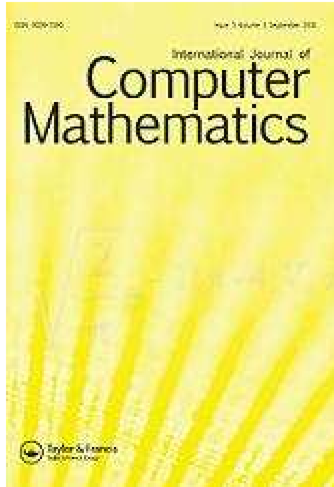
Combining random generators by group operation.

Grzegorz Oleksik



Combining random generators by group operation.

Journal:	*International Journal of Computer Mathematics*
Manuscript ID:	GCOM-2011-0184-A.R1
Manuscript Type:	Original Article
Date Submitted by the Author:	15-Jun-2011
Complete List of Authors:	Oleksik, Grzegorz; University of Lodz, Faculty of Mathematics and Computer Science
Keywords:	65C10 - Random Number Genaration, 68Q87 - Probability in Computer Science, G3 [Mathematics of Computing]: Probability and Statistic - Random Number Generation, G3 [Mathematics of Computing]: Probability and Statistic - Markov processes, 60J10 - Markov chains

International Journal of Computer Mathematics
Vol. 00, No. 00, February 2011, 0–8

RESEARCH ARTICLE

Combining random generators by group operation

Grzegorz Oleksik*

Faculty of Mathematics and Computer Science, University of Lodz, Banacha 22, 90-238 Lodz, Poland

(*Received 00 Month 200x; in final form 00 Month 200x*)

In the article we show that combining random generators by group operation improves the statistical properties of the composite. It gives an effective way of finding random generators more and more close to the uniform. Moreover we obtain an effective estimation of the speed of convergence to the uniform generator.

Keywords: bit generator, random number generator, uniform distribution, Markov chains

AMS Subject Classification: 65C10; 68Q87

1. Introduction

Empirical studies indicate that combining two or more simple generators, by means of the operations such as $+, -, *, \oplus$ (exclusive or) improves the statistical properties of the composite. References [2, 12, 18, 22] seem to be the first, which deal with combining generators. Brown and Salomon [3] provided a theoretical support for such combinations. They gave an elaborate proof that $x + y \bmod m$ was at least as uniform as x or $y \bmod m$, which was based on the techniques of majorization. Marshall and Olkin [20] made the result more general in the elegant book on inequalities and majorization. Combined generators have more advantages than simple ones: they passed more practical tests (see [17–19, 22]) and generally their periods increase (see [4, 5, 14–16]).

From theoretical point of view random generators are random variables with values in finite groups. The case of independent variables taking values in compact topological groups was considered by many authors (see [1, 7–11, 21]). In the article we give similar results for independent random variables with values in any finite groups (in particular in $\mathbb{Z}_2 = \{0, 1\}$) using only elementary methods. Moreover we give an effective estimation of the speed of convergence to the uniform generator. The estimations are important in applications, because they help to find better and better generators.

To describe the results more precisely we take Ω a probabilistic space, $G = \{g_1, \ldots, g_n\}$ a finite group and $X \colon \Omega \longrightarrow G$ a random variable. If $G = \mathbb{Z}_2$ we may treat X as a bit generator. X is called *uniform* if the probability of taking value g_i by X is the same for $i = 1, \ldots, n$ i.e.

$$\Pr\{X = g_i\} = \frac{1}{n}.$$

* Email: oleksig@math.uni.lodz.pl

In practise it is difficult to obtain the uniform generator. In the article we give an effective method of finding random generator closer and closer to uniform.

