Linear Approximations of Addition Modulo 2^n-1*

Xiutao Feng, Chunfang Zhou and Chuankun Wu

State Key Laboratory of Information Security, Institute of Software,
Chinese Academy of Sciences, Beijing, 100190, China.
{fengxt, zhcf, ckwu}@is.iscas.ac.cn

Abstract. Addition modulo $2^{31}-1$ is a basic arithmetic operation in the stream cipher ZUC. For evaluating ZUC in resistance to linear cryptanalysis, it is necessary to study properties of linear approximations of the addition modulo $2^{31}-1$. In this paper we discuss linear approximations of the addition modulo 2^n-1 for integer $n \geq 2$. As results, an exact formula on the correlations of linear approximations of the addition modulo 2^n-1 is given for the case when two inputs are involved, and an iterative formula for the case when more than two inputs are involved. For a class of special linear approximations with all masks being equal to 1, we further discuss the limit of their correlations when n goes to infinity. Let k be the number of inputs of the addition modulo 2^n-1. It's shows that when k is even, the limit is equal to zero, and when k is odd, the limit is bounded by a constant depending on k.

Key words: Linear approximation, modular additions, linear cryptanalysis.

1 Introduction

Linear cryptanalysis [1] is one of the most powerful and general cryptanalytic methods. Its main task is to find linear relations between the inputs and outputs of target functions. In block ciphers, we usually find some linear relations among keys, plaintexts and ciphertexts that hold with certian probability. If some plain-cipher text pairs are known, some bits of the key can be recovered with high probability [1, 2]. In stream ciphers, linear cryptanalysis is usually combined with distinguishing cryptanalysis together, and its goal is to establish a linear distinguisher to distinguish the keystream generated by the target algorithm from a random sequence [3, 4].

For both block ciphers and stream ciphers, it is important to find an efficient method for evaluating their resistance against linear cryptanalysis. It is known that most cipher algorithms are usually composed of some certain components and operations. Hence first of all we can calculate linear approximations of those components or operations. The addition modulo 2^n, specially when n is equal

* This work was supported by the Natural Science Foundation of China (Grant No. 60833008 and 60902024)

to the length of a computer word, e.g., 8, 16 or 32, is one of the most common operations, and is widely used in the design of cipher algorithms [5–8]. Rich results on the addition modulo 2^n have been obtained, see [9–15].

The addition modulo $2^n - 1$ is another important arithmetic operation [16, 17]. Some properties on the addition modulo $2^n - 1$ have been explored in [18, 19]. However few results on linear approximations on the addition modulo $2^n - 1$ can be found from public literatures. Recently a new stream cipher ZUC [20], together with 128-EEA3 and128-EIA3, is recommended as the third suit of LTE encryption and integrity candidate, see [21] for details. In ZUC, the addition modulo $2^{31} - 1$ is a basic operation since the LFSR of ZUC is defined over the prime field $\mathbb{F}_{2^{31}-1}$. For evaluating ZUC in resistance to linear cryptanalysis, it is necessary to study properties of linear approximations on the addition modulo $2^{31} - 1$. In this paper, by means of known results on the addition modulo 2^n, we directly derive a formula of correlations of arbitrary linear approximations of the addition modulo $2^n - 1$ with two inputs. As for the case where more than two inputs are involved, we further give an iterative formula. What's more, for a class of special linear approximations with all masks being equal to 1, we discuss the limit of their correlations when n goes to infinity. Let k be the number of inputs of the addition modulo $2^n - 1$. It's shows that when k is even, the limit is equal to zero, and when k is odd, the limit is a constant depending on k.

The rest of this paper is organized as follows: In section 2, we give the definitions of linear approximations and their correlations and recall some properties on the addition modulo 2^n briefly. In section 3 some basic properties of linear approximation of the addition modulo $2^n - 1$ are given, and more properties for the case $k = 2$ are given in section 4. In section 5 we further discuss the limit of linear approximations with all masks being equal to 1. Finally we conclude in section 6.

2 Preliminaries

2.1 Linear approximation and its correlation

Let n be a positive integer. Denoted by Z_{2^n} the set of integers x such that $0 \le x \le 2^n - 1$. Given an integer $x \in Z_{2^n}$, let

$$x = x^{(n-1)}x^{(n-2)} \cdots x^{(0)} = \sum_{i=0}^{n-1} x^{(i)}2^i$$

be the binary representation of x, where $x^{(i)} \in \{0, 1\}$. We call $x^{(i)}$ the i-th bit of x, $0 \le i \le n - 1$. In the rest of this paper, without further specification, we always denote by $x^{(i)}$ the i-th bit of the integer x in the binary representation. For arbitrary two integers $w, x \in Z_{2^n}$, the inner product of w and x is defined as below

$$w \cdot x = \bigoplus_{i=0}^{n-1} w^{(i)}x^{(i)}.$$

Let k be a positive integer and f be a function from $Z_{2^n}^k$ to Z_{2^n}. Given $k+1$ constants $u, w_1, \cdots, w_k \in Z_{2^n}$, the linear approximation of the function f determined by $u, w_1, \cdots, w_k$ is an approximate relation of the form

$$u \cdot f(x_1, \cdots, x_k) = \bigoplus_{i=1}^{k} w_i \cdot x_i, \tag{1}$$

and the $(k+1)$-tuple $(u, w_1, \cdots, w_k)$ is called to be a linear mask of f. The efficiency of the linear approximation (1) is measured by its correlation, which is defined as below

$$\mathbf{cor}_f(u; w_1, \cdots, w_k) = 2\Pr(u \cdot f(x_1, \cdots, x_k) = \bigoplus_{i=1}^{k} w_i \cdot x_i) - 1, \tag{2}$$

where the probability is taken over uniformly distributed $x_1, \cdots, x_k$.

2.2 Linear approximations of the addition modulo 2^n

In this section we recall linear approximations of the addition modulo 2^n briefly, for more details please refer to [9, 10].

Denote by $\boxplus$ the addition modulo 2^n, that is, for any $x_1, x_2 \in Z_{2^n}$, we have $x_1 \boxplus x_2 = (x_1 + x_2) \mod 2^n$. Let (u, w_1, w_2) be a linear mask of the addition $\boxplus$, and denote by $\mathbf{cor}_{\boxplus}(u; w_1, w_2)$ the correlation of the linear approximation $u \cdot (x_1 \boxplus x_2) = w_1 \cdot x_1 \oplus w_2 \cdot x_2$. From the linear mask (u, w_1, w_2) we derive a sequence $\underline{z} = z_{n-1} \cdots z_0$ as follows

$$z_i = u^{(i)}2^2 + w_1^{(i)}2 + w_2^{(i)}, \quad i = 0, 1, \cdots, n-1.$$

It's easy to see that $0 \le z_i \le 7$ for all $0 \le i \le n-1$. Define

$$M_n(u, w_1, w_2) = \prod_{i=0}^{n-1} A_{z_i}, \tag{3}$$

where A_j $(j = 0, 1, \cdots, 7)$ are constant matrices of size 2×2 and defined as follows

$$A_0 = \frac{1}{4}\begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}, A_1 = A_2 = -A_4 = \frac{1}{4}\begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix},$$
$$-A_3 = A_5 = A_6 = \frac{1}{4}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}, A_7 = \frac{1}{4}\begin{pmatrix} 3 & -1 \\ 1 & -3 \end{pmatrix}.$$

