdots,x_n)=x_i,\ (x_1,x_2,\cdots,x_n)\in GF^n(2),\ 1\leqslant i\leqslant n$

这样就得到该概率空间上的 n 个布尔函数随机变量 $X_1, X_2, \cdots, X_n$。容易验证它们相互独立且具有相同的分布律：

$$P\{X_i=0\}=P\{X_i=1\}=\frac{1}{2},\ i=1,2,\cdots,n$$

容易看出，对任意的一个 n 元布尔函数 $f(x_1,x_2,\cdots,x_n)$，$f(X_1,X_2,\cdots,X_n)$也是概率空间$(GF^n(2), F, P)$上的布尔随机变量。

定义1 设 $x=(x_1,x_2,\cdots,x_n)\in GF^n(2)$，$\omega=(\omega_1,\omega_2,\cdots,\omega_n)\in GF^n(2)$。$x$ 和 ω 的点积定义为 $\omega\cdot x=\omega_1x_1+\omega_2x_2+\cdots+\omega_nx_n(\mathrm{mod}\ 2)$。$n$ 元布尔函数 $f(x)$，$x\in GF^n(2)$的Walsh循环谱定义为

$$S_{(f(x))}(\omega)=\frac{1}{2^n}\sum_{x\in GF^n(2)}(-1)^{f(x)}(-1)^{x\cdot\omega}$$

线性谱定义为

$$S_{f(x)}(\omega)=\frac{1}{2^n}\sum_{x\in GF^n(2)}f(x)(-1)^{x\cdot\omega}$$

n 元布尔函数 $f(x_1,x_2,\cdots,x_n)$的 Hamming 重量是指集合

$$\{(x_1,x_2,\cdots,x_n):(x_1,x_2,\cdots,x_n)\in GF^n(2),\ f(x_1,x_2,\cdots,x_n)=1\}$$

所含元素的个数，记为 $W(f(x))$。可知 $W(f(x))=2^nS_{f(x)}(0)$。类似地，称 $\omega(=(\omega_1,\omega_2,\cdots,\omega_n)\in GF^n(2))$的不为零的分量个数为 ω 的 Hamming 重量，记为 $W(\omega)$。

定义2 设 $f(x_1,x_2,\cdots,x_n)$，$(x_1,x_2,\cdots,x_n)\in GF^n(2)$，是布尔函数，$X_1, X_2,\cdots,X_n$ 是定义在某概率空间(B,F,P)上相互独立的 n 个布尔随机变量，满足

$P\{X_i=0\}=P\{X_i=1\}=\frac{1}{2}$，$1\leqslant i\leqslant n$ 记 $X=(X_1,X_2,\cdots,X_n)$

若对取定的正整数 $m\leqslant n$，对任意的 $1\leqslant i_1<\cdots<i_m\leqslant n$，与布尔函数 $f(x_1,x_2,\cdots,x_n)$相应的布尔随机变量 $f(X_1,X_2,\cdots,X_n)$与布尔随机向量$(X_1,X_2,\cdots,X_n)$都相互独立，即对任意$(a_1,a_2,\cdots,a_m)\in GF^m(2)$都有

$$P\{f(X_1,X_2,\cdots,X_n)=1,X_{x_1}=a_1,\cdots,X_{i_m}=a_m\}=\frac{1}{2^m}P\{f(X_1,X_2,\cdots,X_n)=1\}$$

或等价地有

$$P\{f(X_1,X_2,\cdots,X_n)=1\mid X_{x_1}=a_1,\cdots,X_{i_m}=a_m\}=P\{f(X_1,X_2,\cdots,X_n)=1\}$$

则称布尔函数 $f(x_1,x_2,\cdots,x_n)$，$(x_1,x_2,\cdots,x_n)\in GF^n(2)$，是 m 阶相关免疫的。

在本文中，我们记 $e_i=(\overbrace{0,\cdots,0,1}^{i},0,\cdots,0)\in GF^n(2)$，1

*)国家自然科学基金项目(60473028)。肖 鸿 博士研究生，讲师，主要研究方向为密码学；周 宇 博士研究生，主要研究方向为密码学；肖国镇 博士生导师，教授，主要研究方向为密码学和信息编码理论。

