The Decomposition Formula of the Joint Distribution for Random Variables over Finite Fields

Teng Ji-hong, Huang Xiao-ying

PLA Information Engineering University, Zhengzhou 450002, China
Email address: *tengjihong@263.net*

Abstract: The properties and construction of the perfect function over finite fields can be turned to the relation of random variables over finite fields. The paper proposes a decomposition formula of the joint distribution for random variables over finite fields by using the trace functions of finite field F_q over its prime fields F_p, where $q=p^l$, and p is a prime. While l=1, the results proposed here is just the joint distribution for p-valued random variables presented in paper [4]. As the application of the decomposition formula of the joint distribution for random variables over finite fields, it can be used to study the cryptographic properties of logical functions over finite fields.

Keywords: p-valued random variable; q-valued random variable; trace function; decomposition formula of the joint distribution for random variable

有限域上随机变量联合分布的分解式

滕吉红　　黄晓英
解放军信息工程大学理学院　中国郑州　450002

【摘要】有限域上完全非线性函数的性质、构造等问题，其实质可归结为有限域上随机变量之间的关系，论文利用有限域上迹函数作为主要工具，给出了有限域 $F_q(q=p^l, p$ 为素数)上随机变量联合分布的分解式。特别地，l=1 时即得 p 值随机变量联合分布的分解式[4]. 有限域上随机变量联合分布的分解式为有限域上逻辑函数密码性质的研究提供了理论工具和方法。

【关键词】 p 值随机变量；q 值随机变量；迹函数；随机变量联合分布分解式

1. 引言

现代通信领域中，为保证信息传输的安全性，需要对发送的明文进行加密，对称密码体制因为实现速度快而在实际中应用广泛. 根据加密方式的不同又可将对称密码分为序列密码和分组密码两种. 在序列密码中常用的密钥流生成器是非线性组合生成器，其中，非线性组合函数的密码性质是保证密码体制安全的关键. 而布尔函数作为一种逻辑运算因其实现快速，结构简单而常被选做非线性组合函数，同时布尔函数不仅在序列密码中应用广泛，在分组密码、编码和信号设计中也有重要的应用价值，因此对布尔函数密码性质如平衡性、相关免疫性、非线性度等等的研究和构造几十年来都是密码学研究的热点. 最初对布尔函数密码性质的研究主要用的是代数方法，后来[1]在研究布尔函数的密码学性质的时候，发现布尔函数的许多性质可以归结为布尔随机变量间的相互性质，如布尔函数的相关免疫性实质上是考察布尔随机变量之间的独立性，布尔函数的 *Walsh* 变换（研究布尔函数密码性质的重要工具）可以看作是某一随机变量的数学期望. 其实，布尔随机变量间的相互性质实质上就是考察布尔随机变量联合分布的特点[2]，为此，[3]给出了布尔随机变量联合分布的分解式，布尔随机变量联合分布的分解式的给出，为研究布尔函数的性质、构造等问题提供了新的思路和工具，使研究更为深入.

随着计算机的广泛应用及密码分析理论的日益成熟，人们对密码体制的安全性的要求更高了，密码设计也自然地要考虑从二元域向一般的有限域乃至剩余类环 Z_m 上扩展，而研究多值逻辑函数的密码性质是密码设计和应用的理论基础. 文献[4]讨论了一般剩余类环 Z_m（m 为素数 p 或 p^l）上的 m 值随机变量联合分布的分解式，揭示了 p 值随机变量联合分布与其各分量的任意非零线性和的分布间的内在联系，这样对剩余类环 Z_m（m 为素数 p 或 p^l）上的多值逻辑函数的密码性质的研究也可以归结到随机变量之间的性质研究上.

代数方法也是研究有限域上逻辑函数密码性质的

国家自然科学基金资助项目（批准号：60803154）

978-1-935068-01-3 © 2009 SciRes.

