

Progressive Randomization of a Deck of Playing Cards: Experimental Tests and Statistical Analysis of the Riffle Shuffle

M. P. Silverman

Department of Physics, Trinity College, Hartford, CT, USA

Email: mark.silverman@trincoll.edu, jwmgibbs@gmail.com

How to cite this paper: Silverman, M.P. (2019) Progressive Randomization of a Deck of Playing Cards: Experimental Tests and Statistical Analysis of the Riffle Shuffle. *Open Journal of Statistics*, 9, 268-298. <https://doi.org/10.4236/ojs.2019.92020>

Received: March 22, 2019

Accepted: April 25, 2019

Published: April 28, 2019

Copyright © 2019 by author(s) and Scientific Research Publishing Inc. This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

Abstract

The question of how many shuffles are required to randomize an initially ordered deck of cards is a problem that has fascinated mathematicians, scientists, and the general public. The two principal theoretical approaches to the problem, which differed in how each defined randomness, has led to statistically different threshold numbers of shuffles. This paper reports a comprehensive experimental analysis of the card randomization problem for the purposes of determining 1) which of the two theoretical approaches made the more accurate prediction, 2) whether different statistical tests yield different threshold numbers of randomizing shuffles, and 3) whether manual or mechanical shuffling randomizes a deck more effectively for a given number of shuffles. Permutations of 52-card decks, each subjected to sets of 19 successive riffle shuffles executed manually and by an auto-shuffling device were recorded sequentially and analyzed in respect to 1) the theory of runs, 2) rank ordering, 3) serial correlation, 4) theory of rising sequences, and 5) entropy and information theory. Among the outcomes, it was found that: 1) different statistical tests were sensitive to different patterns indicative of residual order; 2) as a consequence, the threshold number of randomizing shuffles could vary widely among tests; 3) in general, manual shuffling randomized a deck better than mechanical shuffling for a given number of shuffles; and 4) the mean number of rising sequences as a function of number of manual shuffles matched very closely the theoretical predictions based on the Gilbert-Shannon-Reed (GSR) model of riffle shuffles, whereas mechanical shuffling resulted in significantly fewer rising sequences than predicted.

Keywords

Randomization of Cards, Number of Riffle Shuffles, Rising Sequences, GSR Model, Entropy and Information

1. Introduction: The Card Randomization Problem

Proposed solutions to the problem of determining the number of shuffles required to randomize a deck of cards have drawn upon concepts from probability theory, statistics, combinatorial analysis, group theory, and communication theory [1] [2]. The methods employed transcend pure mathematics, and have implications for statistical physics (e.g. random walk; diffusion theory; theory of phase transitions) [3] [4], quantum physics [5], computer science [6] [7], and other fields in which randomly generated data sequences are investigated. Not only mathematicians and scientists, but the general public as well have shown much interest in the card randomization problem, as reported in popular science periodicals and major news media [8] [9] [10] [11]. This paper reports what the author believes to be the most thorough experimental examination to date of the randomization of shuffled cards, using statistical tests previously employed in nuclear physics to search for violations of physical laws by testing different radioactive decay processes for non-randomness [12] [13] [14] [15].

1.1. Background

Probability as a coherent mathematical theory is said to have been “born in the gaming rooms of the seventeenth century” in attempts to solve one or another betting problem [16]. Among the most ancient forms of gambling are card games, which developed initially in Asia but became popular in Europe after the invention of printing [17]. Depending on what one considers a distinct game, experts in the subject estimate the number of card games to be between 1000 and 10,000 [18] [19]. Most card games are conducted under the assumption that the deck in play has been initially randomized. From a practical standpoint, a deck is considered random if players are unable to predict any sequence of cards following a revealed card. (Mathematically, there is on average 1 chance in n of guessing correctly the value of any unrevealed card in a deck of n randomly distributed cards).

The standard way to mix a deck of cards randomly is to shuffle it, for which purpose the riffle shuffle is perhaps the most widely studied form. To execute a riffle shuffle, one separates (“cuts”) the deck into two piles, then interleaves the cards by dropping them alternately from each pile to reform a single deck. The process can be performed either by hand or mechanically by an auto shuffler, like the device shown in **Figure 1** used to acquire some of the data reported in this paper. Clearly, a single riffle shuffle cannot randomize an ordered deck because the order of cards from each pile is maintained. Indeed, in a perfect riffle shuffle of an even-numbered deck, whereby the deck is cut exactly in half and 1 card is dropped alternately from each pile, there would be no randomization at all. Instead, the sequences of cards resulting from a series of perfect riffle shuffles cycle through a fixed number of permutations leading back to the original card order. For example, a pack of 52 cards recycles after only 8 perfect “out-shuffles” (*i.e.* where the top card remains on top) [20]. However, under ordinary circumstances



Figure 1. Motor-driven mechanical card shuffler used to generate auto-shuffled card sequences. Two piles of cards placed as shown are displaced from below by rotating wheels so as to drop sequentially into the central chamber.

where shuffles are not perfect, the order of the cards from each pile is degraded with each successive riffle shuffle.

The central question comprising the card randomization problem is this: How many riffle shuffles are required to randomize a deck of cards? More accurately stated: After how many shuffles can one detect no evidence of non-randomness? Various researchers have studied this question theoretically and arrived at statistically different answers, depending on the adopted measure of randomness. In the analysis of Bayer and Diaconis [1], the measure of randomness of the deck is the so-called variation distance (VD) [4] [21] between the probability density $Q_{n,m}$ of n cards shuffled m times and the uniform density $U_n = 1/n!$ of the permutation group S_n of n distinct objects. In the limit of large n , the VD analysis predicted that

$$m_{\text{VD}}(n) \approx \frac{3}{2} \log_2(n) \quad (1)$$

shuffles should adequately randomize a deck of n cards. Thus $m_{\text{VD}}(52)$ is about 8 - 9. According to [1], VD quantifies the mean rate at which a gambler could expect to win against a fair house by exploiting any residual pattern of the cards. The researchers also showed that the VD between $Q_{n,m}$ and U_n takes the form

$$\|Q_{n,m} - U_n\| = 1 - \frac{2}{\sqrt{2\pi}} \int_{-\infty}^{-1/4\sqrt{3}} e^{-\frac{t^2}{2}} dt \approx 0.115 \quad (2)$$

for large n with m given by Equation (1). For complete randomness, the VD would equal 0.

In a numerical analysis by Trefethen and Trefethen [2], the adopted measure of randomness was based on the Shannon entropy of the deck in the sense of information theory [22] [23]. If p_j ($j = 1, \dots, n!$) is the probability of the j^{th} permutation of S_n , then the Shannon entropy of the deck is given by

$$H = -\sum_{j=1}^{n!} p_j \log_2 p_j \quad (3)$$

where, by completeness,

$$\sum_{j=1}^{n!} p_j = 1, \quad (4)$$

and the information associated with the set of probabilities $\{p_j\}$ was defined as

$$I_n = \log_2(n!) - H. \quad (5)$$

According to [2] I_n in Equation (5) quantifies the rate at which an ideally competent coder could expect to transmit information if the signals were encoded in shuffled decks of cards. In the limit of large n , the information theoretic (IT) calculation predicted that

$$m_{\text{IT}}(n) \approx \log_2(n) \quad (6)$$

shuffles should adequately randomize a deck of n cards. Thus $m_{\text{IT}}(52)$ is about 5 - 6, in contrast to $m_{\text{VD}}(52)$. The numerically obtained results of [2] were subsequently proved theoretically by another research group [24].

The structure of relation (5) provides a mathematical definition of the word “information” consistent with its general vernacular use. If there is no uncertainty in the communication of any n -symbol message based on card sequence, then $p_j = 1$ for each permutation j . In that case $H = 0$ and the information $I_n = \log_2 n!$ is maximum. If, however, every message received is completely uncertain as to card order, then $p_j = 1/n!$ for each permutation j , and therefore, by use of Equation (4), the information $I_n = 0$. Alternatively [25], physicists and other scientists usually associate the concept of information with entropy H , Equation (3). The rationale is that the greater the uncertainty (*i.e.* H) of a message or physical system, the more information one gains by a binary decision (or measurement) that reduces the uncertainty. In a system with perfect order, $H = 0$; the outcome of any measurement or decision is completely predictable, and therefore no new information is to be gained. Both definitions of information prove useful later in the paper (Section 3.4).

Although the two analyses [1] and [2] led to statistically different distributions of randomness as a function of shuffle number, they both started from the same mathematical model of shuffling, referred to as the GSR shuffle, named for Gilbert and Shannon [26] and, independently, for Reeds [27]. The GSR shuffle involves the following steps. The deck is cut roughly in half according to a binomial distribution in which the probability that a pile contains k out of n cards is $2^{-n} C_k^n$ where

$$C_k^n \equiv \frac{n!}{k!(n-k)!} \quad (7)$$

is the binomial combinatorial coefficient. The two halves are then riffled together such that the probability of a card being dropped from a pile is proportional to the number of cards in the pile.

1.2. Outline of Paper

The research literature on the randomization of cards by shuffling is vast. An

extensive list of references that survey the development of the problem, of which virtually all papers are theoretical analyses or numerical modeling by computer simulation, can be found in [28]. To the best of the author's knowledge, there has been no comprehensive, systematic experimental examination of the card ordering and patterns produced by manual shuffling to test whether the results conform to the GSR model or support the published theoretical predictions.

This paper reports on an extensive set of tests by which was measured the progression toward randomness of card sequences produced in multiple riffle shuffles manually and, for comparison, by a mechanical auto shuffler.

The basic theory and experimental outcomes of the following measures of randomness are discussed in Section 2: 1) runs with respect to the mean, 2) runs up/down, 3) rank ordering, 4) serial correlation (lag 1), and 5) theory of rising sequences.

Analysis of the data by information theory is discussed in Section 3.

Conclusions are presented in Section 4.