Then we have

Theorem 1 ([9]). *For any given linear mask (u, w_1, w_2), let $M_n(u, w_1, w_2)$ be defined as above. Set $M_n(u, w_1, w_2) = (M_{i,j})_{0 \le i,j \le 1}$. Then we have*

$$\begin{aligned} M_{i,j} &= \Pr(u \cdot (x_1 \boxplus x_2) = w_1 \cdot x_1 \oplus w_2 \cdot x_2 \wedge c_n = i \wedge c_0 = j) \\ &\quad - \Pr(u \cdot (x_1 \boxplus x_2) \ne w_1 \cdot x_1 \oplus w_2 \cdot x_2 \wedge c_n = i \wedge c_0 = j), \end{aligned}$$

where c_0 is an initial carry bit, and c_n is the n-th carry bit of the addition x_1 and x_2 with the initial carry bit c_0. By convention $c_0 = 0$, we have

$$\mathbf{cor}_{\boxplus}(u, w_1, w_2) = M_{0,0} + M_{1,0}. \tag{4}$$

Note that for any integers x_1 and x_2, if $c_0 = 1$, then the addition of x_1 and x_2 modulo 2^n with the initial carry c_0 is equivalent to $(x_1 + x_2 + 1) \mod 2^n$. Therefore we have the following conclusion.

Corollary 1. *Let $x_1 \overline{\boxplus} x_2 = x_1 \boxplus x_2 \boxplus 1$ and (u, w_1, w_2) be a linear mask of $\overline{\boxplus}$. Denote by $\mathbf{cor}_{\overline{\boxplus}}(u, w_1, w_2)$ the correlation of the linear approximation $u \cdot (x_1 \overline{\boxplus} x_2) = w_1 \cdot x_1 \oplus w_2 \cdot x_2$. Then we have*

$$\mathbf{cor}_{\overline{\boxplus}}(u, w_1, w_2) = M_{0,1} + M_{1,1}. \tag{5}$$

3 Some properties on linear approximations of the addition modulo $2^n - 1$

In this section we will discuss some properties of linear approximations of the addition modulo $2^n - 1$ with k inputs, where we always assume that $n \geq 2$ and $k \geq 2$. For consistency with the definition of the addition of the prime field $\mathbb{F}_{2^n-1}$ in ZUC [20], here we make convention that the set of representatives of the residue class modulo $2^n - 1$ are $\{1, 2, \cdots, 2^n - 1\}$ instead of $\{0, 1, \cdots, 2^n - 2\}$. It should be pointed out that all results in this paper can deduce the corresponding ones in $\{0, 1, \cdots, 2^n - 2\}$ directly.

Let $J = \{1, 2, \cdots, 2^n - 1\}$, and denote by $\hat{\boxplus}$ the addition modulo $2^n - 1$ as defined in ZUC, more precisely, for any $x_1, x_2 \in J$, we have

$$x_1 \hat{\boxplus} x_2 = \begin{cases} x_1 + x_2 & \text{if } x_1 + x_2 < 2^n, \\ (x_1 + x_2 + 1) \mathrm{mod} 2^n & \text{if } x_1 + x_2 \geq 2^n. \end{cases} \tag{6}$$

For example, set $n = 3$, then $J = \{1, 2, \cdots, 7\}$, and $2 \hat{\boxplus} 6 = 1$, $3 \hat{\boxplus} 4 = 7$.

Below we consider the addition modulo $2^n - 1$ over J with k inputs. For any given linear mask $(u, w_1, \cdots, w_k)$, we denote by $\mathbf{cor}_{\hat{\boxplus}}(u; w_1, \cdots, w_k)$ the correlation of the linear approximation

$$u \cdot (x_1 \hat{\boxplus} \cdots \hat{\boxplus} x_k) = \bigoplus_{i=1}^{k} w_1 \cdot x_k.$$

For simplicity we write $\mathbf{cor}_{\hat{\boxplus}}(u; w_1, \cdots, w_k)$ as $\mathbf{cor}(u; w_1, \cdots, w_k)$.

The following two theorems can be easily derived. In fact, Theorem 2 follows directly from the symmetry of $x_1, \cdots, x_k$ in the addition modulo $2^n - 1$, and Theorem 3 from the fact that $(x \hat{\boxplus} x') \lll l = (x \lll l) \boxplus (x' \lll l)$ for $\forall x, x' \in J$ and $1 \leq l \leq n - 1$, where $x \lll l$ means the cyclic shift of x to the left for l bits.

Theorem 2. *For any given linear mask $(u; w_1, \cdots, w_k)$ and an permutation $(i_1, \cdots, i_k)$ of $(1, \cdots, k)$, we have*

$$\mathbf{cor}(u; w_1, \cdots, w_k) = \mathbf{cor}(u; w_{i_1}, \cdots, w_{i_k}). \tag{7}$$

Proof. By the definition of the correlation we only need to prove that $\Pr(u \cdot (x_1 \hat{\boxplus} \cdots \hat{\boxplus} x_k) = \bigoplus_{j=1}^{k} w_j \cdot x_j) = \Pr(u \cdot (x_1 \hat{\boxplus} \cdots \hat{\boxplus} x_k) = \bigoplus_{j=1}^{k} w_{i_j} \cdot x_j)$. Define

$$J(u; w_1, \cdots, w_k) = \{ (x_1, \cdots, x_k) \in J^k \mid u \cdot (x_1 \hat{\boxplus} \cdots \hat{\boxplus} x_k) = \bigoplus_{j=1}^{k} w_j \cdot x_j \} .$$

By the symmetry of $x_1, \cdots, x_k$ in the addition modulo 2^n-1, it's obvious that for any $(x_1, \cdots, x_k) \in J(u; w_1, \cdots, w_k)$, we have $(x_{i_1}, \cdots, x_{i_k}) \in J(u; w_{i_1}, \cdots, w_{i_k})$, and vice versa. So $\#J(u; w_1, \cdots, w_k) = \#J(u; w_{i_1}, \cdots, w_{i_k})$, where the notation $\#$ denotes the cardinality of a set. Therefore

$$\Pr(u \cdot (x_1 \hat{\boxplus} \cdots \hat{\boxplus} x_k) = \bigoplus_{j=1}^{k} w_j \cdot x_j) = \Pr(u \cdot (x_1 \hat{\boxplus} \cdots \hat{\boxplus} x_k) = \bigoplus_{j=1}^{k} w_{i_j} \cdot x_j).$$

■

Theorem 3. *For any given linear mask $(u; w_1, \cdots, w_k)$ and integer $1 \leq l \leq n-1$, we have*

$$\mathbf{cor}(u; w_1, \cdots, w_k) = \mathbf{cor}(u \lll l; w_1 \lll l, \cdots, w_k \lll l). \tag{8}$$

Proof. Similarly to the proof of Theorem 2, we only need to prove that $\Pr(u \cdot (x_1 \hat{\boxplus} \cdots \hat{\boxplus} x_k) = \bigoplus_{j=1}^{k} w_j \cdot x_j) = \Pr(u \cdot x_1 \hat{\boxplus} \cdots \hat{\boxplus} x_k) = \bigoplus_{j=1}^{k} (w_j \lll l) \cdot x_j)$. Keep the notation $J(u; w_1, \cdots, w_k)$ as above. For any $(x_1, \cdots, x_k) \in J(u; w_1, \cdots, w_k)$, since $(x_1 \hat{\boxplus} \cdots \hat{\boxplus} x_k) \lll l = (x_1 \lll l) \hat{\boxplus} \cdots \hat{\boxplus} (x_k \lll l)$, we have

$$(x_1 \lll l, \cdots, x_k \lll l) \in J(u; w_1 \lll l, \cdots, w_k \lll l),$$

which shows that $\#J(u; w_1, \cdots, w_k) \leq \#J(u; w_1 \lll l, \cdots, w_k \lll l)$. Note that $(x \lll l) \lll (n-l) = x$ for any $x \in J$, further we have

$$\begin{aligned}
&\#J(u; w_1 \lll l, \cdots, w_k \lll l) \\
\leq &\#J(u; (w_1 \lll l) \lll (n-l), \cdots, (w_k \lll l) \lll (n-l)) \\
= &\#J(u; w_1, \cdots, w_k).
\end{aligned}$$