主要方法，文献[5]通过有限域上随机变量的特征函数引入了完全非线性函数的概念，对这类函数的构造和计数的研究也主要用的是代数的方法。本文的主要目的是将随机变量联合分布的分解式推广到有限域上，为有限域上逻辑函数密码性质的研究中提供理论基础。

本文的基本结构如下：第二部分介绍了一些基本概念，建立了文中所涉及到的概率空间；第三部分利用有限域上迹函数的一些特殊性质，以及素域 F_p 上随机变量联合分布的分解式[4]，给出了有限域 F_q 上 q 值随机变量的联合分布的分解式.

2．基本概念

以下如无特别说明，总设 $q=p^l$，$l\geq 2$，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[6]知，F_q 是素域 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，则由[6]知存在 F_q 在 F_p 上的一组正规基 α、α^p、…、$\alpha^{p^{l-1}}$ 满足：

(1) α 是 F_q 中的本原元；

(2) $Tr(\alpha)=Tr(\alpha^p)=\cdots=Tr(\alpha^{p^{l-1}})=1$.

定义 1[6] 对任意的 $\beta\in F_q$，称

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

为 β 在 F_p 上的迹（*trace*）.

引理 1[6] 设 $Tr(\cdot)$ 是有限域 F_q 到 F_p 的迹函数，则 $Tr(\cdot)$ 具有下面的性质：

(1) $Tr(\alpha+\beta)=Tr(\alpha)+Tr(\beta)$，对任意的 $\alpha,\beta\in F_q$;

(2) $Tr(c\alpha)=c\,Tr(\varepsilon)$，对任意的 $\alpha\in F_q$ 及 $c\in F_p$;

(3) $Tr(\cdot)$ 是有限域 F_q 到 F_p 的线性变换;

(4) $Tr(a)=l\,a$，对任意 $a\in F_p$;

(5) $Tr(\alpha^p)=Tr(\alpha)$，对任意的 $\alpha\in F_q$;

(6) 记 $T^{(i)}=\{\beta:\beta\in F_q, Tr(\beta)=i\}$，$i\in F_p$，则 $|T^{(i)}|=p^{l-1}$.

引理 2 设 α、α^p、…、$\alpha^{p^{l-1}}$ 是 F_q 在 F_p 上的一组正规基，则方程组 $\begin{cases} Tr(\alpha x)=0,\\ Tr(\alpha^p x)=0,\\ \cdots\\ Tr(\alpha^{p^{l-1}}x)=0. \end{cases}$ 有唯一解 $x=0$.

证明 充分性显然；

（必要性） 否则，若 $\gamma\in F_q\setminus\{0\}$ 是方程组的解，即 $\begin{cases} Tr(\alpha\gamma)=0,\\ Tr(\alpha^p\gamma)=0,\\ \cdots\\ Tr(\alpha^{p^{l-1}}\gamma)=0. \end{cases}$

而 $\alpha\gamma$、$\alpha^p\gamma$、$\alpha^{p^2}\gamma$、…、$\alpha^{p^{l-1}}\gamma$ 也是 F_q 在 F_p 上的一组基，只要证明它们线性无关即可：若存在 a_0、a_1、…、$a_{l-1}\in F_p$，使得

$$a_0\alpha\gamma+a_1\alpha^p\gamma+\cdots+a_{l-1}\alpha^{p^{l-1}}\gamma$$
$$=(a_0\alpha+a_1\alpha^p\gamma+\cdots+a_{l-1}\alpha^{p^{l-1}})\gamma=0,$$

由于有限域中无零因子，因此

$$a_0\alpha+a_1\alpha^p+\cdots+a_{l-1}\alpha^{p^{l-1}}=0,$$

但 α、α^p、…、$\alpha^{p^{l-1}}$ 是 F_q 在 F_p 上的一组基，所以 $a_i=0$，$0\leq i\leq l-1$．这样对任意的 $\beta\in F_q$，存在 $(b_0,b_1,\cdots,b_{l-1})\in F_p^l$，使得，

$$\beta=b_0\alpha\gamma+b_1\alpha^p\gamma+b_2\alpha^{p^2}\gamma+\cdots+b_{l-1}\alpha^{p^{l-1}}\gamma,$$

