IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 21 July 2025, accepted 21 September 2025, date of publication 29 September 2025, date of current version 7 October 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3615472

THEORY

Summing Modulo 2 of Stationary Binary Stochastic Processes

MIECZYSŁAW JESSA AND JAKUB NIKONOWICZ, (Senior Member, IEEE)
Poznań University of Technology, 60-965 Poznań, Poland

Corresponding author: Mieczysław Jessa (mieczyslaw.jessa@put.poznan.pl)

This work was supported by Polish Ministry of Science and Higher Education.

ABSTRACT In the paper, we analyze the properties of the stochastic process obtained as the result of summing modulo 2 without carry of a finite number of stationary binary stochastic processes, some of which do not satisfy the independence condition. The primary goal of the mathematical analysis is to determine the formula for the minimum number of independent stochastic processes that will ensure the mean and the covariance values between adjacent elements of the output process are acceptable to the user, regardless of the number of dependent stochastic processes at the input. We assume that we do not know which of the summed processes are dependent and which are independent. To the authors' knowledge, this problem has not been addressed in the literature so far, and it may be helpful when using the modulo 2 summation of binary stationary independent random processes with binary dependent processes. Possible applications include random sequence generation, cryptography, simulations, coding theory, etc.

INDEX TERMS Binary stochastic processes, binary random variables, sum modulo 2, XOR operation, mean, covariance, random bit sequences.

I. INTRODUCTION

The sum modulo 2 without carry, or alternatively, exclusive or (XOR) operation, is used in many formulas or functions. The result of XORing (combining XOR) binary stochastic processes is also a stochastic process, but the analytical derivation of its properties is often complex. Most theoretical results assume the independence of input processes, but even in this case, mathematically finding all parameters of the random process at the output is not simple. In this work, we focus on the summation modulo 2 without carry of many binary stochastic stationary processes. The cases of XOR combining two binary variables, two correlated pairs of variables, and the XOR operation of independent correlated pairs were considered in [1]. This analysis is limited to single random variables and does not consider the influence of correlations between an unknown number of random variables on the properties of the output.

In this work, we assume that the XOR operation is performed on R binary stationary stochastic processes, of which N processes are independent and M dependent, and the relation between N and M is unknown. Using mathematical transformations we determine formulas for the mean value of the output process and for the value of covariance between neighboring elements of this process. Then, we determine the smallest number of input stochastic processes that must be independent to obtain the mean and the covariance between neighboring random variables of the output process within the acceptable range, assumed earlier by the user, independently of the number of dependent stochastic processes participating in the XOR summation.

In Section II, we derive formulas for the bias and covariance between adjacent elements of the binary stochastic process resulting from XORing a finite number of stationary binary stochastic processes, where some processes are dependent and some are independent. Section III outlines a method to reduce the bias and covariance between adjacent elements of the output process, particularly when the bias and covariance values, and the number of dependent processes are unknown. In Section IV, we present formulas to determine the minimum number of combined XOR independent binary stationary stochastic processes necessary to achieve and maintain the specified limits for the bias and covariance between adjacent elements of the output process, regardless of the number and parameters of XORed dependent processes. The work concludes with a summary asserting that

The associate editor coordinating the review of this manuscript and approving it for publication was Ahmed Almradi.

the introduced formulas and findings are applicable across various scientific areas.

II. CORRELATION AND COVARIANCE BETWEEN ADJACENT ELEMENTS OF BINARY STOCHASTIC PROCESS OBTAINED AS THE RESULT OF SUMMING MODULO 2 OF MANY BINARY STOCHASTIC PROCESSES

Suppose we are given R binary stochastic processes: $X_1 = \{X_{1,i}\}, X_2 = \{X_{2,i}\}, \ldots, X_R = \{X_{R,i}\}$, $i = 0, 1, \ldots$ [2] which are summed modulo 2 without carry. This operation can also be done using logical operation XOR, which is often preferred due to the greater speed of producing the final result. The result of XORing R binary stochastic processes is also a binary stochastic process, denoted in the paper as $Y = \{Y_i\}$, $i = 0, 1, \ldots.,$ where

$$Y = X_1 \oplus X_2 \oplus \cdots \oplus X_R. \tag{1}$$

The i-th binary random variable Y_i is the XOR sum of R binary random variables, i.e.

$$Y_i = X_{1,i} \oplus X_{2,i} \oplus \cdots \oplus X_{R,i}, i = 0, 1, \ldots. \tag{2}$$

In general, the random variables $X_{r,i}$, where $r = 1, 2, \ldots, R$, can exhibit diverse distributions for different r and i values.

In this paper, we assume that among R stochastic processes from (1), N processes are independent and M=R-N processes are dependent. Notably, we cannot establish which processes are independent or dependent, and we lack information regarding the specifics of this dependence, i.e., if processes are dependent in pairs, triples, quadruples, etc. We assume also that in the all combined processes the greatest covariance occurs between adjacent elements, i.e., $X_{r,i}$ and $X_{r,i+1}$, $r = 1, 2, \ldots, R$.

Given that the variables $\left\{X_{1,i}, X_{2,i}, \ldots, X_{R,i}\right\}$ can theoretically be grouped into two independent sets – one containing independent variables and the second containing dependent variables – (2) can be written as

$$Y_i = A_i \oplus B_i, \tag{3}$$

where A_i represents the XOR sum of N independent binary variables, and B_i denotes the XOR sum of M dependent binary variables at instant i. Both A_i and B_i are considered binary random variables and $A = \{A_i\}$ or $B = \{B_i\}$ are binary stochastic processes.

Let $c_{A,i} = C(A_i, A_{i+1})$ be the covariance of variables A_i and A_{i+1} and $c_{B,i} = C(B_i, B_{i+1})$ be the covariance of variables B_i and B_{i+1},where $i = 0, 1, \ldots..$ Also let $E[A_i] = \mu_{A,i}$, where $E[A_i]$ is the expected value of A_i. Similarly, $E[B_i] = \mu_{B,i}$ is the expected value of B_i. We search the value of covariance

$$c_{Y,i} = C(Y_i, Y_{i+1}) = C(A_i \oplus B_i, A_{i+1} \oplus B_{i+1}) \tag{4}$$

for $i = 0, 1, \ldots.$

To compute the covariance $c_{Y,i}$, we use formulas proposed by R. B. Davies in a private paper published on the Internet [1] (Section IV). When the random variable Y_i is considered to take values of 0 or 1, then $f(Y_i)$=1-$2Y_i$, and (4) takes the following form [1]:

$$C(Y_i, Y_{i+1}) = \frac{1}{4}C(f(Y_i), f(Y_{i+1})). \tag{5}$$

Substituting (3) into (5), we obtain

$$C(Y_i, Y_{i+1}) = \frac{1}{4}C(f(A_i \oplus B_i), f(A_{i+1} \oplus B_{i+1})). \tag{6}$$

Because A_i and B_i are independent and A_{i+1} and B_{i+1} are independent, we obtain [1]

$$C(Y_i, Y_{i+1}) = \frac{1}{4}C(f(A_i)f(B_i), f(A_{i+1}) \cdot f(B_{i+1})). \tag{7}$$

Using (4), (7) can be written in the following form

$$\begin{aligned} C(Y_i, Y_{i+1}) &= \frac{1}{4}E\{[f(A_i)f(B_i) - E(f(A_i)f(B_i))] \\ &[f(A_{i+1})f(B_{i+1}) - E(f(A_{i+1})f(B_{i+1}))]\} \\ &= \frac{1}{4}E\{f(A_i)f(A_{i+1})f(B_i)f(B_{i+1})\} - \frac{1}{4}E\{f(A_{i+1})f(B_{i+1}) \\ &E[f(A_i)f(B_i)]\} - \frac{1}{4}E\{f(A_i)f(B_i)E[f(A_{i+1})f(B_{i+1})]\} \\ &+ \frac{1}{4}E\{E[f(A_i)f(B_i)]E[f(A_{i+1})f(B_{i+1})]\} \end{aligned} \tag{8}$$