In case $G = \mathbb{Z}_2$, which we consider separetely (because we obtain in this case a stronger result), we prove the following. Let X_i, $i = 1, 2, \ldots,$ be a sequence of arbitrary independent bit generators and $\Pr\{X_i = 0\} = p_i$, $\Pr\{X_i = 1\} = 1 - p_i$. If p_i's are not "close enough" to 0 and 1 then the sum distribution modulo 2 of X_i's i.e. the distribution of $X_1 + ... + X_i \mod 2$ tends toward uniform (Thms. 2.1, 2.6 and Cors. 2.3, 2.7) in a controlled rate. So, in practise if we have a sequence of "not uniform" generators then by taking their sum modulo 2 in sufficiently large quantity we can obtain more and more uniform bit generators. Observe that taking the sum $X_1 + ... + X_i \mod 2$ is equivalent to the operation "XOR" i.e. exclusive or.

In the general case, i.e. for an arbitrary finite group G (in particular for $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ with summing mod $n, n = 1, 2, \ldots$ or $\mathbb{Z}_p \setminus \{0\}$ with multiplying mod p for prime p) we obtain a similar result in a slightly weaker form (Thm. 3.1 and Cors. 3.2, 3.4).

Recently some authors (see for example [6, 13]) have studied a "weak" type of uniformity called the ϵ-uniformity. Let Ω be a probabilistic space, $G = \{g_1, \ldots, g_n\}$ be a finite group and $X : \Omega \longrightarrow G$ be a random variable. We say that X is *ϵ-uniform* if for every $i = 1, \ldots, n$

$$\left|\Pr(X = g_i) - \frac{1}{n}\right| \leq \frac{\epsilon}{n}.$$

In [6] J.D. Dixon constructed the sequence of random cube to get a 1/4-uniform generator and in [13] A. Lukács gave an efficient method, which provably generates ϵ-uniform random elements of an abelian group.

2. Combining random generators mod 2

Let $(X_i)_{i\in\mathbb{N}}$ be a sequence of the independent random variables with values in $\mathbb{Z}_2$, i.e.

$$X_i \colon \Omega \longrightarrow \mathbb{Z}_2, \qquad i = 1, 2, \ldots .$$

Let δ_i, $|\delta_i| \leq 1$ be real numbers such that

$$\Pr\{X_i = 1\} = \frac{1}{2}(1 - \delta_i), \Pr\{X_i = 0\} = \frac{1}{2}(1 + \delta_i), \qquad i = 1, 2, \ldots .$$

If we write $X_1 + X_2$, by "+" we mean summing in the group $\mathbb{Z}_2$. Then we have the first limit theorem.

Theorem 2.1 *For every $b \in \{0, 1\}$ we have*

$$\left|\Pr\{X_1 + \ldots + X_i = b\} - \frac{1}{2}\right| = \frac{1}{2}\prod_{k=1}^{i} |\delta_k|, \quad i \in \mathbb{N}.$$

Proof Without loss of generality we may suppose that $b = 1$. Set

$$u_i := \Pr\{\sum_{k=1}^{i} X_k = 1\}, \quad i \in \mathbb{N}.$$

Then from independence of the random variables $X_1, \ldots, X_{i+1}$ we easily get independence of the random variables $\sum_{k=1}^{i} X_k$ and X_{i+1} and hence

$$u_{i+1} = u_i \Pr\{X_{i+1} = 0\} + (1 - u_i) \Pr\{X_{i+1} = 1\}, \quad i \in \mathbb{N}.$$

Since $\Pr\{X_i = 0\} = \frac{1}{2}(1 + \delta_i)$, $\Pr\{X_i = 1\} = \frac{1}{2}(1 - \delta_i)$ then putting $u_i = \frac{1}{2}(1 - \epsilon_i)$, $\epsilon_i \in [-1, 1]$, $i \in \mathbb{N}$, we get

$$\frac{1}{2}(1 - \epsilon_{i+1}) = \frac{1}{2}(1 - \epsilon_i)\frac{1}{2}(1 + \delta_{i+1}) + \frac{1}{2}(1 + \epsilon_i)\frac{1}{2}(1 - \delta_{i+1}), \quad i \in \mathbb{N}.$$

After easy transformations we obtain

$$\epsilon_{i+1} = \epsilon_i \delta_{i+1}, \quad i \in \mathbb{N}.$$

Observe that $\epsilon_1 = \delta_1$, hence

$$\epsilon_i = \prod_{k=1}^{i} \delta_k, \quad i \in \mathbb{N}. \tag{1}$$

From (1) we easily get $|u_i - \frac{1}{2}| = \frac{1}{2} \prod_{k=1}^{i} |\delta_k|$. It finishes the proof. ∎

As a direct consequence of the above theorem we have the following.