因而 $Tr(\beta)$

$$=Tr(b_0\alpha\gamma+b_1\alpha^p\gamma+\cdots+b_{l-1}\alpha^{p^{l-1}}\gamma)$$
$$=b_0Tr(\alpha\gamma)+b_1Tr(\alpha^p\gamma)+\cdots+b_{l-1}Tr(\alpha^{p^2}\gamma)\quad 。。,$$

即对任意的 $\beta\in F_q$，都有 $Tr(\beta)=0$，这与 $|T^{(0)}|=p^{l-1}$ (引理 1 的(6))矛盾，所以方程组有唯一解 $x=0$.　　#

文献[7]曾经指出，概率论作为研究大量现象“随机性”的一门学科，其科学性必须在建立了精确的概率空间的基础上才能体现，因此我们首先建立本文所涉及到的概率空间：

设 (Ω, F, P) 是任一概率空间，$X:\Omega\to F_q$ 满足：$\{w:X(w)=\beta\}\in F$，$\beta\in F_q$，则称 X 为 (Ω, F, P) 上的 q 值随机变量，且称 $P\{X=\beta\}$，$\beta\in F_q$ 为 X 的分布率．易知，若 X 为 (Ω, F, P) 上的 q 值随机变量，则 $Tr(X)$ 为 (Ω, F, P) 上的 p 值随机变量.

为了研究有限域上逻辑函数的密码性质，我们建立特殊的概率空间如下：

取样本空间 $\Omega=F_q^n$，Ω 上的 $\sigma-$ 代数取为：$F=\{A:A\subset\Omega\}$，定义 $P(A)=\dfrac{|A|}{q^n}$，$A\subset\Omega$，$|A|$ 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：

$$X_i(x_1,x_2,\cdots,x_n)=x_i,\quad (x_1,x_2,\cdots,x_n)\in F_q^n,$$

$1\leq i\leq n$，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：$P\{X_i=j\}=\dfrac{1}{q}$，$j\in F_q$，$i=1,2,\cdots,n$．对上面的 q 值随机变量 $X_1,X_2,\cdots,X_n$，$Tr(X_i)$，$i=1,2,\cdots,n$，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： $P\{Tr(X_i)=j\}=\frac{1}{p}$， $j\in F_p$， $i=1,2,\cdots,n$.

3. 有限域上 q 值随机变量联合分布的分解式

文献[4]给出了 p 值随机变量联合分布的分解式如下：

定理 1[4] 设 $Y=(Y_1,Y_2,\cdots,Y_n)$ 是概率空间 (Ω, F, P) 上的任一 n 维 p 值随机变量，B 为任一 F 可测集，则对任意的 $a=(a_1,a_2,\cdots,a_n)\in F_p^n$， 都有

$$P\{B,Y=a\},$$

$$=\frac{1}{p^{n-1}}\sum_{\lambda\in\Lambda}P\{B,\lambda\cdot Y=\lambda\cdot a\}-\frac{p^{n-1}-1}{(p-1)p^{n-1}}P(B) \quad (1)$$

其 中 $\Lambda=\{(0,0,\cdots,0,1,\lambda_i,\cdots,\lambda_n)$ ： $2\le i\le n$ ， $\lambda_j\in F_p$， $i\le j\le n\}$.

下面的定理表明利用有限域上迹函数的性质，可以将有限域上随机变量间的性质转化到其素域上去考虑。

定理 2 设 Y 是概率空间 (Ω, F, P) 上的任一 q 值随机变量，B 为任一 F 可测集，记

$$X=(Tr(\alpha Y),\ Tr(\alpha^p Y),\ \cdots,\ Tr(\alpha^{p^{l-1}}Y)),$$

则

$$P\{B,Y=0\}$$

$$=P\{B,Tr(\alpha Y)=0,Tr(\alpha Y\ )=0,\cdots,Tr(\alpha^{p^{l-1}}Y)=0\}$$

$$=\frac{1}{p^{l-1}}\sum_{\lambda\in\Lambda}P\{B,\lambda\cdot X=0\}-\frac{p^{l-1}-1}{(p-1)p^{l-1}}P(B), \quad (2)$$

其 中 $\Lambda=\{(0,0,\cdots,0,1,\lambda_i,\cdots,\lambda_{l-1})$ ： $1\le i\le l-1$ ， $\lambda_j\in F_p$， $i\le j\le l-1\}$.