Using the independence of A_i and B_i, A_{i+1} and B_{i+1}, $f(A_i)f(A_{i+1})$ and $f(A_{i+1})f(B_{i+1})$, and the property that $E[E(\cdot)] = E(\cdot)$, (8) simplifies to:

$$\begin{aligned} C(Y_i, Y_{i+1}) = &\frac{1}{4}E[f(A_i)f(A_{i+1})]E[f(B_i)f(B_{i+1})] \\ &- \frac{1}{4}E\{f(A_{i+1})f(B_{i+1})E[f(A_i)]E[f(B_i)]\} \\ &- \frac{1}{4}E\{f(A_i)f(B_i)E[f(A_{i+1})]E[f(B_{i+1})]\} \\ &+ \frac{1}{4}E[f(A_i)]E[f(B_i)]E[f(A_{i+1})]E[f(B_{i+1})] \end{aligned} \tag{9}$$

or

$$\begin{aligned} &C(Y_i, Y_{i+1}) \\ &= \frac{1}{4}E[f(A_i)f(A_{i+1})]E[f(B_i)f(B_{i+1})] \\ &\quad - \frac{1}{4}E[f(A_{i+1})]E[f(B_{i+1})]E[f(A_i)]E[f(B_i)] \\ &\quad - \frac{1}{4}E[f(A_i)]E[f(B_i)]E[f(A_{i+1})]E[f(B_{i+1})] \\ &\quad + \frac{1}{4}E[f(A_i)]E[f(B_i)]E[f(A_{i+1})]E[f(B_{i+1})] \\ &= \frac{1}{4}E[f(A_i)f(A_{i+1})]E[f(B_i)f(B_{i+1})] \\ &- \frac{1}{4}E[f(A_i)]E[f(B_i)]E[f(A_{i+1})]E[f(B_{i+1})]. \end{aligned} \tag{10}$$

We also obtain

$$\begin{aligned} 4c_{A,i} = C[f(A_i), f(A_{i+1})] = E[f(A_i)f(A_{i+1})] \\ - E[f(A_i)]E[f(A_{i+1})] \end{aligned} \tag{11}$$

or

$$E[f(A_i)f(A_{i+1})] = 4c_{A,i} + E[f(A_i)]E[f(A_{i+1})]. \qquad (12)$$

Similarly,

$$4c_{B,i} = C[f(B_i), f(B_{i+1})] = E[f(B_i)f(B_{i+1})] - E[f(B_i)]E[f(B_{i+1})]. \qquad (13)$$

or

$$E[f(B_i)f(B_{i+1})] = 4c_{B,i} + E[f(B_i)]E[f(B_{i+1})]. \qquad (14)$$

Because

$$E[f(A_i)] = E(1-2A_i) = 1 - 2E[A_i] = \mu_{A,i} \qquad (15)$$

and

$$E[f(B_i)] = E(1-2B_i) = 1 - 2E[B_i] = \mu_{B,i}, \qquad (16)$$

(12) and (14) take the following forms, respectively

$$E[f(A_i)f(A_{i+1})] = 4c_{A,i} + (1-2\mu_{A,i})(1-2\mu_{A,i+1}), \qquad (17)$$

$$E[f(B_i)f(B_{i+1})] = 4c_{B,i} + (1-2\mu_{B,i})(1-2\mu_{B,i+1}). \qquad (18)$$

Substituting (15), (16), (17), and (18) into (10), we obtain

$$c_{Y,i} = C(Y_i, Y_{i+1}) = \frac{1}{4}\{[4c_{A,i} + (1-2\mu_{A,i})(1-2\mu_{A,i+1})] \cdot [4c_{B,i} + (1-2\mu_{B,i})(1-2\mu_{B,i+1})] - (1-2\mu_{A,i})(1-2\mu_{A,i+1}) \cdot (1-2\mu_{B,i})(1-2\mu_{B,i+1})\}. \qquad (19)$$

Let us further assume stationarity of $A = \{A_i\}$ and $B = \{B_i\}$, i.e. that covariances $c_{A,i} = C(A_i, A_{i+1})$, $c_{B,i} = C(B_i, B_{i+1})$ and expected values $\mu_{A,i}$, $\mu_{B,i}$ assume values c_A, c_B, μ_A and μ_B, respectively. Consequently, (19) takes the following form:

$$c_Y = \frac{1}{4}\{[4c_A + (1-2\mu_A)^2][4c_B + (1-2\mu_B)^2] - (1-2\mu_A)^2(1-2\mu_B)^2\}. \qquad (20)$$

or

$$c_Y = 4c_Ac_B + c_A(1-2\mu_B)^2 + c_B(1-2\mu_A)^2. \qquad (21)$$

The expected value of variable Y_i can be computed directly from the formula proposed by R. B. Davies in [1]

$$\mu_{Y,i} = E[Y_i] = E[A_i \oplus B_i] = \mu_{A,i} + \mu_{B,i} - 2\mu_{A,i}\mu_{B,i} \qquad (22)$$

For stationary $A = \{A_i\}$ and $B = \{B_i\}$ it is that

$$\mu_Y = \mu_A + \mu_B - 2\mu_A\mu_B, \qquad (23)$$

Formula (23) can also be written as

$$\mu_Y = \frac{1}{2} - 2\Delta_A\Delta_B, \qquad (24)$$

where $\Delta_A = \mu_A - 0.5$ and $\Delta_B = \mu_B - 0.5$ are biases corresponding to processes A and B, respectively. From (19) to (24), it follows that the bias and covariance between adjacent elements of process $Y = \{Y_i\}$, depend on both the parameters of independent and dependent processes. Moreover, in [1], it has been shown that even a small correlation between combined XOR random variables can significantly increase the bias of the output. Thus, in our case, this correlation could cause the value of μ_B to deviate significantly from 0.5.

Let us notice, that dependent stochastic processes do not influence μ_Y and c_Y if and only if $\mu_A = 0.5$ and $c_A = 0$. In such a case, $\mu_Y = 0.5$ and $c_Y = 0$, regardless of the quality of dependent processes. This distinctive property of XOR operation finds common application in stream ciphers, where $\{B_i\}$ models the data bit stream and $\{A_i\}$ is the sequence of independent and identically distributed (*i.i.d*) random variables with uniform distribution modeling a random bit sequence. Consequently, regardless of the statistical properties of $\{B_i\}$, sequence $\{Y_i\}$ is the sequence of *i.i.d.* random variables with uniform distribution [3], [4]. Achieving this state in a real systems, e.g. in random bit generators exploiting entropy sources like noise, metastable states, jitter in ring oscillators (RO) etc., is challenging and requires additional processing (see e.g. [5]).

In the subsequent part of the article, we investigate whether and under what conditions we will obtain $\mu_Y \to 0.5$ and $c_Y \to 0$, regardless of the quality of summed modulo 2 dependent stochastic processes when R is finite.

Since the quantity of dependent processes and the specifics of their interdependence remain unknown and furthermore, when XOR is applied, even a minor correlation between dependent random variables can significantly increase the bias of the resultant output random variable, we encounter a challenge in estimating the values of parameters μ_B and c_B. Consequently, we must resort to assuming the worst values for μ_B and c_B while endeavouring to assess the values and characteristics of changes in μ_A and c_A values based on the number of independent processes. It is important to take into account that biases of the summed XOR binary independent processes may be notable and the covariance of the adjacent elements in each of the combined XOR processes might also be significant.