2. Experiment and Statistical Tests

Experiments were undertaken to examine the permutations of card order in a deck of $n = 52$ cards as a function of shuffle number m for $m = 0, 1, \dots, M$ implemented N times. For the experiments reported here, the number of shuffles per set is $M = 19$ and the number of sets is $N = 12$. In addition to manual shuffles, the experiments were also carried out with the mechanical auto shuffler of **Figure 1**. The cards used in manual shuffling were not new, but had already been flexed many times previously in play and were therefore more pliant than stiff new cards. This requirement was irrelevant for auto shuffling, since the cards were flat, not flexed, when distributed by the machine into two piles. A sample of the data obtained from one set of M shuffles is shown in **Table 1**.

The experiment began with an ordered deck (column $m = 0$, highlighted in red), with card values increasing from 1 (top card) to 52 (bottom card). Permutations of card order for each shuffle $m = 1, 2, \dots, M$ are recorded sequentially in columns from left to right. A cursory examination of the table immediately reveals patterns of ascending sequences (highlighted in yellow) and descending sequences (highlighted in green) that extend across all the columns. Each of the N sets of card shuffles was subject to a variety of statistical tests to quantify the non-randomness of the permuted orderings indicated by these and other patterns.

2.1. Theory of Runs

A run is defined as a succession of similar events preceded and succeeded by a different event. For example, the sequence of 12 symbols

$$b \ b \ a \ a \ b \ b \ b \ a \ b \ a \ b$$

contains:

Table 1. Card sequences after 19 riffle shuffles of an initially ordered deck.

Shuffle Number		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Card Value	1	1	38	38	38	13	13	50	50	50	50	50	50	50	50	50	50	14	14	23	23
	2	2	39	39	39	18	18	20	20	41	41	41	41	41	41	51	50	50	30	30	30
	3	3	40	40	40	32	32	23	23	20	21	21	43	42	42	41	51	51	22	22	22
	4	4	41	41	5	38	19	24	24	23	47	47	44	39	39	42	49	49	19	19	19
	5	5	42	42	6	39	12	13	13	24	22	22	37	28	28	39	10	2	32	31	31
	6	6	43	20	29	40	38	31	31	13	3	3	29	17	17	28	37	46	14	13	13
	7	32	44	21	30	5	39	18	28	31	1	1	21	26	45	17	15	5	50	4	4
	8	7	45	47	41	15	40	32	25	27	20	11	18	30	4	45	6	35	51	36	36
	9	33	32	22	42	6	5	16	34	12	23	25	47	43	36	40	29	4	49	26	26
	10	34	1	8	20	29	33	1	35	38	24	34	22	44	26	25	41	36	27	32	32
	11	35	2	9	31	30	34	2	52	39	13	35	27	37	30	34	42	26	21	33	33
	12	36	3	43	25	41	35	46	15	28	31	42	48	29	43	35	39	33	1	14	14
	13	8	4	44	21	42	15	19	6	25	14	17	19	21	44	4	28	10	48	50	50
	14	9	5	45	47	51	6	27	29	34	7	51	32	18	16	36	17	37	7	51	51
	15	28	6	28	22	20	29	12	18	35	43	20	4	47	3	26	27	15	45	49	49
	16	10	16	32	8	23	48	38	48	42	44	23	36	22	49	20	21	6	2	9	9
	17	11	46	23	9	24	49	39	32	51	37	24	16	51	10	23	1	29	40	10	10
	18	12	17	24	26	31	30	40	16	52	27	13	3	40	37	30	48	20	46	37	37
	19	29	18	10	50	10	41	5	1	15	12	31	1	20	29	43	7	11	5	15	15
	20	30	7	11	16	11	42	43	14	6	38	49	11	23	21	44	45	47	43	6	6
	21	31	19	12	46	25	51	44	7	8	39	2	25	24	1	24	40	41	44	29	29
	22	13	33	48	43	14	8	45	37	29	28	52	34	13	18	13	38	42	38	27	27
	23	14	34	49	44	7	9	10	17	18	45	14	35	27	2	16	9	39	35	21	21
	24	15	35	1	45	21	26	11	49	48	10	15	12	48	5	3	8	28	24	1	1
	25	37	36	2	28	47	50	33	2	32	11	6	38	19	11	12	18	17	31	48	48
	26	38	20	3	17	22	20	28	46	16	25	7	9	32	47	14	25	23	13	20	20
	27	39	21	4	13	19	23	25	19	40	34	8	33	31	22	49	34	30	4	7	7
	28	40	47	5	18	12	24	34	30	5	35	46	42	45	52	10	2	22	36	16	16
	29	41	22	6	32	33	31	35	41	21	42	43	39	4	51	37	46	19	26	3	3
	30	42	8	29	14	34	16	52	27	47	17	44	28	36	40	15	5	32	33	8	8
	31	43	9	30	15	35	1	15	12	22	51	37	17	16	25	6	35	27	9	18	18
	32	44	28	31	51	48	2	6	38	3	49	29	26	3	34	29	4	21	10	12	12
	33	45	23	25	23	49	46	29	39	1	2	18	30	49	35	27	36	1	37	11	11
	34	16	24	26	24	8	27	48	42	14	52	27	51	10	20	21	26	48	15	45	45
	35	46	10	50	10	9	43	14	51	7	15	48	40	1	23	1	33	7	6	2	2
	36	17	11	16	11	26	44	7	8	43	6	19	20	2	24	48	20	45	29	40	40
	37	18	12	46	7	50	45	37	40	44	8	32	23	5	13	7	11	40	20	47	47
	38	19	48	17	19	16	10	17	5	37	46	4	24	11	12	38	47	43	16	41	41
	39	20	49	13	12	1	11	49	21	45	29	36	13	52	14	9	23	44	3	42	42
	40	21	29	18	33	2	28	30	47	10	18	16	31	25	15	8	30	38	8	39	39
	41	47	30	14	34	46	25	41	22	11	48	12	45	34	6	18	22	24	18	28	28
	42	22	31	15	35	27	52	42	3	17	19	38	49	35	27	2	19	31	12	17	17
	43	23	25	51	48	43	14	51	43	49	32	9	10	12	48	46	32	13	11	46	46
	44	24	26	7	49	44	7	8	44	2	4	33	2	14	7	5	43	9	47	5	5
	45	48	50	19	1	45	37	21	45	46	36	39	5	15	38	33	44	16	41	52	52
	46	49	13	33	2	28	17	47	10	19	16	28	52	6	9	11	24	3	42	43	43
	47	25	14	34	27	52	21	22	11	4	9	26	14	7	8	47	31	8	39	44	44
	48	26	15	35	52	37	47	3	4	36	33	30	15	38	46	22	13	18	28	38	38
	49	50	51	27	37	17	22	4	36	9	26	40	6	9	33	19	16	12	17	35	35
	50	51	27	52	3	3	3	36	9	33	30	45	7	8	19	32	3	52	52	24	24
	51	27	52	37	4	4	4	9	33	26	40	10	8	46	32	31	12	25	25	25	25
	52	52	37	36	36	36	36	26	26	30	5	5	46	33	31	52	52	34	34	34	34

- 2 runs of a of length 1
 - 2 runs of b of length 1
 - 1 run of b of length 2
 - 1 run of a of length 3
 - 1 run of b of length 3
- (8)

or a total of 7 runs. If a sequence is random, then all permutations of symbol order should have the same probability of occurrence. From this invariance principle, as applied to a sequence containing n_a symbols of type a , n_b symbols of type b , and $n = n_a + n_b$ symbols in all, it can be deduced that [29]:

- the mean number of runs of a of length precisely k (where $k \geq 1$) is

$$\bar{r}_{ka} = \frac{n_a! n_b! (n_b + 1)(n - k - 1)!}{(n_a - k)! n!} \quad (9)$$

- the mean number of runs of a of length k or greater (*i.e.* inclusive runs) is

$$\bar{R}_{ka} = \frac{n_a!(n_b+1)(n-k)!}{(n_a-k)!n!} \quad (10)$$

- the mean number of total runs of both kinds is

$$\bar{R} = \bar{R}_{1a} + \bar{R}_{1b} = \frac{n + 2n_a n_b}{n}. \quad (11)$$

Expressions for \bar{r}_{kb} , \bar{R}_{kb} follow, *mutatis mutandis*, from Equation (9) and Equation (10). Proofs of these expressions are given in [30] [31].

Two methods were employed in this paper to generate runs of binary symbols from the experimentally recorded sequences of digital card values.

2.1.1. Target Runs

The card value x_i ($i = 1, \dots, n$) at location i in the sequence resulting from a particular shuffle is compared with a target value X , here taken to be the mean

$$X = \frac{1}{n} \sum_{i=1}^n x_i \rightarrow 26.5 \quad (12)$$

which reduces as shown for the case $n = 52$ with set of card values $\{x = 1, 2, \dots, 52\}$. If $x_i < X$, the symbol 0 is assigned to location i ; if $x_i > X$, the symbol 1 is assigned to location i . Because the set $\{x_i\}$ is comprised of integers, the event $x_i = X$ cannot occur. Moreover, the set is equally partitioned:

$$n_1 = n_0 = \frac{1}{2}n,$$

and the mean number of total runs, Equation (11), reduces to

$$\bar{R}_{\text{mean}} = \frac{n+2}{2} \rightarrow 27 \quad (13)$$

where the numerical value again applies to the case of $n = 52$.

The associated variance (with corresponding standard deviation) is given by [29]

$$\begin{aligned} \sigma_{\text{mean}}^2 &\approx \frac{n}{4} \left(1 - \frac{1}{n-1} \right) \approx \frac{n-1}{4} \\ \sigma_{\text{mean}} &\rightarrow 3.57 \end{aligned} \quad (14)$$

with numerical evaluation for $n = 52$. It can also be shown that the test statistic

$$z_{\text{mean}} = \frac{R - \bar{R}_{\text{mean}}}{\sigma_{\text{mean}}} \rightarrow N(0,1) \quad (15)$$

for the observed total number of runs is approximately Gaussian for sufficiently large n . The symbol $N(0,1)$ designates the standard normal distribution of mean 0 and variance 1.

