On Approximating Addition by Exclusive OR

Palash Sarkar
Applied Statistics Unit
Indian Statistical Institute
203, B.T. Road, Kolkata
INDIA 700 108
e-mail: palash@isical.ac.in

Abstract

Let $X^{(1)}, X^{(2)}, \ldots, X^{(n)}$ be independent and uniformly distributed over the non-negative integers $\{0, 1, \ldots, 2^i - 1\}$; $S^{(n)} = X^{(1)} + X^{(2)} + \cdots + X^{(n)}$ and $L^{(n)} = X^{(1)} \oplus X^{(2)} \oplus \cdots \oplus X^{(n)}$. Denote the i-th bits of $S^{(n)}$ and $L^{(n)}$ by $S_i^{(n)}$ and $L_i^{(n)}$ respectively. We show that as $i \to \infty$, $\Pr[S_i^{(n)} = L_i^{(n)}] \to \gamma^{(n)} = \frac{1}{2} + \frac{2^{n+1}(2^{n+1}-1)}{2(n+1)} \times \frac{b_{n+1}}{n!}$, where b_n is the n-th Bernoulli number. As a consequence, $\gamma^{(2r)} = 1/2$ for every r; and we show that $\gamma^{(2r+1)} \to 1/2$ as $r \to \infty$. For small values of r, $\gamma^{(2r+1)}$ is significantly different from $1/2$; for example $\gamma^{(3)} = 1/3$ and $\gamma^{(5)} = 17/30$. The behaviour of $\gamma^{(n)}$ for even and odd values of n was earlier shown by Staffelbach and Meier without actually obtaining the formula mentioned above. For every fixed $n \geq 2$, we give a simple method for computing $\Pr[S_i^{(n)} = L_i^{(n)}]$ for each $i \geq 0$. The expression involving Bernoulli numbers is arrived at via the Eulerian number triangle which in turn arises in relation to the stationary distribution of a Markov chain formed by the carry values.

1 Introduction

Computer arithmetic is performed on w-bit words where w is usually a power of 2. Modern processors use $w = 32$ and processors using $w = 64$ are slowly coming into the market. Two of the most common computer arithmetic operations are addition modulo 2^w and the bitwise exclusive OR (XOR) of two w-bit words. The first operation is addition over the ring of integers modulo 2^w while the second operation is addition over $\mathbb{F}_2^w$, where $\mathbb{F}_2$ is the finite field of two elements. Addition will be denoted by $+$ while exclusive OR will be denoted by $\oplus$.

Addition of two w-bit words involves the carry values at each step. The carry into the i-th step depends nonlinearly on all the bits upto and including the $(i-1)$st step. Here nonlinearity is intended to mean that the operation is not a linear operation over $\mathbb{F}_2^w$. Thus, $+$ is a nonlinear operation over $\mathbb{F}_2^w$ while $\oplus$ is a linear operation over $\mathbb{F}_2^w$. So, one can form a linear approximation of $+$ by replacing it with $\oplus$. In this paper, we study this approximation.

Consider the addition of n w-bit words and the linear approximation of the sum by the XOR of these words. Let $\gamma_i^{(n)}$ be the probability that the i-th bit of the sum of n independent and uniform random words is equal to their XOR. This paper analyses the behaviour of $\gamma_i^{(n)}$ as i increases. Let the limiting value of $\gamma_i^{(n)}$ be denoted by $\gamma^{(n)}$.

Our analysis starts with a systematic analysis of the behaviour of the carry values when n words are added. It is rather easily shown that the carry values form a Markov chain having a unique stationary distribution. Somewhat surprisingly, the stationary distribution turns out to be defined from the Eulerian number triangle, which is a well-known sequence of integers. Our proof of the stationarity actually provides a new relation for the Eulerian number triangle. Having established the link to one well-known sequence,

Table 1: Values of $\gamma^{(n)}$ for some odd values of n.

n	3	5	7	9
$\gamma^{(n)}$	1/3	17/30	149/315	2897/5670

we pursue it further to obtain links with the Bernoulli numbers and the so-called up/down numbers. It is shown that $\gamma^{(n)}$ has a closed form formula in terms of the Bernoulli numbers. We found the link between the carry values and well known sequences to be particularly nice.

The formula for $\gamma^{(n)}$ is used to show that if n is even, then $\gamma^{(n)} = 1/2$; while if n is odd, then $\gamma^{(n)} \neq 1/2$, but, the sequence $\gamma^{(n)}$ tends to 1/2 as n goes to infinity through odd values. For small values of odd n, the value of $\gamma^{(n)}$ is significantly away from 1/2. Examples of values of $\gamma^{(n)}$ for small odd values of n are given in Table 1. Apart from the asymptotic analysis, for every fixed $n \geq 2$, we provide a simple method to compute $\gamma_i^{(n)}$ for $i \geq 0$.

Motivation. A major motivation of the work comes from cryptography. Designers of (symmetric key) cryptographic algorithms are particularly interested in nonlinear operations which are simple and efficient to implement in modern computers. Addition is a particularly good choice satisfying this requirement. There are many designs [3, 10, 9] where additions play a significant role in providing nonlinearity.

