模 m 加法的一类线性逼近关系研究

王 健,戚文峰,郑群雄
(解放军信息工程大学数学工程与先进计算国家重点实验室,河南郑州 450001)

摘 要: 该文研究模 m 加法的线性逼近问题,其中 m 为大于 3 的整数.利用分类计数方法,文中给出了任意 k 个整数求和模 m 的最低两个比特异或值用每一个整数的最低两个比特异或值去逼近时概率值的精确计算公式.此外,对于 $k=2$、3 或 4,文中还进一步分析了这类线性逼近的效果.

关键词: 密码学; 线性分析; 模加法; 线性逼近
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2015)11-2194-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2015.11.009

Research on the Linear Approximation Relationship of Addition Modulo m

WANG Jian, QI Wen-feng, ZHENG Qun-xiong
(*PLA Information Engineering University State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, Henan* 450001, *China*)

Abstract: The linear approximation of addition modulo m is studied in this paper, where $m>3$. Using classification counting method, an exact probability formula of the XOR of the lowest two bits of the summation of k integers modulo m approximate to the XOR of the lowest two bits of every integer is given in this paper. Moreover, the effect of this approximation is discussed for $k=2,3$ or 4.

Key words: cryptography; linear cryptanalysis; modular addition; linear approximation

1 引言

线性分析是 M Matsui[1]于 1993 年针对 DES 算法提出的一种密码分析方法,其核心思想是通过寻找密钥、明文和密文之间具有(明显)偏差的线性关系,在已知一定量的明密文对的条件下以较高的概率恢复出部分密钥.自提出以来,线性分析广泛应用于分组密码的设计与分析中,并且能够抵抗线性分析也成了分组密码算法设计的一项基本准则.线性分析也广泛应用于序列密码中,它通常与区分攻击相结合,通过建立线性区分器来将目标算法产生的密钥序列与随机序列区分开来[2].

线性分析的核心在于寻找目标密码算法输入和输出之间具有(明显)偏差的线性关系.然而由于密码算法的输入输出空间往往非常庞大,因此通过遍历输入输出全体空间来寻找具有(明显)偏差的线性关系往往是不实用的.通常人们首先分析密码算法中某些非线性组件的最佳线性逼近,然后优化组合得到目标密码算法输入和输出之间具有(明显)偏差的线性关系.在许多情况下,密码算法的非线性组件是由一些基本运算所构建,如模加运算和模乘运算等,因此国内外许多学者开始研究密码算法中常用的基本运算的线性逼近关系.

模 2^n 加法运算是广泛应用的一类基本运算,特别当 n 是计算平台的比特数时更是如此,如 $n=8,16$ 或 32.关于模 2^n 加法的线性逼近,J Wallén 等人[3]已经给出了任意多个整数模 2^n 加的线性逼近优势的具体计算公式;孙莹等人[4]分析了进位返加运算与异或运算及模 2^n 加法运算的相容性,并给出了其相容概率,从中可知进位返加运算与模 2^n 加法运算具有很大的相似性;张龙等人[5]分析了模 2^n 加运算与二元域上异或运算差值的概率分布,并给出了其递推公式;陈士伟等人[6]研究了模 2^n 加整体逼近模 2 加产生的噪声函数的概率分布;薛帅等人[7,8]对任意多个整数模 2^n 加法和减法的最佳线性逼近优势问题做了详细研究.目前模 2^n 加法的研究成果广泛应用于密码算法的攻击中,如 Trivium[9]、SNOW 2.0[10]、MD5[11]等.由于模 2^n-1 加法运算比模 2^n 加法运算具有更为复杂的进位关系,因此近年来模 2^n

收稿日期:2014-05-04;修回日期:2015-03-05;责任编辑:马兰英
基金项目:国家自然科学基金(No.61272042,No.61402524);信息保障技术重点实验室开放基金(No.KJ-13-005)

-1 加法运算受到了许多关注.特别地,模 $2^{31}-1$ 加法运算已经应用于 3GPP LTE 加密算法——ZUC 算法[12]的设计中.2011 年,冯秀涛等[13]利用模 2^n 加法线性逼近的成果给出了两个输入时的模 2^n-1 加法线性逼近优势的计算公式,并进一步用递归的方法给出了任意多个输入时线性逼近优势的计算公式,这为研究 ZUC 算法抵抗线性分析的能力提供了很好的依据.

