Josai Mathematical Monographs
vol. 7 (2014), pp. 75-83

A note on a two-dimensional integer sequence arised from a study of physical random number generation

Koji Nuida

Abstract. In the research area of physical random number generation, a kind of "post-process" function to improve the randomness of the generated bit sequence has been studied. There a two-dimensional integer sequence indexed by the input and the output lengths of the post-process functions is associated to the evaluation of optimal quality of such functions. In this short note, we briefly survey the previous work on the study of this integer sequence, and propose some research topics for future work.

1. Introduction

Randomness is an essential resource for information security. In cryptographic technologies (encryption, digital signature, authentication, etc.) to provide enough level of security, bit sequences that are random enough (ideally, uniformly at random) are usually used as auxiliary inputs to the protocols. Cryptographic pseudorandom number generators (PRNGs) are well-studied tools to generate bit sequences sufficiently random for the cryptographic purposes. For such tools, it should be noted that even such tools cannot create random sequences from nothing; roughly speaking, PRNGs can only stretch a short but highly random input sequence to long and enough random output sequence. Therefore, we need other technologies to provide the random inputs for the PRNGs. A possible candidate is so-called physical random number generators, which aim at extracting random sequences from some physical phenomena of computers as physically implemented devices. However, bit sequences generated by such devices may be not sufficiently random in general. Therefore, we need some methodologies to extract highly random sequences from given, possibly less random bit sequences.

In the present paper, we study the problem under the following simple model: A given bit sequence consists of bits that are independent of each other, and each bit has common bias ε; that is, a bit becomes 1 with probability $1/2+\varepsilon$ and 0 with $1/2-\varepsilon$. In the setting, the classical technique of von Neumann [**2**] can convert such a biased bit sequence to a completely unbiased one (by converting blocks 01 and 10 to bits 0 and 1, respectively, and discarding blocks 00 and 11), but the output length of the technique is not constant (and it may even be empty in the worst case). On the other hand, in the following, we discuss the conversion methodologies with constant input and output lengths, as studied in e.g., [**1, 3, 4**]

1.1. Problem statement

Put $\Sigma = \{0, 1\}$. We consider functions $F\colon \Sigma^n \to \Sigma^m$, where $1 \leq m \leq n$. We regard it as a kind of "post-process" function for the random number generation. Namely, given an n-bit "biased" sequence $x = (x_1, \ldots, x_n)$ as above (i.e., we have $Pr[x_i = 1] = 1/2 + \varepsilon$), we want to decrease the "bias" of the output sequence $F(x) = y = (y_1, \ldots, y_m)$, which is defined as follows. For $y \in \Sigma^m$, let $P_{F,y}(\varepsilon) = Pr[F(x) = y]$ denote the occurrence probability of output y with random input $x \in \Sigma^n$ as above. Let $\overline{P}_{F,y}(\varepsilon) = P_{F,y}(\varepsilon) - 1/2^m$ denote the difference of the occurrence probability of y from the uniformly random case. Then $P_{F,y}(\varepsilon)$ is the sum of the occurrence probabilities $Pr(x)$ of inputs $x \in F^{-1}(y)$, while we have

$$Pr(x) = (1/2 + \varepsilon)^w (1/2 - \varepsilon)^{n-w} \tag{1}$$

for any $x \in \Sigma^n$, where $w = \mathrm{wt}(x) = \sum_{j=1}^{n} x_j$ denotes the weight of x. This implies that each $P_{F,y}(\varepsilon)$, hence each $\overline{P}_{F,y}(\varepsilon)$, is a polynomial in ε of degree at most n. Since at least one $\overline{P}_{F,y}(\varepsilon)$ is nonzero for any F (see [**1**, Theorem 1]), we can define an integer $\deg(F)$ by

$$\deg(F) = \max\{d \in \mathbb{Z} \mid \left[\varepsilon^k\right]\overline{P}_{F,y}(\varepsilon) = 0 \text{ for any } y \in \Sigma^m,\ 0 \leq k \leq d-1\} \ , \tag{2}$$

where $\left[t^j\right]Q(t)$ denotes the coefficient of a monomial t^j in a polynomial $Q(t)$. We regard such a function F as being better if $\deg(F)$ is larger; in such a case, when $\varepsilon \to 0$, the biases of the output probabilities of F from uniform will converge to 0 more quickly. Motivated from the argument above, we want to know the optimal value of $\deg(F)$ for any m and n, that is, the following value

$$\deg(n, m) = \max\{\deg(F) \mid F\colon \Sigma^n \to \Sigma^m\}$$

for any parameters $1 \leq m \leq n$.