III. REDUCTION OF BIAS AND COVARIANCE OF ADJACENT ELEMENTS OF $Y = \{Y_I\}$ WITH OPTIMAL DESIGN

To simplify calculations let us assume that independent processes have indexes $1, 2, 3, \ldots, N$. Then $\mu_{X,i}(1) = E[X_i(1)]$, $\mu_{X,i}(2) = E[X_i(2)]$, ..., $\mu_{X,i}(N) = E[X_i(N)]$ are expected values of random variables $X_i(1)$, $X_i(2)$,..., $X_i(N)$, respectively. Similarly, $c_{X,i}(1) = C[X_i(1), X_{i+1}(1)]$, $c_{X,i}(2) = C[X_i(2), X_{i+1}(2)]$, ..., $c_{X,i}(N) = C[X_i(N), X_{i+1}(N)]$ are covariances between adjacent bits in sequences $\{X_i(1)\}, \{X_i(2)\}, \ldots, \{X_i(N)\}$, $i = 0, 1, \ldots$. The subsequent steps of combining XOR N random variables can be modeled with N random variables $Z_i(n)$, $n = 1, 2, \ldots, N$, $i = 0, 1, \ldots,$

i.e.,

$$\begin{aligned}
&Z_i(1) = X_i(1),\\
&Z_i(2) = X_i(1) \oplus X_i(2),\\
&Z_i\,(3) = X_i\,(1) \oplus X_i\,(2) \oplus X_i\,(3) = Z_i\,(2) \oplus X_i\,(3)\,,\\
&\quad\vdots\\
&Z_i\,(N) = X_i\,(1) \oplus X_i\,(2) \oplus \ldots \oplus X_i\,(N) = Z_i\,(N-1) \oplus\\
&X_i\,(N) = A_i. \qquad (25)
\end{aligned}$$

We search for expected values of subsequent $Z_i(n)$, $n = 1,2,\ldots, N$, $i = 0, 1, \ldots$, i.e., $\mu_{Z,i}(1) = E\,[Z_i(1)]$, $\mu_{Z,i}(2) = E\,[Z_i(2)],\ldots$, $\mu_{Z,i}(N) = E\,[Z_i(N)]$ and covariances $c_{Z,i}(1) = C\,[Z_i\,(1)\,, Z_{i+1}\,(1)]$, $c_{Z,i}(2) = C\,[Z_i\,(2)\,, Z_{i+1}\,(2)], \ldots, c_{Z,i}\,(N) = C\,[Z_i\,(N)\,, Z_{i+1}\,(N)]$.

Exploiting the reasoning described in the preceding section, we derive that

$$\begin{aligned}
\mu_{z,i}\,(n+1) &= E\,[Z_i\,(n+1)] = E\,[Z_i\,(n) \oplus X_i\,(n+1)]\\
&= \mu_{Z,i}(n) + \mu_{X,i}(n+1) - 2\mu_{Z,i}(n)\mu_{X,i}(n+1) \qquad (26)
\end{aligned}$$

and

$$\begin{aligned}
c_{Z,i}\,(n+1) &= C\,(Z_i\,(n+1)\,, Z_{i+1}\,(n+1)) = \frac{1}{4}\{[4c_{Z,i}(n)\\
&+(1-2\mu_{Z,i}(n))(1-2\mu_{Z,i+1}(n))][4c_{X,i}(n+1)\\
&+(1-2\mu_{X,i}(n+1))(1-2\mu_{X,i+1}(n+1))]\\
&-(1-2\mu_{Z,i}(n))(1-2\mu_{Z,i+1}(n))\cdot\\
&(1-2\mu_{X,i}(n+1))(1-2\mu_{X,i+1}(n+1))\}, \qquad (27)
\end{aligned}$$

where $n = 1,2,\ldots, N-1$.

Assuming stationarity of the combined processes, i.e., that values of $\mu_{X,i}(1) = E\,[X_i(1)]$, $\mu_{X,i}(2) = E\,[X_i(2)],\ldots$, $\mu_{X,i}(N) = E\,[X_i(N)]$ and the values of $c_{X,i}(1) = C\,[X_i\,(1)\,, X_{i+1}\,(1)]$, $c_{X,i}(2) = C\,[X_i\,(2)\,, X_{i+1}\,(2)]$, $\ldots$, $c_{X,i}(N) = C\,[X_i\,(N)\,, X_{i+1}\,(N)]$ do not depend on $i = 0,1\ldots$, we have N expected values $\mu_X(1)$, $\mu_X\,(2)\,, \ldots, \mu_X(N)$ and N covariances $c_X(1)$, $c_X(2),\ldots$, $c_X(N)$. Formula (26) then reduces to

$$\mu_Z(n+1) = \mu_Z(n) + \mu_X(n+1) - 2\mu_Z(n)\mu_X(n+1) \qquad (28)$$

or

$$\mu_Z(n+1) = \frac{1}{2} - 2\left(\mu_Z(n) - \frac{1}{2}\right)\left(\mu_X(n+1) - \frac{1}{2}\right), \qquad (29)$$

where $\mu_Z\,(1) = \mu_X\,(1)$. For $n = N-1$ it is also that $\mu_Z\,(N) = \mu_A$.

Formula (27) takes the following form:

$$\begin{aligned}
c_Z\,(n+1) &= \frac{1}{4}\{[4c_Z(n) + (1-2\mu_Z(n))^2][4c_X(n+1)\\
&+(1-2\mu_X(n+1))^2]\\
&-(1-2\mu_Z(n))^2(1-2\mu_X(n+1))^2\}, \qquad (30)
\end{aligned}$$

where $c_Z\,(1) = c_X(1)$ and $c_A = c_Z\,(N)$.