As an example, consider the 10-card decimal sequence generated by a uniform random number generator (RNG) over the integer range (1 ... 52):

$$x = \{29 \ 47 \ 45 \ 32 \ 6 \ 34 \ 44 \ 36 \ 38 \ 5\} \quad (16)$$

The resulting binary series with target taken to be the mean (12) is then

$$y_{\text{mean}} = \{1 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1 \ 0\} \quad (17)$$

which comprises the following set of target runs

$$\begin{aligned} &2 \text{ runs of } 0 \text{ of length } 1 \\ &2 \text{ runs of } 1 \text{ of length } 4 \end{aligned} \quad (18)$$

for a total of 4 runs with respect to the mean.

For a long equipartitioned sequence ($n_1 = n_0 \gg 1$), the contribution of runs at the start or end of a sequence becomes negligible compared with the number of runs within the sequence, and Equation (9) and Equation (10) may be approximated as follows [32]

$$\bar{r}_{ka} \approx \frac{n}{2^{k+2}} \quad (19)$$

$$\bar{R}_{ka} \approx \frac{n}{2^{k+1}}. \quad (20)$$

Equation (19) and Equation (20) are illustrative of the general exact relation

$$\bar{r}_{ka} = \bar{R}_{ka} - \bar{R}_{(k+1)a} \quad (21)$$

that follows from the definitions of \bar{r}_{ka} and \bar{R}_{ka} .

2.1.2. Runs Up/Down (or Difference Runs)

An alternative method of generating sequences of binary symbols that provides an independent test for non-random symbol patterns is to calculate sequential differences of the card values as follows

$$y_j = x_{j+1} - x_j \quad (j = 1, \dots, n-1) \quad (22)$$

and assign 1 to a positive difference ($y_j > 0$) and 0 to a negative difference ($y_j < 0$). Since there is no repeating integer in the set $\{x_i\}$, the value $y_j = 0$ cannot occur. Thus, a sequence of 52 card values is transformed into a sequence of 51 binary difference values.

For example, consider again the 10-card decimal sequence (16):

$$x = \{29 \ 47 \ 45 \ 32 \ 6 \ 34 \ 44 \ 36 \ 38 \ 5\}. \quad (23)$$

The resulting binary difference series is then

$$y_{\text{diff}} = \{1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0\} \quad (24)$$

which comprises the following set of up/down runs

$$\begin{aligned} &2 \text{ runs of } 1 \text{ of length } 1 \\ &2 \text{ runs of } 0 \text{ of length } 1 \\ &1 \text{ run of } 1 \text{ of length } 2 \\ &1 \text{ run of } 0 \text{ of length } 3 \end{aligned} \quad (25)$$

for a total of 6 up/down runs.

Comparison of binary sequences (24), (17) and corresponding runs tabulations (25), (18) illustrates how the same decimal sequence (16) can lead to com-

pletely different outcomes of up/down and target runs tests. Thus, the two kinds of runs procedures independently test the same decimal sequence for different symbol patterns.

A major difference between the target runs and the up/down runs is that variates in the former (e.g. series (17)) are realizations of Bernoulli random variables (*i.e.* the probability of occurrence is the same irrespective of location within the series), whereas the variates in the latter (e.g. series (24)) are not. For up/down runs, the greater the length of a run, the less probable is the occurrence of yet another symbol of the same kind. The expectation values of up/down runs, therefore, differ from those of target runs. Instead, the expressions corresponding to (9)-(11) are [29]:

- the mean number of up and down runs of length precisely k (where $k \leq n-2$) is

$$\bar{r}_k = \frac{2}{(k+3)!} \left[n(k^2 + 3k + 1) - (k^3 + 3k^2 - k - 4) \right] \quad (26)$$

- the mean number of up and down runs of length k or greater (where $k \leq n-1$) is

$$\bar{R}_k = \frac{2}{(k+2)!} \left[n(k+1) - (k^2 + k - 1) \right] \quad (27)$$

- the mean total number of up and down runs is

$$\bar{R}_{u/d} = \frac{1}{3}(2n-1) \rightarrow 34.33 \quad (28)$$

with associated variance and standard deviation

$$\begin{aligned} \sigma_{u/d}^2 &= \frac{1}{90}(16n-29) \\ \sigma_{u/d} &\rightarrow 2.99 \end{aligned} \quad (29)$$

Evaluations in Equation (28) and Equation (29) pertain to $n = 52$. The statistic

$$z_{u/d} = \frac{R - \bar{R}_{u/d}}{\sigma_{u/d}} \rightarrow N(0,1) \quad (30)$$

is again approximately normally distributed.

2.1.3. Runs Tests of Shuffled Cards

The total numbers of target runs and up/down runs were calculated as a function of shuffle number for each of the N sets of M shuffles, such as exemplified by **Table 1**. Note that the ascending sequences (yellow) and descending sequences (green) respectively correspond to examples of up and down runs. The mean of the N values for each shuffle number was then calculated and converted to standard normal forms expressed by (15) and (30). **Figure 2** shows plots of $\langle z_{\text{mean}} \rangle$ in frame A and $\langle z_{u/d} \rangle$ in frame B as a function of shuffle number. Examination of the figure shows that, when gauged by runs, the deck of cards becomes randomized after a threshold of about 7 - 8 shuffles, where, by the definition adopted here, the point of randomization occurs when the standard normal

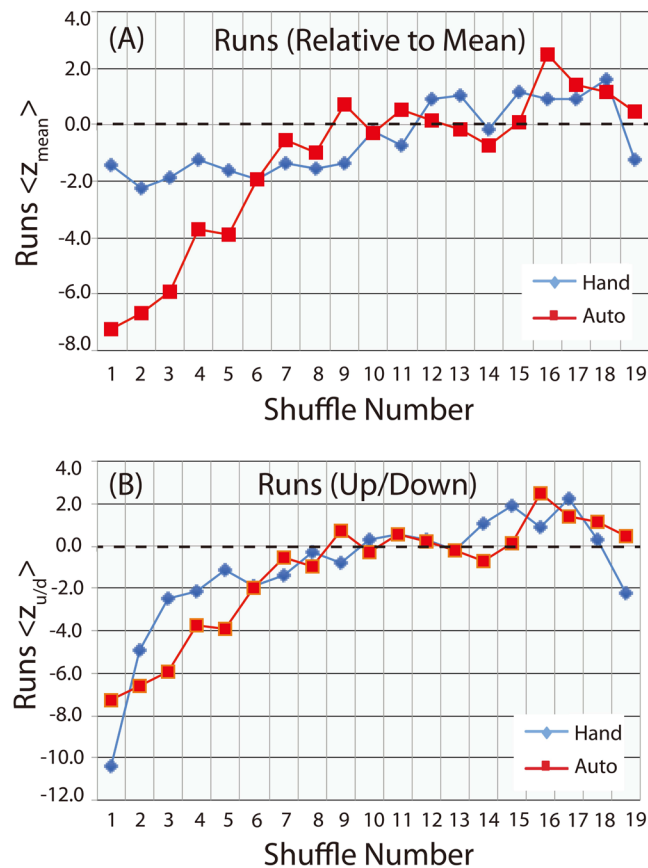


Figure 2. Runs statistics as a function of number of shuffles obtained by hand (blue curve) and machine (red curve) for (A) runs relative to the mean and (B) runs up/down. Values within about ± 1 standard deviation of the expected value 0 can be taken to indicate a randomly ordered deck.

statistic $|z| \leq 1$. Also, for shuffle numbers below threshold, decks shuffled by hand (blue curves) manifested greater disorder than decks mixed by the auto shuffler (red curves).

2.2. Rank Correlation (or Rank Order)

The Spearman rank correlation coefficient r_s is a nonparametric measure of the association between two random variables X and Y as defined by their rank order in a sequence of n pairs [33]

$$r_s = 1 - \frac{6 \sum_{i=1}^n D_i^2}{n(n^2 - 1)} \quad (31)$$

in which

$$D_i = r(x_i) - r(y_i) \quad (32)$$

is the difference between the ranks assigned to samples x_i and y_i (When a distinction is necessary, lower case letters (e.g. x) represent realizations of the abstract random variable which is usually expressed by an upper case letter (e.g.

X)).

Values of r_s range from -1 to $+1$, respectively signifying perfect anti-correlation (*i.e.* reverse rankings) and perfect correlation. It is r_s^2 , however, rather than r_s , that has a statistical interpretation; r_s^2 is a measure of the variability of the data attributable to the correlation between variables X and Y [34]. Thus a relatively high correlation coefficient such as $r_s = 0.7$, means that only 49% of the variability is accounted for by the association between X and Y .

For independent variables (and therefore uncorrelated ranks), the expectation value and variance are respectively

$$\langle r_s \rangle = 0 \quad (33)$$

$$\sigma_{r_s}^2 = \frac{1}{n-1}, \quad (34)$$

and the test statistic

$$z_{\text{rank}} = \frac{r_s - \langle r_s \rangle}{\sigma_{r_s}} = r_s \sqrt{n-1} \rightarrow N(0,1) \quad (35)$$

follows a standard normal distribution to good approximation [35].

Applied to the shuffling of cards, the variable Y signifies the initial card sequence $\{y_i\}_{m=0} = \{1, 2, \dots, 52\}$ and variable X signifies the card sequence $\{x_i\}_m = \{x_1, \dots, x_n\}$ of the m^{th} shuffle. Since the face values of the cards range from 1 to 52, the rank of a card is equal to its face value. Therefore an equivalent, but simpler, way to perform the rank correlation test is to calculate the cross correlation of ranks

$$C_{\text{rank}} \equiv \sum_{j=1}^n r(x_j) r(y_j) = \sum_{j=1}^n j r(x_j) \quad (36)$$

where the second equality in (36) pertains specifically to the sequence of cards in a deck of n cards. The expectation value and variance of C_{rank} are respectively

$$\langle C_{\text{rank}} \rangle = \frac{1}{4} n(n+1)^2 \rightarrow 36517 \quad (37)$$

$$\sigma_{\text{rank}}^2 = \frac{1}{444} (n-1)n^2(n+1)^2 \quad (38)$$

$$\sigma_{\text{rank}} \rightarrow 1640.15$$

with numerical evaluations for $n = 52$. The test statistic

$$z_{\text{rank}} = \frac{C_{\text{rank}} - \langle C_{\text{rank}} \rangle}{\sigma_{\text{rank}}} \quad (39)$$

can be shown to be identical to that of Equation (35) [33].