Cryptanalysts, on the other hand, would like to have good linear approximations to the nonlinear components of a design. Consequently, good linear approximations of additions are of significant interest. There are well known designs which use addition of more than three words. For example, the SHA-2 algorithm is a standard of the NIST of USA [9]. This algorithm uses 8 registers labelled a to h which are updated in each step. The updation of the registers at the t-th, step $t \geq 0$, is done from the register values at the $(t-1)$st step in the following manner. The values of $(a_{-1}, \ldots, h_{-1})$ are initially set to some fixed values called the initialization vector.

$$\left.\begin{array}{rcl} a_t & = & \Sigma_0(a_{t-1}) + f_{MAJ}(a_{t-1}, b_{t-1}, c_{t-1}) + \Sigma_1(e_{t-1}) + f_{IF}(e_{t-1}, f_{t-1}, g_{t-1}) + h_{t-1} + K_t + W_t \\ b_t & = & a_{t-1} \\ c_t & = & b_{t-1} \\ d_t & = & c_{t-1} \\ e_t & = & d_{t-1} + \Sigma_1(e_{t-1}) + f_{IF}(e_{t-1}, f_{t-1}, g_{t-1}) + h_{t-1} + K_t + W_t \\ f_t & = & e_{t-1} \\ g_t & = & f_{t-1} \\ h_t & = & g_{t-1}. \end{array}\right\} \tag{1}$$

Here f_{MAJ} and f_{IF} are three variable Boolean functions; Σ_0 and Σ_1 are linear transformations; K_t is the constant at the t-th step and W_t is the message word used at the t-th step. Note that the update function of the a-register involves the addition of 7 words while the update function of the e-register involves the addition of 6 words. Looking at the a-register, it follows from our analysis that the i-th bit of a_t is equal to the i-th bit of $\Sigma_0(a_{t-1}) \oplus f_{MAJ}(a_{t-1}, b_{t-1}, c_{t-1}) \oplus \Sigma_1(e_{t-1}) \oplus f_{IF}(e_{t-1}, f_{t-1}, g_{t-1}) \oplus h_{t-1} \oplus K_t \oplus W_t$ with probability approximately equal to $\gamma^{(7)} = 149/315$. This observation has not been reported earlier. It is possible that similar observations can be made for other algorithms which use addition as a basic nonlinear operation.

Previous work. A general analysis for approximating the sum of n integers by their XOR was done in [8]. For the initial part, we proceed as in [8] and obtain the same state transition matrix of the Markov

Table 2: Values of $\genfrac{\langle}{\rangle}{0pt}{}{n}{s}$ for $n = 2$ to 10.

n	s from 0 to $n-1$
2	1, 1
3	1, 4, 1
4	1, 11, 11, 1
5	1, 26, 66, 26, 1
6	1, 57, 302, 302, 57, 1
7	1, 120, 1191, 2416, 1191, 120, 1
8	1, 247, 4293, 15619, 15619, 4293, 247, 1
9	1, 502, 14608, 88234, 156190, 88234, 14608, 502, 1
10	1, 1013, 47840, 455192, 1310354, 1310354, 455192, 47840, 1013, 1

chain formed by the carry values. From this point onwards, the analysis of [8] differs from our work. We obtain the closed form solution for the stationary distribution and use it to obtain a formula for $\gamma^{(n)}$ from which we deduce the behaviour for even and odd n. On the other hand, in [8] the eigenvalues of the state transition matrix are obtained and it is shown that the stationary distribution is the eigenvector corresponding to the eigenvalue 1. This property is then used to obtain the behaviour of $\gamma^{(n)}$. Thus, even though the result on the behaviour of $\gamma^{(n)}$ is same in both [8] and our work, the interests in the two works are different. They work with eigenvalues which we do not; while we solve for the stationary distribution, which [8] does not do. Additionally, we also describe how to compute $\gamma_i^{(n)}$ and obtain closed form solutions for $\gamma_i^{(n)}$ for $n \leq 4$.

The case of addition of 3 integers was again subsequently addressed in [6, 5] and the case of general n was briefly tackled in the appendix of [5].

2 Some Well Known Sequences

We describe the sequences and some of their properties which have been used in this paper. These information have been obtained from [7, 2, 1].

Triangle of Eulerian numbers. For $n \geq 1$ and $0 \leq s \leq n-1$, define $\genfrac{\langle}{\rangle}{0pt}{}{n}{s}$ to be the number of permutations of the numbers 1 to n in which exactly s elements are greater than the previous element (permutations with s ascents). This is a well known sequence of numbers and information about them can be found at several places on the net [7, 2]. They satisfy a recurrence given by

$$\left.\begin{array}{rcll} \genfrac{\langle}{\rangle}{0pt}{}{2}{s} & = & 1 & \text{if } s = 0, 1; \\ \genfrac{\langle}{\rangle}{0pt}{}{n}{s} & = & (s+1)\genfrac{\langle}{\rangle}{0pt}{}{n-1}{s} + (n-s)\genfrac{\langle}{\rangle}{0pt}{}{n-1}{s-1} & \text{if } n > 2. \end{array}\right\} \tag{2}$$

The values of $\genfrac{\langle}{\rangle}{0pt}{}{n}{s}$ for $n = 2$ to 10 are shown in Table 2. These computations and all other computations in this work was done using Mathematica [11]. The Eulerian numbers satisfy some interesting properties. For example, it is easy to prove the following two facts by induction on n or from the combinatorial definition of $\genfrac{\langle}{\rangle}{0pt}{}{n}{s}$.

$$\genfrac{\langle}{\rangle}{0pt}{}{n}{s} = \genfrac{\langle}{\rangle}{0pt}{}{n}{n-1-s}. \tag{3}$$

$$\sum_{s=0}^{n-1} \left\langle {n \atop s} \right\rangle \quad = \quad n!. \tag{4}$$

A closed form formula is also known [2].

$$\left\langle {n \atop s} \right\rangle \quad = \quad \sum_{k=0}^{s} (-1)^k \binom{n+1}{k} (s+1-k)^n. \tag{5}$$

Bernoulli numbers. This is also a well known sequence and there are different ways of defining them [1, 7]. A simple way to view them is to consider their exponential generating function, i.e.,

$$\sum_{n=0}^{\infty} b_n \frac{x^n}{n!} = \frac{x}{e^x - 1}. \tag{6}$$

If n is odd, then it is known that $b_n = 0$; bounds on the b_n for even n are known [1]. For $n > 1$,

$$4\sqrt{\pi n}\left(\frac{n}{\pi e}\right)^{2n} \leq \quad |b_{2n}| \quad \leq 5\sqrt{\pi n}\left(\frac{n}{\pi e}\right)^{2n}. \tag{7}$$