Corollary 2.2 *For every $b \in \{0, 1\}$ we have*

$$\lim_{i\to\infty} \Pr\{X_1 + \ldots + X_i = b\} = \frac{1}{2} \Longleftrightarrow \prod_{i=1}^{\infty} |\delta_i| = 0.$$

Corollary 2.3 *Suppose that there exists a positive constant $\delta \in \mathbb{R}$ such that $|\delta_i| \leq \delta < 1$, $\Pr\{X_i = 1\} = \frac{1}{2}(1 - \delta_i)$, $i \in \mathbb{N}$. Then for every $b \in \{0, 1\}$*

$$\lim_{i\to\infty} \Pr\{X_1 + \ldots + X_i = b\} = \frac{1}{2},$$

and the distribution of $X_1 + \ldots + X_i$ tends to the uniform distribution at a geometric rate i.e.

$$\left|\Pr\{X_1 + \ldots + X_i = b\} - \frac{1}{2}\right| \leq \frac{1}{2}\delta^i.$$

Generally it is difficult to check the condition $\prod_{i=1}^{\infty} |\delta_i| = 0$, so we give the following helpful known proposition.

Proposition 2.4 *Let $a_i \in \mathbb{R}$, $i \in \mathbb{N}$. Then the product $\prod_{i=1}^{\infty}(1 + |a_i|)$ is convergent if and only if the series $\sum_{i=1}^{\infty} |a_i|$ is convergent.*

Proof It is a direct consequence of inequalities

$$\sum_{i=1}^{k}|a_i| < 1+\sum_{i=1}^{k}|a_i| < \prod_{i=1}^{k}(1+|a_i|) \leq \prod_{i=1}^{k} e^{|a_i|} = e^{\sum_{i=1}^{k}|a_i|}, k\in\mathbb{N}.$$

■

This implies following proposition.

PROPOSITION 2.5 *Let* $\delta_i \in [-1,1]$, $i\in\mathbb{N}$. *Then*

$$\prod_{i=1}^{\infty}|\delta_i| = 0 \iff \left(\sum_{i=1}^{\infty}(1-|\delta_i|) = +\infty \vee \exists_{i\in\mathbb{N}}\,\delta_i = 0\right).$$

Proof In the beginning observe that if $\delta_i = 0$ for some $i\in\mathbb{N}$ then of course the equivalence is true. So we can assume that $\delta_i \neq 0\,, i\in\mathbb{N}$. We have

$$\prod_{i=1}^{\infty}|\delta_i| = 0 \Leftrightarrow \prod_{i=1}^{\infty}\frac{1}{|\delta_i|} = +\infty \Leftrightarrow \prod_{i=1}^{\infty}\left(1+\frac{1-|\delta_i|}{|\delta_i|}\right) = +\infty \Leftrightarrow \sum_{i=1}^{\infty}\frac{1-|\delta_i|}{|\delta_i|} = +\infty.$$

The last equivalence follows from Proposition 2.4. So that to finish the proof it is enough to show that

$$\sum_{i=1}^{\infty}(1-|\delta_i|) = +\infty \iff \sum_{i=1}^{\infty}\frac{1-|\delta_i|}{|\delta_i|} = +\infty.$$

Because $0 < |\delta_i| \leq 1$, we have "$\Rightarrow$" implication. Now suppose that $\sum_{i=1}^{\infty}(1-|\delta_i|)/|\delta_i| = +\infty$. Put $A := \{i\colon |\delta_i| \leq 1/2\}$. If the set A is finite then $(1-|\delta_i|)/|\delta_i| < 2(1-|\delta_i|)$, $i \notin A$, so this inequality is true for all i besides a finite number. Hence $\sum_{i=1}^{\infty}(1-|\delta_i|) = +\infty$. If the set A is infinite then $1-|\delta_i| \geq 1/2$ for infinite number i, and so $\sum_{i=1}^{\infty}(1-|\delta_i|) = +\infty$. It finishes the proof. ■