证明 由引理 2 知 Y=0 的充要条件是对任意的 $0\le j\le l-1$， $Tr(\alpha^{p^j}Y)=0$，所以

$$P\{B,Y=0\}$$

$$=P\{B,Tr(\alpha Y)=0,Tr(\alpha^p Y)=0,\cdots,Tr(\alpha^{p^{l-1}}Y)=0\}$$

而 $Tr(\alpha^{p^j}Y)$， $0\le j\le l-1$ 是 (Ω, F, P) 上的 p 值随机变量，再由定理 1 即可得结论． #

定理 3 设 Y 是概率空间 (Ω, F, P) 上的任一 q 值随机变量，B 为任一 F 可测集，记

$$X=(Tr(\alpha[Y-a]),\ \cdots,\ Tr(\alpha^{p^{l-1}}[Y-a])),$$

则对任意的 $a\in F_q$，

$$P\{B,Y=a\}$$

$$=P\{B,Tr[\alpha(Y-a)]=0,\cdots,Tr[\alpha^{p^{l-1}}(Y-a)]=0\}$$

$$=\frac{1}{p^{l-1}}\sum_{\lambda\in\Lambda}P\{B,\lambda\cdot X=0\}-\frac{p^{l-1}-1}{(p-1)p^{l-1}}P(B), \quad (3)$$

其 中 $\Lambda=\{(0,0,\cdots,0,1,\lambda_i,\cdots,\lambda_{l-1})$ ： $1\le i\le l-1$ ， $\lambda_j\in F_p$， $i\le j\le l-1\}$.

证明 只要在定理 2 中取 Y=Y-a 即可． #

利用 p 值随机变量联合分布的分解式以及有限域 F_q 上迹函数的性质可以得到下面 n 维 q 值随机变量联合分布的分解式：

定理 4 设 $Y=(Y_1,Y_2,\cdots,Y_n)$ 是概率空间 (Ω, F, P) 上的任一 n 维 q 值随机向量，B 为任一 F 可测集，则]

$$P\{B,Y=0\}$$

$$=\frac{1}{q^{n-1}}\sum_{\lambda\in\Lambda}P\{B,\lambda\cdot Y=0\}-\frac{q^{n-1}-1}{(q-1)q^{n-1}}P(B) \quad (4)$$

其 中 $\Lambda=\{(0,0,\cdots,0,1,\lambda_i,\cdots,\lambda_n)$ ： $2\le i\le n$ ， $\lambda_j\in F_q$， $i\le j\le n\}$.

证明 首先由引理 2 及定理 2 知

$$P\{B,Y=0\}$$

$$=P\{B,Tr(\alpha Y_1)=0,\cdots,Tr(\alpha^{p^{l-1}}Y_1)=0,$$

$$,Tr(\alpha Y_2)=0,Tr(\alpha^p Y_2)\ )=0,\cdots,Tr(\alpha^{p^{l-1}}Y_2)=0,\cdots\cdots,$$

$$,Tr(\alpha Y_n)=0,Tr(\alpha^p Y_n)=0,\cdots,Tr(\alpha^{p^{l-1}}Y_n)=0\}$$

$$=\frac{1}{p^{nl-1}}\sum_{\lambda^*\in\Lambda^*}P\{B,\lambda^*\cdot X=0\}-\frac{p^{nl-1}-1}{(p-1)p^{nl-1}}P(B). \quad (5)$$

其中 $X=(Tr(\alpha Y_1),\cdots,Tr(\alpha^{p^{l-1}}Y_1),\cdots\cdots,Tr(\alpha Y_n),\cdots,Tr(\alpha^{p^{l-1}}Y_n))$，

而 $\Lambda^*=\{(0,0,\cdots,0,1,\lambda_i^*,\cdots,\lambda_{n\cdot l}^*)$： $2\le i\le nl$ ， $\lambda_j^*\in F_p$， $i\le j\le nl\}$.