The relation to Eulerian numbers is given by the following relation.

$$\sum_{s=0}^{n-1} (-1)^s \left\langle {n \atop s} \right\rangle \quad = \quad \frac{2^{n+1}(2^{n+1}-1)}{n+1} \times b_{n+1}. \tag{8}$$

Up/Down numbers. For $n \geq 1$, define T_n to be the number of alternating permutations of the set $\{1, 2, \ldots, n\}$, i.e., permutations that alternately rise and fall, starting with a rise. These numbers are called up/down numbers. Examples of T_n for $n = 1, \ldots, 12$ are

$$T_n = 1, 1, 1, 2, 5, 16, 61, 272, 1385, 7936, 50521, 353792.$$

The following gives the relation between b_n and T_n [1].

$$b_{2r} \quad = \quad (-1)^r \frac{(2r)}{2^{2r} - 4^{4r}} T_n. \tag{9}$$

3 Basic Analysis

The results in this section have been earlier obtained in [8]. Our description here is for the sake of completeness.

Let $X^{(1)}, X^{(2)}, \ldots, X^{(n)}$ be non-negative integers; $S^{(n)} = X^{(1)} + X^{(2)} + \cdots + X^{(n)}$ and $L^{(n)} = X^{(1)} \oplus X^{(2)} \oplus \cdots \oplus X^{(n)}$. Let X_i denote the i-th bit of the binary representation of the non-negative integer X. We are interested in $\Pr[S_i^{(n)} = L_i^{(n)}]$. Here and in what follows below, probabilities are taken over independent and uniform random choices of the bits $X_0^{(j)}, X_1^{(j)}, \ldots, X_i^{(j)}$, $1 \leq j \leq n$. While considering $\Pr[S_i^{(n)} = L_i^{(n)}]$, there is no need to consider the $(i+1)$st, $(i+2)$nd and other bits in higher positions.

Visualize the column-by-column binary addition of $X^{(1)}, X^{(2)}, \ldots, X^{(n)}$ starting from the column $i = 0$ and increasing i step-by-step. The i-th step adds $X_i^{(1)}, X_i^{(2)}, \ldots, X_i^{(n)}$ and the carry from the $(i-1)$-th step to produce the bit $S_i^{(n)}$ and a carry. Since n can be greater than 2, the carry can be greater than 1; in general it will be a non-negative number. To understand the addition, we need to understand the carry. To this end, we define the following two sequences.

Define $A_{-1}^{(n)} = 0$ and for $i \geq 0$, define

$$\left.\begin{array}{rcl} B_i^{(n)} & = & X_i^{(1)} + X_i^{(2)} + \cdots + X_i^{(n)}; \\ A_i^{(n)} & = & \left\lfloor \frac{A_{i-1}^{(n)} + B_i^{(n)}}{2} \right\rfloor. \end{array}\right\} \tag{10}$$

Lemma 1 *For $i \geq 0$, the carry into the i-th step is $A_{i-1}^{(n)}$ and the carry out of the i-th step is $A_i^{(n)}$.*

Proof : This is proved by induction on i.
Base $i = 0$. Since $A_{-1} = 0$ by definition, the statement about carry into the i-th step holds. In this step, the bits $X_0^{(1)}, X_0^{(2)}, \ldots, X_0^{(n)}$ are added to obtain $B_0^{(n)}$. The least significant bit of $B_0^{(n)}$ is $S_0^{(n)}$ and the carry is $\lfloor B_0^{(n)}/2 \rfloor$. So the statement regarding the carry out of the i-th step also holds.
Inductive step. Suppose $i > 0$. By induction, the carry out of the $(i-1)$st step is $A_{i-1}^{(n)}$, which is the carry into the i-th step. So, in the i-th step $A_{i-1}^{(n)}$ is added to $B_i^{(n)} = X_i^{(1)} + X_i^{(2)} + \cdots + X_i^{(n)}$. Let the binary representation of the result be a bit string x_i. The least significant bit of x_i is equal to $S_i^{(n)}$ and the other bits provide the binary representation of the carry out of the i-th step. So, the carry out of the i-th step is $x_i \gg 1$. The integer value of $x_i \gg 1$ is easily seen to be equal to $\lfloor (A_{i-1}^{(n)} + B_i^{(n)})/2 \rfloor$. Since, by definition, this is equal to $A_i^{(n)}$, the carry out of the i-th step is $A_i^{(n)}$. ■

The following result is now easy to see.

Lemma 2 *For $i \geq 0$, $L_i^{(n)} = B_i^{(n)} \bmod 2$ and $S_i^{(n)} = A_{i-1}^{(n)} + B_i^{(n)} \bmod 2$. Consequently,*

$$\Pr[S_i^{(n)} = L_i^{(n)}] = \Pr[A_{i-1}^{(n)} \bmod 2 = 0].$$

For $i \geq 0$, define

$$\gamma_i^{(n)} = \Pr[A_{i-1}^{(n)} \bmod 2 = 0]. \tag{11}$$

Then, $\gamma_i^{(n)} = \Pr[S_i^{(n)} = L_i^{(n)}]$. Also, note that $\gamma_0^{(n)} = 1$. We wish to study the behaviour of $\gamma_i^{(n)}$ as i increases and in particular, we will be interested in the limiting behaviour of $\gamma_i^{(n)}$ as $i \to \infty$. Assuming that the limit exists (which will follow later), we denote the limit by $\gamma^{(n)}$. Our final goal is to obtain a formula for $\gamma^{(n)}$.

