中国科学 : 数学　2017 年　第 47 卷　第 11 期 : 1571 ~ 1578
SCIENTIA SINICA　Mathematica
论　文

布尔变量的形式概率分析

献给万哲先教授 90 华诞

黄民强

中国科学院信息工程研究所, 北京 100093
E-mail: mhuang@iss.ac.cn

收稿日期: 2016-12-30; 接受日期: 2017-02-17; 网络出版日期: 2017-07-18

摘要　本文将布尔变量的概率度量分解为白噪音部分和确定性部分, 阐述了后者的概率意义, 提出了有别于经典概率的形式概率概念, 并以此建立了一种简洁的分析和计算方法, 以解决经典方法不易分析和计算的布尔变量的分布问题.

关键词　布尔变量　布尔函数　偏差度　形式概率

MSC (2010) 主题分类　06E30, 68Q87

1　引言

为表述简便计, 本文将定义于概率空间 Ω 且取值于二元域 $\mathbb{F}_2=\{0,1\}$ 的随机变量 ξ 称为布尔变量, 这是信息论和密码学中最重要和最基本的研究对象.

在分析 $\mathbb{F}_2$ 上的多变量系统时, 经常需要计算和分析随机事件的概率和布尔变量的分布. 经典的方法是直接计算、测定和分析其 0/1 分布概率. 对于稍为复杂的布尔变量, 概率的计算和分析相当困难. 另一方面, 不携带任何信息的白噪音源 (均匀的布尔变量) 也有 $p=1/2$ 的 '0' 率, 因此一般布尔变量的取 '0' 概率 $p_0=\mathrm{prob}(\xi=0)$ 中有别于白噪音水平 ("真正有意义") 的成分不等于 p_0.

本文通过引进偏差度和形式概率的概念, 建立了一种新的概率观念和分析计算方法, 以滤除布尔变量中 "白噪音" 的影响, 萃取其中更为本质的成分, 提升分析和计算的效率.

本文中布尔变量之间在 $\mathbb{F}_2$ 上的加法运算 (模 2 加) 记作 $\oplus$. 另外, 由于概率计算的需要, 在表达式没有歧义的情形下, 布尔变量也按其 0、1 取值嵌入实数域运算, 如 $(-1)^\xi$ 和 $1-2\xi$ 等.

1.1　布尔变量的偏差度

设 ξ 为布尔变量, 根据经典理论, 其统计特征完全取决于概率分布 $P(\xi)=(p_0,p_1)$, 其中

$$p_0=\mathrm{prob}(\xi=0),\quad p_1=\mathrm{prob}(\xi=1).$$

定义 1.1　设布尔变量 ξ 如上, 记 $\hat{p}_\xi=p_0-p_1$, 称为 ξ 的偏差度.

英文引用格式: Huang M Q. Analysis of Boolean variables using formal probability (in Chinese). Sci Sin Math, 2017, 47: 1571–1578, doi: 10.1360/N012016-00246

© 2017《中国科学》杂志社

显然, $\hat{p}_\xi$ 与 $P(\xi)$ 之间可以相互转换: 作极性化映射 $\xi \mapsto \hat{\xi} = (-1)^\xi$, 则

$$\hat{p}_\xi = \mathrm{E}\hat{\xi} = 2p_0 - 1, \tag{1.1}$$

$$p_0 = \frac{1 + \hat{p}_\xi}{2}. \tag{1.2}$$

通过下述简单的例子可以看到, $\hat{p}_\xi$ 实际上是相对于 $P(\xi)$ 更为本质的特征参数.