1.2. Notations

For $k \in \mathbb{R}$, let $\vec{k}$ denote a vector whose all components are k, where the length of $\vec{k}$ should be clear from the context. For a row vector $v = (v_0, v_1, \ldots, v_k)$, we write $v \geq \vec{0}$ if $v_j \geq 0$ for all j, and put $\lfloor v \rfloor = (\lfloor v_0 \rfloor, \ldots, \lfloor v_k \rfloor)$ and $\lceil v \rceil = (\lceil v_0 \rceil, \ldots, \lceil v_k \rceil)$. Similar notations are used for column vectors $v = {}^t(v_0, \ldots, v_k)$. Let $\oplus$ denote the XOR operation.

2. Preliminary observations

First, it can be easily seen that $\deg(F) > 0$ if and only if F is *balanced*, that is, the sets $F^{-1}(y)$ have the same cardinality for any $y \in \Sigma^m$. Since a balanced function $F\colon \Sigma^n \to \Sigma^m$ always exists, we may restrict our attention to the balanced functions F.

Dichtl [**1**] showed that $\deg(16, 8) = 6$, and constructed a concrete function $F\colon \Sigma^{16} \to \Sigma^8$ that attains the optimal value of $\deg(F)$. Suzuki and Iwata [**4**] proved the following properties:

PROPOSITION 1 (SUZUKI–IWATA [**4**]). *1.* $\deg(n, n) = 1$ *for any* $n \geq 1$.

2. $\deg(n, n-1) = 2$ *for any* $n \geq 2$.

3. $\deg(n, m) \geq \deg(n, m+1)$ *for any* $n > m \geq 1$.

4. $\deg(n, m) \leq \deg(n+1, m)$ *for any* $n \geq m \geq 1$.

Proof (sketch). The optimal values of $\deg(F)$ for the cases $m = n$ and $m = n - 1$ are attained by any bijection $\Sigma^n \to \Sigma^n$ and any function $F\colon \Sigma^n \to \Sigma^{n-1}$ with the sets $F^{-1}(y)$ being of the form $\{x, x \oplus \vec{1}\}$, respectively. The last two relations are derived by considering compositions of functions F with natural projections $\Sigma^{n+1} \to \Sigma^n$ and $\Sigma^{m+1} \to \Sigma^m$. □

In particular, the values of $\deg(n, m)$ for the largest choice of m are determined. On the other hand, the values of $\deg(n, m)$ for the smallest choice of m are also determined by the author as follows:

PROPOSITION 2 (NUIDA [**3**]). $\deg(n, 1) = n$ *for any* $n \geq 1$.

Proof (sketch). The optimal value of $\deg(F)$ for $m = 1$ is attained by the parity function $F^n_{\oplus}\colon \Sigma^n \to \Sigma$, $F^n_{\oplus}(x) = x_1 \oplus \cdots \oplus x_n$. □

We also have a kind of "composition theorem" for lower bounds of $\deg(n, m)$:

PROPOSITION 3 (NUIDA [**3**]). *If* n_1 *is an integer, then* $\deg(n_1 n_2, m) \geq n_1 \deg(n_2, m)$.