Lemma 3 *For $i \geq 0$, $\gamma_i^{(n)} = \sum_{\text{even } s} \Pr[A_{i-1}^{(n)} = s]$.*

Proof : Clearly, $\Pr[A_{i-1}^{(n)} \bmod 2 = 0] = \sum_{\text{even } s} \Pr[A_{i-1}^{(n)} = s]$. ■

This implies that we should consider the values that $A_{i-1}^{(n)}$ can take.

Lemma 4 *For $i \geq -1$, $0 \leq A_i^{(n)} \leq n - 1$.*

Proof : From the definition, clearly $A_i^{(n)} \geq 0$ for all $i \geq -1$. The upper bound follows by induction on i. For $i = -1$, $A_i^{(n)} = 0 \leq n - 1$ holds. For $i \geq 0$, $A_i^{(n)} = \lfloor (A_{i-1}^{(n)} + B_i^{(n)})/2 \rfloor \leq \lfloor (n - 1 + n)/2 \rfloor \leq n - 1$. ■

The maximum value of $(n-1)$ is in fact achieved for each n. To see this consider the situation where $B_i^{(n)} = n$ for all $i \geq 0$. This corresponds to the situation where all the bits are 1. Then if $A_{i-1}^{(n)} < n - 1$, we have $n - 1 \geq A_i^{(n)} > A_{i-1}^{(n)}$, i.e., the values of the $A_i^{(n)}$ increase from 0 to $(n-1)$ and do not increase any further. So, for each i, $A_i^{(n)}$ is a random variable taking values from the set $\{0, \ldots, n-1\}$ under some distribution. The following result gives a recurrence relation for $\Pr[A_i^{(n)} = t]$.

Theorem 5 *For $i \geq 0$ and $0 \leq t \leq n-1$,*

$$\Pr[A_i^{(n)} = t] = \sum_{s=0}^{n-1} \delta_{s,t}^{(n)} \Pr[A_{i-1}^{(n)} = s] \tag{12}$$

where

$$\delta_{s,t}^{(n)} \quad = \quad \frac{1}{2^n} \times \binom{n+1}{2t-s+1}. \tag{13}$$

Proof : Since $A_{i-1}^{(n)}$ can take the values $0, \ldots, n-1$, we have

$$\Pr[A_i^{(n)} = t] \quad = \quad \sum_{s=0}^{n-1} \Pr[A_i^{(n)} = t | A_{i-1}^{(n)} = s] \times \Pr[A_{i-1}^{(n)} = s].$$

Since $A_i^{(n)} = \lfloor (A_{i-1}^{(n)} + B_i^{(n)})/2 \rfloor$, it follows that the event $(A_i^{(n)} = t | A_{i-1}^{(n)} = s)$ occurs if and only if $B_i^{(n)} = 2t - s$ or $B_i^{(n)} = 2t - s + 1$. Again, note that $B_i^{(n)} = X_i^{(1)} + X_i^{(2)} + \cdots + X_i^{(n)}$ where $X_i^{(j)}$ are mutually independent and uniformly distributed over $\{0, 1\}$. So, for any k, the probability that $B_i^{(n)} = k$ is equal to $\binom{n}{k}/2^n$. Hence,

$$\begin{aligned} \Pr[A_i^{(n)} = t | A_{i-1}^{(n)} = s] &= \Pr[B_i^{(n)} = 2t - s \text{ or } 2t - s + 1] \\ &= \frac{1}{2^n} \left(\binom{n}{2t-s} + \binom{n}{2t-s+1} \right) \\ &= \frac{1}{2^n} \binom{n+1}{2t-s+1}. \end{aligned}$$

The result now follows by setting $\delta_{s,t}$ to the last expression. ■

Note. It has been shown in [8] that the eigenvalues of P_n are 2^{-k} for $0 \leq k \leq n-1$.

4 The Markov Chain Formed by the Carry Values

Theorem 5 shows that the sequence $\{A_i^{(n)}\}$ actually forms a Markov chain (MC) $\mathcal{M}_n$. The state space of $\mathcal{M}_n$ is $\{0, \ldots, n-1\}$ and the transition matrix is P_n where the (s,t)-th entry $P_n[s,t]$ is equal to $\delta_{s,t}^{(n)}$. P_6 is shown below.

$$P_6 = \begin{pmatrix} \frac{7}{64} & \frac{35}{64} & \frac{21}{64} & \frac{1}{64} & 0 & 0 \\ \frac{1}{64} & \frac{21}{64} & \frac{35}{64} & \frac{7}{64} & 0 & 0 \\ 0 & \frac{7}{64} & \frac{35}{64} & \frac{21}{64} & \frac{1}{64} & 0 \\ 0 & \frac{1}{64} & \frac{21}{64} & \frac{35}{64} & \frac{7}{64} & 0 \\ 0 & 0 & \frac{7}{64} & \frac{35}{64} & \frac{21}{64} & \frac{1}{64} \\ 0 & 0 & \frac{1}{64} & \frac{21}{64} & \frac{35}{64} & \frac{7}{64} \end{pmatrix}.$$

For every s, the probability $P_n[s,s]$ is non-zero and for $0 < s < n-1$, the probabilities $P_n[s,t-1]$ and $P_n[s,t+1]$ are both non-zero. This shows that $\mathcal{M}_n$ is irreducible and aperiodic. Since the chain is finite (i.e., the state space is finite) not all states are transient and none is a null state. So, there exists a persistent non-null state. Again since $\mathcal{M}_n$ is irreducible, all states are of the same type, so that all states are aperiodic and persistent non-null. Hence, $\mathcal{M}_n$ has a unique stationary distribution $(\alpha_0^{(n)}, \ldots, \alpha_{n-1}^{(n)})$.