So $\#J(u; w_1, \cdots, w_k) = \#J(u; w_1 \lll l, \cdots, w_k \lll l)$, and the conclusion follows. ■

3.1 The case $k = 2$

In this section we will derive the exact formula of $\mathbf{cor}(u; w_1, w_2)$ for any linear mask (u, w_1, w_2) from Theorem 1. For any given linear mask (u, w_1, w_2), keep the notations $\underline{z}$, $M_n(u; w_1, w_2)$ and $M_{i,j}$ $(0 \leq i, j \leq 1)$ defined in the section 2.

It's noticed that when $x_1 + x_2 < 2^n$, we have $x_1 \hat{\boxplus} x_2 = x_1 \boxplus x_2$, and when $x_1 + x_2 \geq 2^n$, we have $x_1 \hat{\boxplus} x_2 = x_1 \boxplus x_2 \boxplus 1$. Thus by Theorem 1 and Corollary 1, it seems that $\mathbf{cor}(u; w_1, w_2)$ is equal to $M_{0,0} + M_{1,1}$ regardless of the difference between Z_{2^n} and J. Below we give an exact formula for $\mathbf{cor}(u; w_1, w_2)$.

Theorem 4. *Let (u, w_1, w_2) be a linear mask of the addition $\hat{\boxplus}$ modulo $2^n - 1$, and $M_n(u, w_1, w_2) = (M_{i,j})_{0 \le i,j \le 1}$ be defined as above. Then we have*

$$\mathbf{cor}(u; w_1, w_2) = \frac{2^{2n}(M_{0,0} + M_{1,1}) + 2^n \cdot c + 1}{(2^n - 1)^2}, \tag{9}$$

where

$$c = \begin{cases} -3, & \text{if } u = w_1 = w_2 \text{ and } w_{\mathrm{H}}(w_2) \text{ is even}, \\ 1, & \text{if } u \ne w_1 = w_2 \text{ and } w_{\mathrm{H}}(w_2) \text{ is odd}, \\ 0, & \text{if } u, w_1 \text{ and } w_2 \text{ are pairwise different}, \\ -1, & \text{otherwise}, \end{cases}$$

and $w_{\mathrm{H}}(w_2)$ denotes the hamming weight of w_2 in the binary representation.

Proof. For any given $x_1, x_2 \in J$, we consider $x_1 \hat{\boxplus} x_2$ from the following two aspects.

First, when $x_1 + x_2 < 2^n$, it's known that $x_1 \hat{\boxplus} x_2 = x_1 \boxplus x_2$. By Theorem 1, we have

$$\begin{aligned} M_{0,0} = &\Pr(u \cdot (x_1 \boxplus x_2) = w_1 \cdot x_1 \oplus w_2 \cdot x_2 \wedge x_1 + x_2 < 2^n) \\ &- \Pr(u \cdot (x_1 \boxplus x_2) \ne w_1 \cdot x_1 \oplus w_2 \cdot x_2 \wedge x_1 + x_2 < 2^n) \end{aligned}$$

Since

$$\begin{aligned} &\Pr(u \cdot (x_1 \boxplus x_2) = w_1 \cdot x_1 \oplus w_2 \cdot x_2 \wedge x_1 + x_2 < 2^n) \\ + &\Pr(u \cdot (x_1 \boxplus x_2) \ne w_1 \cdot x_1 \oplus w_2 \cdot x_2 \wedge x_1 + x_2 < 2^n) \\ = &\Pr(x_1 + x_2 < 2^n) = \frac{2^n + 1}{2^{n+1}}, \end{aligned}$$

thus we have

$$\Pr(u \cdot (x_1 \boxplus x_2) = w_1 \cdot x_1 \oplus w_2 \cdot x_2 \wedge x_1 + x_2 < 2^n) = \frac{1}{2} M_{0,0} + \frac{2^n + 1}{2^{n+2}}.$$

It follows that there are $2^{n-2}(2^n + 1) + 2^{2n-1} M_{0,0}$ pairs (x_1, x_2) satisfying $u \cdot (x_1 \boxplus x_2) = w_1 \cdot x_1 \oplus w_2 \cdot x_2$ and $x_1 + x_2 < 2^n$ simultaneously. We consider those pairs of the form $(0, x_2)$. When $x_1 = 0$, we get $(u \oplus w_2) \cdot x_2 = 0$ due to $u \cdot x_2 = w_2 \cdot x_2$. It follows that there are 2^{n-1} solutions x_2 if $u \ne w_2$ and 2^n solutions if $u = w_2$. Hence there are 2^{n-1} pairs of the form $(0, x_2)$ among the above all pairs not in $J \times J$ if $u \ne w_2$ and 2^n pairs not in $J \times J$ if $u = w_2$. By the symmetry of x_1 and x_2, we have the same conclusion for $x_2 = 0$. In addition, the pair $(0, 0)$ always satisfies $u \cdot (x_1 \boxplus x_2) = w_1 \cdot x_1 \oplus w_2 \cdot x_2$ but is not in $J \times J$.

Second, when $x_1 + x_2 \ge 2^n$, we have $x_1 \hat{\boxplus} x_2 = x_1 \boxplus x_2 \boxplus 1$. Similarly to the above case, there are totally $2^{n-2}(2^n + 1) + 2^{2n-1} M_{1,1}$ pairs (x_1, x_2) satisfying both $x_1 + x_2 + 1 \ge 2^n$ and $u \cdot (x_1 \boxplus x_2 \boxplus 1) = w_1 \cdot x_1 \oplus w_2 \cdot x_2$. Now we consider how to remove some pairs (x_1, x_2) satisfying $x_1 + x_2 + 1 = 2^n$ from the above pairs. Note that $x_1 \boxplus x_2 \boxplus 1 = 0$, thus we only need to count pairs (x_1, x_2) such that $x_1 + x_2 = 2^n - 1$ and $w_1 \cdot x_1 = w_2 \cdot x_2$. Since $x_1 + x_2 = 2^n - 1 = x_1 \oplus x_2$, it follows that

$$(w_1 \oplus w_2) \cdot x_1 = w_2 \cdot (2^n - 1). \tag{10}$$

If $w_1 \neq w_2$, Equality (10) has 2^{n-1} solutions; if $w_1 = w_2$, when the weight of w_2, that is, the number of 1's in the binary representation of w_2, denoted by $w_{\mathrm{H}}(w_2)$, is an odd number, Equality (10) has no solutions, and when $w_{\mathrm{H}}(w_2)$ is an even number, it has 2^n solutions.