相对于模 2^n 加法和模 2^n-1 加法,模一般整数 m 加法具有更为复杂的进位关系,各比特之间的关系更难以刻画,进而对其线性逼近的分析也更难.目前只有田甜等[14]给出了模奇数 m 加法最低比特的线性逼近优势的计算公式,并将这个结果应用于 l-序列[15]的线性分析.本文研究模 m 加法最低两比特之间的线性关系,其中 m 是大于 3 的整数,并利用分类计数方法得到了其线性逼近优势的精确公式.此外,对于 $k=2$、3 或 4,文中还进一步分析了这类线性逼近的效果,这些结果有助于分析模 m 加法抗线性分析的能力.

2　准备知识

本文中常用的符号定义如下:

$\lfloor x\rfloor$	小于或等于 x 的最大整数;
$\lceil x\rceil$	大于或等于 x 的最小整数;
$+$、$-$、$\cdot$	普通的整数加法、减法和乘法运算;
Z_m	m 元集$\{x\mid 0\leqslant x\leqslant m-1, x$ 为整数$\}$;
Z_m^k	k 个 Z_m 的笛卡尔积,即 $Z_m^k=\{(x_1,x_2,\cdots,x_k)\mid x_i\in Z_m, 1\leqslant i\leqslant k\}$;
$x^{(i)}$	x 二进制展开的第 i 比特,例如 $5^{(0)}=1, 5^{(1)}=0, 5^{(2)}=1$,从而 $5=5^{(0)}+5^{(1)}\cdot 2+5^{(2)}\cdot 2^2$;
$\oplus$	模 2 加运算;
$\otimes$	内积运算,定义为 $\omega\otimes x=\bigoplus_{i=0}^{n-1}\omega^{(i)}\cdot x^{(i)}$,其中 $x=\sum_{i=0}^{n-1}x^{(i)}\cdot 2^i$, $\omega=\sum_{i=0}^{n-1}\omega^{(i)}\cdot 2^i$;
$\lvert A\rvert$	若 A 是集合,则 $\lvert A\rvert$ 表示 A 中元素的个数;若 A 是实数,则 $\lvert A\rvert$ 表示 A 的绝对值;
$\binom{n}{k}$	组合数 $\frac{n!}{k!\,(n-k)!}$,并且当 $k>n$ 时规定 $\binom{n}{k}=0$;
$a \bmod m$	a 模 m 的最小非负剩余;
$a\equiv b \bmod m$	a 与 b 模 m 同余.

在本文中,总假定 m 是任意给定的大于 3 的整数且 $2^{n-1}\leqslant m<2^n$.设 k 是大于 1 的整数,f 是 Z_m^k 到 Z_m 的函数.对任意给定的 $k+1$ 个元素 $\mu,\omega_1,\cdots,\omega_k\in Z_m$,由 $\mu,\omega_1,\cdots,\omega_k$ 确定的 f 的线性逼近关系定义为:

$$\mu\otimes f(x_1,x_2,\cdots,x_k)=\bigoplus_{i=1}^{k}\omega_i\otimes x_i$$

上式对 f 函数的线性逼近优势可以用如下定义的偏差来衡量:

$$cor_f(\mu;\omega_1,\cdots,\omega_k)=2\Pr\Big(\mu\otimes f(x_1,x_2,\cdots,x_k)=\bigoplus_{i=1}^{k}\omega_i\otimes x_i\Big)-1,$$

其中 $x_1,x_2,\cdots,x_k$ 是 Z_m 上相互独立且服从均匀分布的随机变量.显然 $cor_f(\mu;\omega_1,\cdots,\omega_k)\in[-1,1]$,并且 $\lvert cor_f(\mu;\omega_1,\cdots,\omega_k)\rvert$ 越大,线性逼近优势越明显.

本文我们研究 $f(x_1,x_2,\cdots,x_k)=(x_1+x_2+\cdots+x_k \bmod m)$ 且 $\mu=\omega_1=\cdots=\omega_k=3$ 时的线性逼近关系.为了方便叙述,以后简记

$$\Pr\Big(3\otimes(x_1+x_2+\cdots+x_k \bmod m)=\bigoplus_{i=1}^{k}(3\otimes x_i)\Big)$$

为 $P_m(k)$,并简记 $cor_f(\mu;\omega_1,\cdots,\omega_k)$ 为 $cor_m(k)$,那么 $cor_m(k)=2P_m(k)-1$.

3　主要结论

在给出本文的主要结论之前,我们首先给出若干必要的引理.

将组合论中关于分配问题的公式转化为方程解的个数公式可得到下述引理,详见(文献[16],定理 7.3.3).