Figure 3 shows a plot of $\langle z_{\text{rank}} \rangle$, *i.e.* Equation (35) or (39) averaged over the N sets of data for each shuffle number m for both manual (blue) and auto (red) shuffled cards. The correlation between the card sequence of the m^{th} shuffle and the initial card sequence ($m = 0$) is interpreted as statistically 0 (*i.e.* for $|z_{\text{rank}}| \leq 1$) starting at about $m = 6$ or 7.

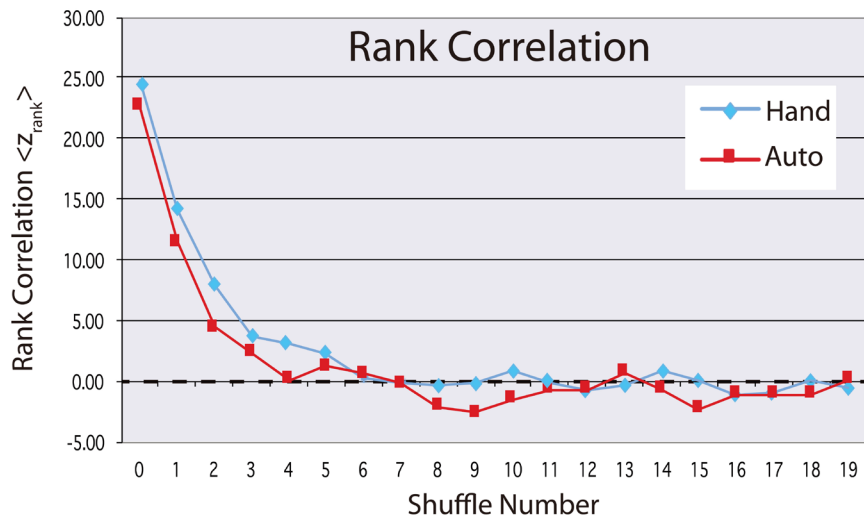


Figure 3. Rank ordering statistics as a function of shuffle number for manually (blue) and auto (red) shuffled cards. Values within about ± 1 standard deviation of the expected value 0 can be taken to indicate a randomly ordered deck.

2.3. Serial Correlation Lag-1

Serial correlation refers to the relationship between elements of the same series separated by a fixed interval. Given a sequence of elements $\{x_j\}$ for $j = 1, 2, \dots, n$, the serial correlation coefficient lag- k is defined by [36]

$$\rho_k = \frac{\sum_{j=1}^n x_j x_{j+k} - \frac{1}{n} \left(\sum_{j=1}^n x_j \right)^2}{\sum_{j=1}^n x_j^2 - \frac{1}{n} \left(\sum_{j=1}^n x_j \right)^2} \quad (40)$$

where x_{j+k} is to be replaced by x_{j+k-n} for all values of j such that $j+k > n$.

For the purpose of testing correlations in card order following shuffling, the most useful serial coefficient is ρ_1 , which measures the correlations between pairs of consecutive cards. It can be shown, however, that a test based upon the simpler statistic [37]

$$c_1 = \sum_{j=1}^n x_j x_{j+1} \quad (41)$$

is equivalent to a test based on ρ_1 . The mean and variance of c_1 are given by the following expressions [36] [37]

$$\langle c_1 \rangle = \frac{S_1^2 - S_2}{n-1} \quad (42)$$

$$\sigma_{c_1}^2 = \frac{S_2^2 - S_4}{n-1} + \frac{S_1^4 - 4S_1^2 S_2 + 4S_1 S_3 + S_2^2 - 2S_4}{(n-1)(n-2)} \quad (43)$$

where

$$S_k = \sum_{j=1}^n x_j^k. \quad (44)$$

For large n , the statistic

$$z_{\text{serial}} = \frac{c_1 - \langle c_1 \rangle}{\sigma_{c_1}} \quad (45)$$

follows a standard normal distribution to good approximation.

Figure 4 shows a plot of $\langle z_{\text{serial}} \rangle$, *i.e.* Equation (45) averaged over the N sets of data for each shuffle number m for both manually (blue) and auto (red) shuffled cards. The correlation between the card sequence of the m^{th} shuffle and the initial card sequence ($m = 0$) is interpreted as statistically 0 (*i.e.* for $|z_{\text{serial}}| \leq 1$) starting at about $m = 8$ (manual) and $m = 16$ (auto).

2.4. Rising Sequences

A rising sequence, as defined in [1], is a maximal consecutively increasing subset of an arrangement of cards. For example, consider a hand of 8 cards with the sequence of face values: 1 6 2 3 7 8 4 5. By displaying the cards in the following way

$$\{x_i\} = \left\{ \begin{array}{cccccc} 1 & & 2 & 3 & & 4 & 5 \\ & 6 & & & 7 & 8 & \end{array} \right\} \quad (46)$$

one sees that the hand consists of two rising sequences (1,2,3,4,5) and (6,7,8) interleaved together. Successive riffle shuffles tend to double the number of rising sequences up to a maximum number of $\frac{1}{2}(n+1)$ in the limit of an infinite number of shuffles. Note that a rising sequence is different from an ascending sequence (*i.e.* a run up): 1) The elements of a run up merely ascend, but do not have to increment successively; 2) The elements of a rising sequence do not have to be contiguous (as in a run), but can be separated by other elements.

It is shown in [1] that the probability of a particular permutation following a

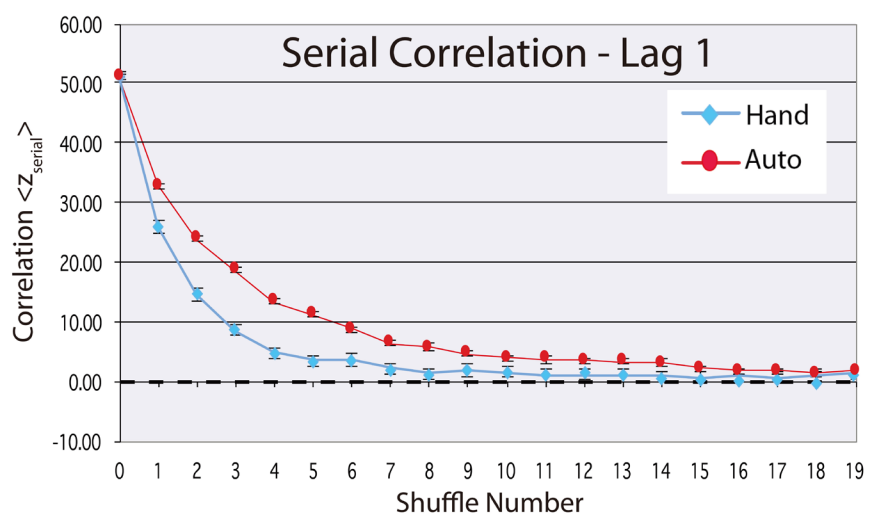


Figure 4. Serial correlation lag-1 as a function of shuffle number for manually (blue) and auto (red) shuffled cards. Values within about ± 1 standard deviation of the expected value 0 can be taken to indicate a randomly ordered deck.

riffle shuffle depends only on the deck size n and the number r of rising sequences in the permutation. Specifically, the probability that the m^{th} riffle shuffle of an ordered deck has r rising sequences is

$$Q_{n,m}(r) = \frac{1}{2^{mn}} C_n^{2+n-r}. \quad (47)$$

The mean number of rising sequences in the permutation following m shuffles is then given by

$$\langle r_{n,m} \rangle = \sum_{r=1}^n r E_n(r) Q_{n,m}(r) \quad (48)$$

where the Eulerian number [38]

$$E_n(r) = \sum_{j=1}^{r+1} (-1)^{r-j} j^n C_{r-j}^{n+1} \quad (49)$$

is the number of permutations containing r rising sequences. Substitution of Equation (49) into Equation (48) leads to the simpler expression [39]

$$\langle r_{n,m} \rangle = 2^m - \frac{n+1}{2^{mn}} \sum_{r=1}^{2^m-1} r^n. \quad (50)$$

The sum of powers of an uninterrupted sequence of positive integers, such as contained in expression (50), is given by Faulhaber's formula [40]

$$\sum_{r=1}^R r^n = \frac{R^{n+1}}{n+1} + \frac{1}{2} R^n + \sum_{k=2}^n \frac{B_k}{k!} \frac{n!}{(n-k+1)!} R^{n-k+1} \quad (51)$$

in which B_k is a Bernoulli number, defined by the generating function [41]

$$\frac{t}{e^t - 1} = \frac{t}{2} (\coth(t/2) - 1) = \sum_{k=0}^{\infty} \frac{B_k t^k}{k!} \quad (52)$$

and given explicitly by

$$B_0 = 1 \quad B_1 = -\frac{1}{2} \quad B_k = \begin{cases} 0 & k = 3, 5, 7, \dots \\ -(-1)^{k/2} (2\pi)^{-k} 2k! \zeta(k) & k = 2, 4, 6, \dots \end{cases} \quad (53)$$

where the Riemann zeta function is defined by (Ref. [41], pp. 329-330)

$$\zeta(p) = \sum_{k=1}^{\infty} k^{-p}. \quad (54)$$

In the limit $R \rightarrow \infty$, the sum in the right side of Equation (51) becomes negligible, and therefore

$$\lim_{R \rightarrow \infty} \sum_{r=1}^R r^n \rightarrow \frac{R^{n+1}}{n+1} - \frac{1}{2} R^n. \quad (55)$$

Substitution of relation (55) into (50) with $R = 2^m$ leads to the asymptotic number of rising sequences after an infinite number of riffle shuffles

$$\lim_{m \rightarrow \infty} \langle r_{n,m} \rangle = r_{n,\infty} = \frac{1}{2} (n+1) \rightarrow 26.5 \quad (56)$$

as stated without proof at the start of this section. The numerical evaluation pertains to a deck with $n = 52$.