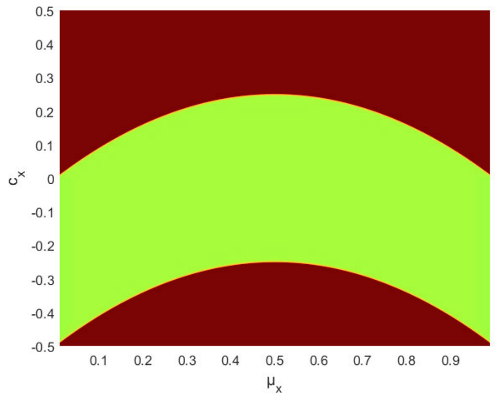


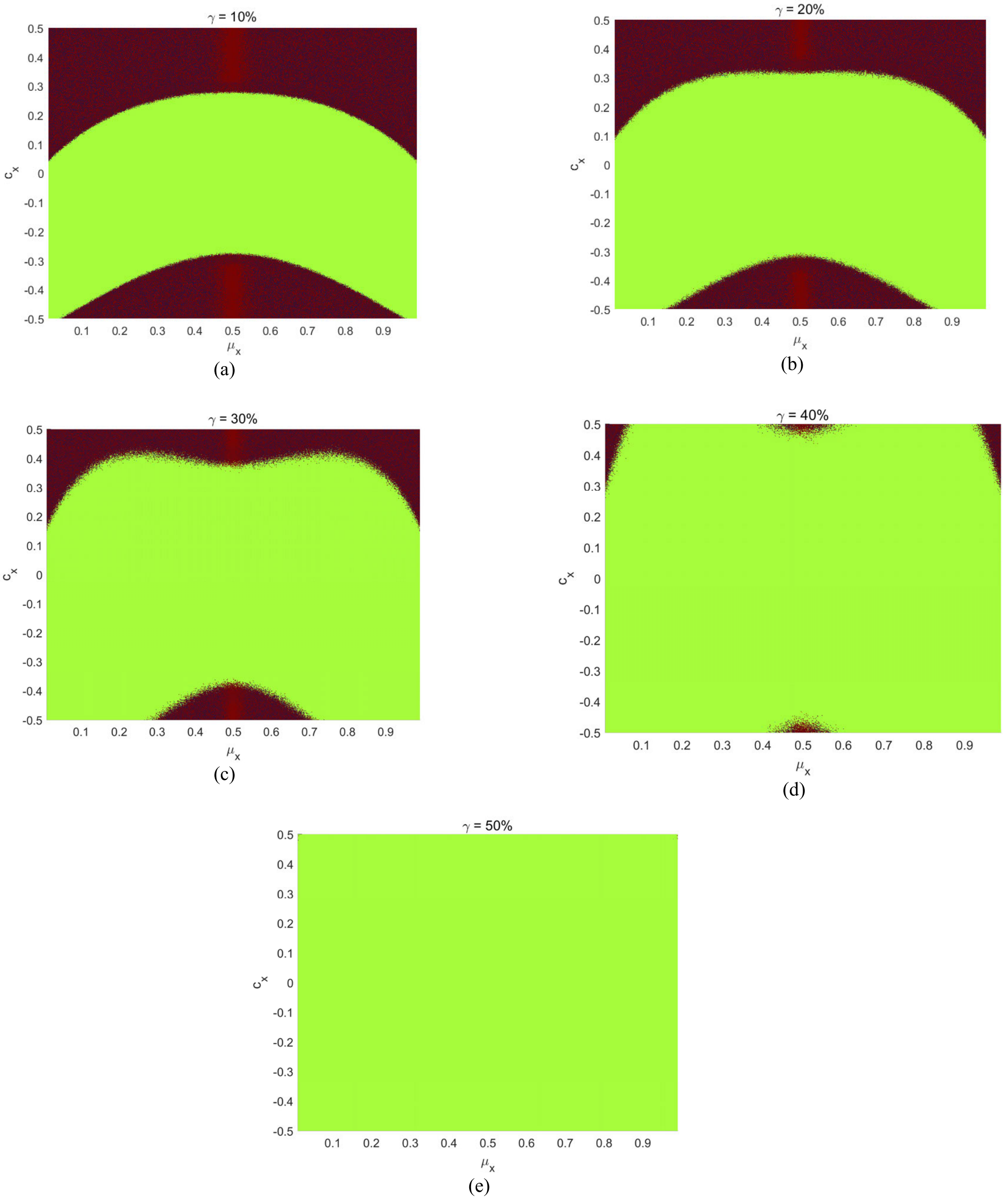
FIGURE 1. Areas of values for c_X and μ_X, where $c_Z\,(N)$ tends to zero with the increase of N (green), and areas where the absolute covariance value increases (red).

The formulas (28)-(30) enable the calculation of expected values and covariances between adjacent random variables of the processes $Z(n) = \{Z_i(n)\}$ with the increase of the number n of combined XOR independent binary stochastic processes, where $Z(N) = A$.

The form of (29) significantly influences the subsequent analysis. Excluding extreme cases $\mu_X\,(n) = 0$ or $\mu_X\,(n) = 1$, for $n = 1, 2, \ldots, N-1$, the value of $\mu_Z(n)$ consistently approaches 0.5 as n increases. This holds true regardless of the bias values of independent processes as it was demonstrated in previous studies such as [1], [6], and [7] for independent random variables.

The computation of covariance values between adjacent random variables at the output obtained as the result of summing modulo 2 only independent binary stochastic processes is more challenging. For not all covariance values $c_X(1)$, $c_X(2),\ldots$, $c_X\,(N)$ and for not all expected values $\mu_X(1)$, $\mu_X\,(2)\,, \ldots, \mu_X(N)$, the covariance $c_A = c_Z\,(N)$ tends to zero as N increases. Figure 1 illustrates areas of values for c_X and μ_X, where $c_Z\,(N)$ tends to zero with increasing N (green color) and areas where the absolute value of covariance between adjacent binary random variables increases (red color). For greater clarity it was assumed that $c_X\,(1) = c_X\,(2) =,\ldots, = c_X\,(N) = c_X$ and $\mu_X\,(1) = \mu_X\,(2) = \,,\ldots, = \mu_X\,(N) = \mu_X$. To better represent the nature of the obtained mathematical relationships, the range of c_X values was expanded twice compared to the real range of changes in c_X in binary stochastic processes. If the computed covariance exceeded 0.5 on the plot, it was assigned the value of 0.5. If it was less than -0.5, it was assigned the value of -0.5.

Drawing observations from Fig. 1, we can note the following: 1) if all $c_X(1)$, $c_X(2),\ldots$, $c_X\,(N)$ are positive, there exist pairs of initial covariances and expected values for which increasing the number of independent processes combined using the XOR operation will not reduce the covariance values between adjacent binary random variables in the output stochastic process; 2) if all $c_X(1)$, $c_X(2),\ldots$, $c_X\,(N)$ are negative but greater than -0.25, $c_Z\,(N)$ always tends towards zero with an increasing N; 3) if one or more of the combined



(a)

(b)

(c)

(d)

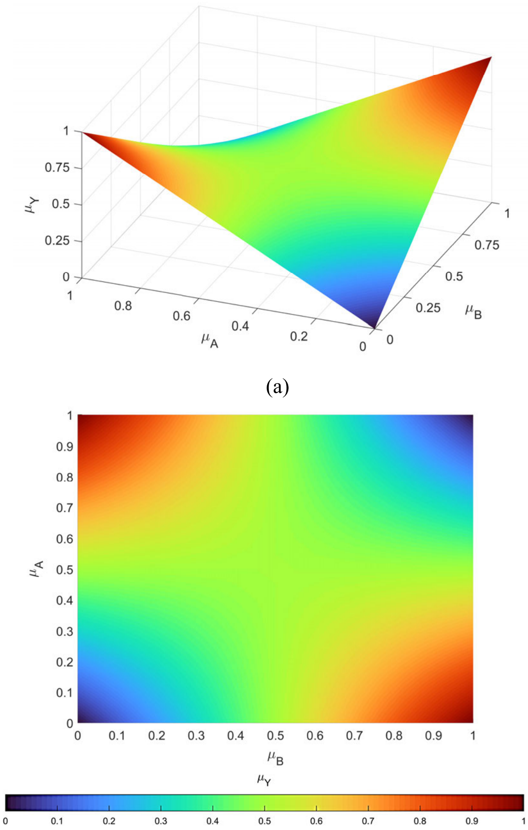
(e)

FIGURE 2. The regions of the c_X and μ_X values for which $c_Z(N)$ approaches zero with the increase of N (green), as well as the regions where the absolute covariance value grows (red) for different values of γ.

XOR independent processes have zero covariance between adjacent elements, then the adjacent elements of the output stochastic process also have zero covariance, and the process itself is unbiased, regardless of the covariance values between adjacent elements of the remaining processes and the values of $\mu_X(1)$, $\mu_X(2), \ldots, \mu_X(N)$, The latter property is known but was obtained with the use of a new methodology.

In real-world scenarios, particularly for larger N, independent stationary stochastic processes may exhibit simultaneously positive and negative covariance values between adjacent random variables. Let's explore how this impacts the value of $c_A = c_Z(N)$. To achieve this, processes with positive covariances between adjacent elements were combined XOR with processes with negative covariances between adjacent elements. For simplicity, the same covariance value was assigned to processes with positive covariances, and random negative covariance values were selected from the open interval (–0.25, 0). The expected values of all component stationary stochastic processes were kept identical. The outcomes are depicted in Fig. 2. The contribution of γ processes with initially negative covariances was incrementally increased by 10%, starting from a value of 10%. The total number of processes was set to $N = 700$.

Analysing graphs from 2a to 2e, we can observe that as the proportion of processes with negative covariance increases, the range of values for c_X and μ_X,where $c_Z(N)$ tends to



(a)

(b)

FIGURE 3. The dependency of the expected value μ_Y of the output process Y=$\{Y_i\}$ as a function of expected values μ_A and μ_B (a) and the projection of the surface from figure (a) onto the plane (μ_B,μ_A).