So, the probability $\Pr[A_i^{(n)} = s]$ tends to $\alpha_s^{(n)}$ as i tends to infinity. Further, we have

$$\gamma_i^{(n)} = \sum_{\text{even } s} \Pr[A_{i-1}^{(n)} = s] \to \sum_{\text{even } s} \alpha_s^{(n)}. \tag{14}$$

Thus, the limit $\gamma^{(n)}$ of $\gamma_i^{(n)}$ exists and is equal to

$$\gamma^{(n)} = \sum_{\text{even } s} \alpha_s^{(n)}. \tag{15}$$

Our task now is to obtain the stationary distribution $(\alpha_0^{(n)}, \ldots, \alpha_{n-1}^{(n)})$.

The following result shows the importance of Eulerian number triangle in our context. See Section 2 for the definition of Eulerian number triangle.

Theorem 6 *For $n \geq 2$, $0 \leq s \leq n-1$,*

$$\alpha_s^{(n)} = \frac{\left\langle {n \atop s} \right\rangle}{n!}.$$

In other words, the stationary distribution of $\mathcal{M}_n$ is obtained from the Eulerian numbers. We find this to be a surprising connection!

Proof : From (4) in Section 2 we have $\sum_{s=0}^{n-1} \left\langle {n \atop s} \right\rangle = n!$ and so $\sum_{s=0}^{n-1} \alpha_s^{(n)} = 1$. This shows that $(\alpha_0^{(n)}, \ldots, \alpha_{n-1}^{(n)})$ is a probability distribution on the set $\{0, \ldots, n-1\}$. Now, we have to prove that this is invariant under multiplication with P_n, i.e., we have to show

$$(\alpha_0^{(n)}, \ldots, \alpha_{n-1}^{(n)}) P_n = (\alpha_0^{(n)}, \ldots, \alpha_{n-1}^{(n)}).$$

This will be proved if we can show that using the given value of $\alpha_s^{(n)}$, for $0 \leq t \leq n-1$ we have

$$\sum_{s=0}^{n-1} \alpha_s^{(n)} \delta_{s,t}^{(n)} = \alpha_t^{(n)}. \tag{16}$$

where $\delta_{s,t}^{(n)}$ is given by (13). This actually provides a new relation for Eulerian numbers. Even though these numbers are well studied, we did not find this relation in the literature. Hence, we provide a proof of (16).

$$\begin{aligned}
\sum_{s=0}^{n-1} \alpha_s^{(n)} \delta_{t,s}^{(n)} &= \frac{1}{2^n} \times \sum_{s=0}^{n-1} \alpha_s^{(n)} \binom{n+1}{2t-s+1} \\
&= \frac{1}{2^n} \times \sum_{s=0}^{2t+1} \alpha_s^{(n)} \binom{n+1}{2t-s+1} \\
&= \frac{1}{2^n} \times \sum_{s=0}^{2t+1} \alpha_{2t+1-s}^{(n)} \binom{n+1}{s}.
\end{aligned}$$

Using the given expression for $\alpha_s^{(n)}$ and (5) from Section 2, we get

$$\alpha_s^{(n)} = \frac{1}{n!} \left\langle {n \atop s} \right\rangle = \frac{1}{n!} \times \sum_{k=0}^{s} (-1)^k \binom{n+1}{k} (s+1-k)^n.$$

Using this value, we have

$$\begin{aligned}
\sum_{s=0}^{n-1} \alpha_s^{(n)} \delta_{t,s}^{(n)} &= \frac{1}{n!2^n} \times \sum_{s=0}^{2t+1} \binom{n+1}{s} \sum_{k=0}^{2t+1-s} (-1)^k \binom{n+1}{k} (2t+2-s-k)^n \\
&= \frac{1}{n!2^n} \times \sum_{s=0}^{2t+1} \binom{n+1}{s} \sum_{k=0}^{2t+1-s} (-1)^{s+k+1} \binom{n+1}{2t+1-s-k} (k+1)^n \\
&= \frac{1}{n!2^n} \times \sum_{s=0}^{2t+1} \sum_{k=0}^{2t+1-s} (-1)^{s+k+1} \binom{n+1}{s} \binom{n+1}{2t+1-s-k} (k+1)^n \\
&= \frac{1}{n!2^n} \times \sum_{k=0}^{2t+1} \sum_{s=0}^{2t+1-k} (-1)^{s+k+1} \binom{n+1}{s} \binom{n+1}{2t+1-s-k} (k+1)^n \\
&= \frac{1}{n!2^n} \times \sum_{k=0}^{2t+1} (-1)^{k+1} (k+1)^n \sum_{s=0}^{2t+1-k} (-1)^s \binom{n+1}{s} \binom{n+1}{2t+1-s-k}.
\end{aligned}$$

For even k,

$$(-1)^s \binom{n+1}{s} \binom{n+1}{2t+1-s-k} = -\left((-1)^{2t+1-k-s} \binom{n+1}{2t+1-s-k} \binom{n+1}{s} \right)$$

and so for even k, the sum

$$\sum_{s=0}^{2t+1-k} (-1)^s \binom{n+1}{s} \binom{n+1}{2t+1-s-k} \quad = \quad 0.$$

Now putting $k = 2r+1$, we have that as r ranges from 0 to t, k ranges from 1 to $2t+1$ through odd values. This gives

$$\begin{aligned}
\sum_{s=0}^{n-1} \alpha_s^{(n)} \delta_{t,s}^{(n)} &= \frac{1}{n!2^n} \times \sum_{r=0}^{t} (-1)^{2r+2} (2r+2)^n \sum_{s=0}^{2(t-r)} (-1)^s \binom{n+1}{s} \binom{n+1}{2(t-r)-s} \\
&= \frac{1}{n!} \times \sum_{r=0}^{t} (r+1)^n \sum_{s=0}^{2(t-r)} (-1)^s \binom{n+1}{s} \binom{n+1}{2(t-r)-s} \\
&= \frac{1}{n!} \times \sum_{r=0}^{t} (t+1-r)^n \sum_{s=0}^{2r} (-1)^s \binom{n+1}{s} \binom{n+1}{2r-s} \\
&= \frac{1}{n!} \times \sum_{r=0}^{t} (t+1-r)^n (-1)^r \binom{n+1}{r} \\
&= \frac{1}{n!} \times \left\langle {n \atop t} \right\rangle \\
&= \alpha_t^{(n)}.
\end{aligned}$$

The equality $\sum_{s=0}^{2r} (-1)^s \binom{n+1}{s} \binom{n+1}{2r-s} = (-1)^r \binom{n+1}{r}$ follows by equating the coefficient of x^{2r} on both sides of $(1-x^2)^r = (1-x)^r (1+x)^r$. ■

Now we are in a position to derive the value of $\gamma^{(n)}$ for even n.