例 1.1 设布尔变量 ξ 如上, 从信息论的角度描述其不确定性的参数是 Shannon [1] 给出的熵:

$$H(\xi) = -p_0 \log_2 p_0 - p_1 \log_2 p_1 = -p_0 \log_2 p_0 - (1 - p_0) \log_2 (1 - p_0). \tag{1.3}$$

显然, $H(\xi)$ 作为 $p_0 \in [0, 1]$ 的函数, 在 $[0, 1/2]$ 中从 0 单调递增到 1, 且以 $p_0 = 1/2$ 为中心呈左右对称, 但其关于 p_0 的变化性状并不直观清晰. 从 $\hat{p}_\xi$ 的角度描述, 由 (1.2) 和 (1.3) 不难得到如下命题:

命题 1.1 设 ξ 和 $\hat{p}_\xi$ 如上, 则 ξ 的熵 $H(\xi)$ 是 $\hat{p}_\xi$ 的偶函数, 且

$$H(\xi) = 1 - \frac{1}{\ln 2} \sum_{k \geqslant 1} \frac{\hat{p}_\xi^{2k}}{2k(2k-1)}. \tag{1.4}$$

这个快速收敛的幂级数形式更加清晰地给出了 $\hat{p}_\xi$ 与熵 $H(\xi)$ 之间的解析关系.

例 1.2 设 $x_1, \ldots, x_n$ 为独立的布尔变量, 根据经典概率论的方法, 计算其 $\mathbb{F}_2$ 上求和变量 $x = x_1 \oplus x_2 \oplus \cdots \oplus x_n$ 的分布相当不便:

$$p(x = 0) = \sum_{\substack{(c_1, \ldots, c_n) \in \mathbb{F}_2^n \\ c_1 + \cdots + c_n = 0}} \prod_{i=1}^{n} p(x_i = c_i). \tag{1.5}$$

另一方面, 由于布尔变量 x_i 之间的独立性, 因此有

$$\mathrm{E}(-1)^x = \mathrm{E}(-1)^{x_1 + \cdots + x_n} = \prod_{i=1}^{n} \mathrm{E}(-1)^{x_i}.$$

由 (1.1) 直接得到具有重要密码学意义的堆积引理 (参见文献 [2,3]):

命题 1.2 设 $x_1, \ldots, x_n$ 为独立的布尔变量, $x = x_1 \oplus x_2 \oplus \cdots \oplus x_n$, 则

$$\hat{p}_x = \hat{p}_{x_1} \times \hat{p}_{x_2} \times \cdots \times \hat{p}_{x_n}, \tag{1.6}$$

$$p(x = 0) = \frac{1 + \prod_{i=1}^{n} \hat{p}_{x_i}}{2}. \tag{1.7}$$

上述结论表明, 基于偏差度的表达方式 (1.6) 或 (1.7) 相对经典方式 (1.5) 更为简洁, 易于计算与分析.

例 1.3 对于一个参数 $p_0 = \mathrm{prob}(\xi = 0)$ 未知的布尔变量 ξ, 通过 n 次数据采样后作 $p = 1/2$ 的假设检验, 则其基本的统计参数为

$$\chi_n = \frac{\xi_n - np}{\sqrt{np(1-p)}} = \frac{\xi_n - n/2}{\sqrt{n/4}} = \left(\frac{2\xi_n}{n} - 1 \right) \sqrt{n}, \tag{1.8}$$

其中 ξ_n 为 n 次采样中 '0' 的出现频次. 根据中心极限定理 [4] (Lindeberg-Lévy 定理), χ_n 的极限分布为标准正态分布 $N(0, 1)$, 且由 Borel 强大数定律 [4], ξ_n/n 以概率 1 收敛于 p_0, 故 χ_n 渐近于

$$\chi = (2p_0 - 1)\sqrt{n} = \hat{p}_\xi \sqrt{n}. \tag{1.9}$$

这个渐近结果给出了大样本量下 ξ 相对于 $p=1/2$ 的统计偏差水平, 具有重要的统计意义, 其中 n 为统计的样本规模, $\hat{p}_\xi$ 是 ξ 的分布特征, 而 $\chi^2=n\hat{p}_\xi^2$ 的意义可以类比于质量为 m 的物体以 v 的速度运动所产生的动能 $E=\frac{1}{2}mv^2$.