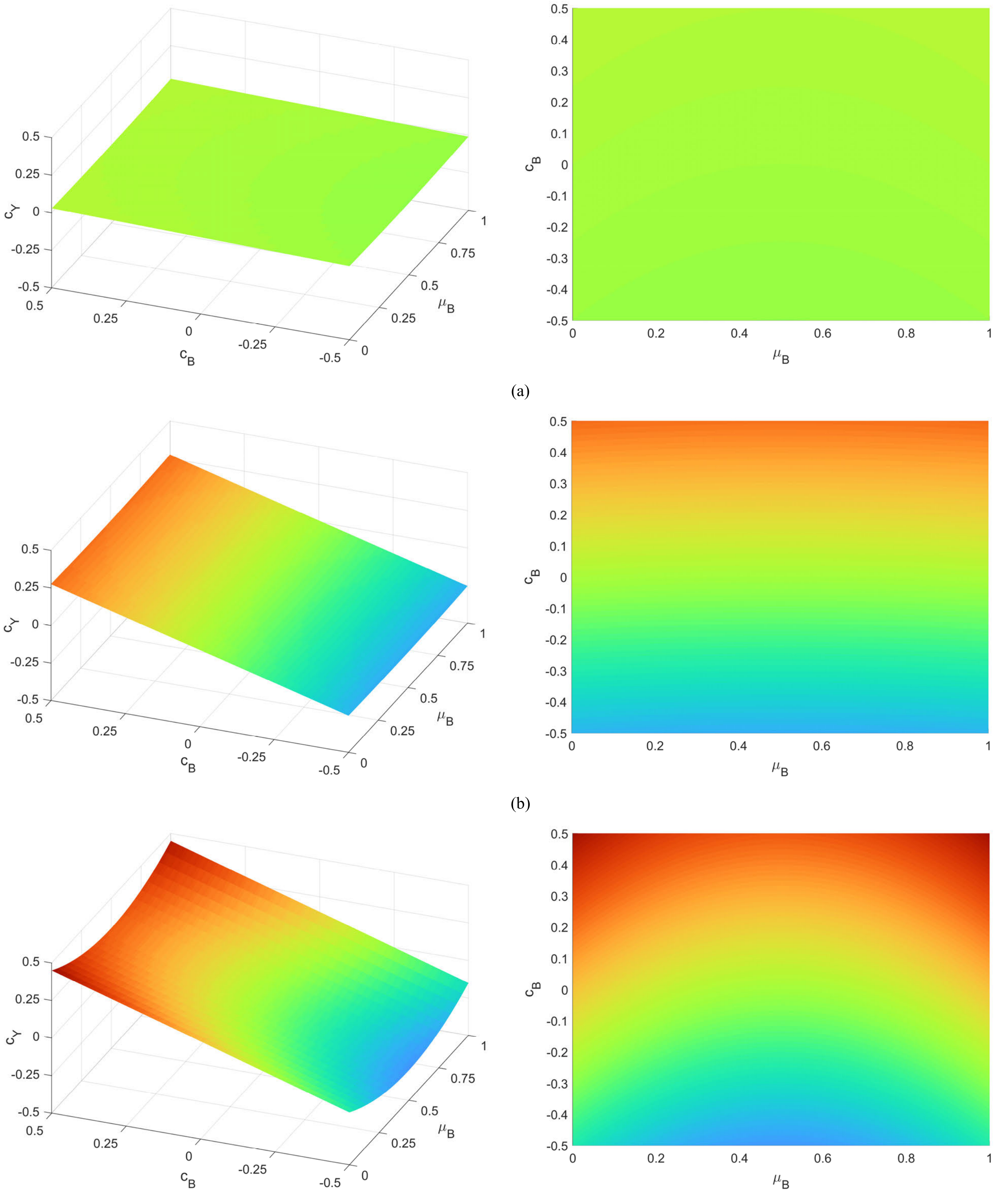
zero, undergoes rapid expansion. For 40% or more participation of processes with negative covariance, it encompasses all c_X values within the interval (-0.25, 0.25) and all μ_X values within the interval (0, 1). Since even for relatively small N, real binary and independent stochastic processes have positive and negative covariance values between adjacent pairs, combining them using XOR operations will result in covariance reduction in most cases. Thus, witnessing an increase in covariance values after applying XOR operations in real-world conditions is theoretically possible but difficult to observe.

Figs. 1 and 2 show a scenario in which only independent binary stochastic processes are combined using XOR. Suppose we combine the process $Z(N) = A$ with the process resulting from combining XOR dependent binary stochastic processes, denoted as B in this paper. In that case, the final result depends on the properties of A and B simultaneously. The closer the covariance of process A is to zero and the expected value is to 0.5, the less influence process B has on the mean value and the covariance between adjacent elements of Y. In Fig. 3, the impact of the expected values μ_A and μ_B on the expected value μ_Y of the output process Y is illustrated. If μ_A or μ_B equals 0.5, the output will always be an unbiased, i.e., with μ_Y= 0.5. If μ_B takes extreme values of 0 or 1, then $\mu_Y = \mu_A$ for μ_B= 0, and $\mu_Y = 1 - \mu_A$ for $\mu_B = 1$. If process A is biased (μ_A deviates from 0.5), the bias of process B not only does not increase the bias of Y compared to A but may even reduce it, except for extreme cases of μ_B= 0 or $\mu_B = 1$. For example, with μ_A= 0.6 and μ_B= 0.15, according to formula (23), we get μ_Y =0.57 or Δ_Y= 0.07, resulting in bias less than the bias Δ_A= 0.1 of process A obtained by combining XOR independent stochastic processes. In summary, if independent processes produce a biased A, dependent processes will reduce the bias of process Y, making it less biased than A. The degree of this reduction depends on both μ_A and μ_B values.

The influence of the covariance and the expected value of B on the covariance between adjacent elements of Y is more complex, as illustrated in Figs. 4 and 5. The left-hand plots depict the shape of the surface on which the values of covariance c_Y align with changes in the covariance and expected value of process B for selected pairs of covariance and expected value of process A. The values of these pairs are obtained by combining XOR independent processes. The color of the surface corresponds to the numerical values of c_Y. The right-hand plots are projections of the obtained surfaces onto the plane (μ_B,c_B). The graphs in Fig. 4 are obtained for positive values of c_A, while the graphs in Fig. 5 are for negative c_A. In both cases, the absolute values of covariance were identical.

Analyzing the graphs from Figs. 4 and 5, the following conclusions can be formulated:

1) If XORing independent processes yields process A with low covariance c_A, whether positive or negative, and with a small bias μ_A, the dependent processes do not significantly impact the covariance value c_Y (graphs 4a and 5a).
2) If the covariance c_A of A is close to zero but the bias μ_A is significant, dependent processes can significantly alter the covariance value c_Y. The final outcome is significantly influenced by the covariance value c_B of B, while the impact of the expected value μ_B on c_Y is small (see graphs 4b and 5b).
3) If the covariance c_A of A significantly deviates from zero, and the bias μ_A of this process is small, dependent generators can significantly alter the covariance value c_Y. The final result is significantly influenced by both the covariance value c_B and the expected value μ_B (graphs 4c and 5c).
4) If the covariance c_A of A significantly deviates from zero, and the bias μ_A is large, dependent generators can significantly alter the covariance value c_Y. The final result is significantly influenced by both the covariance value c_B and its expected value μ_B. Regarding point 3, the range of μ_B and c_B values that can yield c_Y close to zero is very small (graphs 4d and 5d).
5) Negative values of covariance c_A expand the range of μ_B and c_B values for which c_Y can be close to zero, in comparison to positive values of c_A.