Proof (sketch). For any $F\colon \Sigma^{n_2} \to \Sigma^m$, the function $G : \Sigma^{n_1 n_2} \to \Sigma^m$ given by

$$G(x^{(1)}, \ldots, x^{(n_2)}) = F(F^{n_1}_{\oplus}(x^{(1)}), \ldots, F^{n_1}_{\oplus}(x^{(n_1)})) \ ,$$

where $x^{(i)} \in \Sigma^{n_1}$ and $F^{n_1}_{\oplus}$ is defined as in the proof of Proposition 2, satisfies that $\deg(G) = n_1 \deg(F)$. □

3. Vector presentation

We define a vector presentation of a function $F\colon \Sigma^n \to \Sigma^m$ in the following manner. For $1 \leq i \leq 2^m$, let y_i denote the i-th element of Σ^m (with some fixed ordering). Then we define

$$\lambda^{(i)}_j = |\{x \in F^{-1}(y_i) \mid \mathrm{wt}(x) = j\}| \text{ for } 1 \leq i \leq 2^m \, , \, 0 \leq j \leq n \ . \tag{3}$$

We call the collection of 2^m vectors $\lambda^{(i)} = {}^t(\lambda_0^{(i)}, \dots, \lambda_n^{(i)})$ the *vector presentation* of F. We note that a collection of integer vectors $\lambda^{(i)} = {}^t(\lambda_0^{(i)}, \dots, \lambda_n^{(i)})$, $1 \leq i \leq 2^m$, is the vector presentation of some function $F\colon \Sigma^n \to \Sigma^m$ if and only if we have $\lambda^{(i)} \geq \vec{0}$ for every $1 \leq i \leq 2^m$ and $\sum_{i=1}^{2^m} \lambda^{(i)} = {}^t(\binom{n}{0}, \binom{n}{1}, \dots, \binom{n}{n})$. The author showed in [**3**] that the evaluation of $\deg(n, m)$ can be interpreted as the following in terms of the vector presentation:

THEOREM 4 (NUIDA [**3**]). *Let $1 \leq m \leq n$, $e \geq 1$ and $0 \leq e' \leq e$ be integers. Then we have $\deg(n, m) > e$ if and only if there is a collection of vectors $\lambda^{(h)}$, $1 \leq h \leq 2^m$, satisfying the conditions for vector presentation of a function $\Sigma^n \to \Sigma^m$ and that*

$$\sum_{j=0}^{n} \lambda_j^{(h)} j!(n-j)![\varepsilon^{j-i}]Q_{n-e',d}(\varepsilon) = \delta_{d,0} n! 2^{n-e'-m} \tag{4}$$

for any $0 \leq i \leq e'$ and any $0 \leq d \leq e - e'$, where $\delta_{a,b}$ denotes the Kronecker delta and we put $Q_{n,a}(\varepsilon) = (1-\varepsilon)^a (1+\varepsilon)^{n-a}$.

Proof (sketch). We note that the value $\deg(F)$ for a function F is determined solely by its vector presentation. Then it can be shown that a straightforward interpretation of the existence of a function $F\colon \Sigma^n \to \Sigma^m$ with $\deg(F) > e$ in terms of the vector presentation is equivalent (by using some identities for binomial coefficients) to the condition in the statement for the case $e' = 0$. On the other hand, it can be shown that for any $0 \leq e' \leq e - 1$, the condition for the case of $e' + 1$ is equivalent to the condition for the case of e'. □

In particular, by applying the relation $[\varepsilon^{j-i}]Q_{n-e,0}(\varepsilon) = \binom{n-e}{j-i}$ to the case $e' = e$, we have the following corollary:

COROLLARY 5 (NUIDA [**3**]). *Let $1 \leq m \leq n$ and $e \geq 1$ be integers. Then we have $\deg(n, m) > e$ if and only if there is a collection of integer vectors $\lambda^{(h)}$, $1 \leq h \leq 2^m$, satisfying that $\lambda^{(h)} \geq \vec{0}$ for every h, $\sum_{h=1}^{2^m} \lambda^{(h)} = {}^t(\binom{n}{0}, \binom{n}{1}, \dots, \binom{n}{n})$, and $A^{(n,e)}\lambda^{(h)} = b_{n,m,e}$ for every h, where the matrix $A^{(n,e)} = (A_{i,j}^{(n,e)})_{0 \leq i \leq e, 0 \leq j \leq n}$ is defined by*

$$A_{i,j}^{(n,e)} = \binom{n-e}{j-i} j!(n-j)! \text{ for any } 0 \leq i \leq e\,,\ 0 \leq j \leq n \tag{5}$$

and we put $b_{n,m,e} = n! 2^{n-e-m} \cdot \vec{1} \in \mathbb{R}^{e+1}$.