It is easy to check that $1-|1-2t| = 2\min\{t, 1-t\}$ for all $t\in\mathbb{R}$. Hence if we put $p_i := (1/2)(1-\delta_i)$, $i\in\mathbb{N}$, we get $\delta_i = 1-2p_i$ and $1-|\delta_i| = 1-|1-2p_i| = 2\min\{p_i, 1-p_i\}$ So the condition $\sum_{i=1}^{\infty}(1-|\delta_i|) = +\infty$ is equivalent to $\sum_{i=1}^{\infty}\min\{p_i, 1-p_i\} = +\infty$. Then by Proposition 2.5 we can reformulate Theorem 2.1 and Corollary 2.3.

THEOREM 2.6 *Let* $(X_i)_{i\in\mathbb{N}}$ *be the sequence of the independent random variables with values in* $\mathbb{Z}_2$ *such that* $\Pr\{X_i = 0\} = p_i$, $\Pr\{X_i = 1\} = 1-p_i$, $i\in\mathbb{N}$. *Then for every* $b\in\{0,1\}$

$$\lim_{i\to\infty}\Pr\{X_1+...+X_i = b\} = \frac{1}{2} \iff \left(\sum_{i=1}^{\infty}\min\{p_i, 1-p_i\} = +\infty \vee \exists_{i\in\mathbb{N}}\,p_i = \frac{1}{2}\right).$$

and

$$\left|\Pr\{X_1+\ldots+X_i = b\} - \frac{1}{2}\right| = \frac{1}{2}\prod_{k=1}^{i}|1-2p_k|.$$

Corollary 2.7 *Let* $(X_i)_{i\in\mathbb{N}}$ *be the sequence of the independent random variables with values in* $\mathbb{Z}_2$ *such that* $\Pr\{X_i = 0\} = p_i$, $\Pr\{X_i = 1\} = 1 - p_i$, $i \in \mathbb{N}$. *Suppose that there exist constants* $\alpha, \beta \in \mathbb{R}$ *such that* $0 < \alpha \le p_i \le \beta < 1$, $i \in \mathbb{N}$. *Then for every* $b \in \{0, 1\}$

$$\lim_{i\to\infty} \Pr\{X_1 + ... + X_i = b\} = \frac{1}{2},$$

and distribution of $X_1 + ... + X_i$ *tends to uniform distribution at a geometric rate i.e.*

$$\left|\Pr\{X_1 + ... + X_i = b\} - \frac{1}{2}\right| \le \frac{1}{2}\delta^i,$$

where $\delta = \max\{1 - 2\alpha, 2\beta - 1\}$.

Proof Let $i \in \mathbb{N}$. From our assumptions, if $p_i \le 1/2$ we get that $|1 - 2p_i| = 1 - 2p_i \le 1 - 2\alpha \le \delta$ and if $p_i > 1/2$ we get $|1 - 2p_i| = 2p_i - 1 \le 2\beta - 1 \le \delta$. So $|\delta_i| = |1 - 2p_i| \le \delta$ and by using Corollary 2.3 we get the thesis. ■

Remark 1 The above result is true for every two-element group because every two-element group is isomorphic to $\mathbb{Z}_2$.

Remark 2 It is a standard fact of probability theory that if we have arbitrary distributions μ_n, $n \in \mathbb{N}$ on a finite group G we may construct probabilistic space Ω and independent random variables $X_n : \Omega \longrightarrow G$ with distributions μ_n. Moreover if we have a finite sequence of independent random variables $X_1, \ldots, X_k$ we may always extend it to infinite sequence $X_1, \ldots, X_k, X_{k+1}, X_{k+2}, \ldots$ preserving independence with arbitrary distributions $\mu_{k+1}, \mu_{k+2} \ldots$.