引理 1[16]　设 y 和 k 是整数且 $k\geqslant 2$,记 $M_m(k,y)$ 为 k 元一次不定方程

$$x_1+x_2+\cdots+x_k=y$$

在 Z_m^k 上的解个数,则

$$M_m(k,y)=\sum_{i=0}^{k}(-1)^i\cdot\binom{k}{i}\cdot\binom{y+k-m\cdot i-1}{k-1}$$

对 $0\leqslant j\leqslant k-1$,令

$$\Omega_j=\{(x_1,x_2,\cdots,x_k)\in Z_m^k\mid j\cdot m\leqslant x_1+x_2+\cdots+x_k<(j+1)\cdot m\}\tag{1}$$

则 $\Omega_0,\Omega_1,\cdots,\Omega_{k-1}$ 构成 Z_m^k 的一个拆分,即 $\Omega_0,\cdots,\Omega_{k-1}$ 两两互不相交,且 $Z_m^k=\bigcup_{j=0}^{k-1}\Omega_j$.

引理 2　设 s 和 k 是整数且 $k\geqslant 2, 0\leqslant s\leqslant k$.对 $0\leqslant j\leqslant k-1$,记 $\Gamma_m(k,s,j)$ 为 Ω_j 中满足

$$x_1^{(0)}+x_2^{(0)}+\cdots+x_k^{(0)}=s$$

的 $(x_1,x_2,\cdots,x_k)$ 的个数,则

$$\Gamma_m(k,s,j)=\begin{cases}\binom{k}{s}\cdot\sum_{p=0}^{k-s}\binom{k-s}{p}\cdot\sum_{q=\lceil(j\cdot m-s)/2\rceil-(m-1)/2\cdot p}^{\lfloor((j+1)\cdot m-1-s)/2\rfloor-(m-1)/2\cdot p}M_{\frac{m-1}{2}}(k-p,q), & \text{若 } m \text{ 为奇数;}\\ \binom{k}{s}\cdot\sum_{q=\lceil(j\cdot m-s)/2\rceil}^{\lfloor((j+1)\cdot m-1-s)/2\rfloor}M_{\frac{m}{2}}(k,q), & \text{若 } m \text{ 为偶数.}\end{cases}$$

证明 令 $\Gamma'_m(k,s,j)$表示 Ω_j 中满足

$$x_1^{(0)}=x_2^{(0)}=\cdots=x_s^{(0)}=1,x_{s+1}^{(0)}=\cdots=x_k^{(0)}=0 \quad (2)$$

的$(x_1,x_2,\cdots,x_k)$的个数,则由对称性可知

$$\Gamma_m(k,s,j)=\binom{k}{s}\cdot\Gamma'_m(k,s,j) \quad (3)$$

下面计算 $\Gamma'_m(k,s,j)$的值.

由式(2)知 $x_1,x_2,\cdots,x_s$ 为奇数,$x_{s+1},\cdots,x_k$ 为偶数,不妨设

$$\begin{cases}x_i=2y_i+1, & \text{若 } 1\leqslant i\leqslant s\\ x_i=2y_i, & \text{若 } s+1\leqslant i\leqslant k\end{cases}$$

则

$$\begin{aligned}&(x_1,x_2,\cdots,x_k)\in\Omega_j\\ \Leftrightarrow&j\cdot m\leqslant x_1+x_2+\cdots+x_k\leqslant(j+1)\cdot m-1\\ \Leftrightarrow&j\cdot m\leqslant 2(y_1+y_2+\cdots+y_k)+s\leqslant(j+1)\cdot m-1\\ \Leftrightarrow&\lceil(j\cdot m-s)/2\rceil\leqslant y_1+y_2+\cdots+y_k\leqslant\lfloor((j+1)\cdot m-1-s)/2\rfloor\end{aligned} \quad (4)$$

情形 *A*　*m* 为奇数

此时 $0\leqslant y_1,\cdots,y_s\leqslant(m-3)/2,0\leqslant y_{s+1},\cdots,y_k\leqslant(m-1)/2$.设 $y_{s+1},\cdots,y_k$ 中取值为$(m-1)/2$ 的有 p 个,$0\leqslant p\leqslant k-s$.注意到在 $y_{s+1},\cdots,y_k$ 这 $k-s$ 个变元中任意指定 p 个的取值为$(m-1)/2$ 时,满足式(4)的$(y_1,\cdots,y_k)$的个数均相同.因此不妨先假设 $y_{k-p+1},\cdots,y_k$ 的值为$(m-1)/2$,此时式(4)等价于

$$\begin{aligned}&\lceil(j\cdot m-s)/2\rceil-p\cdot(m-1)/2\leqslant y_1+y_2+\cdots+y_{k-p}\\ &\leqslant\lfloor((j+1)\cdot m-1-s)/2\rfloor-p\cdot(m-1)/2\end{aligned} \quad (5)$$