The result above yields a constructive way to prove a lower bound for $\deg(n, m)$. On the other hand, a naive strategy to deduce an upper bound for $\deg(n, m)$ based on the result above is to check the nonexistence of a collection of vectors $\lambda^{(h)}$ satisfying the criterion above (for some given e) by an exhaustive search. In fact,

the author also gave a somewhat weaker but constructive way to prove an upper bound for $\deg(n,m)$:

THEOREM 6 (NUIDA [**3**]). *Let $1 \le m \le n$ and $1 \le e \le n$ be integers. Put $g_n = {}^t(\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n})$. If there exists a real vector $y = (y_0, y_1, \ldots, y_e)$ satisfying either*

$$yb_{n,m,e} < \lceil 2^{-m} \lfloor yA^{(n,e)} \rfloor g_n \rceil \tag{6}$$

or

$$yb_{n,m,e} > \lfloor 2^{-m} \lceil yA^{(n,e)} \rceil g_n \rfloor \ , \tag{7}$$

then we have $\deg(n,m) \le e$.

Proof (sketch). Suppose that $\lambda^{(h)}$, $1 \le h \le 2^m$, is a vector presentation of a function $F\colon \Sigma^n \to \Sigma^m$ with $\deg(F) > e$. Then, by choosing an index h for which the value $\lfloor yA^{(n,e)} \rfloor \lambda^{(h)}$ attains the maximum, the criterion in Corollary 5 implies that

$$2^{-m} \lfloor yA^{(n,e)} \rfloor g_n \le \lfloor yA^{(n,e)} \rfloor \lambda^{(h)} \le yA^{(n,e)} \lambda^{(h)} = yb_{n,m,e} \ . \tag{8}$$

Since the second term above is an integer, it follows that the condition $yb_{n,m,e} \ge \lceil 2^{-m} \lfloor yA^{(n,e)} \rfloor g_n \rceil$ should be satisfied if $\deg(n,m) > e$. The remaining part of the proof is similar. □

4. Upper and lower bounds

The results above enable us to obtain upper bounds (or, in some cases, precise values) of $\deg(n,m)$ for some cases. First, we have the following result:

THEOREM 7 (NUIDA [**3**]). *If $2 \le m \le n-2$, then we have* $\deg(n,m) \le n-m$.

Proof (sketch). Assume for contrary that there exists a collection of vectors $\lambda^{(h)}$, $1 \le h \le 2^m$, satisfying the criterion in Corollary 5 for $e = n - m$. Then, since $\binom{n}{n} = 1$, at least one of the integer vectors $\lambda = \lambda^{(h)}$ should satisfy that $\lambda_n = 1$. Let $B = (B_{i,j})_{0 \le i \le e-1, 0 \le j \le e-1}$ be the leftmost-uppermost $e \times e$ submatrix of $A^{(n,e)}$, which is upper triangular and nonsingular by the construction. Then, by putting $\mu = {}^t(\mu_0, \ldots, \mu_{e-1}, 0, \ldots, 0, 1) \in \mathbb{R}^{n+1}$ with ${}^t(\mu_0, \ldots, \mu_{e-1}) = n! B^{-1} \vec{1}$, and by putting $\nu = \lambda - \mu$, we have $\nu_j \ge 0$ for any index $e \le j \le n$ and $A^{(n,e)} \nu = \vec{0}$ by the definition of the matrix $A^{(n,e)}$. Now the construction of $A^{(n,e)}$ implies that the last (i.e., $(e+1)$-th) row of $A^{(n,e)}\nu$ is a linear combination of ν_j for $e \le j \le n$ with positive coefficients, therefore we have $\nu_j = 0$ for any $e \le j \le n$. This implies that the first e rows of $A^{(n,e)}\nu$ (which is $\vec{0}$) is equal to $B \cdot {}^t(\nu_0, \ldots, \nu_{e-1})$, therefore we

have $\nu_j = 0$ for any $0 \leq j \leq e-1$ since B is singular. Hence, we have $\nu = 0$ and $\mu = \lambda$, while we have $\mu_{e-2} = -(n-e-1)\binom{n}{e-2} < 0$ by the choice of μ. This is a contradiction. □

COROLLARY 8 (NUIDA [**3**]). $\deg(n, n-2) = 2$ *for any* $n \geq 4$.