3. Combining random generator by group operation

Let $G = \{g_1, \ldots, g_n\}$ be a finite n-element group with operation $\circ$ and let $(X_i)_{i\in\mathbb{N}}$ be a sequence of independent random variables with values in G i.e.

$$X_i : \Omega \longrightarrow G, \qquad i = 1, 2, \ldots .$$

Let p_{ik}, $0 \le p_{ik} \le 1$ be real numbers such that $p_{i1} + \ldots + p_{in} = 1$ and

$$\Pr\{X_i = g_k\} = p_{ik}, \; k = 1, \ldots, n, \; i \in \mathbb{N}.$$

Set $p_i := \min\{p_{il} : l = 1, \ldots, n\}$, $i \in \mathbb{N}$. Then we have the second limit theorem.

Theorem 3.1 *For every* $k \in \{1, 2, \ldots, n\}$

$$\left|\Pr\{X_1 \circ \ldots \circ X_i = g_k\} - \frac{1}{n}\right| \le \max_{m=1}^{n} \left|p_{1m} - \frac{1}{n}\right| \prod_{m=2}^{i} (1 - p_m), \; i \in \mathbb{N}$$

and if $\sum_{i=1}^{\infty} p_i = +\infty$ *then*

$$\lim_{i\to\infty} \Pr\{X_1 \circ \ldots \circ X_i = g_k\} = \frac{1}{n}.$$

Remark 1 It is easy to see that if $G = \mathbb{Z}_2$ with summing modulo 2 Theorem 3.1 is a "weaker form" of Theorem 2.6

Remark 2 Observe, that the converse of the second part of the above theorem isn't true. Indeed, if X_{i_0} has uniform distribution then it is easy to check that all $X_1 \circ \ldots \circ X_j$, $j \geq i_0$ have the uniform distibution independent of distribution of random variable X_i, $i \neq i_0$. So we may take X_1 a random variable with the uniform distribution and $X_2, X_3, \ldots$ arbitrary such that $\sum_{i=2}^{\infty} p_i < \infty$. Another counterexample in which no random variables X_i has the uniform distribution is: take $G = \mathbb{Z}_3$ with summing modulo 3 and sequence of the independent random variables $(X_i)_{i\in\mathbb{N}}$, such that $\Pr\{X_i = 0\} = 0$, $\Pr\{X_i = 1\} = \Pr\{X_i = 2\} = 1/2$, $i \in \mathbb{N}$, then of course $\sum_{i=1}^{\infty} p_i = 0$ but one can check using Markov chain method that $\lim_{i\to\infty} \Pr\{X_1 + \ldots + X_i = k\} = 1/3$, $k = 0, 1, 2$ (Compare this remark to the first part of Theorem 2.6).

Corollary 3.2 *For every* $k \in \{1, 2, \ldots, n\}$

$$\left|\Pr\{X_1 \circ \ldots \circ X_i = g_k\} - \frac{1}{n}\right| \leq \left(1 - \frac{1}{n}\right) \prod_{m=1}^{i} (1 - p_m),\ i \in \mathbb{N}. \tag{2}$$

Proof It is a direct consequence of Theorem 3.1 and following inequality:

$$\max_{i=1}^{n} \left|a_i - \frac{1}{n}\right| \leq \left(1 - \frac{1}{n}\right) (1 - \min_{i=1}^{n} a_i)$$

for $a_i \geq 0$ such, that $\sum_{i=1}^{n} a_i = 1$. Indeed for $n = 1$ or $n = 2$ one can easily check this inequality. Let $n > 2$. There exist i_0 such that $\max_{i=1}^{n} |a_i - 1/n|$ is attained.

If $a_{i_0} \leq 1/n$, then

$$\left|a_{i_0} - \frac{1}{n}\right| = \frac{1}{n} - a_{i_0} \leq \frac{1}{n}. \tag{3}$$

On the other hand observe that $\min_{i=1}^{n} a_i \leq 1/n$, so

$$\left(1 - \frac{1}{n}\right) (1 - \min_{i=1}^{n} a_i) \geq \left(1 - \frac{1}{n}\right)^2 > \frac{1}{n}. \tag{4}$$

From (3) and (4) we get our inequality in this case.