$\leqslant i \leqslant n$，在不引起混淆的情况下用 0 表示 $GF^n(2)$ 上的零向量。

引理 1 （Xiao-Massey 定理）布尔函数 $f(x), x \in GF^n(2)$，是 m 阶相关免疫的充分必要条件是对任意的 $\omega \in GF^n(2), 1 \leqslant W(\omega) \leqslant m$，都有

$S_{(f(x))}(\omega)=0$ 或等价 $S_{f(x)}(\omega)=0$

用概率描述语言，Xiao-Massey 定理可以叙述为：

引理 2 布尔函数 $f(x), x \in GF^n(2)$，是 m 阶相关免疫的充分必要条件是对任意的 $\omega \in GF^n(2), 1 \leqslant W(\omega) \leqslant m$，都有

$$P\{f(X)=\omega \cdot X\}=\frac{1}{2}$$

引理 3[2] 设 $f(x), g(x)$ 都是 n 元布尔函数，则

$S_{f+g}(\omega)=S_f(\omega)+S_g(\omega)-2S_{fg}(\omega), \omega \in GF^n(2)$

引理 4[8] 若布尔函数 $f(x), x \in GF^n(2)$，是 m 阶相关免疫的，则 $W(f)$ 必是 2^m 的整数倍，即存在非负整数 r，使 $W(f)=2^m r$ 。

3 主要结果

由于布尔函数的许多密码学性质都可通过 Walsh 谱来刻画，所以布尔函数的 Walsh 谱在布尔函数性质的研究和有关构造以及应用研究中占有非常重要地位。

下面的定理给出了一个 n 元布尔函数的 Walsh 谱的一种表示 。

定理 1 设 $f(x), x \in GF^n(2)$，为 n 元布尔函数，则

(1) 当 $W(\omega)=0$ 时，$S_f(\omega)=S_f(0)$；

(2) 当 $W(\omega)=1$ 时，不妨设 $\omega=e_i, 1 \leqslant i \leqslant n$，$S_f(e_i)=S_f(0)-2S_{x_i f}(0)$；

(3) 当 $W(\omega)=2$ 时，不妨设 $\omega=e_i+e_j, 1 \leqslant i \neq j \leqslant n$

$S_f(e_i+e_j)=S_f(0)-2S_{x_i f}(0)-2S_{x_j f}(0)+4S_{x_i x_j f}(0)$；

(4) 若 $W(\omega)=3$，不妨设 $\omega=e_i+e_j+e_k, 1 \leqslant i<j<k \leqslant n$，

$S_f(e_i+e_j+e_k)=S_f(0)-2S_{x_i f}(0)-2S_{x_j f}(0)-2S_{x_j f}(0)+4S_{x_i x_k f}(0)+4S_{x_i x_j f}(0)+4S_{x_i x_k} f(0)-8S_{x_i x_j x_k f}(0)$

……

($n+1$) 当 $W(\omega)=n$ 时，$\omega=e_1+e_2+\cdots+e_n$，$S_f(e_1+e_2+\cdots+e_n)=S_f(0)+(-2)^1\sum_{i=1}^{n}S_{x_i f}(0)+(-2)^2\sum_{i\neq j}^{n}S_{x_i x_j f}(0)+(-2)^3\sum_{i\neq j\neq k}^{n}S x_i x_j x_k f(0)+\cdots+(-2)^n S_{x_1 x_2 \cdots x_n f}(0)$

证明：已知

$$S_{f(x)}(\omega)=\frac{1}{2^n}\sum_{x \in GD(2)} f(x)(-1)^{x \cdot \omega}= P\{f(X)=1, \omega \cdot X=0\}-P\{f(X)=1, \omega \cdot X=1\}$$

下面对 $W(\omega)$ 分情况进行讨论。

(1) 若 $W(\omega)=0$，则 $\omega=0$，此时 $S_f(\omega)=S_f(0)$；

(2) 若 $W(\omega)=1$，不妨设 $\omega=e_i, 1 \leqslant i \leqslant n$ ，则

$S_f(e_i)=P\{f(X)=1, X_i=0\}-P\{f(X)=1, X_i=1\}=P\{f(X)=1\}-P\{f(X)=1, X_i=1\}-P\{f(X)=1, X_i=1\}$