PROOF. We have $2 = \deg(n, n-1) \leq \deg(n, n-2) \leq 2$ by Proposition 1 and Theorem 7. □

We note that the optimal value of $\deg(F)$ for $F\colon \Sigma^n \to \Sigma^{n-2}$, $n \geq 4$, given above is attained by $F(x) = (x_1 \oplus x_{n-1}, x_2 \oplus x_{n-1}, \ldots, x_{n-2} \oplus x_{n-1})$. We can also determine the value of $\deg(6, 2)$ as $\deg(6, 2) = 4$, since $4 = 2\deg(3, 2) \leq \deg(6, 2) \leq 4$ by Proposition 1, Proposition 3 and Theorem 7.

On the other hand, the author obtained (in [**3**]) upper bounds for some $\deg(n, m)$ by using Theorem 6 and computer experiments to find a vector y as in the statement. More precisely, for each parameter (n, m, e), we put $\alpha = 2^{n-e-m}n! + 1$, and choose e indices $j_1, j_2, \ldots, j_e$, $0 \leq j_k \leq n$. Then we calculate $y \in \mathbb{R}^{e+1}$ by solving equations $\sum_{i=0}^{e} y_i A^{(n,e)}_{i,j_k} = 0$ for all $1 \leq k \leq e$ and $\sum_{i=0}^{e} y_i = 1/\alpha$ (if possible), and check if $yb_{n,m,e} < \lceil 2^{-m} \lfloor yA^{(n,e)} \rfloor g_n \rceil$ is satisfied. Table 1 shows upper bounds of $\deg(n, m)$ for $n \leq 13$ derived by this approach, which coincide with all the known precise values of $\deg(n, m)$ given in [**3, 4**] except for $\deg(12, 2) \leq 9$ (the precise value for the case $(n, m) = (12, 2)$ is $\deg(12, 2) = 8$).

The author also calculated (in [**3**]) upper bounds of $\deg(n, m)$ for $n = 14$, 15, 16, 24, 32, 48 and 64. See Table 2 for the results. The strategy is similar to the case of smaller n above, but the choices of indices $j_1, \ldots, j_e$ for the cases $n \geq 24$ are restricted to $\{j_1, \ldots, j_e\} = \{n', n'+1, \ldots, n'+e-1\}$, where $n' = \lfloor (n-e)/2 \rfloor$, for the sake of reducing the computation time. Although the bounds obtained in this manner would not be so tight, the required computation time was practically reasonable, in contrast to the computation based on the exhaustive search which takes too long time.

5. Future work

The author would like to propose a problem of studying more properties of the two-dimensional integer sequence $(\deg(n, m))_{n,m}$. In particular, here we note the following conjecture:

CONJECTURE 9. *We would have* $\deg(n, m) \geq \deg(n+1, m+1)$ *for any* $1 \leq m \leq n$.

In other words, for the table of $\deg(n, m)$ as in Table 1, the conjecture says that the values would be weakly decreasing in the upper-left to lower-right direction (while Proposition 1 shows that the values are weakly increasing in the upper to

Table 1. Upper bounds of $\deg(n,m)$, $1 \le n \le 13$

Here the value in bold font is larger than the precise value of $\deg(n,m)$; for the underlined values, the precise values of $\deg(n,m)$ are not known so far; and the other values are equal to the precise values of $\deg(n,m)$.

$n\backslash m$	1	2	3	4	5	6	7	8	9	10	11	12	13
1	1												
2	2	1											
3	3	2	1										
4	4	2	2	1									
5	5	3	2	2	1								
6	6	4	3	2	2	1							
7	7	4	4	3	2	2	1						
8	8	5	4	4	2	2	2	1					
9	9	6	5	4	3	2	2	2	1				
10	10	7	6	5	4	3	2	2	2	1			
11	11	8	6	6	4	4	3	2	2	2	1		
12	12	**9**	7	6	5	4	4	3	2	2	2	1	
13	13	10	8	7	6	5	4	4	3	2	2	2	1

lower direction and weakly decreasing in the left to right direction).