1.2 随机事件的形式概率

定义 1.2 对于 Ω 上随机事件 A, 其经典概率为 $p(A)$, 称

$$\hat{p}(A)=p(A)-p(\bar{A})=2p(A)-1 \tag{1.10}$$

为 A 的形式概率.

显然, $\hat{p}(A)$ 与 $p(A)$ 可以互相表示, 且有

$$p(A)=\frac{1+\hat{p}(A)}{2}. \tag{1.11}$$

对于随机事件 A, 可唯一定义布尔变量

$$\xi=\begin{cases}0, & \text{如果 } A \text{ 发生},\\ 1, & \text{如果 } A \text{ 不发生}.\end{cases}$$

反之, 对于布尔变量 ξ, 可唯一定义 Ω 中一个随机事件 $A=\{\xi=0\}$. 我们称上述 ξ 和 A 是伴生的, 这种对应关系使后面的分析可以在事件的形式概率与布尔变量的偏差度之间自然地转换, 且有

$$\hat{p}(A)=\hat{p}_\xi. \tag{1.12}$$

根据定义, 不难推出如下性质:

命题 1.3 (互反性) 对任意随机事件 A, 有

$$\hat{p}(\bar{A})=-\hat{p}(A). \tag{1.13}$$

命题 1.4 (可乘性) 设 x、y 和 z 为布尔变量, $A_1=\{x=y\}$, $A_2=\{y=z\}$. 若 A_1 与 A_2 互相独立, 则

$$\hat{p}(x=z)=\hat{p}(A_1)\cdot\hat{p}(A_2)=\hat{p}(x=y)\hat{p}(y=z). \tag{1.14}$$

命题 1.5 (可加性) 设事件 $D_1,\dots,D_n$ 为全空间 Ω 的分解系, 即 D_i $(i=1,2,\dots,n)$ 之间互斥, 且 $\bigcup_{i=1}^n D_i=\Omega$, 则

$$\hat{p}(A)=\sum_{i=1}^n p(D_i)\hat{p}(A\mid D_i). \tag{1.15}$$

上述命题表明, 形式概率不仅蕴含着一定的概率意义, 而且也具有概率运算的某些重要性质和类似的基本规则, 从而可以理解为某种特殊意义上的概率.

在密码学研究中, 相对于经典概率 p, 形式概率 $\hat{p}=2p-1$ 是更为重要的参数 (参见文献 [5]).

2 形式概率的基本意义

随机事件的形式概率一方面具有内在的概率意义, 另一方面却有正负性, 从而超越了熟知的概率概念, 其本质需要从一个新的角度来理解.

为进一步阐述形式概率的意义, 我们给出如下定义:

定义 2.1 设 A 和 $B_1,\ldots,B_n$ 是 Ω 上的随机事件, $B_1,\ldots,B_n$ 之间两两互斥, B 为 $\{B_i\}$ 之并, 如果条件概率满足以下关系:

(1) 对任意 i, $p(A\mid B_i)=0$ 或 $p(A\mid B_i)=1$;

(2) $p(A\mid \bar{B})=1/2$,

则称 $B_1,\ldots,B_n$ 为 A 的一个完整的控制事件组, 并称常数

$$C_i=\hat{p}(A\mid B_i)=\begin{cases}1, & \text{如果 } p(A\mid B_i)=1,\\ -1, & \text{如果 } p(A\mid B_i)=0\end{cases}$$

为 B_i 对 A 的控制示性数.