其中 $0\leqslant y_1,\cdots,y_{k-p}\leqslant(m-3)/2$,也即 $y_1,\cdots,y_{k-p}\in Z_{(m-1)/2}$.由引理 1 知满足式(5)的 $k-p$ 元组$(y_1,\cdots,y_{k-p})$的个数为

$$\sum_{q=\lceil(j\cdot m-s)/2\rceil-(m-1)/2\cdot p}^{\lfloor((j+1)\cdot m-1-s/2\rfloor-(m-1))/2\cdot p}M_{\frac{m-1}{2}}(k-p,q)$$

从而

$$\Gamma'_m(k,s,j)=\sum_{p=0}^{k-s}\binom{k-s}{p}\cdot\sum_{q=\lceil(j\cdot m-s)/2\rceil-(m-1)/2\cdot p}^{\lfloor((j+1)\cdot m-1-s/2\rfloor-(m-1)/2\cdot p}\cdot M_{\frac{m-1}{2}}(k-p,q) \quad (6)$$

将式(6)代入式(3)即得引理结论.

情形 *B*　*m* 为偶数

此时 $0\leqslant y_1,\cdots,y_k\leqslant(m-2)/2$,即 $y_1,\cdots,y_k\in Z_{m/2}$,从而由引理 1 知

$$\Gamma'_m(k,s,j)=\sum_{q=\lceil(j\cdot m-s)/2\rceil}^{\lfloor(j+1)\cdot m-1-s/2\rfloor}M_{\frac{m}{2}}(k,q) \quad (7)$$

将式(7)代入式(3)即得引理结论.

引理 3 设 y,j 为整数,则 $3\otimes(y-j \bmod 4)=3\otimes y$ 当且仅当如下三种情形有其一成立:

(1)$j\equiv 0 \bmod 4$.

(2)$j\equiv 1 \bmod 4$ 且 y 为偶数.

(3)$j\equiv 3 \bmod 4$ 且 y 为奇数.

证明 注意到

$$\begin{aligned}&3\otimes(y-j \bmod 4)\\ &=(y-j \bmod 4)^{(0)}\oplus(y-j \bmod 4)^{(1)}\\ &=(y^{(0)}\oplus j^{(0)})\oplus(y-j \bmod 4)^{(1)}\\ &=\begin{cases}(y^{(0)}\oplus j^{(0)})\oplus(y^{(1)}\oplus j^{(1)}), & \text{若 } y^{(0)}\geqslant j^{(0)}\\ (y^{(0)}\oplus j^{(0)})\oplus(y^{(1)}\oplus j^{(1)}\oplus 1), & \text{若 } y^{(0)}<j^{(0)}\end{cases}\\ &=\begin{cases}(3\otimes y)\oplus(3\otimes j), & \text{若 } y^{(0)}\geqslant j^{(0)}\\ (3\otimes y)\oplus(3\otimes j)\oplus 1, & \text{若 } y^{(0)}<j^{(0)}\end{cases}\end{aligned}$$

因此 $3\otimes(y-j \bmod 4)=3\otimes y$ 当且仅当

$$3\otimes j=\begin{cases}0, & \text{若 } y^{(0)}\geqslant j^{(0)}\\ 1, & \text{若 } y^{(0)}<j^{(0)}\end{cases} \quad (8)$$

验证易知式(8)成立当且仅当题设三个条件有其一成立.

注 1 由引理 3 知 $3\otimes(y-j \bmod 4)=(3\otimes y)\oplus 1$ 当且仅当 $j\equiv 2 \bmod 4$;或者 $j\equiv 1 \bmod 4$ 且 y 为奇数;或者 $j\equiv 3 \bmod 4$ 且 y 为偶数.

为了叙述方便,以下总记

$$S_i=\{s\mid 0\leqslant s\leqslant k \text{ 且 } s\equiv i \bmod 4\},0\leqslant i\leqslant 3$$

则 S_0,S_1,S_2,S_3 构成集合$\{0,1,\cdots,k\}$的一个拆分.

引理 4 对任意的非负整数 $x_1,x_2,\cdots,x_k$,令

$$s=x_1^{(0)}+x_2^{(0)}+\cdots+x_k^{(0)}$$

则 $3\otimes(x_1+x_2+\cdots+x_k)=\bigoplus_{i=1}^{k}(3\otimes x_i)$当且仅当 $s\in S_0\cup S_1$.