$=S_f(0)-2S_{x_i f}(0)$；

(3) 若 $W(\omega)=2$，不妨设 $\omega=e_i+e_j, 1 \leqslant i \neq j \leqslant n$，则

$S_f(e_i+e_j)=P\{f(X)=1, X_i+X_j=0\}-P\{f(X)=1, X_i+X_j=1\}$

$=P\{f(X)=1, X_i=1, X_j=1\}+P\{f(X)=1, X_i=0, X_j=0\}-P\{f(X)=1, X_i=1, X_j=0\}-P\{f(X)=1, X_i=0, X_j=1\}$

$=P\{f(X)=1, X_i=1\}-P\{f(X)=1, X_i=1, X_j=0\}+P\{f(X)=1, X_j=0\}-P\{f(X)=1, X_i=1, X_j=0\}-P\{f(X)=1, X_i=1\}+P\{f(X)=1, X_i=1, X_j=1\}$

$=P\{f(X)=1, X_i=1\}-P\{f(X)=1, X_i=1, X_j=1\}+P\{f(X)=1, X_j=0\}-P\{f(X)=1, X_j=0\}$

$=P\{f(X)=1, X_j=0\}-P\{f(X)=1, X_j=1\}$

$=P\{f(X)=1, X_j=0\}-P\{f(X)=1, X_j=1\}-P\{f(X)=1, X_j=1\}+P\{f(X)=1, X_i=1, X_j=1\}$

$=P\{f(X)=1, X_j=0\}-P\{f(X)=1, X_j=1\}-2(P\{f(X)=1, X_i=1, X_j=1\}-P\{f(X)=1, X_i=1, X_j=1\})$

$=S_f(0)-2S_{x_i f}(0)-2S_{x_j f}(0)+4S_{x_i x_j f}(0)$

(4) 若 $W(\omega)=3$，不妨设 $=e_i+e_j+e_k, 1 \leqslant i<j<k \leqslant n$，则

$S_f(\omega)=P\{f(X)=1, X_i+X_j+X_k=0\}-P\{f(X)=1, X_i+X_j+X_k=1\}$

$=P\{f(X)=1, X_i+X_j=1, X_k=1\}+P\{f(X)=1, X_i+X_j=0, X_k=0\}-P\{f(X)=1, X_i+X_j=1, X_k=0\}-P\{f(X)=1, X_i+X_j=0, X_k=1\}$

$=P\{f(X)=1, X_i+X_j=1\}-P\{f(X)=1, X_i+X_j=1, X_k=0\}+P\{f(X)=1, X_k=0\}-P\{f(X)=1, X_i+X_j=1, X_k=0\}-P\{f(X)=1, X_i+X_j=1\}+P\{f(X)=1, X_i+X_j=1, X_k=1\}-P\{f(X)=1, X_k=1\}+P\{f(X)=1, X_i+X_j=1, X_k=1\}$

$=P\{f(X)=1, X_k=0\}-P\{f(X)=1, X_k=1\}-2(P\{f(X)=1, X_i+X_j=1, X_k=0\}-P\{f(X)=1, X_i+X_j=1, X_k=1\})$

$=S_f(e_k)-2S_{(x_i+x_j)f}(e_k)$

$=S_f(e_k)-2[S_{x_i f}(e_k)+S_{x_j f}(e_k)-2S_{x_i x_j f}(e_k)]$

$=S_f(e_k)-2S_{x_i f}(e_k)-2S_{x_j f}(e_k)+4S_{x_i x_j f}(e_k)$

$=S_f(0)-2S_{x_i f}(0)-2S_{x_j f}(0)-2S_{x_k f}(0)+4S_{x_i x_j f}(0)+4S_{x_i x_k f}(0)+4S_{x_j x_k f}(0)-8S_{x_i x_j x_k f}(0)$

……

($n+1$) 若 $W(\omega)=n$，不妨设 $\omega=e_1+e_2+\cdots+e_n$，则

$S_f(e_1+e_2+\cdots+e_n)=P\{f(X)=1, \sum_{i=1}^{n}X_i=0\}-P\{f(X)=1, \sum_{i=1}^{n}X_i=1\}$

$=P\{f(X)=1, \sum_{i=1}^{n-1}X_i=0, X_n=0\}+P\{f(X)=1, \sum_{i=1}^{n-1}X_i=1, X_n=1\}-P\{f(X)=1, \sum_{i=1}^{n-1}X_i=1, X_n=0\}-P\{f(X)=1, \sum_{i=1}^{n-1}X_i=0, X_n=1\}$