Proposition 1 *If n is even, then $\gamma^{(n)} = 1/2$.*

Proof : The stationary distribution $(\alpha_0^{(n)}, \ldots, \alpha_{n-1}^{(n)})$ satisfies $\sum_{s=0}^{n-1} \alpha_s^{(n)} = 1$. Also, using (3) from Section 2 we have $\alpha_s^{(n)} = \alpha_{n-1-s}^{(n)}$ and so, $\sum_{s=0}^{n/2-1} \alpha_s^{(n)} = 1/2$. Now,

$$\begin{aligned}
\gamma^{(n)} = \sum_{s \text{ even}} \alpha_s^{(n)} &= \sum_{s \text{ even}, s<n/2} \alpha_s^{(n)} + \sum_{s \text{ even}, s \geq n/2} \alpha_s^{(n)} \\
&= \sum_{s \text{ even}, s<n/2} \alpha_s^{(n)} + \sum_{s \text{ even}, s \geq n/2} \alpha_{n-1-s}^{(n)} \\
&= \sum_{s \text{ even}, s<n/2} \alpha_s^{(n)} + \sum_{s \text{ odd}, s<n/2} \alpha_s^{(n)} \\
&= \sum_{s=0}^{n/2-1} \alpha_s^{(n)} = \frac{1}{2}.
\end{aligned}$$

■

More generally, we have the following result.

Theorem 7 *For $n \geq 2$,*

$$\gamma^{(n)} = \frac{1}{2} + \frac{2^{n+1}(2^{n+1}-1)}{2(n+1)} \times \frac{b_{n+1}}{n!}.$$

Here b_n is the n-th Bernoulli number. (See Section 2 for the definition of this sequence.)

Proof : Recall from (15) that $\gamma^{(n)} = \sum_{\text{even } s} \alpha_s^{(n)}$. From Theorem 6, we have $\alpha_s^{(n)} = \left\langle {n \atop s} \right\rangle / n!$. Also, $\sum_{s=0}^{n-1} \alpha_s^{(n)} = 1$ and from (8)

$$\sum_{s=0}^{n-1} (-1)^s \alpha_s^{(n)} = \frac{2^{n+1}(2^{n+1}-1)}{n+1} \times \frac{b_{n+1}}{n!}.$$

Adding these two equations, we obtain the desired result. ■

It is known that $b_n = 0$ if n is odd and so Theorem 7 provides another proof that $\gamma^{(n)} = 1/2$ for even n. As shown in Proposition 1, we do not need this property of Bernoulli numbers to obtain the result for even n. Some values of $\gamma^{(n)}$ for odd values of n are given in Table 1. From this table it is clear that even though $\gamma^{(n)}$ is not equal to $1/2$ for odd n, the value approaches $1/2$ as n increases through odd values.

Proposition 2 $\gamma^{(n)} \to 1/2$ *as $n \to \infty$ through odd values.*

Proof : From Stirling's formula,

$$\sqrt{2\pi} n^{n+\frac{1}{2}} e^{-n} \times e^{(12n+1)^{-1}} < n! < \sqrt{2\pi} n^{n+\frac{1}{2}} e^{-n} \times e^{(12n)^{-1}}.$$

Combining Theorem 7 and (7) we have

$$\begin{aligned}
\left| \gamma^{(2r+1)} - \frac{1}{2} \right| &= \left| \frac{2^{2r+2}(2^{2r+2}-1)}{4(r+1)} \times \frac{b_{2r+2}}{(2r+1)!} \right| \\
&< \frac{2^{4(r+1)}}{2(2r+2)(2r+1)!} \times \left(5\sqrt{\pi(r+1)} \left(\frac{r+1}{\pi e} \right)^{2r+2} \right) \\
&< \frac{5}{2} \sqrt{\pi(r+1)} \times \left(\frac{4}{\pi e} \right)^{2r+2} \times \frac{(r+1)^{2r+2}}{(2r+2)!}
\end{aligned}$$

Putting $m = 2r+2$, and using the lower bound of Stirling's approximation, we have

$$\left| \gamma^{(2r+1)} - \frac{1}{2} \right| < \frac{5}{4} \times \left(\frac{2}{\pi} \right)^m \times \frac{1}{e^{(12m+1)^{-1}}} < \frac{5}{4} \times \left(\frac{2}{\pi} \right)^m \to 0$$

as $m \to \infty$. ■

Table 3: Values of $\gamma_i^{(n)}$ of lower order bits.

$n\backslash i$	1	2	3	4	5	6	7
2	0.75	0.625	0.5625	0.53125	0.515625	0.507813	0.503906
3	0.5	0.375	0.34375	0.335938	0.333984	0.333496	0.333374
4	0.375	0.390625	0.439453	0.468994	0.484406	0.492191	0.496094
5	0.375	0.5	0.548828	0.562134	0.565529	0.566382	0.566595
6	0.4375	0.546875	0.536865	0.520226	0.51034	0.505199	0.502603
7	0.5	0.523438	0.489136	0.477278	0.474096	0.473287	0.473084
8	0.53125	0.491699	0.482151	0.488944	0.494192	0.49706	0.498526
9	0.53125	0.48584	0.5	0.507857	0.510143	0.510735	0.510885
10	0.515625	0.49646	0.507328	0.505477	0.502989	0.501527	0.500767

Note. Propositions 1 and 2 were obtained earlier in [8]. The technique used was different. The explicit solution of the stationary distribution was not obtained; instead it was shown that the two results can be obtained from the fact that the stationary distribution is the eigenvector of P_n corresponding to the eigenvalue 1.