(a)

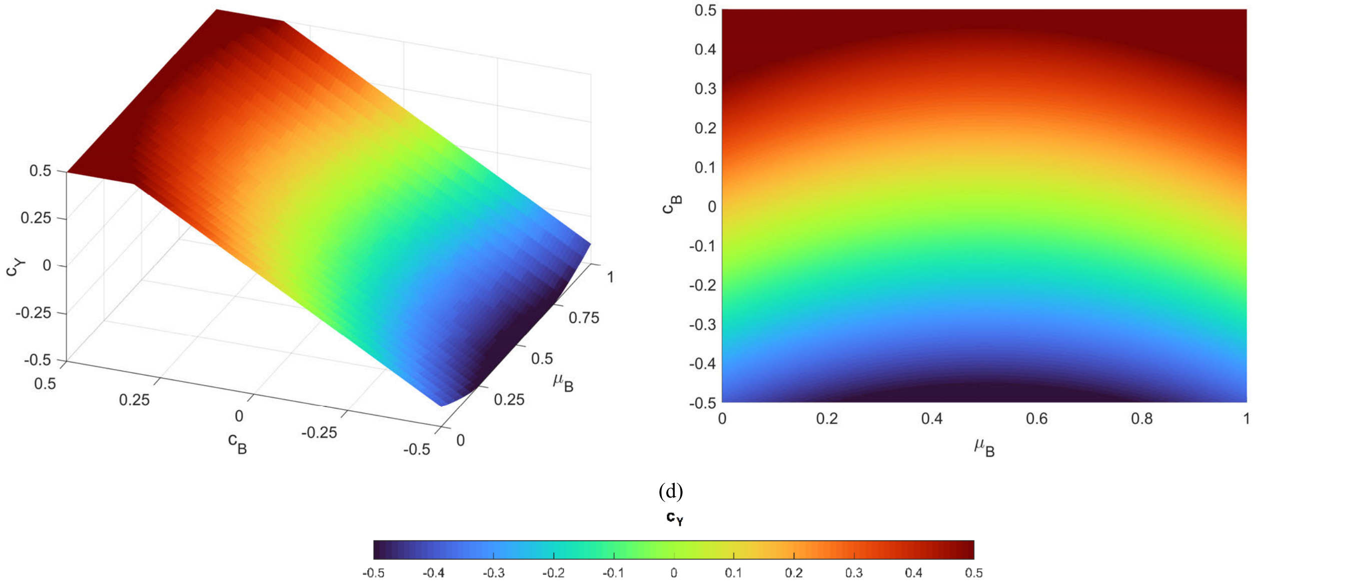
(b)

(c)

FIGURE 4. **The covariance c_Y of Y as a function of the expected value μ_B and the covariance c_B of the B - positive values of c_A; (a) $c_A = 0.01$, $\mu_A = 0.51$; (b) $c_A = 0.01$, $\mu_A = 0.85$; (c) $c_A = 0.15$, $\mu_A = 0.01$; (d) $c_A = 0.15$, $\mu_A = 0.85$.**

IV. MINIMAL NUMBER OF INDEPENDENT GENERATORS THAT PROVIDE ACCEPTABLE BIAS AND COVARIANCE

Considering the user's standpoint, a key information is the minimum number of processes that must be independent to obtain $Y = \{Y_i\}$, with acceptable bias and covariance between variables Y_i and Y_{i+1}, regardless of the bias and covariance values of process B. Notice that the value of μ_B can significantly deviate from 0.5 because even a small correlation



(d)

FIGURE 4. ***(Continued.)*** **The covariance c_Y of Y as a function of the expected value μ_B and the covariance c_B of the B - positive values of c_A; (a) $c_A = 0.01$, $\mu_A = 0.51$; (b) $c_A = 0.01$, $\mu_A = 0.85$; (c) $c_A = 0.15$, $\mu_A = 0.01$; (d) $c_A = 0.15$, $\mu_A = 0.85$.**

between stochastic processes combined with XOR operation can introduce substantial bias to the output [1]. From the previous section, we know that the bias of B not only does not increase the bias of Y but can even decrease it, compared to the bias of A. The boundary case when B cannot reduce the bias of Y occurs for $\mu_B = 0$ or $\mu_B = 1$. In this scenario, (23) takes the form:

$$\mu_Y = \frac{1}{2} \pm \left(\mu_A - \frac{1}{2}\right) = \frac{1}{2} \pm \Delta_A, \tag{31}$$

where the plus sign is obtained for $\mu_B = 0$, and the minus sign for $\mu_B = 1$.

Calculating the number of independent processes that will ensure acceptably low covariance between variables Y_i and Y_{i+1}, is significantly more challenging, as c_Y depends on four parameters. To simplify the analysis, we assume that the covariance between adjacent variables is very high for the dependent processes. As negative values of c_B yield a more favorable situation than positive ones, the worst-case scenario for binary stochastic processes occurs when $c_B = 0.25$. In this case, (21) takes the form:

$$c_Y = c_A + c_A(1 - 2\mu_B)^2 + 0.25(1 - 2\mu_A)^2 \tag{32}$$

or

$$c_Y = c_A + \Delta_A^2 + 4c_A\Delta_B^2, \tag{33}$$

where $\Delta_A = \mu_A - 0.5$ and $\Delta_B = \mu_B - 0.5$. Note that the covariance value c_Y does not depend on the sign of the biases Δ_A, Δ_B.

Formulas (29)-(33) can be utilized to determine the minimum number of independent processes that will ensure an acceptable bias and covariance values between adjacent elements of process Y, regardless of the number of dependent processes. Assuming the worst-case scenario, i.e., that dependent processes operate with the most unfavorable covariance and bias values, i.e., $c_B = 0.25$, $\mu_B = 0$ ($\Delta_B = -0.5$) or $\mu_B = 1$ ($\Delta_B = 0.5$), we obtain