$=S_f(e_1+e_2+\cdots+e_{n-1})-2S_{x_n f}(e_1+e_2+\cdots+e_{n-1})$

$=S_f(0)+(-2)^1\sum_{i=1}^{n}S_{x_i f}(0)+(-2)^2\sum_{i\neq j}^{n}S_{x_i x_j f}(0)+(-2)^3\sum_{i\neq j\neq k}^{n}S_{x_i x_j x_k f}(0)+\cdots+(-2)^n S_{x_1 x_2 \cdots x_n f}(0)$

定理 1 表明一个 n 元布尔函数 $f(x)$ 在任一点的 Walsh 谱值完全由相关函数在 0 点的 Walsh 谱值确定。由于布尔函数的 Hamming 重量由其在 0 点的 Walsh 谱所确定，因此根据 Xiao-Massey 定理，函数的相关免疫性可以用 Hamming 重量进行刻画。我们知道一个 n 元布尔函数 $f(x)$ 是 m 阶相关免疫的必要条件是 $W(f)=2^m r$，其中 r 为非负整数。自然地，问题是满足 $W(f)=2^m r$ 的布尔函数 $f(x)$ 什么时候是 m 阶相关免疫的，也就是怎样扩充条件 $W(f)=2^m r$，使 $f(x)$ 成为 m 阶相关免疫的充要条件。下面的定理就回答了这一问题。

定理 2 n 元布尔函数 $f(x)$ 为 m 阶相关免疫的充要条件是 $W(f)=2^m r$，r 为非负整数，且 $W(x_{i_1} x_{i_2} \cdots x_{i_t} f)=2^{m-t} r$，其中 $1 \leqslant t \leqslant m$，$1 \leqslant i_1<i_2<\cdots<i_t \leqslant n$。

证明：必要性。设 $f(x)$ 是 m 阶相关免疫函数，则 $W(f)=2^m r$（r 为非负正整数），即

$S_f(0)=2^{m-n} r$

另一方面，由 Xiao-Massey 定理知，对任意的 $\omega \in GF^n$

(2),$1\leqslant W(\omega)\leqslant m$,有

$S_{f(x)}(\omega)=0$

(1) 当$W(\omega)=1$时,不妨设$\omega=e_i$,$1\leqslant i\leqslant n$,由定理1和Xiao-Massey定理得

$S_f(e_i)=S_f(0)-2S_{x_i f}(0)=0$,因此$S_{x_i f}(0)=2^{m-n-1}r$,也就是$W(x_i f)=2^{m-1}r$。

(2) 当$W(\omega)=2$时,不妨设$\omega=e_i+e_j$,$1\leqslant i\neq j\leqslant n$,由定理1和Xiao-Massey定理得$S_f(e_i+e_j)=S_f(0)-2S_{x_i f}(0)-2S_{x_j f}(0)+4S_{x_i x_j f}(0)$,由$S_f(0)=2^{m-n}r$,$S_{x_i f}(0)=2^{m-n-1}r$,

可以得到$S_{x_i x_j f}(0)=2^{m-n-2}r$,也就是$W(x_i x_j f)=2^{m-2}r$。

继续上述过程,依次可得到$W(x_i x_j x_k f)=2^{m-3}r$,$1\leqslant i<j<k\leqslant n$;…;$W(x_{i_1}x_{i_2}\cdots x_{i_m}f)=r$,$1\leqslant i_1<i_2<\cdots<i_m\leqslant n$。

必要性。假设对任意非负整数$t(0\leqslant t\leqslant m)$及任意$i_1,i_2,\cdots,i_t\in\{1,2,\cdots,n\}$,且$i_1,i_2,\cdots,i_t$互不相等,有

$$W(x_{i_1}x_{i_2}\cdots x_{i_t}f)=2^{m-t}r$$

则

$S_f(0)=2^{m-n}r$,$S_{x_i f}(0)=2^{m-n-1}r(1\leqslant i\leqslant n)$,$S_{x_i x_j f}(0)=2^{m-n-2}r(1\leqslant i\neq j\leqslant n),\cdots$,