注意(4)式右边为

$$\frac{1}{q^{n-1}}\sum_{\lambda\in\Lambda}P\{B,\lambda\cdot Y=0\}-\frac{q^{n-1}-1}{(q-1)q^{n-1}}P(B)$$

$$=\frac{1}{q^{n-1}}\sum_{\lambda\in\Lambda}P\{B,Tr(\alpha\lambda\cdot Y)=0,\cdots,Tr(\alpha^{p^{l-1}}(\lambda Y))=0\}$$

$$-\frac{q^{n-1}-1}{(q-1)q^{n-1}}P(B)$$

$$=\frac{1}{q^{n-1}}\sum_{\lambda\in\Lambda}[\frac{1}{p^{l-1}}\sum_{\gamma\in\Pi}P\{B,\gamma\cdot T_\lambda=0\}-\frac{p^{l-1}-1}{p^{l-1}(p-1)}P(B)]$$

$$-\frac{q^{n-1}-1}{(q-1)q^{n-1}}P(B), \quad (6)$$

其中 $T_\lambda=(Tr(\alpha\lambda\cdot Y),\cdots,Tr(\alpha^{p^{l-1}}\lambda\cdot Y))$，

而 $\Pi=\{(0,0,\cdots,0,1,\gamma_i,\cdots,\gamma_{l-1})$ ： $1\le i\le l-1$ ， $\lambda_j\in F_p$， $i\le j\le l-1\}$.

可以证明对任意的 $\lambda\in\Lambda$ 以及 $\gamma\in\Pi$， 都存在 $\lambda^*\in\Lambda^*$，使得

$$P\{B,\gamma\cdot T_\lambda=0\}=P\{B,\lambda^*\cdot X=0\}, \quad (7)$$

又

978-1-935068-01-3 © 2009 SciRes.

$$|\Lambda^*| = p^{l\cdot n-1} + p^{l\cdot n-2} + \cdots + p + 1 = \frac{p^{l\cdot n}-1}{p-1},$$

$$|\Lambda| = q^{n-1} + q^{n-2} + \cdots + q + 1 = \frac{q^n-1}{q-1} = \frac{p^{l\cdot n}-1}{q-1},$$

$$|\Pi| = p^{l-1} + p^{l-2} + \cdots + p + 1 = \frac{p^l-1}{p-1} = \frac{q-1}{p-1},$$

显然$|\Lambda^*| = |\Lambda| \cdot |\Pi| = \frac{q^n-1}{p-1}$,

因此(6)式右方为

$$\frac{1}{q^{n-1}}\sum_{\lambda\in\Lambda}[\frac{1}{p^{l-1}}\sum_{\gamma\in\Pi}P\{B,\gamma\cdot T_\lambda=0\}] - \frac{1}{q^{n-1}}\cdot\frac{q^n-1}{q-1}\frac{p^{l-1}-1}{p^{l-1}(p-1)}P(B) - \frac{q^{n-1}-1}{(q-1)q^{n-1}}P(B)$$

$$= \frac{1}{q^{n-1}}\sum_{\lambda\in\Lambda}[\frac{1}{p^{l-1}}\sum_{\gamma\in\Pi}P\{B,\gamma\cdot T_\lambda=0\}] - \frac{q^{n-1}p^{l-1}-1}{q^{n-1}p^{l-1}(p-1)}P(B)$$

$$= \frac{1}{q^{n-1}}\sum_{\lambda\in\Lambda}[\frac{1}{p^{l-1}}\sum_{\gamma\in\Pi}P\{B,\gamma\cdot T_\lambda=0\}] - \frac{p^{l\cdot n-1}-1}{p^{l\cdot n-1}(p-1)}P(B) \quad (8)$$