Combine the above two cases, and we can get the desired conclusion. ■

3.2 The case $k > 2$

Theorem 5. *For any given linear mask $(u, w_1, \cdots, w_k)$ and integer $k > 2$, we have*

$$\mathbf{cor}(u; w_1, \cdots, w_k) = \frac{2^n - 1}{2^n} \sum_{w=0}^{2^n-1} \mathbf{cor}(w; w_1, \cdots, w_{k-1}) \mathbf{cor}(u; w, w_k). \quad (11)$$

Proof. By the definition of the correlation $\mathbf{cor}(u; w_1, \cdots, w_k)$, we have

$$\mathbf{cor}(u; w_1, \cdots, w_k) = \frac{1}{(2^n - 1)^k} \sum_{(x_1, \cdots, x_k) \in J^k} (-1)^{u \cdot (x_1 \hat{\boxplus} \cdots \hat{\boxplus} x_k) \oplus \bigoplus_{i=1}^{k} w_i \cdot x_i}.$$

Denote $y = x_1 \hat{\boxplus} \cdots \hat{\boxplus} x_k$ and $y' = x_1 \hat{\boxplus} \cdots \hat{\boxplus} x_{k-1}$. Then we have

$$\begin{aligned}
&\sum_{w=0}^{2^n-1} \mathbf{cor}(w; w_1, \cdots, w_{k-1}) \mathbf{cor}(u; w, w_k) \\
&= \frac{1}{(2^n - 1)^{k+1}} \sum_{w=0}^{2^n-1} \sum_{(x_1, \cdots, x_{k-1}) \in J^{k-1}} (-1)^{w \cdot y' \oplus \bigoplus_{i=1}^{k-1} w_i \cdot x_i} \sum_{x_k \in J} (-1)^{u \cdot y \oplus w \cdot y' \oplus w_k \cdot x_k} \\
&= \frac{1}{(2^n - 1)^{k+1}} \sum_{(x_1, \cdots, x_k) \in J^k} (-1)^{u \cdot y \oplus \bigoplus_{i=1}^{k} w_i \cdot x_i} \sum_{w=0}^{2^n-1} (-1)^{w \cdot y' \oplus w \cdot y'} \\
&= \frac{2^n}{2^n - 1} \mathbf{cor}(u; w_1, \cdots, w_k).
\end{aligned}$$

■

4 More properties of linear approximations on the addition modulo $2^n - 1$ with two inputs

In this section we will provide more properties of linear approximations on the addition modulo $2^n - 1$ with two inputs, that is, $k = 2$. First we introduce some notations and concepts.

Let $\mathbb{Q}$ be the rational field. Define

$$\mathrm{I} = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} | a, b \in \mathbb{Q} \right\},$$

$$\mathrm{II} = \left\{ \begin{pmatrix} a & -b \\ b & -a \end{pmatrix} | a, b \in \mathbb{Q} \right\},$$

and call a matrix in the set I (or II) to be type-I (or type-II). It is easily seen that $A_0, A_3, A_5, A_6 \in \mathrm{I}$ and $A_1, A_2, A_4, A_7 \in \mathrm{II}$ (which are defined in section 2). The following two properties can be easily verified.

Lemma 1. *The product of arbitrary two type-I (or type-II) matrices is a type-I matrix.*

Lemma 2. *The product of a type-I matrix and a type-II matrix is a type-II matrix.*

By the definition of $M_n(u; w_1, w_2)$ and Lemmas 1 and 2, we have

Lemma 3. *For any given linear mask (u, w_1, w_2), $M_n(u, w_1, w_2)$ is either type-I or type-II.*

For any given square matrix M, denote by $\mathbf{Tr}(M)$ the trace of the matrix M, that is, the sum of elements on the main diagonal of M. Since the trace of an arbitrary type-II matrix is zero, thus the following conclusions hold.

Corollary 2. *For any given linear mask (u, w_1, w_2), let $\underline{z} = z_{n-1} \cdots z_0$ be a sequence derived by (u, w_1, w_2). If the number of elements z_i such that $z_i \in \{1, 2, 4, 7\}$ is odd, $i = 0, 1, \cdots, n-1$, then $\mathbf{Tr}(M_n(u, w_1, w_2)) = 0$.*

Corollary 3. *Let $u \in Z_{2^n}$ and $w_{\mathrm{H}}(u)$ be odd. Then $\mathbf{Tr}(M_n(u, u, u)) = 0$. Thus we have*

$$\mathbf{cor}(u; u, u) = -\frac{1}{2^n - 1}$$

and

$$\lim_{n\to\infty} \mathbf{cor}(u; u, u) = 0.$$

Corollary 4. *Let $u \in Z_{2^n}$ and $w_{\mathrm{H}}(u)$ be even. Then $M_n(u, u, u)$ is type-I, that is, $M_{0,0} = M_{1,1}$. Thus we have*

$$\mathbf{cor}(u; u, u) = \frac{2^{2n} \cdot 2M_{0,0} - 3 \cdot 2^n + 1}{(2^n - 1)^2}.$$

If all 1's of u in the binary representation are adjacent, then we have

$$\mathbf{cor}(u; u, u) = \frac{2^{2n} \cdot (2^{\frac{w_{\mathrm{H}}(u)}{2} - n} + 2^{-\frac{w_{\mathrm{H}}(u)}{2}}) - 3 \cdot 2^n + 1}{(2^n - 1)^2}$$

and

$$\lim_{n\to\infty} \mathbf{cor}(u; u, u) = 2^{-\frac{w_{\mathrm{H}}(u)}{2}}.$$

Below we give some facts on A_i, $0 \le i \le 7$, which will be used later.

Lemma 4. *1. $A_0 A_i = \frac{1}{2} A_i$, for $\forall\ i \in \{1, 2, 3, 4, 5, 6\}$;*
2. $A_i A_0 = A_i$ if $i \in \{1, 2, 4\}$ and $A_i A_0 = \frac{1}{2} A_i$ if $i \in \{3, 5, 6\}$;
3. $A_i A_j = 0$, $i \in \{1, 2, 4\}$ and $j \in \{1, 2, 3, 4, 5, 6\}$;
4. $A_1 A_7 = A_2 A_7 = -A_4 A_7 = A_6$.

Now we consider a class of special linear mask $(u, 1, w)$. Let $\underline{z} = z_{n-1} \cdots z_0$ be the sequence derived from $(u, 1, w)$. It is easy to see that $z_0 \in \{1, 3, 5, 7\}$ and $z_i \in \{0, 2, 4, 6\}$, $1 \le i \le n-1$. In the rest we write $M_n(u, 1, w)$ as M simply.

Lemma 5. *For any integers $u, w \in Z_{2^n}$, if $\mathbf{Tr}(M) \neq 0$, then the sequence $\underline{z}$ is of the form either $\{0,6\}^{n-1}\{3,5\}$ or $\{0,6\}^*\{2,4\}0^*7$.*

Proof. Let r be the number of z_i such that $z_i \in \{2, 4\}$, $i = 1, 2, \cdots, n-1$. We first prove that $r \le 1$. Assume that $r > 1$. Then there exist two indexes i and j such that $z_i, z_j \in \{2, 4\}$, $1 \le i < j \le n-1$. By Items 2 and 3 of Lemma 4, we have $A_{z_i} \cdots A_{z_j} = 0$. It follows that $M = 0$, which contradict $\mathbf{Tr}(M) \neq 0$.

When $r = 0$, if $z_0 \in \{1, 7\}$, by Corollary 2, it's known that the matrix M is type-II, which contradict $\mathbf{Tr}(M) \neq 0$ as well. Thus $z_0 \in \{3, 5\}$. So $\underline{z}$ is of the form $\{0,6\}^{n-1}\{3,5\}$.