$S_{x_{i_1}x_{i_2}\cdots x_{i_m}f}(0)=r\ (1\leqslant i_1<i_2<\cdots<i_m\leqslant n)$

由定理1可得

$S_f(e_i)=S_f(e_i+e_j)=\cdots=S_f(e_{i_1}+e_{i_2}+\cdots+e_{i_m})=0$

也就是说,对任意$\omega\in GF^n(2)$,$1\leqslant W(\omega)\leqslant m$,$S_f(\omega)=0$。所以由Xiao-Massey定理知$f(x)$是$m$阶相关免疫的。

推论1 n元m阶相关免疫函数$f(x)$是$m+1$阶相关免疫的充要条件是

$$W(x_{i_1}x_{i_2}\cdots x_{i_m}f)=2W(x_{j_1}x_{j_2}\cdots x_{j_m}x_{j_{m+1}}f)$$

其中$1\leqslant i_1<i_2<\cdots<i_m\leqslant n$,$1\leqslant j_1<j_2<\cdots<j_m<j_{m+1}\leqslant n$。

注意到对于n元平衡函数$f(x)$总有$W(f)=2^{n-1}$。我们有

推论2 n元平衡函数$f(x)$为m阶相关免疫的充要条件是

$$W(x_{i_1}x_{i_2}\cdots x_{i_t}f)=2^{n-t-1}。$$

其中$1\leqslant t\leqslant m$,$i_1,i_2,\cdots,i_t\in\{1,2,\cdots,n\}$且互不相同。

在相关免疫函数的研究中,经常会碰到需要构造新的相关免疫函数的情况。对于两个布尔函数之和的情形(以3元布尔函数为例),有:若两个都不是相关免疫的,和是相关免疫的;如$f_1=x_1+x_2+x_3+x_1x_2$,$f_2=x_1x_3+x_2x_3$。若一个是,另外一个不是,和是相关免疫的;如$f_1=x_1+x_2$,$f_2=x_3$。若两个都是的,和也是的。如$f_1=x_1+x_2$,$f_2=1+x_1+x_2$。可以知道和的相关免疫性与各个的相关免疫性没有直接联系。下面我们讨论相关免疫的和函数的相关免疫性。

定理3 设n元布尔函数$f(x)$和$g(x)$都是m阶相关免疫,则下列条件等价

(1) $f(x)+g(x)$是m阶相关免疫;

(2) $f(x)g(x)$是m阶相关免疫;

(3) 对任意$\omega\in GF^n(2)$,$1\leqslant W(\omega)\leqslant n$,$P\{f(X)g(X)=\omega\cdot X\}=\frac{1}{2}$。

证明:因为$f(x)$,$g(x)$均为m阶相关免疫,所以对于任意$\omega\in GF^n(2)$,$1\leqslant W(\omega)\leqslant n$,$S_f(\omega)=S_g(\omega)=0$。由$S_{f+g}(\omega)=S_f(\omega)+S_g(\omega)-2S_{fg}(\omega)$及Xiao-Massey定理知,$f(x)+g(x)$是$m$阶相关免疫的当且仅当$f(x)g(x)$是$m$阶相关免疫的,即(1)与(2)等价。由引理2知(2)与(3)等价的。

定理3的结果不难推广到有限多个函数的和的情况。同两个函数之和的情况类似,$k(\geqslant 2)$个之和是m阶相关免疫时,不能保证$t(<k)$个之和是m阶相关免疫。例如3元1阶相关免疫函数$f_1=x_1+x_2+x_3+x_1x_3+x_1x_2+x_2x_3$,$f_2=x_1+x_2+x_3$,$f_3=1+x_1$,其和为$f=1+x_1+x_1x_3+x_1x_2+x_2x_3$是1阶相关免疫,但$f_1+f_2$和$f_1+f_3$却不是1阶相关免疫的。

推论3 设n元布尔函数$f_1(x),f_2(x),\cdots,f_k(x)$是$m$阶相关免疫,且满足对任意$i_1,i_2,\cdots,i_t\in\{1,2,\cdots,k\}$,$1\leqslant t\leqslant k-1$,$f_{i_1}(x)+f_{i_2}(x)+\cdots+f_{i_t}(x)$为$m$阶相关免疫,则下列条件等价:

(1) $f_1(x)+f_2(x)+\cdots+f_k(x)$是$m$阶相关免疫;

(2) $f_1(x)f_2(x)\cdots f_k(x)$是$m$阶相关免疫;

(3) 对任意$\omega\in GF^n(2)$,$1\leqslant W(\omega)\leqslant n$,$P\{f_1(X)f_2(X)\cdots f_k(X)\}=\frac{1}{2}$。

推论3表明,可以通过已知的m阶相关免疫函数构造新的m阶相关免疫函数。

文[3]给出了一种典型的构造m阶相关免疫函数的方法。设$f(x),g(x),x\in GF^n(2)$都是m阶相关免疫的布尔函数,则$n+1$元布尔函数

$$\Psi(x,x_{n+1})=x_{n+1}f(x)+(x_{n+1}+1)g(x),x\in GF^n(2),\ x_{n+1}\in GF(2)$$

是至少m阶相关免疫的充分必要条件是$P\{f(x)=1\}=P\{g(x)=1\}$。

这种构造办法可以推广用于n元m阶相关免疫函数构造$n+2$元m阶相关免疫。

定理4 设$f_1(x),f_2(x),f_3(x),f_4(x)$是$n$元$m$阶相关免疫函数。则$n+2$元布尔函数$\Psi(x,x_{n+1},x_{n+2})=(x_{n+1}+1)(x_{n+2}+1)f_1(x)+x_{n+1}(x_{n+2}+1)f_2(x)+(x_{n+1}+1)x_{n+2}f_3(x)+x_{n+1}x_{n+2}f_4(x)$是至少$m$阶相关免疫的充分必要条件是

$$P\{f_1(X)=1\}+P\{f_3(X)=1\}=P\{f_2(X)=1\}+P\{f_4(X)=1\} \tag{1}$$

$$P\{f_1(X)=1\}+P\{f_2(X)=1\}=P\{f_3(X)=1\}+P\{f_4(X)=1\} \tag{2}$$

$$P\{f_1(X)=1\}+P\{f_4(X)=1\}=P\{f_2(X)=1\}+P\{f_3(X)=1\} \tag{3}$$

证明:设$\bar{\omega}=(\omega,\omega_{n+1},\omega_{n+2})$,$(x,x_{n+1},x_{n+2})\in GF^n(2)$,其中$\omega,x\in GF^{n-2}(2)$,$\omega_{n+1},\omega_{n+2},x_{n+1},x_{n+2}\in GF(2)$,则

$$S_{(\Psi)}(\bar{\omega})=\frac{1}{2^n}\sum_{x,x_{n-1},x_n}(-1)^{\Psi+\omega\cdot x+\omega_{n-1}x_{n-1}+\omega_n x_n}$$

$$=\frac{1}{4}[(-1)^0S_{(f_1)}(\omega)+(-1)^{\omega_{n-1}}S_{(f_2)}(\omega)+(-1)^{\omega_n}S_{(f_3)}(\omega)+(-1)^{\omega_n+\omega_{n-1}}S_{(f_4)}(\omega)]$$

进而我们有

$$4S_{(\Psi)}(\omega,0,0)=S_{(f_1)}(\omega)+S_{(f_2)}(\omega)+S_{(f_3)}(\omega)+S_{(f_4)}(\omega) \tag{4}$$

$$4S_{(\Psi)}(\omega,1,0)=S_{f_1}(\omega)-S_{(f_2)}(\omega)+S_{(f_3)}(\omega)-S_{(f_4)}(\omega) \tag{5}$$

$$4S_{(\Psi)}(\omega,0,1)=S_{f_1}(\omega)+S_{(f_2)}(\omega)-S_{(f_3)}(\omega)-S_{(f_4)}(\omega) \tag{6}$$

$$4S_{(\Psi)}(\omega,1,1)=S_{(f_1)}(\omega)-S_{(f_2)}(\omega)-S_{(f_3)}(\omega)+S_{(f_4)}(\omega) \tag{7}$$