The mean-square number of rising sequences for m shuffles can be calculated numerically from Equation (47) and Equation (49)

$$\langle r_{n,m}^2 \rangle = \sum_{r=1}^n r^2 E_n(r) Q_{n,m}(r) \quad (57)$$

from which follows, also numerically, the theoretical (*i.e.* population) variance

$$\sigma_{n,m}^2 = \langle r_{n,m}^2 \rangle - \langle r_{n,m} \rangle^2. \quad (58)$$

The author was unable to determine an analytical closed-form expression for (57) or (58).

Table 2 summarizes the relevant statistics of rising sequences based on the GSR model as a function of shuffle number m for a deck of 52 cards. It is seen that about 13 shuffles are required to achieve the asymptotic result of Equation (56). In **Figure 5** the theoretically predicted mean number of rising sequences

Table 2. Statistics of Rising Sequences in a deck of 52 cards.

Shuffle Number m	Mean $\langle r_{52,m} \rangle$	Mean Square $\langle r_{52,m}^2 \rangle$	Standard Deviation $\sigma_{52,m}$
0	1	1	0
1	2	4	0
2	4	15.9999	0.0041
3	7.9489	63.2337	0.2224
4	14.0994	199.9632	1.0814
5	19.6053	387.4865	1.7657
6	22.9482	530.6637	2.0110
7	24.7104	614.9224	2.0785
8	25.6034	659.9288	2.0958
9	26.0515	683.0915	2.1001
10	26.2757	694.8289	2.1012
11	26.3879	700.7354	2.1015
12	26.4439	703.6980	2.1016
13	26.4720	705.1815	2.1016
14	26.4860	705.9239	2.1016
15	26.4930	706.2952	2.1016
16	26.4965	706.4809	2.1016
17	26.4982	706.5738	2.1016
18	26.4991	706.6202	2.1016
19	26.4996	706.6435	2.1016
20	26.4998	706.6550	2.1016

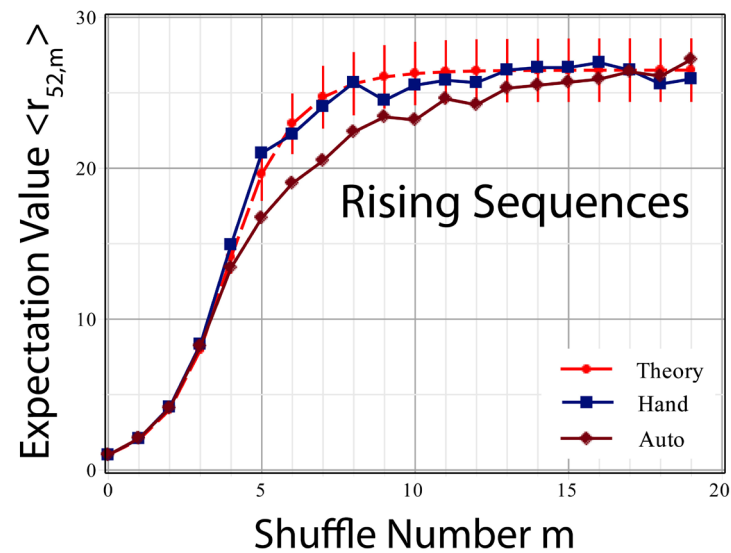


Figure 5. Mean number of rising sequences for manual (blue) and auto (burgundy) shuffling as a function of shuffle number. Superposed is the theoretical (red) mean and uncertainty (± 1 standard deviation) predicted for the GSR model of the riffle shuffle.

$\langle r_{n,m} \rangle$ is compared with the observed numbers obtained by manually and auto shuffled cards averaged over the N data sets. Several features are to be noted:

- In contrast to the statistical behavior graphically displayed in preceding figures which showed gradual randomization with increasing shuffle number m , the mean number of rising sequences underwent a relatively abrupt transition from a non-random state to the asymptotically random state at a threshold shuffle number $m = 7$ or 8 for manual shuffles and $m = 11$ or 12 for auto shuffles.
- For $m < 4$, the three curves (theory, manual shuffle, auto shuffle) yielded virtually identical results.

For $m \geq 5$, the rising sequences due to manual shuffling were statistically coincident with theoretical predictions, whereas shuffling by machine yielded too few rising sequences at each shuffle number up to the asymptotic number $m_A \approx 13$. This feature suggests one can randomize a deck better by shuffling it manually than by use of a mechanical auto shuffling device like that in **Figure 1**.

3. Entropy and Information Loss

3.1. Entropy of Rising Sequences

As discussed briefly in Section 1.1, the Shannon entropy of a set of n symbols is given by

$$H = -\sum_{j=1}^{n!} p_j \log_2 p_j \quad (59)$$

where p_j ($j = 1, \dots, n!$) is the probability of the j^{th} permutation of the $n!$ total number of ways to permute the symbols. By completeness, the set of probabilities $\{p_j\}$ satisfies Equation (4). Multiplied by a universal physical constant

(Boltzmann's constant k_B), the Shannon entropy, usually expressed in terms of natural logarithms, provides the basis for deriving the partition function—and therefore all the thermodynamic potentials—of equilibrium statistical mechanics [42]. From a physicist's perspective, H is a universal measure of the disorder of a system, maximum randomization occurring when all p_j are equal. For a maximally randomized system of $n = 52$ symbols, $H = \log_2 n! \approx 225.58$ bits.

Although Equation (59) yields the entropy of a sequence of n distinct uncorrelated symbols, it does not predict the entropy correctly when the permutations are constrained by rules that create correlations among the symbols. To chart the increasing disorder in a system of n cards as a function of the number m of riffle shuffles one can calculate the entropy of all configurations of a fixed number r of rising sequences and then sum that entropy over the total number of rising sequences produced in the shuffle. In this case, the relevant probability function is

$$p_{n,m}(r) = E_n(r) Q_{n,m}(r) \quad (60)$$

with expressions for $E_n(r)$ and $Q_{n,m}(r)$ given respectively by Equation (49) and Equation (47). This procedure leads to a much *lower* maximum entropy than Equation (59) because it respects the constraints imposed on possible orderings by the physical mechanism of the riffle shuffle. It has been shown that the possible outcomes to m riffle shuffles of an ordered deck are equivalent to the outcomes of cutting a deck into 2^m packets and interleaving the cards from different packets in such a way that the cards from each packet maintain their relative order among themselves [1] [39].

Figure 6 shows the variation in $p_{n,m}(r)$ as a function of r for various increasing values of m . In the limit of large m , which for all practical purposes

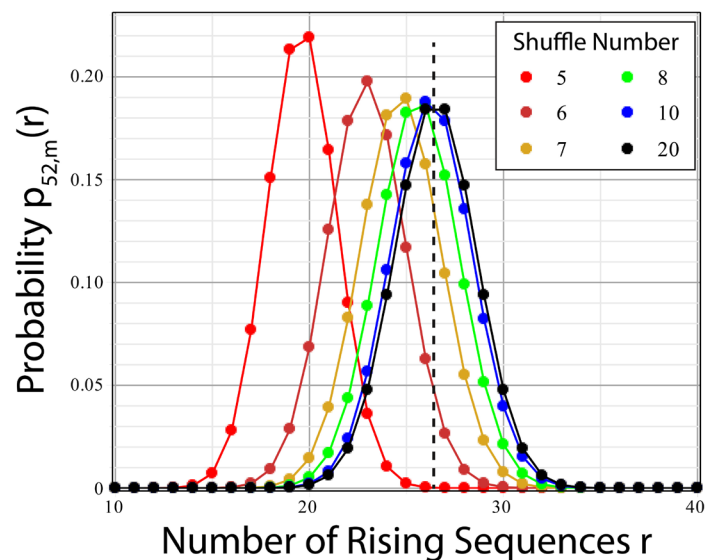


Figure 6. Probability that m riffle shuffles of an ordered deck of $n = 52$ cards produces a card permutation with r rising sequences. Density functions are plotted for shuffle numbers $m = 5$ (red), 6 (orange), 7 (yellow), 8 (green), 10 (blue), 20 (black). The vertical dashed line marks the asymptotic shuffle number $m_\infty = 26.5$. The probability function is discrete; connecting lines serve only to facilitate visualization.

starts at about $m = 10$ (blue curve), the distribution over r is a nearly perfect Gaussian function, shown by the dashed red curve in **Figure 7**, centered on the asymptotic number of rising shuffles, Equation (56), marked in the figures by a vertical black dashed line. The width (*i.e.* standard deviation) of the Gaussian is approximately 2.10, as given in **Table 2** for $m \geq 9$.

The entropy of a deck of n cards as a function of shuffle number m , calculated from the probability distribution (60), takes the form

$$H_{n,m} = -\sum_{r=0}^n p_{n,m}(r) \log_2 p_{n,m}(r) \quad (61)$$

and is plotted in **Figure 8** for decks of size $n = 14, 26$, and 52 . The transition between initial complete order $H_{n,0} = 0$ and maximum disorder is sharp like a phase transition, such as exhibited by the mean number of rising sequence in **Figure 5**. For $n = 52$, the maximum entropy $H_{52,m \geq 7} \approx 3.12$ bits is reached by the 7th shuffle.

3.2. Conditional Entropy

Equation (61) yields the total entropy of a card deck subject to m riffle shuffles. However, it does not provide information on the randomization of specific card associations, which is the kind of information that serious players might rely on for advantage in competition or gambling. For this purpose, the conditional entropy of pairs of ordered sequences was determined experimentally.