Proposition 3 *For $r \geq 1$,*

$$\gamma^{(2r+1)} = \frac{1}{2} + \frac{(-1)^r}{2} \times \frac{T_{2r+2}}{(2r+1)!}$$

where T_n is the sequence of up/down numbers. (See Section 2 for the definition.)

5 Computation of $\gamma_i^{(n)}$

We describe a method to compute the values of $\gamma_i^{(n)}$. Let $\beta_{i,s}^{(n)} = \Pr[A_i^{(n)} = s]$ so that $(\beta_{-1,0}^{(n)}, \ldots, \beta_{-1,n-1}^{(n)}) = (1, 0, \ldots, 0)$. Then for $i \geq 0$, using Theorem 5 we have

$$(\beta_{i,0}^{(n)}, \ldots, \beta_{i,n-1}^{(n)}) \quad = \quad (\beta_{i-1,0}^{(n)}, \ldots, \beta_{i-1,n-1}^{(n)}) P_n. \tag{17}$$

This gives a method for computing $\beta_{i,s}^{(n)}$. For $i \geq 0$, from Lemma 3 we have

$$\gamma_i^{(n)} \quad = \quad \sum_{\text{even } s} \beta_{i-1,s}^{(n)}. \tag{18}$$

Equation (18) together with (17) gives a method for computing $\gamma_i^{(n)}$.

Examples of $\gamma_i^{(n)}$ for $n \geq 2$ are given in Table 3. Since $\gamma_0^{(n)} = 1$, we only show the values for $i \geq 1$. Note that even though $\gamma^{(n)} = 1/2$ for even values of n, the manner and rate at which $\gamma_i^{(n)}$ approaches $1/2$ depends upon the value of n. For example if $n = 4$, deviation of $\gamma_i^{(4)}$ from $1/2$ upto the second digit after decimal is observed for $i = 1, \ldots, 5$.

For small values of n, it is possible to obtain closed form formulas for $\gamma_i^{(n)}$. First, we analyse the sequence $\gamma_i^{(n)}$ in a general manner and then show how to obtain the desired formulas for small n. Using (17) and (18), for $i \geq 0$, we compute as follows.

$$\begin{aligned}\gamma_{i+1}^{(n)} = \sum_{\text{even } t} \beta_{i,t}^{(n)} &= \sum_{\text{even } t} \sum_{s=0}^{n-1} \delta_{s,t}^{(n)} \beta_{i-1,s}^{(n)} \\ &= \sum_{s=0}^{n-1} \beta_{i-1,s}^{(n)} \left(\sum_{\text{even } t} \delta_{s,t}^{(n)} \right).\end{aligned}$$

Define

$$\lambda_{0,s}^{(n)} = \sum_{\text{even } t} \delta_{s,t}^{(n)}. \tag{19}$$

Then we can write

$$\gamma_{i+1}^{(n)} = \sum_{s=0}^{n-1} \lambda_{0,s}^{(n)} \beta_{i-1,s}^{(n)}.$$

Each of $\beta_{i-1,s}^{(n)}$ can be further expanded using (17). We perform two such steps of expansion.

$$\begin{aligned}\gamma_{i+1}^{(n)} &= \sum_{s=0}^{n-1} \lambda_{0,s}^{(n)} \beta_{i-1,s}^{(n)} \\ &= \sum_{s=0}^{n-1} \lambda_{0,s}^{(n)} \sum_{r=0}^{n-1} \delta_{r,s}^{(n)} \beta_{i-2,r}^{(n)} \\ &= \sum_{r=0}^{n-1} \beta_{i-2,r}^{(n)} \left(\sum_{s=0}^{n-1} \delta_{r,s}^{(n)} \lambda_{0,s}^{(n)} \right) \\ &= \sum_{s=0}^{n-1} \beta_{i-2,s}^{(n)} \left(\sum_{r=0}^{n-1} \lambda_{0,r}^{(n)} \delta_{s,r}^{(n)} \right) \\ &= \sum_{s=0}^{n-1} \lambda_{1,s}^{(n)} \beta_{i-2,s}^{(n)} \\ \cdots &\quad \cdots \\ &= \sum_{s=0}^{n-1} \lambda_{2,s}^{(n)} \beta_{i-3,s}^{(n)}.\end{aligned}$$

In the above

$$\lambda_{1,s}^{(n)} = \sum_{r=0}^{n-1} \lambda_{0,r}^{(n)} \delta_{s,r}^{(n)} \text{ and } \lambda_{2,s}^{(n)} = \sum_{r=0}^{n-1} \lambda_{1,r}^{(n)} \delta_{s,r}^{(n)}.$$

This process can be continued and in general, for $0 \leq j \leq n$ we have

$$\gamma_{i+1}^{(n)} = \sum_{s=0}^{n-1} \lambda_{j,s}^{(n)} \beta_{i-j-1,s}^{(n)} \tag{20}$$

where $\lambda_{0,s}^{(n)}$ is defined by (19) and for $j > 0$,

$$\lambda_{j,s}^{(n)} = \sum_{r=0}^{n-1} \lambda_{j-1,r}^{(n)} \delta_{s,r}^{(n)}. \tag{21}$$

The relation between $\gamma_i^{(n)}$ and the sequences of λ values is the following.