If $a_{i_0} > 1/n$, then

$$\left(1 - \frac{1}{n}\right) (1 - \min_{i=1}^{n} a_i) \geq \left(1 - \frac{1}{n}\right) (1 - (1 - a_{i_0})) = \left(1 - \frac{1}{n}\right) a_{i_0} \geq a_{i_0} - \frac{1}{n} = \left|a_{i_0} - \frac{1}{n}\right|$$

and we get our inequality in this case. ∎

Remark 3 From the results of the paper by Brown and Salomon (see [3], Sec. 4) one can deduce similar estimation as in Corollary 3.2, but without the constant factor $1 - 1/n$. This constant is the best possible in inequality (2). Indeed, if we take $G = \mathbb{Z}_2$ and two independent random variables with distributions $\Pr\{X_1 = 0\} = 0, \Pr\{X_1 = 1\} = 1, \Pr\{X_2 = 0\} = 1, \Pr\{X_2 = 1\} = 0$, then the inequality in Corollary 3.2 becomes an equality. Hence inequality (2) couldn't be improved.

Moreover, one can also obtain similar estimations from the case when G is a compact group (see [1]), but without the constant factor $1 - 1/n$ as well.

To prove Theorem 3.1 we give a useful lemma.

Lemma 3.3 *Let* $a_i, x_i \in \mathbb{R}$, $a_i \geq 0$, $i = 1, \ldots, n$ *such that* $\sum_{i=1}^n a_i = 1$ *and* $\sum_{i=1}^n x_i = 0$. *Then*

$$\left|\sum_{i=1}^n a_i x_i\right| \leq \max_{i=1}^n |x_i| \left(1 - \min_{i=1}^n a_i\right).$$

Proof If $x_i = 0$ for every i, then the inequality is trivial. So we can suppose, that there exist i, j such that $x_i x_j < 0$. Hence the sets $A := \{i = 1, \ldots, n \colon x_i > 0\}$, $B := \{i = 1, \ldots, n \colon x_i < 0\}$ are nonempty. We get further

$$\left|\sum_{i=1}^n a_i x_i\right| = \left|\sum_{i\in A} a_i x_i + \sum_{i\in B} a_i x_i\right| = \left|\sum_{i\in A} a_i x_i - \sum_{i\in B} a_i |x_i|\right| \leq \max\left\{\sum_{i\in A} a_i x_i, \sum_{i\in B} a_i |x_i|\right\}.$$

The last inequality is the consequence of the fact that $|a - b| \leq \max\{a, b\}$ for $a, b \geq 0$. On the other side

$$\sum_{i\in A} a_i x_i \leq \max_{i=1}^n |x_i| \sum_{i\in A} a_i \leq \max_{i=1}^n |x_i| (1 - \min_{i=1}^n a_i)$$

and

$$\sum_{i\in B} a_i |x_i| \leq \max_{i=1}^n |x_i| \sum_{i\in B} a_i \leq \max_{i=1}^n |x_i| (1 - \min_{i=1}^n a_i).$$

Reasumming

$$\left|\sum_{i=1}^n a_i x_i\right| \leq \max_{i=1}^n |x_i| \left(1 - \min_{i=1}^n a_i\right).$$

It finishes the proof. ■

The proof of Theorem 3.1

Let $k \in \{1, \ldots, n\}$. We may suppose that $n \geq 2$, because for $n = 1$ the assertion of the theorem is trivial. First observe that from independence of random variables $(X_i)_{i\in\mathbb{N}}$ we easily get independence of the random variables $X_1 \circ \ldots \circ X_i$ and X_{i+1}, $i \in \mathbb{N}$. Hence

$$\begin{aligned} \Pr\{X_1 \circ \ldots \circ X_{i+1} = g_k\} &= \sum_{l=1}^n \Pr\{X_1 \circ \ldots \circ X_i = g_k \circ g_l^{-1} \wedge X_{i+1} = g_l\} = \\ &= \sum_{l=1}^n \Pr\{X_1 \circ \ldots \circ X_i = g_k \circ g_l^{-1}\} p_{i+1,l}. \end{aligned} \tag{5}$$