Another possible direction of enhancing the present results is to consider the same problem for some reasonable subclass of functions $\Sigma^n \to \Sigma^m$. For example, the subclass of functions $F\colon \Sigma^n \to \Sigma^m$ satisfying that $F(x \oplus \vec{1}) = F(x)$ for any $x \in \Sigma^n$ has been studied in [**3, 4**]; we call such a function F *antipodally symmetric* (in [**3, 4**], it was simply called "symmetric"). Let $\deg^{\mathrm{AS}}(n,m)$ denotes the maximum of $\deg(F)$ for antipodally symmetric $F\colon \Sigma^n \to \Sigma^m$. If we will have some results on the values of $\deg^{\mathrm{AS}}(n,m)$ and relations of $\deg^{\mathrm{AS}}(n,m)$ with $\deg(n,m)$, then it would provide some new observations for the properties of $\deg(n,m)$. We would be also possible to do similar studies for some other subclasses of the functions $\Sigma^n \to \Sigma^m$.

Acknowledgments The author would like to thank Professor Manabu Inuma for encouraging him to submit the article. The author would like to thank the anonymous reviewer for precious comments.

Table 2. Upper bounds of $\deg(n,m)$ for $n \in \{14, 15, 16, 24, 32, 48, 64\}$

$n = 14$															
m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	
bound	14	10	9	8	6	6	5	4	4	3	2	2	2	1	
$n = 15$															
m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
bound	15	11	10	8	7	6	6	5	4	4	3	2	2	2	1	
$n = 16$																
m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
bound	16	12	11	9	8	7	6	6	4	4	4	2	2	2	2	1
$n = 24$																
m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
bound	24	22	20	18	16	16	14	12	12	10	10	8	8	6	6	6
m	17	18	19	20	21	22	23	24								
bound	4	4	4	2	2	2	2	1								
$n = 32$																
m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
bound	32	30	28	26	24	22	22	20	18	18	16	14	14	12	12	10
m	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
bound	10	8	8	8	6	6	6	4	4	4	2	2	2	2	2	1
$n = 48$																
m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
bound	48	46	44	42	40	38	36	34	34	32	30	30	28	26	26	24
m	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
bound	22	22	20	20	18	18	16	16	14	14	12	12	12	10	10	8
m	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
bound	8	8	6	6	6	6	4	4	4	4	2	2	2	2	2	1
$n = 64$																
m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
bound	64	62	60	58	56	54	52	50	48	48	46	44	42	42	40	38
m	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
bound	38	36	34	34	32	30	30	28	28	26	26	24	24	22	22	20
m	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
bound	20	18	18	16	16	14	14	14	12	12	12	10	10	10	8	8
m	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
bound	8	6	6	6	6	4	4	4	4	2	2	2	2	2	2	1

References

[1] M. Dichtl, Bad and good ways of post-processing biased physical random numbers, in: *Proceedings of FSE 2007*, Lecture Notes in Computer Science vol.4593, Springer, Heidelberg, pp.137–152, 2007.

[2] J. von Neumann, Various techniques for use in connection with random digits, in: *Von Neumann's Collected Works*, Pergamon, London, pp.768–770, 1963.

[3] K. Nuida, Bounds on fixed-length post-processing functions for stationary biased random number generators, in: *Proceedings of ISITA 2008*, CD-ROM, 2008.

[4] K. Suzuki, T. Iwata, *Analysis of post-processing function for biased physical random number generators*, in: The 2008 Symposium on Cryptography and Information Security (SCIS 2008), Miyazaki, Japan, Jan. 25, 2008.

Koji Nuida

Innovative Security Research Group, Research Institute for Secure Systems, National Institute of Advanced Industrial Science and Technology

AIST Tsukuba Central 2, 1-1-1 Umezono, Tsukuba, Ibaraki 305-0568, Japan

k.nuida@aist.go.jp