在上述定义下, 不难证明如下命题:

命题 2.1 设 $B_1,\ldots,B_n$ 为 A 的一组完整的控制事件, 则

$$\hat{p}(A)=\sum_{i=1}^{n}C_ip(B_i), \tag{2.1}$$

$$p(A)=\frac{1+\sum_{i=1}^{n}C_ip(B_i)}{2}. \tag{2.2}$$

在定义 2.1 的条件下, 事件 A 可以按 B 分成两部分:

(1) 在事件 B 以外, 事件 A 均匀地随机发生;

(2) 在事件 B_i 以内, 事件 A 必然发生或必不发生, 即事件 B_i 为事件 A 提供了值为 $p(B_i)$ 的 "必然" 或 "必否" 概率.

因此, 概率 $p(A)$ 可以分成 "真随机" (白噪音) 和 "非随机" (即有条件地确定) 两部分, 其中真正有意义的是后者. 形式概率 (偏差度) 反映了确定性部分的份额, 其数值是控制事件组概率的正、负代数和, 各分项的符号 C_i 表示了 B_i 控制下事件 A 必然或必否的区别.

最常见的是 $n=1$ 的特殊情形, 即 B 单独构成 A 的完整控制事件, 此时,

$$\hat{p}(A)=\begin{cases}p(B), & \text{如果 } p(A\mid B)=1,\\ -p(B), & \text{如果 } p(A\mid B)=0,\end{cases}$$

$$p(A)=\frac{1+2\hat{p}(A)}{2}=\frac{1\pm p(B)}{2},$$

其中 $|\hat{p}(A)|=p(B)$ 反映了事件 A 中必然或必否的程度, 而 $\hat{p}(A)$ 的正、负指出了必然或必否的极性方向. 因此, 形式概率实际上是倾向性控制条件的发生概率.

需要指出的是, 对于古典概率空间 $\Omega=\mathbb{F}_2^n$ 中的随机事件, 都不难形式地构造出控制事件, 而且一般并不唯一.

3 布尔函数间相关性的形式概率分析

二元域 $\mathbb{F}_2$ 上多变量函数, 即 $\mathbb{F}_2^n \to \mathbb{F}_2$ 的映射, 称为 n 元布尔函数. 布尔函数之间的相关性是密码学中的重要问题.

当自变量 $x_1, \ldots, x_n$ 为独立均匀布尔变量时, 由 n 元布尔函数 $f(x)$ 诱导出相应的布尔变量 f. 因此, 我们定义布尔函数 $f(x)$ 的偏差度为其布尔变量 f 的偏差度 $\hat{p}_f$. 易见,

$$\begin{aligned}\hat{p}_f &= \frac{\#\{x \in \mathbb{F}_2^n \mid f(x) = 0\} - \#\{x \in \mathbb{F}_2^n \mid f(x) = 1\}}{2^n} \\ &= \frac{\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)}}{2^n}.\end{aligned} \tag{3.1}$$

进一步地, 通过极性化映射, 可以将布尔变量 f 唯一地对应为实值随机变量

$$\hat{f} = (-1)^f = 1 - 2f.$$

显然, 布尔函数 $f(x)$ 和 $g(x)$ 的相关性/独立性可以通过实值随机变量 $\hat{f}$ 和 $\hat{g}$ 来讨论. 根据前面关于偏差度的讨论, 易得下列命题:

命题 3.1 $\hat{f}$ 的均值和方差可由 f 的偏差度简单表示:

(1) $\mathrm{E}\hat{f} = \hat{p}_f$, $f(x)$ 为常数当且仅当 $\hat{p}_f = \pm 1$;

(2) $\mathrm{D}\hat{f} = 1 - \hat{p}_f^2$, $f(x)$ 为常数当且仅当 $D\hat{f} = 0$.