$$c_Y = 2c_A + 0.25(1 - 2\mu_A)^2, \tag{34}$$

and

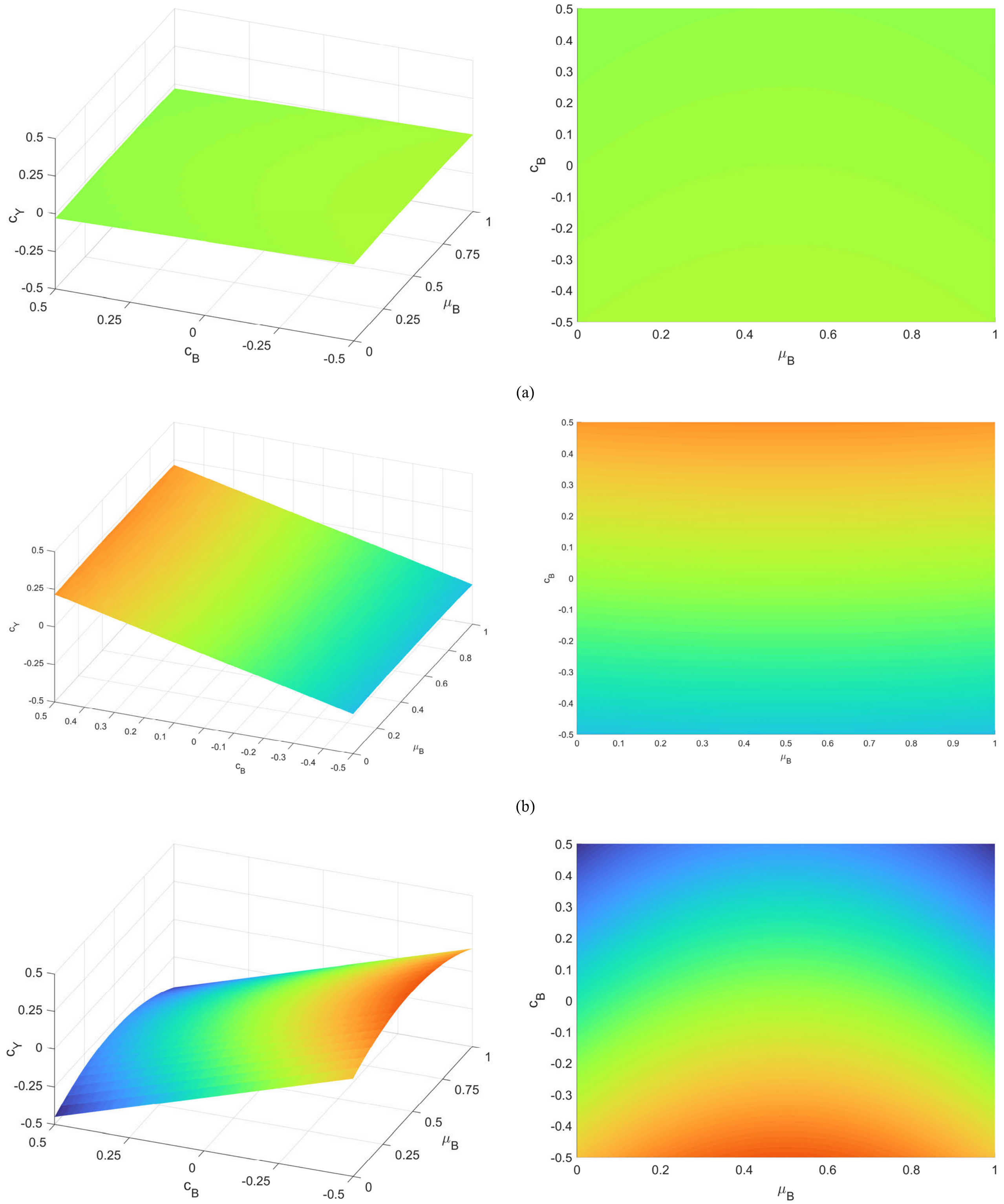
$$c_Y = 2c_A + \Delta_A^2. \tag{35}$$

The utilization of (29)-(35) illustrates the following example.

Example

Let's assume that the acceptable bias of Y is ±0.001, meaning that μ_Y is expected to belong to the symmetrical and closed interval $[0.499, 0.501]$. Let's also assume that the acceptable covariance between adjacent elements of Y is ±0.001, meaning that c_Y belongs to the symmetrical and closed interval $[-0.001, 0.001]$. Furthermore, let's assume that combined XOR processes have the same bias, i.e., $\mu_X(1) = \mu_X(2) = \ldots = \mu_X(N) = \mu_X$ and $\mu_Z(1) = \mu_X(1)$, equal to the least favorable observed value in a real system. Similarly, let's proceed with covariance values, i.e., $c_X(1) = c_X(2) = \ldots =, c_X(N) = c_X$ and $c_Z(1) = c_X(1)$, where c_X is the least favorable observed value in a real system.

Consider four pairs of μ_X and c_X values: $(0.55, 0.1)$, $(0.55, 0.15)$, $(0.85, 0.1)$, and $(0.85, 0.15)$. Tables from I to III show the values of μ_A, μ_Y, c_A and c_Y with precision to five decimal places for the first three pairs. The fourth pair consists of numbers for which μ_A tends to 0.5 but c_A does not converge to zero. The numerical results are presented for N ranging from 1 to 15. All calculations were performed using



(a)

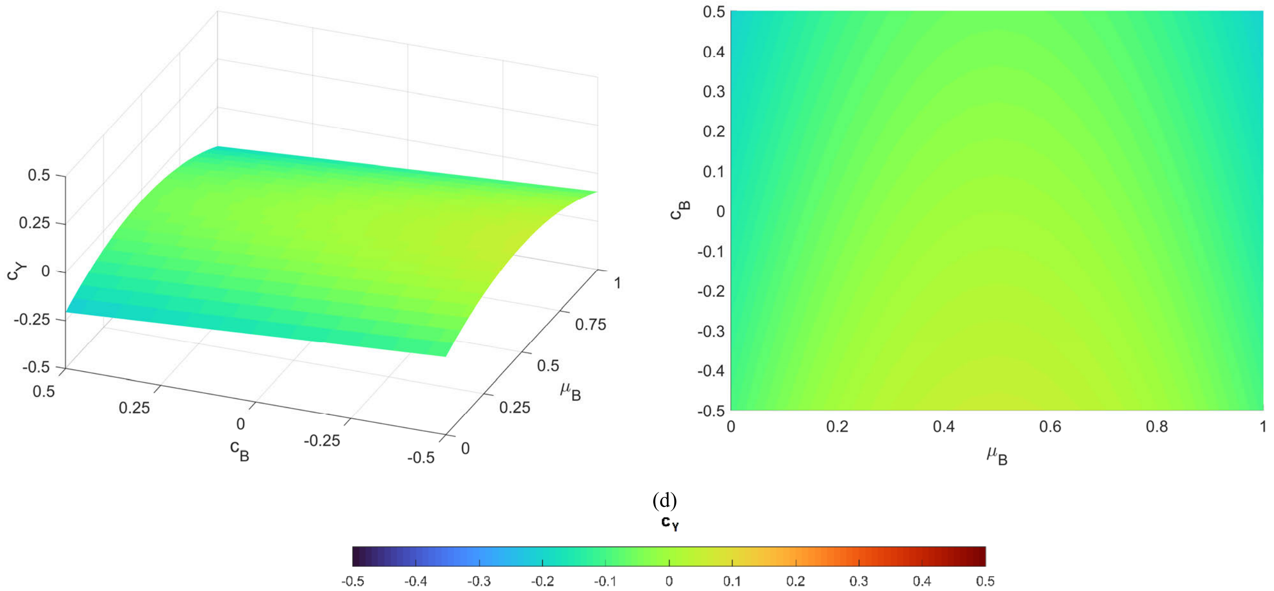
(b)

(c)

FIGURE 5. The covariance c_Y of the Y as a function of the expected value μ_B and the covariance c_B of the B - negative values of c_A; (a) $c_A = -0.01$, $\mu_A = 0.51$; (b) $c_A = -0.01$, $\mu_A = 0.85$; (c) $c_A = -0.15$, $\mu_A = 0.01$; (d) $c_A = -0.15$, $\mu_A = 0.85$.

32-bit arithmetic, rounding the results presented in the tables to five decimal places.

In the case of the pair $\mu_X = 0.55$, $c_X = 0.1$, achieving a bias within the ±0.001 range is possible with 4 or



(d)

FIGURE 5. ***(Continued.)*** **The covariance c_Y of the Y as a function of the expected value μ_B and the covariance c_B of the B - negative values of c_A; (a) $c_A = -0.01$, $\mu_A = 0.51$; (b) $c_A = -0.01$, $\mu_A = 0.85$; (c) $c_A = -0.15$, $\mu_A = 0.01$; (d) $c_A = -0.15$, $\mu_A = 0.85$.**

TABLE 1. **Subsequent values of μ_A, μ_Y, c_A and c_Y for $\mu_X = 0.55$, $c_X = 0.1$.**

N	μ_A	μ_Y		c_A	c_Y
		$\mu_B = 0$	$\mu_B = 1$		
1	0.55000	0.55000	0.45000	0.10000	0.20250
2	0.49500	0.49500	0.50500	0.04200	0.08403
3	0.50050	0.50050	0.49950	0.01723	0.03446
4	0.49995	0.49995	0.50005	0.00706	0.01413
5	0.50001	0.50001	0.49999	0.00290	0.00579
6	0.50000	0.50000	0.50000	0.00119	0.00238
7	0.50000	0.50000	0.50000	0.00049	0.00097
8	0.50000	0.50000	0.50000	0.00020	0.00040
9	0.50000	0.50000	0.50000	0.00008	0.00016
10	0.50000	0.50000	0.50000	0.00003	0.00007
11	0.50000	0.50000	0.50000	0.00001	0.00003
12	0.50000	0.50000	0.50000	0.00001	0.00001
13	0.50000	0.50000	0.50000	0.00000	0.00000
14	0.50000	0.50000	0.50000	0.00000	0.00000
15	0.50000	0.50000	0.50000	0.00000	0.00000