Let X and Y be two discrete random variables spanning the same range of n sequential integers ($i = 1, 2, \dots, n$) with joint probability function $p_{XY}(x, y)$ and marginal probability functions

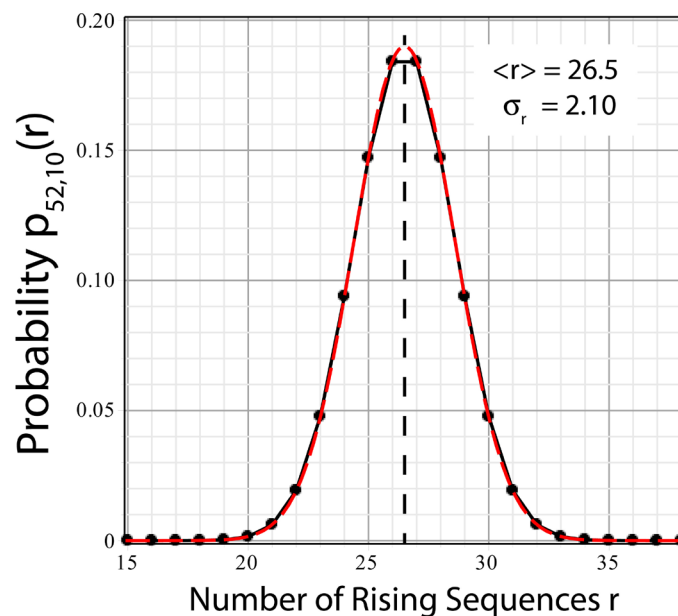


Figure 7. Probability distribution (solid black curve with circle markers) of number of rising sequences in shuffle $m = 10$ of a 52 card deck. Superposed is a Gaussian distribution (dashed red curve) of asymptotic mean 26.5 and standard deviation 2.10.

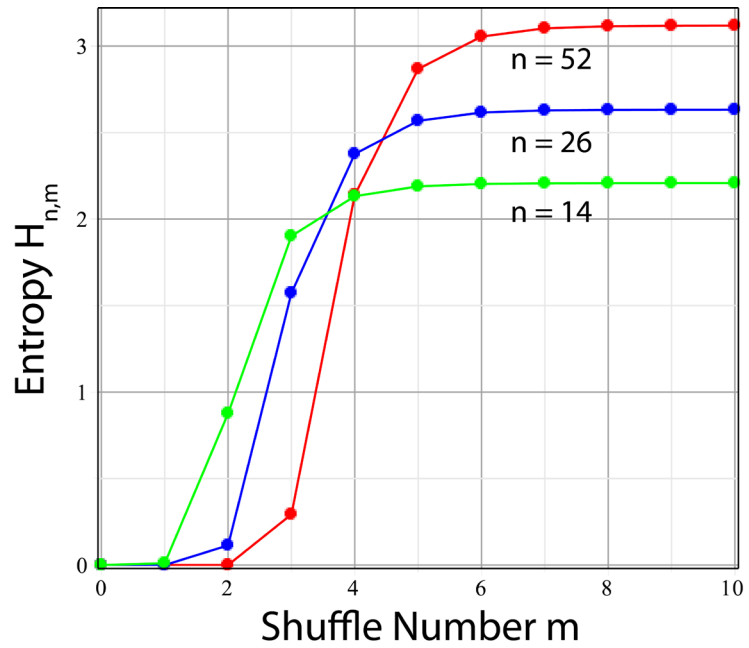


Figure 8. Shannon Entropy (in bits) of the card sequences arising from m shuffles of an ordered deck of n cards for $n = 14$ (green), 26 (blue), 52 (red). The entropy function is discrete; connecting lines serve only to facilitate visualization.

$$p_X(x) = \sum_{y=1}^n p_{XY}(x, y) \quad (62)$$

$$p_Y(y) = \sum_{x=1}^n p_{XY}(x, y)$$

each satisfying the completeness relation. The entropy (mean uncertainty) in receipt of n transmitted symbols $\{x_i\}$ or $\{y_i\}$ is

$$H(X) = -\sum_{x=1}^n p_X(x) \log_2 p_X(x) \quad (63)$$

$$H(Y) = -\sum_{y=1}^n p_Y(y) \log_2 p_Y(y)$$

The conditional entropy of the sequence $\{x_i\}$, given that the sequence $\{y_i\}$ is known, is defined by [43]

$$H(X|Y) = -\sum_{x=1}^n p_{X|Y}(x|y) \log_2 p_{X|Y}(x|y) p_Y(y), \quad (64)$$

where the condition probability $p_{X|Y}(x|y)$ is

$$p_{X|Y}(x|y) = p_{XY}(x, y) / p_Y(y). \quad (65)$$

(See also Ref. [22], pp 52-53.) The joint entropy of X and Y is then given by

$$H(X, Y) = H(X) + H(Y|X) = H(Y) + H(X|Y). \quad (66)$$

Equation (66) states that the entropy of a joint event, e.g. X and Y , is the entropy of the former plus the conditional entropy of the latter when the former is known. One may also define the quantity

$$H_{[XY]} \equiv H(X) - H(X|Y) \quad (67)$$

which is the decrease in entropy of the events X when it is known that events Y have occurred. Given the preceding interpretation, the function expressed by Equation (67) is taken to represent the information provided by knowledge of the events Y [43].

In the analysis of permuted card sequences in the following two sections, the information function $H_{[XY]}$ is one of the important quantities to be deduced experimentally. Substitution into Equation (67) of the conditional probability $H(X|Y)$ from Equation (66) leads to the symmetric relation

$$H_{[XY]} = H(X) + H(Y) - H(XY) \quad (68)$$

which is particularly useful for calculation.

3.3. Entropy of Sequences of Card Pairs: Theoretical

To apply the preceding concepts to riffle shuffles, the experimental sequences of digital card values are transformed into two sets of binary values by the following procedure, schematically shown in **Figure 9**.

- Given a decimal sequence of card values $\{x_i\}$ for $i = 1, 2, \dots, n$, create the binary sequence $\{b_j\}$ for $j = 1, 2, \dots, n-1$ defined by

$$b_j = \begin{cases} 1 & \text{if } x_{j+1} - x_j = 1 \\ 0 & \text{otherwise} \end{cases} \quad (69)$$

- Transform the set $\{b_j\}$ into the set $\{c_k\}$ $k = 1, 2, \dots, n-2$, where

$$c_k = b_{k+1} - \frac{1}{2}b_k. \quad (70)$$

Transformation (69) generates a binary sequence of 1's and 0's, in which the symbol 1 signifies a pair of cards in numerical order (e.g. 4,5). Transformation

(A)			(B)			(C)			(D)		
x	b	c	x	b	c	x	b	c	x	b	c
1			1			1			2		
	1			1			0			0	
2		1/2	2		- 1/2	3		1	1		0
	1			0			1			0	
3			4			4			3		

Figure 9. Schematic of procedure for transformation of digital sequence $\{x_i\}$ into binary sequence $\{b_j\}$ and then into quaternary sequence $\{c_k\}$ from which the pair association statistics are generated for calculating conditional probabilities and conditional entropy of ordered card pairs. Panels A, B, C, D represent the 4 possible outcomes of card pair associations.

(70) converts the binary sequence into a sequence of four values 1, 0, and $\pm\frac{1}{2}$.

Figure 9 illustrates the significance of the four symbols:

Panel *A*: $c = +\frac{1}{2}$ signifies that a 1 follows a 1.

Panel *B*: $c = -\frac{1}{2}$ signifies that a 0 follows a 1.

Panel *C*: $c = 1$ signifies that a 1 follows a 0.

Panel *D*: $c = 0$ signifies that a 0 follows a 0.

Given the set $\{c_k\}$, the following four pair-association statistics

$$n(0,0) = \sum_{k=1}^{n-2} I_0(c_k) \quad (71)$$

$$n(0,1) = \sum_{k=1}^{n-2} I_1(c_k) \quad (72)$$

$$n(1,0) = \sum_{k=1}^{n-2} I_{-\frac{1}{2}}(c_k) \quad (73)$$

$$n(1,1) = \sum_{k=1}^{n-2} I_{\frac{1}{2}}(c_k), \quad (74)$$

in which

$$I_\alpha(c_k) = \begin{cases} 1 & c_k = \alpha \\ 0 & c_k \neq \alpha \end{cases} \quad (75)$$

count the number of events of the kinds represented respectively by panels *A*, *B*, *C*, *D*. To summarize, the statistic $n(\alpha, \beta)$ is the number of events of symbol α followed by symbol β , where both symbols can take on values of 0 or 1. The statistics $n(\alpha, \beta)$ satisfy the sum rule

$$\sum_{\substack{\alpha=0,1 \\ \beta=0,1}} n(\alpha, \beta) = n - 2 \rightarrow 50 \quad (76)$$

evaluated numerically above for a deck of $n = 52$ cards.

In this information theoretic analysis, it is useful to think of the α symbols as the realizations of a “message” variable A that represents a received signal of 1’s and 0’s, whereas the β symbols are the realizations of a following “prediction” variable B that represents a predicted signal of 1’s and 0’s. For each successive shuffle of the deck, the set of conditional probabilities $p(\beta|\alpha)$ determines the conditional entropy $H(B|A)$, which is the uncertainty in predicting B given knowledge of A .

It is straightforward to show that the conditional probabilities $p(\beta|\alpha)$ can be estimated from the pair association statistics (71)-(74) as follows

$$p(0|0) = \frac{n(0,0)}{n(0,0) + n(0,1)} \quad (77)$$

$$p(1|0) = \frac{n(0,1)}{n(0,0) + n(0,1)} \quad (78)$$

$$p(0|1) = \frac{n(1,0)}{n(1,0) + n(1,1)} \quad (79)$$

$$p(1|1) = \frac{n(1,1)}{n(1,0) + n(1,1)} \quad (80)$$

in the limit of a sufficiently large number of sets of shuffles. Note that the order of symbols in the argument of $p(\beta|\alpha)$ signifies that event α precedes event β , which is the reverse of the order of symbols in the argument of $n(\alpha, \beta)$. Regrettably, this potential for confusion is the price required to maintain conventional statistical notation.