Let $s_{ij} = \Pr\{X_1 \circ \ldots \circ X_i = g_j\}$, $i \in \mathbb{N}$, $j \in \{1, \ldots, n\}$ Then we have

$$s_{i+1,k} = \sum_{l=1}^n s_{i,r_{k,l}}\, p_{i+1,l},\ i \in \mathbb{N}, \tag{6}$$

where $r_{k,l} \in \{1, \dots, n\}$ is such number that $g_k \circ g_l^{-1} = g_{r_{k,l}}$. Let $\epsilon_{ij} = s_{ij} - \frac{1}{n}$, $i \in \mathbb{N}$, $j \in \{1, \dots, n\}$. By hypothesis we have $\sum_{l=1}^{n} p_{i+1,l} = 1$, so we can rewrite (6) in the form:

$$\epsilon_{i+1,k} = \sum_{l=1}^{n} \epsilon_{i,r_{k,l}} p_{i+1,l},\ i \in \mathbb{N}. \tag{7}$$

Because $\sum_{j=1}^{n} s_{ij} = 1$, $i \in \mathbb{N}$, so by definition of ϵ_{ij} we have $\sum_{j=1}^{n} \epsilon_{ij} = 0$, $i \in \mathbb{N}$. Hence from (7), using Lemma 3.3, we get

$$|\epsilon_{i+1,k}| \le \max_{l=1}^{n} |\epsilon_{i,r_{k,l}}|(1 - \min_{l=1}^{n} p_{i+1,l}) = \max_{l=1}^{n} |\epsilon_{il}|(1 - \min_{l=1}^{n} p_{i+1,l}),\ i \in \mathbb{N}.$$

Set $\epsilon_i := \max_{l=1}^{n} |\epsilon_{il}|$ and remember that $p_i = \min_{l=1}^{n} p_{il}$, $i \in \mathbb{N}$. Then we have

$$\epsilon_{i+1} \le \epsilon_i(1 - p_{i+1}),\ i \in \mathbb{N}.$$

Observe, that $\epsilon_1 = \max_{l=1}^{n} |p_{1l} - 1/n|$ hence by easy induction

$$\epsilon_i \le \max_{l=1}^{n} |p_{1l} - 1/n| \prod_{m=2}^{i} (1 - p_m),\ i \in \mathbb{N}, \tag{8}$$

and we get the first part of the assertion.

If $\sum_{i=1}^{\infty} p_i = +\infty$, so $\sum_{i=1}^{\infty} \frac{p_i}{1-p_i} = +\infty$, because $0 \le p_i \le \frac{1}{n}$. Then from Proposition 2.4 we have

$$\prod_{m=1}^{\infty} \left(1 + \frac{p_i}{1 - p_i}\right) = +\infty,$$

so $\prod_{m=1}^{\infty} \frac{1}{1-p_i} = +\infty$. Hence $\prod_{m=1}^{\infty}(1 - p_i) = 0$. So from (8) we get $\lim_{i\to\infty} \epsilon_i = 0$. It finishes the second part of the theorem in this case. □

As a direct consequence of Corollary 3.2 we obtain the following corollary.

Corollary 3.4 *Let $(X_i)_{i\in\mathbb{N}}$ be a sequence of independent random variables such that $\Pr\{X_i = g_k\} = p_{ik}$, $k = 1, \dots, n$, $i \in \mathbb{N}$. If there exists $\alpha > 0$ such that $p_i \ge \alpha$, $i \in \mathbb{N}$, then for every $k \in \{1, 2, \dots, n\}$*

$$\lim_{i\to\infty} \Pr\{X_1 \circ \dots \circ X_i = g_k\} = \frac{1}{n}$$

and distribution of $X_1 \circ \dots \circ X_i$ tends to uniform distribution at a geometric rate i.e.