Table 4: Solutions for $\lambda_{j,s}^{(n)}$ for $n = 2, 3$, and $s = 0, \dots, n-1$.

n	$\lambda_{j,0}^{(n)}$	$\lambda_{j,1}^{(n)}$	$\lambda_{j,2}^{(n)}$	$\lambda_{j,3}^{(n)}$
2	$\frac{1}{2}\left(1 + \frac{1}{2^{j+1}}\right)$	$1 - \lambda_{j,0}^{(2)}$		
3	$\frac{1}{3}\left(1 + \frac{1}{2^{2j+1}}\right)$	$\frac{1}{3}\left(1 - \frac{1}{2^{2j+1}}\right)$	$\lambda_{j,0}^{(3)}$	
4	$\frac{1}{2} - \left(\frac{2^{2j+1}-1}{2^{3(j+1)}}\right)$	$\frac{1}{2} - \left(\frac{2^{2j+1}\lambda_{j,0}^{(3)}}{2^{3(j+1)}}\right)$	$1 - \lambda_{j,1}^{(4)}$	$1 - \lambda_{j,0}^{(4)}$

Proposition 4 *For $n \geq 2$ and $i \geq 0$,*

$$\gamma_{i+1}^{(n)} = \lambda_{i,0}^{(n)}.$$

Proof : Putting $j = i$ in (20), we have

$$\gamma_{i+1}^{(n)} = \sum_{s=0}^{n-1} \lambda_{i,s}^{(n)} \beta_{-1,s}^{(n)}.$$

By definition, $\beta_{-1,0}^{(n)} = 1$ and $\beta_{-1,s}^{(n)} = 0$ for $s > 0$. This shows the result. ■

Proposition 4 suggests that we should consider the sequences of λ values. Further, it also shows tha the sequences $\gamma_i^{(n)}$ and $\lambda_{i,0}^{(n)}$ have the same limit $\gamma^{(n)}$ as $i \to \infty$.

From (21) we have that

$$(\lambda_{j,0}^{(n)}, \dots, \lambda_{j,n-1}^{(n)})' = P_n(\lambda_{j-1,0}^{(n)}, \dots, \lambda_{j-1,n-1}^{(n)})'$$

where $()'$ denotes the transpose operator. From this relation, the following properties can be proved by induction.

Proposition 5 *Let $n \geq 2$ and $0 \leq j \leq \lfloor n/2 \rfloor - 1$.*

1. *If n is odd, then $\lambda_{j,s}^{(n)} = \lambda_{j,n-1-s}^{(n)}$.*

2. *If n is even, then $\lambda_{j,s}^{(n)} = 1 - \lambda_{j,n-1-s}^{(n)}$.*

Using this, it is possible to solve for $\lambda_{j,s}^{(n)}$ for $n = 2, 3, 4$. The solutions are given in Table 4. The proofs that these are indeed the solutions are obtained by induction on $j \geq 0$. (The case of $n = 3$ has been done in [4].) It becomes difficult to obtain closed form solutions for $n \geq 5$. In our computations, we have seen that $\lambda_{j,0}^{(n)}$ approaches its limit $\gamma^{(n)}$ quite fast.

6 Conclusion

The approximation of addition of n non-negative integers by their XOR has been analysed. This has led to interesting connection with well-known sequences such as the Eulerian number triangle and the sequence of Bernoulli numbers. The connection comes via the stationary distribution of the Markov chain formed by the carry values. Our results have consequences to the analysis of cryptographic algorithms. A direct application of our result leads to an interesting observation on the NIST standard SHA-2 algorithm. Applications to other cryptographic algorithms form possible future work.

Acknowledgement.

We would like to thank Subhamoy Maitra for proposing the problem of approximating the sum of 3 integers by their XOR and Willi Meier for pointing out [8] to us.

References

[1] Bernoulli number, 2008. Wikipedia, `http://en.wikipedia.org/wiki/Bernoulli_number`.

[2] Eulerian number, 2008. Wikipedia, `http://en.wikipedia.org/wiki/Eulerian_numbers`.

[3] Daniel J. Bernstein. Salsa20. Technical Report 2005/025, eSTREAM, ECRYPT Stream Cipher Project, 2005. See also `http://cr.yp.to/snuffle.html`.

[4] Subhamoy Maitra, Goutam Paul, Shashwat Raizada, and Palash Sarkar. A linear approximation to addition of three integers and its implication to hc-128. Cryptology ePrint Archive, Report 2008/499, 2008. `http://eprint.iacr.org/`.

[5] Kaisa Nyberg and Johan Wallén. Improved linear distinguishers for SNOW 2.0. In Matthew J. B. Robshaw, editor, *FSE*, volume 4047 of *Lecture Notes in Computer Science*, pages 144–162. Springer, 2006.

[6] Gautham Sekar, Souradyuti Paul, and Bart Preneel. New weaknesses in the keystream generation algorithms of the stream ciphers TPy and Py. In Juan A. Garay, Arjen K. Lenstra, Masahiro Mambo, and René Peralta, editors, *ISC*, volume 4779 of *Lecture Notes in Computer Science*, pages 249–262. Springer, 2007.

[7] N. J. A. Sloane. The on-line encyclopedia of integer sequences, 2008. published electronically at `www.research.att.com/~njas/sequences/`.

[8] Othmar Staffelbach and Willi Meier. Cryptographic significance of the carry for ciphers based on integer addition. In Alfred Menezes and Scott A. Vanstone, editors, *CRYPTO*, volume 537 of *Lecture Notes in Computer Science*, pages 601–614. Springer, 1990.

[9] Secure Hash Standard. *Federal Information Processing Standard Publication 180-2*. U.S. Department of Commerce, National Institute of Standards and Technology(NIST), 2002. Available at `http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf`.

[10] David J. Wheeler and Roger M. Needham. TEA, a Tiny Encryption Algorithm. In Bart Preneel, editor, *FSE*, volume 1008 of *Lecture Notes in Computer Science*, pages 363–366. Springer, 1994.

[11] Stephen Wolfram. *The Mathematica Book*. Wolfram Media, 5th edition, 2003. `http://www.wolfram.com`.