The *a priori* probabilities $p_A(\alpha)$ of a received symbol α are given by

$$p_A(\alpha) = \frac{1}{n-2} \sum_{\beta=0,1} n(\alpha, \beta), \quad (81)$$

or explicitly

$$p_A(0) = \frac{n(0,0) + n(0,1)}{n-2}, \quad p_A(1) = \frac{n(1,0) + n(1,1)}{n-2}. \quad (82)$$

Similarly, the *a priori* probabilities $p_B(\beta)$ of a predicted symbol β are

$$p_B(\beta) = \frac{1}{n-2} \sum_{\alpha=0,1} n(\alpha, \beta), \quad (83)$$

or explicitly

$$p_B(0) = \frac{n(0,0) + n(1,0)}{n-2}, \quad p_B(1) = \frac{n(0,1) + n(1,1)}{n-2}. \quad (84)$$

The joint probability $p_{AB}(\alpha, \beta)$ of a received symbol α and predicted symbol β is given by

$$p_{AB}(\alpha, \beta) = p_A(\alpha) p(\beta|\alpha) = \frac{n(\alpha, \beta)}{n-2} \quad (85)$$

where the second equality follows from combining relations (82) and (77)-(80).

Given the probability functions constructed above, the *a priori* entropies of the received (A) and predicted (B) signals are

$$H(A) = - \sum_{\alpha=0,1} p_A(\alpha) \log_2 p_A(\alpha) \quad (86)$$

$$H(B) = - \sum_{\beta=0,1} p_B(\beta) \log_2 p_B(\beta) \quad (87)$$

and the total entropy of A and B is

$$H(AB) = - \sum_{\substack{\alpha=1,0 \\ \beta=1,0}} p_{AB}(\alpha, \beta) \log_2 p_{AB}(\alpha, \beta). \quad (88)$$

The information, or decrease in uncertainty of values of B as a result of knowing values of A , is then given by Equation (68)

$$H_{[BA]} = H(B) - H(B|A) = H(A) + H(B) - H(AB). \quad (89)$$

The entropy and information are in units of bits ("binary digits"). In statistical

physics, where natural logarithms are usually used rather than logarithms to base 2, entropy and information are in units of nats.

3.4. Entropy of Sequences of Card Pairs: Experimental

An experiment was performed in which an initially ordered deck of $n = 52$ cards was subject to $N = 11$ sets of $M = 19$ riffle shuffles per set implemented by the auto shuffler in **Figure 1**, thereby generating M columns of card permutations for each set such as illustrated in **Table 1**. The cards were shuffled mechanically, rather than manually, so that the riffle shuffles would be executed as uniformly as possible. The pair association numbers $n(\alpha, \beta)$ for each of the M shuffles were then averaged over the N sets to yield the mean numbers of pair associations summarized in **Table 3** and plotted in **Figure 10** as a function of shuffle number m .

For a completely ordered deck prior to shuffling ($m = 0$), there are $n - 2 = 50$ occurrences of $\alpha = 1$ followed by $\beta = 1$, as shown by the plot of $n(1, 1)$ (red curve) in **Figure 10**. This number drops rapidly with increasing shuffle number, becoming effectively 0 by about $m \approx 8$. Correspondingly, the occurrence of $\alpha = 0$

Table 3. Mean pair association numbers for a 52-Card Deck.

Shuffle Number m	$n(0, 0)$	$n(0, 1)$	$n(1, 0)$	$n(1, 1)$
0	0.00	0.00	0.00	50.00
1	5.82	12.00	12.27	19.91
2	14.27	11.91	12.36	11.45
3	20.91	10.64	11.09	7.36
4	26.64	10.27	10.27	2.82
5	30.27	8.91	8.91	1.91
6	34.00	7.55	7.27	1.18
7	38.36	5.36	5.36	0.91
8	39.18	5.18	5.27	0.36
9	41.00	4.45	4.36	0.18
10	42.91	3.45	3.45	0.18
11	43.55	3.00	3.09	0.36
12	43.64	3.00	3.00	0.36
13	43.82	3.00	3.00	0.18
14	44.00	2.91	2.91	0.18
15	46.00	2.00	2.00	0.00
16	46.91	1.55	1.55	0.00
17	46.55	1.73	1.73	0.00
18	47.64	1.18	1.18	0.00
19	46.73	1.64	1.64	0.00

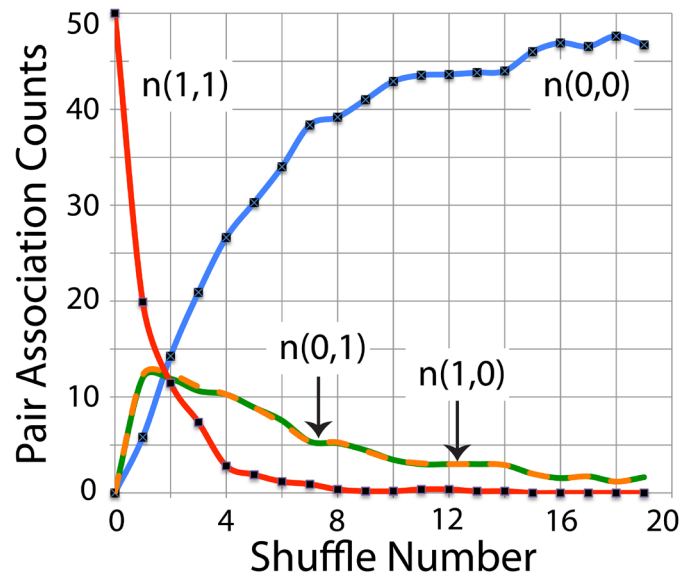


Figure 10. Pair association numbers $n(\alpha, \beta)$ as a function of number of auto-shuffles. Symbols 1 and 0 respectively represent an ordered and non-ordered two-card sequence. Thus $n(1,1)$ = number of 2 ordered pairs (e.g. 1,2; 2,3) (red); $n(0,0)$ = number of 2 non-ordered pairs (e.g. 2,1; 3,5) (blue); $n(1,0)$ = number of non-ordered pairs following an ordered pair (e.g. 1,2; 3,5) (orange); $n(0,1)$ = number of ordered pairs following a non-ordered pair (e.g. 3,5; 1,2) (green). Black squares mark the actual points; colored connecting lines merely facilitate viewing.

followed by $\beta = 0$ rises rapidly with increasing m , approaching ≈ 48 , as shown by the plot of $n(0,0)$ (blue curve). The plots of $n(0,1)$ (green curve) and $n(1,0)$ (orange curve), which start at 0 and then fall off gradually from a maximum of about 12 at $m = 1$, are virtually indistinguishable.

The conditional probabilities $p(\beta|\alpha)$, deduced from the pair-association statistics by means of Equations (77)-(80), are plotted as a function of m in **Figure 11**. In each panel, the conditional probabilities satisfy the completeness relation

$$\sum_{\beta=0,1} p(\beta|\alpha) = 1 \quad (90)$$

for $\alpha = 0, 1$.

The plots in panel A, which show the conditional probabilities of prediction variable β given received variable $\alpha = 0$, begin at $m = 1$ because there is no event 0 in a completely ordered deck ($m = 0$). As the shuffle number m increases, the number of ordered pairs decreases, and $p(0|0)$ approaches 1 while $p(1|0)$ approaches 0. In panel B, the probabilities are conditioned on a received variable 1. As the number of 0 events increase with m , it follows again that $p(0|1)$ approaches 1 and $p(1|1)$ approaches 0. For a gambler or competitive player, the probability $p(1|1)$ is particularly useful, since it quantifies the chance of a third card in order (e.g. 1,2,3), given prior receipt of two cards in order (e.g. 1,2). Empirically, this conditional probability is seen to be about 20% at the 5th shuffle.

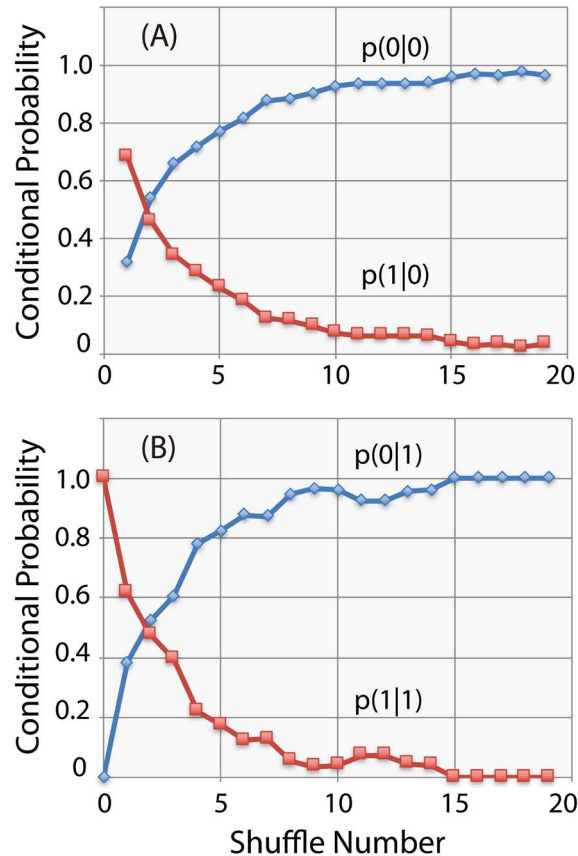


Figure 11. Conditional probabilities $p(\beta|\alpha)$ as a function of shuffle number for 11 auto-shuffled sets, each comprising 19 riffle shuffles. Values of α signify preceding “message” events; values of β signify following “prediction” events. The symbol “1” marks occurrence of an ordered pair (e.g. 4,5); the symbol “0” marks occurrence of a non-ordered pair (e.g. 5,4).