When $r = 1$, let $z_j \in \{2, 4\}$, where $1 \le j \le n-1$. First we claim $z_i = 0$ for all $1 \le i < j$. If there exists some index i such that $z_i \neq 0$, by Items 2 and 3 of Lemma 4, we have $A_{z_i} \cdots A_{z_j} = 0$, further $M = 0$, which is a contradiction. Second, if $z_0 \in \{1, 3, 5\}$, by Items 2 and 3 of Lemma 4, we have $A_{z_0} \cdots A_{z_i} = 0$. So $\underline{z}$ is of the form $\{0,6\}^*\{2,4\}0^*7$. ■

Theorem 6. *For any integers $u, w \in Z_{2^n}$, $\mathbf{Tr}(M) \neq 0$ if and only if $u = w \oplus 2^i$, where $0 \le i \le LNB(w \oplus 1)$, $LNB(x)$ denotes the least position where 1 appears in the binary representation of x if $x \neq 0$, and $LNB(0) = n-1$.*

Proof. The necessity follows directly from Lemma 5. Below we prove the sufficiency. First we prove that $\mathbf{Tr}(A_6^t) = 2^{-t}$ for $\forall t \ge 1$. In fact, It is easy to calculate two characteristic roots 0 and 2^{-1} of A_6. Thus we have $\mathbf{Tr}(A_6^t) = 0^t + (2^{-1})^t = 2^{-t}$.

If $i = 0$, i.e., $u = w \oplus 1$, then $\underline{z}$ is of the form $\{0,6\}^{n-1}\{3,5\}$. Let t be the number of z_i such that $z_i = 6$, $i = 1, 2, \cdots, n-1$. Then 0 occurs in $z_{n-1} \cdots z_1$ for $n-1-t$ times. Thus by Lemma 4, we have

$$\begin{aligned}
\mathbf{Tr}(M) &= \mathbf{Tr}(A_{z_{n-1}} \cdot \cdots \cdot A_{z_0}) \\
&= \mathbf{Tr}(2^{-(n-1-t)} A_6^t A_{z_0}) \\
&= (-1)^w 2^{-(n-1-t)} \mathbf{Tr}(A_6^{t+1}) \\
&= (-1)^w 2^{-(n-1-t)} 2^{-(t+1)} \\
&= (-1)^w 2^{-n}.
\end{aligned}$$

If $i > 0$, then $\underline{z}$ is of the form $\{0,6\}^*\{2,4\}0^*7$ and $z_i \in \{2, 4\}$. Let t be the number of repeats of 6 in $z_{n-1} \cdots z_{i+1}$. Then by Lemma 4, we have

$$\begin{aligned}
\mathbf{Tr}(M) &= \mathbf{Tr}(A_{z_{n-1}} \cdot \cdots \cdot A_{z_0}) \\
&= \mathbf{Tr}(2^{-(n-1-i-t)} A_6^t A_{z_i} A_7) \\
&= (-1)^s 2^{-(n-1-i-t)} \mathbf{Tr}(A_6^{t+1}) \\
&= (-1)^s 2^{-(n-1-i-t)} 2^{-(t+1)} \\
&= (-1)^s 2^{-(n-i)},
\end{aligned}$$

where $s = w^{(i)} \oplus 1$. ■

Theorem 6 gives a sufficient and necessary condition on how to determine whether M is type-II for any linear mask $(u, 1, w)$. From its proof we can get the following result.

Corollary 5. *For any integers $u, w \in Z_{2^n}$ such that $u = w \oplus 2^i$, where $0 \leq i \leq LNB(w \oplus 1)$, we have $\mathbf{Tr}(M) = (-1)^s 2^{-(n-i)}$, where*

$$s = \begin{cases} 0 & \text{if } i = 0 \text{ and } w^0 = 0 \text{ or } i > 0 \text{ and } w^{(i)} = 1, \\ 1 & \text{otherwise.} \end{cases}$$

By Theorem 4 and Corollary 5, further we have

Corollary 6.

$$\mathbf{cor}(w; 1, 1) = \begin{cases} \frac{1}{(2^n-1)^2} & w = 0, \\ -\frac{1}{2^n-1} & w = 1, \\ \frac{-2^{n+i}+2^n+1}{(2^n-1)^2} & w = 2^i + 1, 1 \leq i \leq n-1, \\ \frac{2^n+1}{(2^n-1)^2} & \textit{otherwise} \end{cases}$$

and

$$\mathbf{cor}(1; w, 1) = \begin{cases} \frac{1}{(2^n-1)^2} & w = 0, \\ \frac{2^{n+i}-2^n+1}{(2^n-1)^2} & w = 2^i + 1, 1 \leq i \leq n-1, \\ -\frac{1}{2^n-1} & \textit{otherwise.} \end{cases}$$

Finally we give an upper bound of $|cor(u; 1, w)|$. For any given integer $x \in Z_{2^n}$, define

$$J_x = \{x \oplus 2^i | 1 \leq i \leq LNB(x \oplus 1)\}.$$

Theorem 7. *For any integers $u, w \in Z_{2^n}$, if $w \notin J_u$, then*

$$|cor(u; 1, w)| < \frac{3}{2^n - 1}. \tag{12}$$

Proof. If $w \neq u \oplus 1$, by Theorem 6, we have $\mathbf{Tr}(M) = 0$. Further we can get the desired result by Theorem 4. If $w = u \oplus 1$, by Corollary 5 and Theorem 4, we have

$$|cor(u; 1, w)| \leq \frac{2^{2n} \cdot 2^{-n} + 2^n + 1}{(2^n - 1)^2} = \frac{2 \cdot 2^n + 1}{(2^n - 1)^2} < \frac{3}{(2^n - 1)}.$$

■

5 The limit of $\mathbf{cor}(1; 1^k)$

In this section, we will discuss the limit of $\mathbf{cor}(1; \underbrace{1, \cdots, 1}_{k})$ for some integer $k \geq 2$ when n goes to infinity. For simplicity, we denote it by $\mathbf{cor}(1; 1^k)$.

Lemma 6. *For any integers $n \geq 2$ and $k \geq 2$, we have*

$$\sum_{u \in Z_{2^n}} |\mathbf{cor}(u; 1^k)| < (n+3)^{k-1}.$$

Proof. Note that $|J_x| \leq n$ for all $x \in Z_{2^n}$. When $k = 2$, by Theorem 7, we have

$$\begin{aligned}\sum_{u \in Z_{2^n}} |\mathbf{cor}(u; 1, 1)| &= \sum_{u \in J_1} |\mathbf{cor}(u; 1, 1)| + \sum_{u \notin J_1} |\mathbf{cor}(u; 1, 1)| \\ &\leq \sum_{u \in J_1} 1 + \frac{3}{2^n - 1} \sum_{u \notin J_1} 1 < n + 3.\end{aligned}$$

Suppose that when $k = k_0$, we have $\sum_{u \in Z_{2^n}} |\mathbf{cor}(u; 1^{k_0})| < (n+3)^{k_0 - 1}$. Then

$$\begin{aligned}&\sum_{u \in Z_{2^n}} |\mathbf{cor}(u; 1^{k_0+1})| \\ &= \frac{2^n - 1}{2^n} \sum_{u \in Z_{2^n}} |\sum_{w \in Z_{2^n}} \mathbf{cor}(w; 1^{k_0}) \mathbf{cor}(u; w, 1)| \\ &< \sum_{u \in Z_{2^n}} \sum_{w \in Z_{2^n}} |\mathbf{cor}(w; 1^{k_0}) \mathbf{cor}(u; w, 1)| \\ &= \sum_{u \in Z_{2^n}} (\sum_{w \in J_u} |\mathbf{cor}(w; 1^{k_0}) \mathbf{cor}(u; w, 1)| + \sum_{w \notin J_u} |\mathbf{cor}(w; 1^{k_0}) \mathbf{cor}(u; w, 1)|) \\ &< \sum_{u \in Z_{2^n}} \sum_{w \in J_u} |\mathbf{cor}(w; 1^{k_0})| + \frac{3}{2^n - 1} \sum_{u \in Z_{2^n}} \sum_{w \notin J_u} |\mathbf{cor}(w; 1^{k_0})| \\ &< n \cdot (n+3)^{k_0 - 1} + \frac{3}{2^n - 1} \cdot (2^n - 1) \cdot (n+3)^{k_0 - 1} \\ &= (n+3)^{k_0}.\end{aligned}$$