命题 3.2 设 $f(x)$ 和 $g(x)$ 为 n 元布尔函数, 则 $\hat{f}$ 和 $\hat{g}$ 的协方差为

$$\mathrm{Cov}(\hat{f}, \hat{g}) = \hat{p}_{f \oplus g} - \hat{p}_f \hat{p}_g. \tag{3.2}$$

命题 3.3 布尔函数 $f(x)$ 和 $g(x)$ 不相关当且仅当 $\mathrm{Cov}(\hat{f}, \hat{g}) = 0$, 即

$$\hat{p}_{f \oplus g} = \hat{p}_f \hat{p}_g. \tag{3.3}$$

协方差反映了函数间的相关性, 单位化后可以作为度量相关程度的系数. 当 $f(x)$ 和 $g(x)$ 都不为常数时, 定义其相关系数为

$$C(f, g) = \frac{\mathrm{Cov}(\hat{f}, \hat{g})}{\sqrt{D\hat{f} \cdot D\hat{g}}} = \frac{\hat{p}_{f \oplus g} - \hat{p}_f \hat{p}_g}{\sqrt{(1 - \hat{p}_f^2)(1 - \hat{p}_g^2)}}, \tag{3.4}$$

同时, 我们规定常数函数与任意布尔函数的相关系数为 0. 由 Cauchy-Schwartz 不等式可知 $|C(f, g)| \leqslant 1$. $C(f, g)$ 给出了布尔函数之间的相关程度: 系数为 0 时函数间不相关; 系数的绝对值越大, 则相关性越强; 系数达到 ± 1 当且仅当 $\hat{f} = \pm \hat{g}$, 即 $f(x) = g(x)$ 或 $f(x) = g(x) \oplus 1$, 此时相关性最大.

上述讨论表明, 布尔函数的相关性可以由函数的偏差度简洁地表出, 克服了用经典概率表达的繁琐性.

4 布尔函数关于线性函数的形式概率分解

记 n 元布尔函数全体为 $\mathcal{F}_n$, 对任意 $c = (c_1, \ldots, c_n) \in \mathbb{F}_2^n$, 定义线性函数

$$c \cdot x = \bigoplus_{i=1}^{n} c_i x_i.$$

线性函数是 $\mathcal{F}_n$ 中最简单的函数, 同时我们将看到, 在形式概率意义下也是最基本的函数.

对于布尔函数 $f(x)\in\mathcal{F}_n$, 令

$$W_f(c)=\frac{1}{2^n}\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)\oplus c\cdot x},\quad c\in\mathbb{F}_2^n,$$

称 $W_f=\{W_f(c)\}$ 为 $f(x)$ 的 Walsh 谱. 不难看出,

$$W_f(c)=p(f(x)=c\cdot x)-p(f(x)\neq c\cdot x)=\hat{p}(f(x)=c\cdot x),\tag{4.1}$$

即 $W_f(c)$ 是 $f(x)$ 与 $c\cdot x$ 相等的形式概率 ($f(x)$ 与 $c\cdot x$ "必等" 的概率), 以下简记为 $\hat{p}_f(c)$.

布尔函数的 Walsh 谱具有重要的密码学性质, 这方面已有大量的研究结果, 最基本的结果综述如下 (参见文献 [5–7]):

引理 4.1 将 Walsh 谱 $W_f=(\hat{p}_f(c))_{0\leqslant c<2^n}$ 和极性化函数 $\hat{f}=(\hat{f}(x))_{0\leqslant x<2^n}$ 看作 2^n 维实系数列向量, 其下标为 $c=(c_1,\ldots,c_n)$ 和 $x=(x_1,\ldots,x_n)$ 表示的二进制数, 则

(1) W_f 与 $\hat{f}$ 之间有 Hadamard 变换关系:

$$W_f=H^{-1}\hat{f}=2^{-n}H\hat{f},\tag{4.2}$$

$$\hat{f}=HW_f,\tag{4.3}$$

其中 $H=((-1)^{i\cdot j})_{0\leqslant i,j<2^n}$, $i\cdot j$ 表示 i 和 j 的二进制系数向量在 $\mathbb{F}_2$ 上的内积.