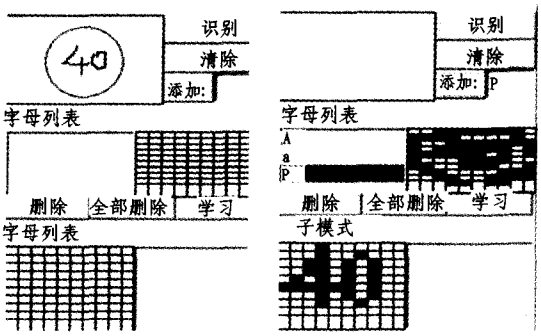
必要性。设Ψ是至少为m阶相关免疫的。则对任意$\bar{\omega}\in GF^{n+2}(2)$,$1\leqslant W(\bar{\omega})\leqslant m$,$S_{(\Psi)}(\bar{\omega})=0$。显然,当$1\leqslant W(\bar{\omega})\leqslant m$时,总有$0\leqslant W(\bar{\omega})\leqslant m-1$。因此当$\omega=0$时,由5),6),7)可得

$$S_{(f_1)}(0)+S_{(f_3)}(0)=S_{(f_2)}(0)+S_{(f_4)}(0) \tag{8}$$

$$S_{(f_1)}(0)+S_{(f_2)}(0)=S_{(f_3)}(0)+S_{(f_4)}(0) \tag{9}$$

$$S_{(f_1)}(0)+S_{(f_4)}(0)=S_{(f_2)}(0)+S_{(f_3)}(0) \tag{10}$$

(下转第202页)



(a) 限速 40 公里的交通标志　　(b) 对图形进行学习

图 4　嵌套映射结构模式识别

图 3 为能对输入模式进行记忆和识别的属性网络，首先在写字板(图左上角)上任画一个模式，如“”，计算机首先将模式“”在写字板中所占据的矩形划分为 10×10 子矩形构成的网格，并令所有与“梨”模式的交非空的子矩形染(黑)色，同时，令以染色子矩形为基准的子定性映射等于 1，并将它们投射到右下角所示的记忆模式区，这时，该记忆区不仅出现了一个由 10×10 个子矩形所构成网格，而且，出现了一个由被染色子矩形构成的模式“”。即：一个以整个网格(整体)为基准的定性映射，和一个分别以 10×10 个子矩形为基准的子定性映射簇之间嵌套映射结构。在添加按纽的空格中，给所写模式命名，如命之为“梨”，再按学习按纽后，机器将在字母列表栏记下学习的结果“梨”，机器显示“学习结束”。重新写字板板中书写一个手写模式“”，按识别键，这时，机器显示“梨”。这个结果说明，计算机不仅记住了字母“”，而且，还将与“”有差异的模式“”也识别为“梨”。

图 4 为对输入的模式使用带有嵌套的属性网络来记忆和识别，也就是在图 3 例子的基础上对模式中重要的子模式单独建立相应的嵌套属性网络。图 4 中被识别的模式为限速 40 公里的交通示意图。假如使用图 3 中的方式来识别，子模式“40”将失真或丢失，所以在建立属性网络的同时，建立子属性网络来表示“40”的模式，这样将有效解决子模式失真或丢失问题。

结论　本文给出如何使用属性网络来实现模式识别，同时本文给出的模拟例子也充分说明了本方法在模式识别中的潜力。

参 考 文 献

1　李文佩. 基于定性映射和转化程度函数的汉字识别[D]:[上海海事大学硕士论文]. 上海:2004
2　王洪，冯嘉礼. 定性映射正交基空间下的模式识别技术. 计算机工程，32(17)
3　Feng Jiali. Qualitative Mapping Orthogonal System Induced by Subdivision Transformation of Qualitative Criterion and Biomimetic Pattern Recognition, CHINESE JOURNAL OF ELECTRONICS, Special Issue on Biomimetic Pattern Recognition, 2006, 15(4):850～856
4　Feng J. Support Vector Machine induced by Subdivision of Qualitative Criterion. In: Proc. of theIJCAI-2007, Workshop Theme: Complex Valued Neural Networks and Neuro-Computing: Novel Methods, Applications and Implementations. Hyderabad. India, January 2007. 48～53

(上接第 192 页)

从而 1)，2)，3)成立。

充分性。设 $\bar{\omega}=(\omega,\omega_{n+1},\omega_{n+2})\in GF^n(2)$，$1\leqslant W(\bar{\omega})\leqslant m$，则总有 $0\leqslant W(\omega)\leqslant m-1$。