By induction the conclusion is correct. ∎

Lemma 7. *For any integer $t \geq 1$ and $i \geq 2$, we have*

$$\lim_{n \to \infty} \sum_{u_1 \in J_1} \sum_{u_2 \in J_{u_1}} \cdots \sum_{u_{t-1} \in J_{u_{t-2}}} \sum_{u_t \notin J_{u_{t-1}}} \mathbf{cor}(u_t; 1^i) \prod_{j=1}^{t} \mathbf{cor}(u_{j-1}; u_j, 1) = 0,$$

where $u_0 = 1$.

Proof. By Lemma 6 and Theorem 7, we have

$$
\begin{aligned}
&|\sum_{u_1\in J_1}\sum_{u_2\in J_{u_1}}\cdots\sum_{u_{t-1}\in J_{u_{t-2}}}\sum_{u_t\notin J_{u_{t-1}}}\mathbf{cor}(u_t;1^i)\prod_{j=1}^{t}\mathbf{cor}(u_{j-1};u_j,1)|\\
&< \frac{3}{2^n-1}\sum_{u_1\in J_1}\sum_{u_2\in J_{u_1}}\cdots\sum_{u_{t-1}\in J_{u_{t-2}}}\sum_{u_t\notin J_{u_{t-1}}}|\mathbf{cor}(u_t;1^i)\prod_{j=1}^{t-1}\mathbf{cor}(u_{j-1};u_j,1)|\\
&\le \frac{3}{2^n-1}\sum_{u_1\in J_1}\sum_{u_2\in J_{u_1}}\cdots\sum_{u_{t-1}\in J_{u_{t-2}}}\sum_{u_t\notin J_{u_{t-1}}}|\mathbf{cor}(u_t;1^i)|\\
&< \frac{3}{2^n-1}(n+3)^{i-1}\sum_{u_1\in J_1}\sum_{u_2\in J_{u_1}}\cdots\sum_{u_{t-1}\in J_{u_{t-2}}}1\\
&< \frac{3}{2^n-1}(n+3)^{i-1}n^{t-1}.
\end{aligned}
$$

Since $\frac{3}{2^n-1}(n+3)^{i-1}n^{t-1}$ approaches 0 when n goes to infinity, thus the conclusion holds. ■

Lemma 8. *For any integer $k\ge 3$, if $\lim_{n\to\infty}\mathbf{cor}(1;1^k)$ exists, then*

$$\lim_{n\to\infty}\mathbf{cor}(1;1^k)=\lim_{n\to\infty}\sum_{u_1\in J_1}\sum_{u_2\in J_{u_1}}\cdots\sum_{u_{k-2}\in J_{u_{k-3}}}\prod_{j=1}^{k-1}\mathbf{cor}(u_{j-1};u_j,1),$$

where $u_0=u_{k-1}=1$.

Proof.

$$
\begin{aligned}
&\lim_{n\to\infty}\mathbf{cor}(1;1^k)\\
&=\lim_{n\to\infty}\sum_{u_1\in Z_{2^n}}\mathbf{cor}(u_1;1^{k-1})\mathbf{cor}(1;u_1,1)\\
&=\lim_{n\to\infty}(\sum_{u_1\in J_1}+\sum_{u_1\notin J_1})\mathbf{cor}(u_1;1^{k-1})\mathbf{cor}(1;u_1,1)\\
&=\lim_{n\to\infty}\sum_{u_1\in J_1}\mathbf{cor}(u_1;1^{k-1})\mathbf{cor}(1;u_1,1)\quad\text{(by Lemma 7)}\\
&=\lim_{n\to\infty}\sum_{u_1\in J_1}\sum_{u_2\in Z_{2^n}}\mathbf{cor}(u_2;1^{k-2})\mathbf{cor}(u_1;u_2,1)\mathbf{cor}(1;u_1,1)\\
&=\lim_{n\to\infty}\sum_{u_1\in J_1}(\sum_{u_2\in J_{u_1}}+\sum_{u_2\notin J_{u_1}})\mathbf{cor}(u_2;1^{k-2})\mathbf{cor}(u_1;u_2,1)\mathbf{cor}(1;u_1,1)\\
&=\lim_{n\to\infty}\sum_{u_1\in J_1}\sum_{u_2\in J_{u_1}}\mathbf{cor}(u_2;1^{k-2})\mathbf{cor}(u_1;u_2,1)\mathbf{cor}(1;u_1,1)\quad\text{(by Lemma 7)}\\
&=\cdots\\
&=\lim_{n\to\infty}\sum_{u_1\in J_1}\sum_{u_2\in J_{u_1}}\cdots\sum_{u_{k-2}\in J_{u_{k-3}}}\prod_{j=1}^{k-1}\mathbf{cor}(u_{j-1};u_j,1).
\end{aligned}
$$

■

Theorem 8. *For any integer $k \geq 3$, if $\lim_{n\to\infty} \mathbf{cor}(1;1^k)$ exists, then*

$$\lim_{n\to\infty} \mathbf{cor}(1;1^k) = \lim_{n\to\infty} \sum_{u_1\in J_1} \sum_{u_2\in J_{u_1}} \cdots \sum_{u_{k-1}\in J_{u_{k-2}}} \prod_{j=1}^{k-1} \mathbf{Tr}(M_n(u_{j-1}, u_j, 1)),$$

where $u_0 = u_{k-1} = 1$.

Proof. By Theorem 4, for any linear mask(u, w_1, w_2), we have

$$\mathbf{cor}(u; w_1, w_2) = \mathbf{Tr}(M_n(u, w_1, w_2)) + \frac{\delta(u, w_1, w_2)}{2^n - 1},$$

where $|\delta(u, w_1, w_2)| < K$, K is some constant. Then

$$\sum_{u_1\in J_1} \sum_{u_2\in J_{u_1}} \cdots \sum_{u_{k-2}\in J_{u_{k-3}}} \prod_{j=1}^{k-1} \mathbf{cor}(u_{j-1}; u_j, 1)$$

$$= \sum_{u_1\in J_1} \sum_{u_2\in J_{u_1}} \cdots \sum_{u_{k-2}\in J_{u_{k-3}}} (\mathbf{Tr}(M_n(1, u_1, 1)) + \frac{\delta(1, u_1, 1)}{p}) \prod_{j=2}^{k-1} \mathbf{cor}(u_{j-1}; u_j, 1)$$

$$= A + B,$$

where

$$A = \sum_{u_1\in J_1} \sum_{u_2\in J_{u_1}} \cdots \sum_{u_{k-2}\in J_{u_{k-3}}} \mathbf{Tr}(M_n(1, u_1, 1)) \prod_{j=2}^{k-1} \mathbf{cor}(u_{j-1}; u_j, 1)$$

and

$$B = \sum_{u_1\in J_1} \sum_{u_2\in J_{u_1}} \cdots \sum_{u_{k-2}\in J_{u_{k-3}}} \frac{\delta(1, u_1, 1)}{2^n - 1} \prod_{j=2}^{k-1} \mathbf{cor}(u_{j-1}; u_j, 1).$$