证明 注意到

$$\begin{aligned}&(x_1+x_2+\cdots+x_k)^{(0)}=x_1^{(0)}\oplus x_2^{(0)}\oplus\cdots\oplus x_k^{(0)},\\ &(x_1+x_2+\cdots+x_k)^{(1)}=(x_1^{(1)}\oplus x_2^{(1)}\oplus\cdots\oplus x_k^{(1)})\\ &\qquad\oplus(\lfloor(x_0^{(0)}+x_1^{(0)}+\cdots+x_k^{(0)})/2\rfloor \bmod 2)\\ &\qquad=(x_1^{(1)}\oplus x_2^{(1)}\oplus\cdots\oplus x_k^{(1)})\oplus s^{(1)}\end{aligned}$$

因此

$$\begin{aligned}3\otimes(x_1+x_2+\cdots+x_k)&=(x_1+x_2+\cdots+x_k)^{(0)}\\ &\quad\oplus(x_1+x_2+\cdots+x_k)^{(1)}\\ &=x_1^{(0)}\oplus x_2^{(0)}\oplus\cdots\oplus x_k^{(0)}\oplus x_1^{(1)}\\ &\quad\oplus x_2^{(1)}\oplus\cdots\oplus x_k^{(1)}\oplus s^{(1)}\\ &=\bigoplus_{i=1}^{k}(3\otimes x_i)\oplus s^{(1)}\end{aligned}$$

可知 $3\otimes(x_1+x_2+\cdots+x_k)=\bigoplus_{i=1}^{k}(3\otimes x_i)$当且仅当 $s^{(1)}=0$,也即 $s\in S_0\cup S_1$.

引理 5 设符号同前,$(x_1,x_2,\cdots,x_k)\in\Omega_j$,则

$3\otimes(x_1+\cdots+x_k \bmod m)=\bigoplus_{i=1}^{k}(3\otimes x_i)$当且仅当 $s=x_1^{(0)}+x_2^{(0)}+\cdots+x_k^{(0)}\in S_{k,m}(j)$,

其中,当 $m\equiv 0 \bmod 4$ 时,$S_{k,m}(j)=S_0\cup S_1$;

当 $m\equiv 1 \bmod 4$ 时,

$$S_{k,m}(j)=\begin{cases}S_0\cup S_1, & \text{若 } j\equiv 0 \bmod 4\\ S_0\cup S_3, & \text{若 } j\equiv 1 \bmod 4\\ S_2\cup S_3, & \text{若 } j\equiv 2 \bmod 4\\ S_1\cup S_2, & \text{若 } j\equiv 3 \bmod 4\end{cases}$$

当 $m\equiv 2 \bmod 4$ 时,

$$S_{k,m}(j)=\begin{cases}S_0\cup S_1, & \text{若 } j\equiv 0 \text{ 或 } 2 \bmod 4\\ S_2\cup S_3, & \text{若 } j\equiv 1 \text{ 或 } 3 \bmod 4\end{cases}$$

当 $m\equiv 3 \bmod 4$ 时,

$$S_{k,m}(j)=\begin{cases}S_0\cup S_1, & \text{若 } j\equiv 0 \bmod 4\\ S_1\cup S_2, & \text{若 } j\equiv 1 \bmod 4\\ S_2\cup S_3, & \text{若 } j\equiv 2 \bmod 4\\ S_0\cup S_3, & \text{若 } j\equiv 3 \bmod 4\end{cases}$$

证明　记 $y=x_1+x_2+\cdots+x_k$. 由 $(x_1,x_2,\cdots,x_k)\in\Omega_j$ 知

$$(y \bmod m)=y-j\cdot m$$

从而

$$3_{\otimes}(y \bmod m)=3_{\otimes}(y-j\cdot m)=3_{\otimes}(y-j\cdot m \bmod 4) \tag{9}$$

当 $m\equiv 0 \bmod 4$ 时,由式(9)知

$$3_{\otimes}(y \bmod m)=3_{\otimes}(y \bmod 4)=3_{\otimes}y$$

从而由引理 4 知 $3_{\otimes}(y \bmod m)=\bigoplus_{i=1}^{k}(3\otimes x_i)$ 当且仅当 $s\in S_0\cup S_1$.