TABLE 2. **Subsequent values of μ_A, μ_Y, c_A and c_Y for $\mu_X = 0.55$. $c_X = 0.15$.**

N	μ_A	μ_Y		c_A	c_Y
		$\mu_B = 0$	$\mu_B = 1$		
1	0.55000	0.55000	0.45000	0.15000	0.30250
2	0.49500	0.49500	0.50500	0.09300	0.18603
3	0.50050	0.50050	0.49950	0.05675	0.11350
4	0.49995	0.49995	0.50005	0.03462	0.06924
5	0.50001	0.50001	0.49999	0.02112	0.04224
6	0.50000	0.50000	0.50000	0.01288	0.02577
7	0.50000	0.50000	0.50000	0.00786	0.01572
8	0.50000	0.50000	0.50000	0.00480	0.00959
9	0.50000	0.50000	0.50000	0.00293	0.00585
10	0.50000	0.50000	0.50000	0.00178	0.00357
11	0.50000	0.50000	0.50000	0.00109	0.00218
12	0.50000	0.50000	0.50000	0.00066	0.00133
13	0.50000	0.50000	0.50000	0.00041	0.00081
14	0.50000	0.50000	0.50000	0.00025	0.00049
15	0.50000	0.50000	0.50000	0.00015	0.00030

more binary stationary stochastic processes operating independently. To attain and maintain a covariance value within the ±0.001 range, we must combine XOR at least 7 binary stationary stochastic processes, regardless of the number and parameters of dependent binary stationary stochastic processes. It is noteworthy that the absolute value of the bias Δ_Y and the covariances c_A and c_Y monotonically approach the limiting value of 0 as N increases.

When $\mu_X = 0.55$, $c_X = 0.15$, the situation is similar, but to achieve a covariance within the range of ±0.001, we need at least 13 binary stationary stochastic processes operating independently.

A slightly different situation arises for the pair $\mu_X = 0.85$, $c_X = 0.1$. Although in this case μ_Y tends toward 0.5 and c_Y toward 0, the monotonic trend is not observed for the covariance c_A. To achieve a bias within the range of ± 0.001, combining XOR at least 18 independent binary stationary stochastic processes is necessary. Obtaining a covariance within the range of ±0.001 requires the independent operation of at least 51 binary stationary stochastic processes.

Upon reviewing the current findings, it is evident that combining binary stationary stochastic processes through XOR operations can significantly reduce the bias and covariance between adjacent elements of the process

TABLE 3. Subsequent values of μ_A, μ_Y, c_A and c_Y for $\mu_X = 0.85$. $c_X = 0.1$.

N	μ_A	μ_Y		c_A	c_Y
		$\mu_B = 0$	$\mu_B = 1$		
1	0.85000	0.85000	0.15000	0.10000	0.32250
2	0.25500	0.25500	0.74500	0.13800	0.33603
3	0.67150	0.67150	0.32850	0.14683	0.32304
4	0.37995	0.37995	0.62005	0.14151	0.29706
5	0.58403	0.58403	0.41597	0.13063	0.26817
6	0.44118	0.44118	0.55882	0.11894	0.24065
7	0.54118	0.54118	0.45882	0.10777	0.21681
8	0.47117	0.47117	0.52883	0.09756	0.19639
9	0.52018	0.52018	0.47982	0.08836	0.17865
10	0.48587	0.48587	0.51413	0.08006	0.16310
11	0.50988	0.50988	0.49012	0.07255	0.14934
12	0.49308	0.49308	0.50692	0.06574	0.13706
13	0.50484	0.50484	0.49516	0.05955	0.12601
14	0.49661	0.49661	0.50339	0.05391	0.11598
15	0.50237	0.50237	0.49763	0.04877	0.10682

$Y = \{Y_i\}$, $i = 0, 1, \ldots$. This holds true regardless of the parameters of dependent binary stochastic processes and regardless of their number. To achieve this, we need $N \geq N_{min}$ independent stationary stochastic processes, where N_{min} can be calculated using formulas proposed in this paper. The value of N_{min} depends significantly on the bias and covariance between adjacent elements of dependent processes. However, it's not guaranteed (see Fig. 1) that for all possible bias and covariance values between adjacent elements of independent binary stationary stochastic processes combined with XOR operation, we will obtain zero covariance c_A and c_Y for $N \to \infty$.

V. CONCLUSION

In this paper, it has been shown that summing modulo 2 without carry of a finite number of stationary binary stochastic processes can be an efficient method for reducing bias and covariance between adjacent elements of binary stochastic processes. The existing mathematical formulas for bias or covariance reduction with the XOR operation assume the independence of random variables and can be found only in a few papers. This article presents a theoretical analysis of XORing binary stochastic processes where none of the independent processes is unbiased with zero covariance between adjacent elements, and scenarios where an unknown number of binary stochastic processes do not meet the independence condition. This situation is typical of many applications, e.g., in cryptography, when sources of true random bits implemented on the same board or circuit are often dependent or susceptible to attacks. The derived formulas and diagrams presented in this paper can also be used to reduce the correlation between adjacent bits in sequences used in many non-cryptographic applications. The next step of the research could be to check whether the reduction of the bias and covariance values described in the paper, resulting from XOR combining binary sequences, some of which do not satisfy the independence criterion, implies an equally effective improvement of the statistical properties of the output sequences in real systems. Well-known statistical test suites, such as NIST SP 800-22, Test U01, or Dieharder, could be used for this assessment.

REFERENCES

[1] R. B. Davies. (Feb. 28, 2002). *Exclusive OR (XOR) and Hardware Random Number Generators*. Accessed: Jul. 17, 2025. [Online]. Available: https://www.robertnz.net/pdf/xor2.pdf

[2] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed., Hoboken, NJ, USA: Wiley, 2006.

[3] A. J. Menezes, P. C. V. Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 1997.

[4] B. Schneier, *Applied Cryptography, Protocols, Algorithms and Source Code in C*. New York, NY, USA: Wiley, 1996.

[5] J. D. J. Golic, "New methods for digital generation and postprocessing of random data," *IEEE Trans. Comput.*, vol. 55, no. 10, pp. 1217–1229, Oct. 2006.

[6] M. Jessa, "On the quality of random sequences produced with a combined random bit generator," *IEEE Trans. Comput.*, vol. 64, no. 3, pp. 791–804, Mar. 2015.

[7] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Proc. Adv. Cryptol. (EUROCRYPT)*, in Lecture Notes in Computer Science, vol. 765, 1994, pp. 386–397.

MIECZYSŁAW JESSA was born in Poland, in 1961. He received the M.Sc.Eng. (Hons.) and Ph.D. degrees from Poznań University of Technology, in 1985 and 1992, respectively. Since 2017, he has held the position of a Professor with the Faculty of Computing and Telecommunications, Institute of Multimedia Telecommunications, Poznań University of Technology. He is the author or co-author of over 150 journals and conference papers and 15 patents. His research interests include phase-locked loops, network synchronization, and the mathematical models of randomness and pseudo-randomness.

JAKUB NIKONOWICZ (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in telecommunications from Poznań University of Technology, in 2014 and 2019, respectively. Since 2019, he has held the position of an Assistant Professor with the Faculty of Computing and Telecommunications, Institute of Multimedia Telecommunications, Poznań University of Technology. He has authored or co-authored over a dozen scientific publications in refereed journals and proceedings of international conferences. He was the project manager of grants supporting young scientists and a co-principal investigator in an international research consortium. His current research interests include innovations in statistical signal processing for next-generation communication and security technologies.