Since

$$\begin{aligned} |B| &\leq \frac{K}{2^n - 1} \sum_{u_1\in J_1} \sum_{u_2\in J_{u_1}} \cdots \sum_{u_{k-2}\in J_{u_{k-3}}} |\prod_{j=2}^{k-2} \mathbf{cor}(u_{j-1}; u_j, 1)| \\ &\leq \frac{K}{2^n - 1} \sum_{u_1\in J_1} \sum_{u_2\in J_{u_1}} \cdots \sum_{u_{k-2}\in J_{u_{k-3}}} 1 \\ &\leq \frac{K}{2^n - 1} n^k \xrightarrow{n\to\infty} 0, \end{aligned}$$

thus we have

$$\lim_{n\to\infty} \mathbf{cor}(1;1^k) = \lim_{n\to\infty} A.$$

Repeat the above procedure, and we always strip $\frac{\delta(u_{j-1}, u_j, 1)}{2^n - 1}$ from $\mathbf{cor}(u_{j-1}; u_j, 1)$, $j = 2, 3, \cdots, k-1$. Then finally we can get the desired conclusion. ■

Corollary 7. $\lim_{n\to\infty} \mathbf{cor}(1;1^2) = 0$ *and* $\lim_{n\to\infty} \mathbf{cor}(1;1^3) = -\frac{1}{3}$.

Proof. Since $M_n(1,1,1) = A_0^{n-1}A_7$ is type-II, thus $\mathbf{Tr}(M_n(1,1,1)) = 0$, further we have $\lim_{n\to\infty} \mathbf{cor}(1;1,1) = 0$. By Theorem 8 and Corollary 6, we have

$$\begin{aligned}
&\lim_{n\to\infty} \mathbf{cor}(1;1^3)\\
&= \lim_{n\to\infty} \sum_{u\in J_1} \mathbf{Tr}(M_n(u,1,1))\mathbf{Tr}(M_n(1,u,1))\\
&= \lim_{n\to\infty} \sum_{i=1}^{n-1} \mathbf{Tr}(M_n(2^i+1,1,1))\mathbf{Tr}(M_n(1,2^i+1,1))\\
&= \lim_{n\to\infty} \sum_{i=1}^{n-1} (-2^{-(n-i)}) \cdot 2^{-(n-i)}\\
&= -\lim_{n\to\infty} \sum_{i=1}^{n-1} 4^{-(n-i)} = -\frac{1}{3}.
\end{aligned}$$

■

In order to deal with the general case $\lim_{n\to\infty} \mathbf{cor}(1;1^k)$, for a given integer $k \geq 3$, we define

$$U_k = \{u_0u_1u_2\cdots u_{k-2}u_{k-1} | u_j \in J_{u_{j-1}}, 1 \leq j \leq k-1, u_{k-1} = u_0 = 1\}. \quad (13)$$

Then Theorem 8 can also be represented as:

Theorem 9. *For given integer* $k \geq 3$, *if* $\lim_{n\to\infty} \mathbf{cor}(1;1^k)$ *exist, then*

$$\lim_{n\to\infty} \mathbf{cor}(1;1^k) = \lim_{n\to\infty} \sum_{u_0u_1\cdots u_{k-1}\in U_k} \prod_{j=1}^{k-1} \mathbf{Tr}(M_n(u_{j-1},u_j,1)).$$

For any string $u_0u_1u_2\cdots u_{k-2}u_{k-1} \in U_k$, by the definition of $J_{u_{j-1}}$, we have $u_j > 0$ for $0 \leq j \leq k-1$, and there is only one bit in u_j different from u_{j-1}, that is, $w_{\mathrm{H}}(u_{j-1}) - w_{\mathrm{H}}(u_j) = \pm 1$. Note that $w_{\mathrm{H}}(u_0) = 1$ is odd, thus $w_{\mathrm{H}}(u_2), w_{\mathrm{H}}(u_4), \cdots$ are odd and $w_{\mathrm{H}}(u_1)$, $w_{\mathrm{H}}(u_3)$, $\cdots$ are even.

When k is even, it's known that $w_{\mathrm{H}}(u_{k-1})$ is even, which contradict $w_{\mathrm{H}}(u_{k-1}) = 1$ since $u_{k-1} = 1$. It follows that $U_k = \emptyset$. Hence we have the following conclusion.

Theorem 10. *For any even positive integer* k, *we have* $\lim_{n\to\infty} \mathbf{cor}(1;1^k) = 0$.

When k is odd, set $u_{2j} = 1$ and $u_{2j+1} = 2^{n-1}+$ for $0 \leq j \leq \frac{k-1}{2}$. Then $u_0\cdots u_{k-2}u_{k-1} \in U_k$. It shows that $U_k \neq \emptyset$. For all odd integer k, we define

$$\begin{aligned}
I_k &= \{i_1i_2\cdots i_{k-1} | 2^{i_j} = u_j \oplus u_{j-1}, u_0\cdots u_{k-2}u_{k-1} \in U_k\},\\
I_{k,d} &= \{i_1i_2\cdots i_{k-1} | d = \sum_{j=1}^{k-1} i_j, i_1i_2\cdots i_{k-1} \in I_k\},
\end{aligned}$$

and denote $N_{k,d} = \# I_{k,d}$.

Theorem 11. *For any odd integer $k \geq 3$, we have*

$$\sum_{u_0 u_1 \cdots u_{k-1} \in U_k} \prod_{j=1}^{k-1} \mathbf{Tr}(M_n(u_{j-1}, u_j, 1)) = (-1)^{\frac{k-1}{2}} \cdot 2^{-(k-1)n} \sum_{d=k-1}^{(k-1)(n-1)} N_{k,d} \cdot 2^d.$$

Proof. For any $u_0 \cdots u_{k-1} \in U_k$, by Corollary 5, when $w_{\mathrm{H}}(u_j) - w_{\mathrm{H}}(u_{j-1}) = 1$, the sign of $Tr(M_n(u_{j-1}, u_j, 1))$ is positive, and when $w_{\mathrm{H}}(u_j) - w_{\mathrm{H}}(u_{j-1}) = -1$, the sign of $Tr(M_n(u_{j-1}; u_j, 1))$ is negative. So the sign of $\prod_{j=1}^{k-1} Tr(M_n(u_{j-1}; u_j, 1))$ is the same with $\prod_{j=1}^{k-1}(w_{\mathrm{H}}(u_j) - w_{\mathrm{H}}(u_{j-1}))$. Note that $\sum_{j=1}^{k-1}(w_{\mathrm{H}}(u_j) - w_{\mathrm{H}}(u_{j-1})) = 0$, it follows that the number of j such that $w_{\mathrm{H}}(u_j) - w_{\mathrm{H}}(u_{j-1}) = 1$ is equal to that of j such that $w_{\mathrm{H}}(u_j) - w_{\mathrm{H}}(u_{j-1}) = -1$. Thus the sign of $\prod_{j=1}^{k-1} Tr(M_n(u_{j-1}; u_j, 1))$ equals $(-1)^{\frac{k-1}{2}}$. Then we have

$$\begin{aligned}
&\sum_{u_0 \cdots u_{k-1} \in U_k} \prod_{j=1}^{k-1} Tr(M_n(u_{j-1}, u_j, 1)) \\
&= (-1)^{\frac{k-1}{2}} \sum_{i_1 i_2 \cdots i_{k-1} \in I_k} \prod_{j=1}^{k-1} 2^{-(n-i_j)} \\
&= (-1)^{\frac{k-1}{2}} \cdot 2^{-(k-1)n} \sum_{d=k-1}^{(k-1)(n-1)} N_k^{(d)} \cdot 2^d.
\end{aligned}$$

■

Theorem 12. *For any odd integer $k \geq 3$, if $\lim_{n\to\infty} \mathbf{cor}(1; 1^k)$ exists, then*

1. $\lim_{n\to\infty} \mathbf{cor}(1; 1^k) \geq \frac{1}{3} 2^{-(k-3)}$, *if* $k \equiv 1 \mod 4$,
2. $\lim_{n\to\infty} \mathbf{cor}(1; 1^k) \leq -\frac{1}{3} 2^{-(k-3)}$, *if* $k \equiv 3 \mod 4$.