当 $m\equiv 1,2$ 或 $3 \bmod 4$ 时,由于证明方法类似,因此我们只给出 $m=1 \bmod 4$ 时的证明. 此时由式(9)知

$$\begin{aligned}3_{\otimes}(y \bmod m)&=3_{\otimes}(y-j\cdot m \bmod 4)\\&=3_{\otimes}(y-j \bmod 4)\end{aligned} \tag{10}$$

下面根据 $j \bmod 4$ 的取值分 4 种情形讨论:

情形 1　$j\equiv 0 \bmod 4$

由引理 3 和式(10)知

$$3_{\otimes}(y \bmod m)=3_{\otimes}(y-j \bmod 4)=3_{\otimes}y$$

从而由引理 4 知 $3_{\otimes}(y \bmod m)=\bigoplus_{i=1}^{k}(3\otimes x_i)$ 当且仅当 $s\in S_0\cup S_1$.

情形 2　$j\equiv 1 \bmod 4$

由引理 3 和式(10)知

$$3_{\otimes}(y \bmod m)=3_{\otimes}(y-j \bmod 4)=\begin{cases}3\otimes y, & \text{若 } y \text{ 是偶数}\\ (3\otimes y)\oplus 1, & \text{若 } y \text{ 是奇数}\end{cases}$$

注意到 y 与 s 的奇偶性相同,因此由引理 4 知

$$\begin{cases}3\otimes y=\bigoplus_{i=1}^{k}(3\otimes x_i) \text{ 当且仅当 } s\in S_0, & \text{若 } y \text{ 是偶数}\\ (3\otimes y)\oplus 1=\bigoplus_{i=1}^{k}(3\otimes x_i) \text{ 当且仅当 } s\in S_3, & \text{若 } y \text{ 是奇数}\end{cases}$$

从而 $3_{\otimes}(y \bmod m)=\bigoplus_{i=1}^{k}(3\otimes x_i)$ 当且仅当 $s\in S_0\cup S_3$.

情形 3　$j\equiv 2 \bmod 4$

由引理 3 和式(10)知

$$3_{\otimes}(y \bmod m)=3_{\otimes}(y-j \bmod 4)=(3_{\otimes}y)\oplus 1,$$

从而由引理 4 知,$3_{\otimes}(y \bmod m)=\bigoplus_{i=1}^{k}(3\otimes x_i)$ 当且仅当 $s\in S_2\cup S_3$.

情形 4　$j\equiv 3 \bmod 4$

由引理 3 和式(10)知

$$3_{\otimes}(y \bmod m)=3_{\otimes}(y-j \bmod 4)=\begin{cases}3\otimes y, & \text{若 } y \text{ 是奇数}\\ (3\otimes y)\oplus 1, & \text{若 } y \text{ 是偶数}\end{cases}$$

类似情形 2 的讨论,$3_{\otimes}(y \bmod m)=\bigoplus_{i=1}^{k}(3\otimes x_i)$ 当且仅当 $s\in S_1\cup S_2$.

综上即得引理结论.

下面给出本文的主要结论,即 $P_m(k)$ 的精确计数公式.

定理 1　设符号同前,则

$$P_m(k)=\frac{\sum_{j=0}^{k-1}\sum_{s\in S_{k,m}(j)}\Gamma_m(k,s,j)}{m^k}$$

证明　对 $0\leqslant j\leqslant k-1$,记

$$\Theta_j=\{(x_1,\cdots,x_k)\in\Omega_j \mid 3_{\otimes}(x_1+\cdots+x_k \bmod m)=\bigoplus_{i=1}^{k}(3\otimes x_i)\}$$

其中 Ω_j 如式(1)定义. 注意到 $\Omega_0,\Omega_1,\cdots,\Omega_{k-1}$ 构成 Z_m^k 的一个拆分,因此

$$\begin{aligned}P_m(k)&=\Pr(3_{\otimes}(x_1+\cdots+x_k \bmod m)=\bigoplus_{i=1}^{k}(3\otimes x_i))\\&=\frac{\sum_{j=0}^{k-1}|\Theta_j|}{m^k}\end{aligned}$$

由引理 2 和引理 5 知 $|\Theta_j|=\sum_{s\in S_{k,m}(j)}\Gamma_m(k,s,j)$,故定理得证.

注 2　当 $m\equiv 0 \bmod 4$ 时,本文考虑的模 m 上加法的这类线性关系可简化为模 4 上加法的线性关系,故此时的结果可以参考文献[3],后文将不再考虑这种情形.

根据定理 1,对于较小的 k,如 $k=2,3,4$,我们可以给出 $P_m(k)$ 比较简洁的计数公式.