$$\left|\Pr\{X_1 \circ \dots \circ X_i = g_k\} - \frac{1}{n}\right| \le \left(1 - \frac{1}{n}\right)(1 - \alpha)^i, \qquad i \in \mathbb{N}.$$

4. Concluding remarks

The results of the paper have a practical meaning. If we have a sequence of random generators $X_1, X_2, \ldots$ (binary or in general in values in $\mathbb{Z}_n$ or in an arbitrary finite group G) satisfying mild conditions, then by combining them via group operation we get the sequence of the random generators $Y_i = X_1 + X_2 + \ldots + X_i$ more and more uniform, when i tends to infinity (see Thm. 2.1, 2.6, 3.1 and Cors. 2.3, 2.7, 3.2, 3.4).

References

[1] R.N. Bhattacharya, *Speed of convergence of the n-fold convolution of a probability measure on a compact group*, Z. Wahrscheinlichkeit 25 (1972), pp. 1–10.
[2] T.A. Bray and G. Marsaglia, *One-line random number generators and their use in combination*, Commun. ACM 11 (1968), pp. 757–759.
[3] M. Brown and H. Salomon, *On combining pseuedorandom number generators*, Ann. Stat. 3 (1979), pp. 691–695.
[4] S. Côté and P. L'Ecuyer, *Implementing a random number package with splitting facilities*, ACM Trans. Math. Softw. 17 (1991), pp. 98–111.
[5] A. Compagner and D. Wang, *On the use of reducible polynomials as random number generators*, Math. Comput. 60 (1993), pp. 363–374.
[6] J.D. Dixon, *Generating random elements in finite groups*, The Electronic Journal of Combinatorics 23 (2008),# R94
[7] B.A. Egorov and V.M. Maksimov, *On a sequence of random variables with values in a compact commutative groups*, Theor. Probab. Appl+ 13 (1968), pp. 584–593.
[8] U. Grenander, *Probabilities on algebraic structures*, Almquist & Wiksell, Stockholm-Göteborg-Uppsala (1963).
[9] K. Ito and Y. Kawada, *On the probability distribution on a compact group*, I. Proc. Phys.-Math. Soc. Japan 22 (1940), pp. 977–998.
[10] B.M. Kloss, *Limit distribution for sums of independent variables with values in bicompact group*, Dokl. Akad. Nauk SSSR 109 (1956), pp. 453–455.
[11] ———, *Probability distributions on bicompact topological groups*, Theor Probab. Appl+ 4 (1959), pp. 237–270.
[12] D.E. Knuth, *The Art of Computer Programming*, vol. II, Addison-Wesley, Reading, Mass. (1981).
[13] A. Lukács, *Generating random elements of abelian groups*, Random Structures Algorithms 26 (2005), pp. 437–445.
[14] P. L'Ecuyer, *Uniform random number generation*, Ann. Oper. Res. 53 (1994), pp. 77–120.
[15] ———, *Combined multiple recursive generators*, Oper. Res. 44 (1996), pp. 816–822.
[16] ———, *Maximally equidistributed combined tausworthe generators*, Math. Comput. 65 (1996), pp. 203–213.
[17] P. L'Ecuyer, *Combined generators with components from different families*, Mathematics and Computers in Simulation 62 (2003), pp. 395–404.
[18] M.D. Maclarin and G. Marsaglia, *Uniform random number generators*, JACM 12 (1965), pp. 83–89.
[19] G. Marsaglia, *A current view of random number generators*, Computer Science and Statistics: Sixteenthy Symposium on the Interface (1985), pp. 3–10.
[20] A. Marshall and I. Olkin, in *Inequalities: Theory of Majorization and its Application*, chap. 13, Academic Press, New York (1979), p. 383.
[21] M. Ullrich and K. Urbanik, *A limit theorem for random variables in compact topological groups*, Colloq. Math. 7 (1960), pp. 191–198.
[22] W.J. Westlake, *A uniform random number generator based on the combination of two congruential generators*, JACM 2 (1967), pp. 337–340.