当 $\omega\neq 0$ 时，$1\leqslant W(\omega)\leqslant m-1$，因为 $f_1(x)$，$f_2(x)$，$f_3(x)$，$f_4(x)$都是 m 阶相关免疫函数，所以 $S_{(f_i)}(\omega)=0$，$i=1,2,3,4$。从而 $S_{(\Psi)}(\bar{\omega})=0$。

当 $\omega=0$ 时，由条件 1)，2)，3)知 8)，9)，10)均成立，从而 $S_{(\Psi)}(\bar{\omega})=0$。

综上所述，我们总有 $S_{(\Psi)}(\bar{\omega})=0$，$\bar{\omega}\in GF^n(2)$，由 Xiao-Massey 定理知 $\Psi(x,x_{n+1},x_{n+2})$是至少 m 阶相关免疫的。

利用数学归纳法容易证明，对于任意 $x_1,x_2,\cdots,x_k\in GF(2)$，

$$(-1)^{x_1x_2\cdots x_k}=\frac{1}{2^{k-1}}[2^{k-1}-1+(-1)^2\sum_{i=1}^{k}(-1)^{x_i}+(-1)^3\sum_{i\neq j}^{k}(-1)^{x_i+x_j}+\cdots+(-1)^{k+1}(-1)^{x_1+x_2+\cdots+x_k} \tag{11}$$

文[6]中给出了一种 Walsh 循环谱的分解式。设 $f(x)$，$g(x)$，$h(x)$都是 n 元布尔函数，则

$$S_{(f+gh)}(\omega)=\frac{1}{2}[S_{(f)}(\omega)+S_{(f+g)}(\omega)+S_{(f+h)}(\omega)-S_{(f+g+h)}(\omega)],\omega\in GF^n(2)$$

由 11)，我们可以很容易证明。

有了上面的基础，我们给出这种 Walsh 谱分解式的推广形式。

引理 5　设 $f(x)$，$f_i(x)$，$1\leqslant i\leqslant k$ 是 $k+1$ 个 n 元布尔函数，则

$$S_{(f+f_1f_2\cdots f_k)}(\omega)=\frac{1}{2^{k-1}}[(2^{k-1}-1)S_{(f)}(\omega)+(-1)^2\sum_{i=1}^{k}S_{(f+f_i)}(\omega)+(-1)^3\sum_{i\neq j}^{k}S(f+f_i+f_j)(\omega)+\cdots+(-1)^{k+1}S_{(f+f_1+f_2+\cdots+f_k)}(\omega)],\omega\in GF^n(2)$$

由引理 5 不难得到：

定理 5　设 $f(x)$，$f(x)+f_i(x)$ $(1\leqslant i\leqslant k)$，$f(x)+f_i(x)+f_j(x)(1\leqslant i,j\leqslant k)$，$\cdots$，$f(x)+f_1(x)+f_2(x)+\cdots+f_k(x)$都是 n 元 m 阶相关免疫函数，则 $f+f_1f_2\cdots f_k$ 是 n 元 m 阶相关免疫函数。

参 考 文 献

1　Xiao Guozheng, Massey. A Spectral Characterization of Correlation-Immune Function. IEEE Transactions on Information Theory, 1988, 34 (3): 569～571
2　丁存生，肖国镇. 流密码及其应用. 国防工业出版社，1994
3　冯登国. 频谱理论及其在密码学中的应用. 北京：科学出版社，2000
4　Siegenthaler T. Correlation-immunity of nonlinear combining functions for cryptographic applications. IEEE Transactions on Information Theory, 1984, 30 (5): 776～780
5　Zhang Weiguo. Construction of plateaued functions satisfying multiple criteria. High Technology Letters, 2005,11(4):364～366
6　Zheng Y, Zhang X M. Improved upper bound on the nonlinearity of high order correlation immune functions. In: Selected Areas in Cryptography. 7th Annual International Workshop, SAC 2000, Lecture Notes in Computer Science, Springer-Verlag, 2001, 2012:262～274
7　Chee S, Lee S, Sung S H. On the correlation immune functions and their nonlinearity. In: Advances in Cryptology-Asiacrypt'96, Lecture Notes in Computer Science, Springer-Verlag, 1996, 1163:232～243
8　王育民，何大可. 保密学——基础与应用. 西安电子科技大学出版社，1990