推论 1　(1)若 $m\equiv 1 \bmod 4$,则 $P_m(2)=\frac{m+1}{2m}$, $P_m(3)=\frac{m^2+2}{3m^2}$, $P_m(4)=\frac{m^3-m^2+2}{2m^3}$,从而

$$|cor_m(2)|=\frac{1}{m},\ |cor_m(3)|=\frac{m^2-4}{3m^2},$$

$$|cor_m(4)|=\frac{m^2-2}{m^3}.$$

(2)若 $m\equiv 2 \bmod 4$,则 $P_m(2)=\frac{m+2}{2m}$,

$P_m(3)=\frac{m^2+4}{2m^2}$,从而$|cor_m(2)|=\frac{2}{m}$,$|cor_m(3)|=\frac{4}{m^2}$.

(3)若 $m\equiv 3 \bmod 4$,则 $P_m(2)=\frac{3m^2+1}{4m^2}$,

$P_m(3)=\frac{2m^2+1}{3m^2}$,从而$|cor_m(2)|=\frac{m^2+1}{2m^2}$,

$|cor_m(3)|=\frac{m^2+2}{3m^2}$.

为更直观的认识定理 1 和推论 1,表 1 列出了当 $m\equiv 1 \bmod 4$ 时部分 m 和 k 对应的线性相关值(保留 10 位有效数字):

表 1 部分 m 和 k 对应的线性相关值

m	k	$P_m(k)$	$cor_m(k)$
2^5+1	2	0.5312500000	0.03030303030
$2^{10}+1$	2	0.5009765625	0.0009756097560
$2^{20}+1$	2	0.5000009537	0.0000009536734069
2^5+1	3	0.3339455158	0.3321089685
$2^{10}+1$	3	0.3333339678	0.3333320642
$2^{20}+1$	3	0.3333333333	0.3333333333
2^5+1	4	0.4848763113	0.03024737735
$2^{10}+1$	4	0.4995121961	0.0009756078989
$2^{20}+1$	4	0.4999995232	0.0000009536734069

注 3 由推论 1 和表 1 可知,这类线性逼近的效果与 m 和 k 的取值密切相关,当 $m\equiv 1 \bmod 4$ 且 m 充分大时,$|cor_m(3)|$的值接近于 1/3,这说明模 m 上 3 个元素加的最低两比特用各元素的最低两比特去逼近时,逼近优势约为 1/3.类似地,当 $m\equiv 3 \bmod 4$ 且 m 充分大时,$|cor_m(2)|$和$|cor_m(3)|$的值分别接近于 1/2 和 1/3;而对于 $k\in\{2,3,4\}$的其它情形,当 m 稍大时逼近优势并不明显.

注 4 直观上来说,随着 k 的增大,$P_m(k)$将越来越接近 1/2,这一现象也可以通过具体计算若干个 $P_m(k)$观察到,但很遗憾到目前为止我们还无法从理论上证明这一规律.

4 结束语

本文主要探讨模 m 加法线性逼近关系的性质,并给出了一类线性逼近优势的精确计数公式.在计算定理 1 中的概率公式时,我们曾试图利用递归方法给出递归关系式,但因为 Z_m^k 中满足要求的 k 元组$(x_1,x_2,\cdots,x_k)$分布不均匀,使得计算过程中无法绕开繁琐的组合计数方法,因而无法给出有效的递归关系式.另外,对于一般的整数 m,由于加法的进位关系非常复杂,而且高位比特的变化规律相比低位比特更难刻画,故目前我们还无法给出其它线性逼近优势的计算公式.下一阶段我们拟进一步考虑以下两个问题:

(1)模 m 加法第 i 比特,即 $\mu=\omega_1=\cdots=\omega_k=2^i$ 时的线性逼近优势.

(2)模 m 加法两相邻比特,即 $\mu=\omega_1=\cdots=\omega_k=2^{i+1}+2^i$ 时的线性逼近优势.

参考文献

[1] Matsui M. Linear cryptanalysis method for DES ciphers[A]. In Advances in Cryptology-EUROCRYPT 1993, Lecture Notes in Computer Science 765[C]. Berlin: Springer-Verlag, 1994. 386 – 397.

[2] Coppersmith D, Halevi S, Jutla C. Cryptanalysis of stream ciphers with linear masking[A]. In Advances in Cryptology-CRYPTO 2002, Lecture Notes in Computer Science 2442[C]. Berlin: Springer-Verlag, 2002. 515 – 532.

[3] Wallén J. Linear approximations of addition modulo 2^n[A]. In Fast Software Encryption 2003, Lecture Notes in Computer Science 2887[C]. Berlin: Springer-Verlag, 2003. 261 – 273.