(2) W_f 满足一次守恒和二次守恒关系:

$$\sum_{c\in\mathbb{F}_2^n}\hat{p}_f(c)=(-1)^{f(0)},\tag{4.4}$$

$$\sum_{c\in\mathbb{F}_2^n}(\hat{p}_f(c))^2=1.\tag{4.5}$$

由引理可以得到如下重要结论:

命题 4.1 在极性化意义下, 布尔函数 $f(x)$ 可唯一表示成线性函数的加权组合:

$$\hat{f}(x)=\sum_{c\in\mathbb{F}_2^n}\hat{p}_f(c)(-1)^{c\cdot x}=\sum_{c\in\mathbb{F}_2^n}\hat{p}_f(c)(c\cdot x)^{\wedge},\tag{4.6}$$

上式称为布尔函数关于线性函数的形式概率分解式.

从形式概率的角度看, 在极性化意义下, $f(x)$ 分解为线性函数族 $\{c\cdot x\mid c\in\mathbb{F}_2^n\}$ 的加权组合, 配权系数恰为 $f(x)$ 的 Walsh 谱. 线性函数族构成了整个布尔函数空间的一组正交基, $f(x)$ 与线性函数 $c\cdot x$ 必等的事件组也构成了形式概率空间的一个完全分解, 示意图见表 1 (表中以 "$a\equiv b$" 简单表示 "a 与 b 必等").

表 1 形式概率分解示意图

Ω 分解	$f(x)\equiv 0$	$f(x)\equiv x_n$	$f(x)\equiv x_{n-1}$	$\cdots$	$f(x)\equiv x_1\oplus\cdots\oplus x_n$
形式概率	$\hat{p}_f(0)$	$\hat{p}_f(1)$	$\hat{p}_f(2)$	$\cdots$	$\hat{p}_f(2^n-1)$

因此, 一般非线性布尔函数的统计性质都可通过线性函数及相应的形式概率来分析, 而线性函数族 $\{c\cdot x \mid c\in \mathbb{F}_2^n\}$ 作为桥梁, 可为非线性问题提供线性化解决方法. 下面给出此方法的两个应用案例.

两个逻辑函数 $f(x)$ 和 $g(x)$ 的符合率是分析其相关性的重要参数, 其形式概率为

$$\hat{p}(f(x)=g(x))=\mathrm{E}(-1)^{f(x)\oplus g(x)}=\mathrm{E}\hat{f}(x)\hat{g}(x)=\frac{\hat{f}\cdot\hat{g}}{2^n}=\frac{W_f^{\mathrm{T}}H^{\mathrm{T}}HW_g}{2^n}=W_f\cdot W_g,$$

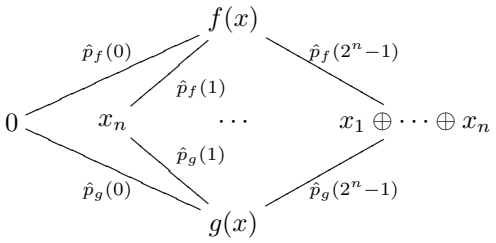
其中 T 表示向量和矩阵的转置. 由此得到如下命题:

命题 4.2 设 $f(x),g(x)\in\mathcal{F}_n$, 则

$$\hat{p}_{f\oplus g}=\hat{p}(f(x)=g(x))=W_f\cdot W_g. \tag{4.7}$$

推论 4.1 $\hat{f}$ 和 $\hat{g}$ 的协方差 $\mathrm{Cov}(\hat{f},\hat{g})=W_f\cdot W_g-\hat{p}_f\hat{p}_g$.