综合(7)式和(8)式即得定理结论. #

特别地，在定理 4 中取 $B=\Omega$ 可得下面的推论：

推论 5 设 $Y=(Y_1,Y_2,\cdots,Y_n)$ 是概率空间 (Ω, F, P) 上的任一 n 维 q 值随机向量，B 为任一 F 可测集，则

$$P\{Y=0\} = \frac{1}{q^{n-1}}\sum_{\lambda\in\Lambda}P\{\lambda\cdot Y=0\} - \frac{q^{n-1}-1}{(q-1)q^{n-1}} \quad (9)$$

其中 $\Lambda=\{(0,0,\cdots,0,1,\lambda_i,\cdots,\lambda_n)$ ： $2\le i\le n$ ，$\lambda_j\in F_q$， $i\le j\le n\}$.

更一般地有下面的结果：

推论 6 设 $Y=(Y_1,Y_2,\cdots,Y_n)$ 是概率空间 (Ω, F, P) 上的任一 n 维 q 值随机向量，B 为任一 F 可测集，对任意的 $a=(a_1,a_2,\cdots,a_n)\in F_q^n$，有

$$P\{B,Y=a\} = \frac{1}{q^{n-1}}\sum_{\lambda\in\Lambda}P\{B,\lambda\cdot(Y-a)=0\} - \frac{q^{n-1}-1}{(q-1)p^{n-1}}P(B).$$

证明 在定理 4 中取 $Y=Y-a$ 即可. #

注. 当 $l=1$，即 $q=p$ 时，推论 6 和文献[4]的结果一致.

4. 结束语

本文利用有限域上迹函数的性质给出了有限域上随机变量联合分布的分解式，为研究有限域上逻辑函数的密码学性质提供了理论工具，对于有限域上完全非线性函数性质、构造的研究有重要意义，从而在密码学和通信领域有比较广的应用前景.

References (参考文献)

[1] Li Shi-qu, Zeng Ben-sheng. The Application of Probability Method in the Study of Correlation-immune of Boolean Function (J), 《Statistic and Applied Probability》1994, 1, 5-9.
李世取，曾本胜，概率方法在布尔函数相关免疫性研究中的应用(J)，《数理统计与应用概率》，1994，1，5-9.

[2] Li Shi-qu, Zeng Ben-sheng, Lian Yu-zhong, Logical Functions in Cryptology[M], Beijing, Publishing Company of Software and Electronic Industry, 2003.
李世取，曾本胜，廉玉忠等，密码学中的逻辑函数[M]，北京，中软电子出版社，2003.

[3] Li Shi-qu, Zeng Ben-sheng, Lian Yu-zhong, The Decomposition Formula of the Joint Distribution for Boolean Random Variables and its Applications[J], Journal of China Institute of communications,1998, 11, 61-64.
李世取，曾本胜，廉玉忠，布尔随机向量联合分布的分解式及其应用[J]，《通信学报》，1998, 11，61-64.

[4] Huang Xiao-ying, Li Shi-qu. The Decomposition Formula of the Joint Distribution for *p*-valued Random Variables and its Applications[J], Chinese Journal of Engineering Mathematics, 1998, 3, 91-95.
黄晓英，李世取，*p* 值随机变量联合分布的分解式及其应用，《工程数学学报》，1998, 3 , 91-95.

[5] Ambrosimov A. S., Bent functions of q-valued logic over finite fields [J], Abstract of 2nd Petrozavodsk Conference "probabilistic Methods in Discrete Math", Petrozavodsk, 1988, 3-4.

[6] Lidl, R., Niederreiter H., Finite Fields[M]. Addison-Wesley Publishing Company, 1984.

[7] Shiryayev, A. N., Probability [M], Springer-verlag, New York. Berlin Heidelberg Tokyo World Publishing Corporation, 1984.