[4] 孙莹,金晨辉. 进位返加与逐位模 2 加及模 2^n 加的相容程度分析[J]. 高校应用数学学报 A 辑, 2005, 20(3): 371 – 376.
Sun Ying, Jin Chen-hui. Consistent degree analysis of ones complement addition with bit-wise exclusive-OR and with addition module 2^n[J]. Appl Math J Chinese Univ Ser A, 2005, 20(3): 371 – 376. (in Chinese)

[5] 张龙,吴文玲,温巧燕. mod 2^n 加运算与 F_2 上异或运算差值的概率分布和递推公式[J]. 北京邮电大学学报, 2007, 30(1): 85 – 89.
Zhang Long, Wu Wen-ling, Wen Qiao-yan. Probability distribution and recursive formula of difference between mod 2^n sum and XOR over F_2[J]. Journal of Beijing University of Posts and Telecommunications, 2007, 30(1): 85 – 89. (in Chinese)

[6] 陈士伟,金晨辉,李席斌. 模 2^n 加整体逼近模 2 加产生的噪声函数的概率分布研究[J]. 电子与信息学报, 2009, 31(10): 2397 – 2401.
Chen Shi-wei, Jin Chen-hui, Li Xi-bin. Research on the noise functions produced by macrocosm approximation of XOR with addition modulo 2^n[J]. Journal of Electronics & Information Technology, 2009, 31(10): 2397 – 2401. (in Chinese)

[7] 薛帅,戚文峰. 模 2^n 加法最佳线性逼近关系研究[J]. 电子与信息学报, 2012, 34(9): 2156 – 2160.
Xue Shuai, Qi Wen-feng. Research on the best linear approximation of addition modulo 2^n[J]. Journal of Electronics & Information Technology, 2012, 34(9): 2156 – 2160. (in Chinese)

[8] 薛帅,戚文峰. 模 2^n 减法最佳线性逼近关系研究[J]. 信息工程大学学报, 2013, 14(1): 1 – 6.
Xue Shuai, Qi Wen-feng. Research on the best linear approximation of subtraction modulo 2^n[J]. Journal of Information En-

gineering University,2013,14(1):1 – 6.(in Chinese)
[9] 丁林,关杰. Trivium 流密码的基于自动推导的差分分析[J].电子学报,2014,42(8):1647 – 1652.
Ding Lin,Guan Jie. Differential cryptanalysis of trivium stream cipher based on automatic deduction[J]. Acta Electronica Sinica,2014,42(8):1647 – 1652.(in Chinese)
[10] Nyberg K,Wallén J. Improved linear distinguishers for SNOW 2.0[A]. In Fast Software Encryption 2006, Lecture Notes in Computer Science 4047[C]. Berlin: Springer-Verlag, 2006. 144 – 162.
[11] Berson T A. Differential cryptanalysis mod 2^{32} with applications to MD5[A]. In Advances in Cryptology-EUROCRYPT 1992, Lecture Notes in Computer Science 658[C]. Berlin: Springer-Verlag,1993. 71 – 80.
[12] ETSI/SAGE. Specification of the 3GPP confidentiality and integrity algorithms 128-EEA3 & 128-EIA3. Document 4:design and evaluation report, version:2.0[EB/OL]. http://zuc.dacas.cn/thread.aspx? ID = 2304,2011.
[13] Feng X T,C F Zhou,C K W. Linear approximations of addition modulo $2^n - 1$[A]. In Fast Software Encryption 2011, Lecture Notes in Computer Science 6733[C]. Berlin: Springer-Verlag,2011. 359 – 377.
[14] Tian T, Qi W F. Linearity properties of binary FCSR sequences[J]. Designs Codes and Cryptography, 2009, 52(3): 249 – 262.
[15] Klapper A, Goresky M. 2-Adic shift registers[A]. In Fast Software Encryption 1993, Lecture Notes in Computer Science 809[C]. Berlin: Springer-Verlag, 1994. 174 – 178.
[16] 柯召,魏万迪.组合论(上册)[M].北京:科学出版社,1981.

作者简介

王　健(通讯作者)　男,1990 年 1 月生于河南商城,硕士研究生,研究方向为密码学.
E-mail:wangj08@yeah.net

戚文峰　男,1963 年生,教授,博士生导师,研究方向为有限域、密码学.
E-mail:wenfeng.qi@263.net

郑群雄　男,1984 年生,博士,研究方向为密码学.
E-mail:qunxiong_zheng@163.com