Proof. For any given $u_0 \cdots u_{k-1} \in U_k$, denote $2^{i_j} = u_j \oplus u_{j-1}$, $1 \leq j \leq k-1$. Then $i_1 i_2 \cdots i_{k-1} \in I_k$. Note that $2^{i_1} \oplus 2^{i_2} \oplus \cdots \oplus 2^{i_{k-1}} = \bigoplus_{j=1}^{k-1}(u_j \oplus u_{j-1}) = 0$, it means that $i_1, i_2, \cdots i_k$ can be divided to two identical sets. So $d = \sum_{j=1}^{k-1} i_j$ is always even. Note that $1 \leq i_j \leq n-1$, thus $k-1 \leq d \leq (k-1)(d-1)$. In addition, by the definition of I_k and $I_{k,d}$, for any even integer $k-1 \leq d \leq (n-1)(k-1)$, there exist $i_1, i_2, \cdots, i_{k-1}$ such that $i_1 i_2 \cdots\ i_{k-1} \in I_{k,d}$, that is, $N_{k,d} \geq 1$. For example, when $d = k-1$, set $i_j = 1$ for $1 \leq j \leq k-1$, then $i_1 \cdots i_{k-1} \in I_{k,k-1}$; when $d = (k-1)(n-1)$, set$i_j = n-1$ for $1 \leq j \leq k-1$, then $i_1 \cdots i_{k-1} \in I_{k,(k-1)(n-1)}$. By Theorem 11, we have

$$\begin{aligned}
&|\lim_{n\to\infty} \mathbf{cor}(1;1^k)| \\
&= \lim_{n\to\infty} 2^{-(k-1)n} \sum_{d=(k-1)/2}^{(k-1)(n-1)/2} N_{k,2d} 2^{2d} \\
&\geq \lim_{n\to\infty} 2^{-(k-1)n} \sum_{d=(k-1)/2}^{(k-1)(n-1)/2} 2^{2d} \\
&= \lim_{n\to\infty} 2^{-(k-1)n} \frac{2^{(k-1)(n-1)+2} - 2^{k-1}}{2^2 - 1} \\
&= \frac{1}{3} 2^{-(k-3)}.
\end{aligned}$$

■

6 Conclusion

In this paper we discuss properties of linear approximations of the addition modulo $2^n - 1$. As results, an exact formula is given for the case when two inputs are involved, and an iterative formula for the case when more than two inputs are involved. For a class of special linear approximations with all masks being equal to 1, we further discuss the limit of their correlations when n goes to infinity. Let k be the number of inputs of the addition modulo $2^n - 1$. It's shows that when k is even, the limit is equal to zero, and when k is odd, the limit is bounded by a constant depending on k.

Finally when both n and k trend to infinite, we give a conjecture on $\mathbf{cor}(1;1^k)$.

Conjecture 1. $\lim_{k\to\infty}\lim_{n\to\infty} \mathbf{cor}(1;1^k) = 0$.

References

1. M. Matsui, Linear cryptanalysis method for DES cipher, In Advance in Cryptology-Eurocrypt 1993, LNCS 950, pp.366-275, Springer-Verlag, 1995.
2. K. Nyberg, Linear approximations of block ciphers, In Advances in Cryptology-Eurocrypt 1994, LNCS 950, pp.439-444, Springer-Verlag, 1995.
3. D. Coppersmith, S. Halevi and C. Jutla, Cryptanalysis of stream ciphers with linear masking, In Advances in Crypto 2002, LNCS 2442, Springer-Verlag, pp.515-532, 2002.
4. D. Watanabe, A. Biryukov and C.D. Canniere, A Distiguishing Attack of SNOW 2.0 with Linear Masking Method, In Selected Areas in Cryptography, SAC 2003, LNCS 3006, Springer-Verlag, 222-233, 2004.
5. X. Lai, On the design and security of block ciphers, ETH Series in Information Processing, v.1, Konstanz: Hartung-Gorre Verlag, 1992.
6. GOST 28147-89, Cryptographic Protection for Data Processing Systems, Government Committee of the USSR for Standards, 1989.

7. R. Rivest, The MD5 Message-Digest Algorithm", RFC 1321, MIT and RSA Data Security, Inc., April 1992.
8. P. Ekdahl and T. Johansson, A new version of the stream cipher SNOW, In Selected Areas in Cryptography, SAC 2002, LNCS 1233, Springer-Verlag , pp.37C46, 2002.
9. K. Nyberg and J. Wallén, Improved Linear Distinguishers for SNOW 2.0, In:M.J.B.Robshaw.(ed.) FSE 2006. LNCS 4047, pp.144-162, 2006.
10. J. Wallén, Linear Approximations of Addition Modulo 2^n, FSE 2003, LNCS 2887, Spring-Verlag, pp.261–273, 2003.
11. T.A. Berson, Differential Cryptanalysis Mod 2^{32} with Applications to MD5, EUROCRYPT92, LNCS658, pp.71-80, 1993.
12. H. Lipmaa and S. Moriai, Efficient algorithms for computing differential properties of addition. In Fast Software Encryption 2001, LNCS 2355, pp.336C350, Springer-Verlag, 2002.
13. N.T. Courtois and B. Debraize, Algebraic Description and Simultaneous Linear Approximations of Addition in Snow 2.0, ICICS2008, LNCS5308, pp.328-344, 2008.
14. A. Maximov and T. Johansson, Fast Computation of Large Distributions and Its Cryptographic Applications, ASIACRYPT2005, LNCS 3788, pp.313-332, 2005.
15. K. Nyberg, Correlation theorems in cryptanalysis, Discrete Applied Mathemaics, pp.177-188, 2001.
16. Z. Tu and Y.A. Deng, Conjecture on Binary String and Its Applications on Constructing Boolean Functions of Optimal Algebraic Immunity, http://eprint.iacr.org/2009/272.
17. Z. Tu and Y.A. Deng, A Class of 1-Resilient Function with High Nonlinearity and Algebraic Immunity, Cryptology ePrint Archive, http://eprint.iacr.org/2010/179.
18. R. Zimmermann, Efficient VLSI implementation of modulo $2^n \pm 1$ addition and multiplication, Proceedings of 14th IEEE Symposium on Computer Arithmetic, pp.158-167, 1999.
19. J.P. Flori, H. Randriambololona, G. Cohen and S. Mesnager, On a conjecture about binary strings distribution, http://eprint.iacr.org/2010/170.
20. Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3, Document 2: ZUC Specification, http://www.gsmworld.com/our-work/programmes-and-initiatives/fraud-and-security/gsm_security_algorithms.htm
21. GSM Algorithms, http://www.gsmworld.com/our-work/programmes-and-initiatives/fraud-and-security/gsm_security_algorithms.htm.