上述命题的分析过程可作直观的理解: $f(x)$ 和 $g(x)$ 都可按形式概率分解到线性函数组成的正交基上, 如下图简示:



从而,

$$\hat{p}(f(x)=g(x))=\sum_{c\in\mathbb{F}_2^n}\hat{p}(f(x)=c\cdot x)\hat{p}(c\cdot x=g(x))=\sum_{c\in\mathbb{F}_2^n}\hat{p}_f(c)\hat{p}_g(c)=W_f\cdot W_g.$$

上述分析方法可以得到进一步的结果. 定义布尔函数 $f(x)$ 的微分谱为

$$D_f=\{\hat{q}_f(d)\mid \hat{q}_f(d)=\hat{p}(f(x)=f(x\oplus d)),d\in\mathbb{F}_2^n\}, \tag{4.8}$$

这是布尔函数的重要特征. 对任意 $d\in\mathbb{F}_2^n$, 令 $g(x)=f(x\oplus d)$, 则

$$\begin{aligned}\hat{p}(g(x)=c\cdot x)&=\hat{p}(f(x\oplus d)=c\cdot x)=\hat{p}(f(x)=c\cdot(x\oplus d))\\&=\hat{p}(f(x)=c\cdot x\oplus c\cdot d)=(-1)^{c\cdot d}\hat{p}(f(x)=c\cdot x).\end{aligned}$$

由命题 4.2 和上式有

$$\hat{q}(d)=\hat{p}(f(x)=g(x))=\sum_{c\in\mathbb{F}_2^n}\hat{p}(f(x)=c\cdot x)\hat{p}(g(x)=c\cdot x)=\sum_{c\in\mathbb{F}_2^n}(-1)^{c\cdot d}\hat{p}_f^2(c).$$

据此可得微分谱与 Walsh 谱的关系 (参见文献 [5,8–10]):

命题 4.3 令 W_f^2 表示 Walsh 谱按分量平方所得的列向量, D_f 也看作列向量 $(\hat{q}_f(d))_{0\leqslant d<2^n}$, 则

$$D_f=HW_f^2.$$

参考文献

1 Shannon C E. A mathematical theory of communication. ACM Sigmobile Mobile Comp Comm, 2001, 5: 3–55
2 Zeng K, Huang M. On the linear syndrome method in cryptoanalysis. In: Advances in Cryptology-CRYPTO'88. Lecture Notes in Computer Science, vol. 403. Berlin: Springer-Verlag, 1990, 469–478
3 Massey J L. Some applications of source coding to cryptography. European Trans Telecomm, 1994, 5: 421–429
4 《现代数学手册》编纂委员会. 现代数学手册 (随机数学卷). 武汉: 华中科技大学出版社, 2000, 35–36
5 Joux A. Algorithmic Cryptanalysis. Boca Raton: CRC Press, 2009, 10–12
6 Shanks J. Computation of the fast Walsh-Fourier transform. IEEE Trans Comput, 1969, 100: 457–459
7 Xiao G Z, Massey J L. A spectral characterization of correlation-immune combining functions. IEEE Trans Inform Theory, 1988, 34: 569–571
8 Forre R. The strict advalanche criterion: Spectral properties of Boolean functions and an extended definition. In: Advances in Cryptology-CRYPTO'88. Lecture Notes in Computer Science, vol. 403. Berlin: Springer-Verlag, 1990, 450–468
9 Chabaud F, Vaudenay S. Links between differential and linear cryptoanalysis. In: Advances in Cryptology—EUROCRYPT'94. Berlin: Springer-Verlag, 1994, 356–365
10 Daemen J, Govaerts R, Vandewalle J. Correlation matrices. In: Fast Software Encryption'94. Berlin: Springer-Verlag, 1994, 275–285

Analysis of Boolean variables using formal probability

HUANG MinQiang

Abstract In this paper, we analyze the probabilistic measurement of random binary variables, by differentiating its deterministic part from white noise, and introduce a new concept of formal probability which is different from the concept of classical probability. Using formal probability, we develop a concise method for analysis and computation of Boolean variables, to solve problems which are difficult to analyze and compute with classical methods.

Keywords **Boolean variable, Boolean function, distribution bias, formal probability**

MSC(2010) **06E30, 68Q87**

doi: 10.1360/N012016-00246