The entropy $H(B)$ of the prediction variable and information $H(B) - H(B|A)$ are summarized in Table 4 and plotted in Figure 12. The plot of information (red curve) was multiplied by a factor 10 to enhance visibility. The black double arrow marks the standard deviation of the information at shuffle number $m = 12$. As shown by Table 4, the information at all shuffle numbers is within ± 1 standard deviation of 0.

Since the randomness of a deck of cards is ordinarily expected to increase with the number of shuffles, as shown explicitly in Figure 8 for the entropy of rising sequences, the decrease of $H(B)$ with shuffle number in Figure 12 calls for an explanation. In the initially ordered deck, all sequential pairs of cards are in order, and therefore both the message variable A and prediction variable B for any pair take the value 1 (as demonstrated in Figure 9). With each successive shuffle, successive pairs of cards become less and less ordered and variables B and A increasingly take the value 0. Thus, as shown in Figure 11, the conditional probabilities become increasingly predictable as they asymptotically approach either 1 (100% chance of an ordered pair occurring) or 0 (100% chance of an ordered

Table 4. Entropy and Information of Auto-Shuffled 52-Card Deck.

Shuffle Number m	Entropy $H(B)$	Conditional Entropy $H(B A)$	Information $H(B) - H(B A)$	Information Std Dev
1	0.9386	0.9382	0.0004	0.0494
2	0.9892	0.9883	0.0010	0.0180
3	0.9353	0.9333	0.0021	0.0611
4	0.8242	0.8269	-0.0027	0.0767
5	0.7463	0.7451	0.0013	0.1158
6	0.6521	0.6458	0.0063	0.1920
7	0.5323	0.5326	-0.0003	0.1770
8	0.4953	0.4977	-0.0024	0.1381
9	0.4370	0.4340	0.0029	0.1516
10	0.3695	0.3733	-0.0038	0.1293
11	0.3474	0.3569	-0.0096	0.1421
12	0.3474	0.3569	-0.0096	0.1421
13	0.3334	0.3417	-0.0083	0.1386
14	0.3290	0.3292	-0.0001	0.1165
15	0.1385	0.1290	0.0094	0.1905
16	0.1201	0.1182	0.0019	0.1781
17	0.2119	0.2092	0.0028	0.1002
18	0.0623	0.0551	0.0072	0.1701
19	0.0702	0.0545	0.0156	0.2276

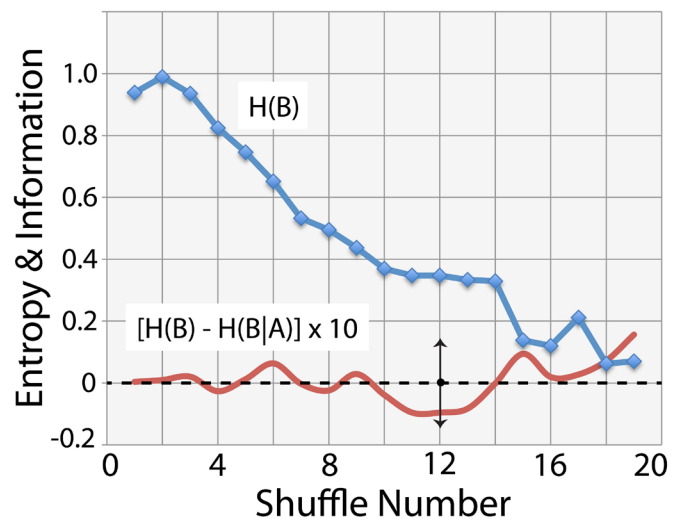


Figure 12. Total entropy (blue) in bits of “prediction” events as a function of number of shuffles. Information (red) in bits—multiplied by 10 for visibility—due to knowledge of preceding “message” events. The black double arrow marks the sample standard deviation of $\approx 0.014(\times 10)$ for the 12th shuffle. The entire information curve lies within ± 1 standard deviation, signifying that uncertainty of card pairs was not significantly reduced by knowledge of preceding pairs.

pair not occurring). Consequently, pair association variables B and A are so defined that their outcomes become more certain and their entropies (*i.e.* uncertainties) decrease as the deck becomes increasingly randomized.

To put into perspective the empirical results of this information theoretical analysis, it is to be recalled that 1 bit of information, as initially construed by Shannon who largely created the subject of information or communication theory [22], corresponds to the reduction of uncertainty by 1 binary-valued decision—e.g. a “yes or no” or “1 or 0”. As pointed out in Section 1, the word information carries two different meanings, both of which are relevant here:

1) Information, as ordinarily defined by scientists, is associated with uncertainty, *i.e.* entropy H . Thus, the decrease in entropy $H(B)$ for about the first 10 shuffles, as seen in **Figure 12**, represents a steady loss in information as the outcome (1 or 0) becomes more predictable.

2) Information can also be construed as a measure of the reduction in uncertainty in one variable (e.g. B) as a result of knowledge of another variable (e.g. A). From this perspective, **Figure 12** shows that the card order of a preceding pair provided no statistically useful information for predicting the card order of the following pair at any shuffle number $m > 0$. The reason is that $H(B|A)$ decreased with m to the same extent as did $H(B)$.

4. Conclusions

In this paper the sequential permutations of an initially ordered deck of cards mixed by riffle shuffles executed manually or mechanically were tested for different statistical measures of random patterns, including 1) runs, 2) rank ordering, 3) pair correlations, 4) rising sequences, and 5) entropy and information loss. The various statistical measures probed different aspects of the symbol patterns within each permuted sequence. Consequently, different measures could result in different threshold shuffle numbers at which the deck could be said to have been randomized for the purposes of competitive card playing or gambling.

Table 5 summarizes the threshold shuffle numbers for randomization according to different statistical measures. It is to be stressed that these threshold values, taken from the empirical plots of the associated sample statistics, are approximate since the point at which a deck of cards can be said to be completely mixed is a subjective judgment. For variates (like rank ordering) expressed in standard normal form with asymptotic Gaussian distribution, the point of complete mixing was estimated visually to occur at a shuffle number for which the sample statistic $|z| \leq 1$. For variates (like rising sequences) that underwent an abrupt change from a state of order to state of disorder, the point of complete mixing was estimated visually to occur at a shuffle number at which the apparent asymptotic limit was reached.

As seen in **Table 5**, there is a fairly wide spread among the different tests in values of the threshold shuffle number. For example, for manually shuffled cards the measure z of randomization by rank ordering indicates a complete mixing by

Table 5. Number of shuffles to achieve satisfactory mixing.

Statistical Test	Hand Shuffles	Auto Shuffles
Runs (relative to mean)	10	10
Runs (up/down)	8	8
Rank Ordering	6	6
Serial Correlation (lag 1)	8	16
Rising Sequences	8	12
Conditional Probability $P(1 1)$	-	9
Conditional Probability $P(1 0)$	-	11
Entropy (Information) $H(B)$	-	17

about the 6th shuffle, whereas the runs test statistic z is close to 0 at about the 8th shuffle. For the statistical variable of rising sequences, the manually shuffled cards met the criterion of complete mixing at about the 8th shuffle, as predicted in [1], whereas the same criterion was met at about the 12th shuffle for mechanically shuffled cards. Large differences in threshold values obtained from different test variables arose because the tests examined different aspects of the residual patterns embedded in the permutations of card order.

However, so as not to misinterpret (or over-interpret) these results, the reader should bear in mind that the statistical tests in themselves do not indicate that any residual pattern would actually be useful to a card player. For example, **Table 1** shows instances of ascending and descending sequences even up to the 19th shuffle, at which point such patterns are almost assuredly uninformative. On the other hand, the residual order remaining at the 7th shuffle, indicated by the conditional probability functions plotted in **Figure 11**, might possibly be useful to an astute and skillful player. The variable results of **Table 5** notwithstanding, it is probably safe to say that 4 shuffles—which have been reported to be standard protocol at casinos [44]—are too few (as suggested by the plots of runs in **Figure 2** and rising sequences in **Figure 5**).

Of the various statistical measures applied to the experimentally generated card sequences, the author is aware of only one measure—mean number of rising sequences—for which a theoretical distribution function pertaining to a particular shuffle model is known. The probability function of this distribution, Equation (60), is based on the GSR model of riffle shuffling. Although there are many references in the statistical literature and on the internet to the theory of riffle shuffling (such as those cited in the References to this paper), the author knows of no previously published experimental test with actual cards, rather than simulations by computer. In this regard, the nearly exact match of the theoretically predicted and experimentally measured mean number of rising sequences shown in **Figure 5** for manually shuffled cards provides an experimental confirmation of the distribution (60) and therefore evidence in support of the GSR model as a satisfactory description of how humans actually perform riffle

shuffles.

Acknowledgements

J. Becker, J. Boreyko, C. Davis, J. Halverson, N. Harrison, A. Lampert, A. Mathis, O. Sanford, C. Sherman, W. Strange, and F. Sullivan participated in data collection at an early phase of this project. The author also thanks Trinity College for partial support through the research fund associated with the George A. Jarvis Chair of Physics.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

- [1] Bayer, D. and Diaconis, P. (1992) Trailing the Dovetail Shuffle to Its Lair. *The Annals of Applied Probability*, **2** 294-313. <https://doi.org/10.1214/aoap/1177005705>
- [2] Trefethen, L.N. and Trefethen, L.M. (2000) How Many Shuffles to Randomize a Deck of Cards? *Proceedings of the Royal Society of London. Series A*, **456**, 2561-2568. <https://doi.org/10.1098/rspa.2000.0625>
- [3] Ogievetsky, O. and Petrova, V. (2018) Cyclotomic Shuffles. *Physics of Particles and Nuclei*, **49**, 867-872. <https://doi.org/10.1134/S1063779618050325>
- [4] Aldous, D. and Diaconis, P. (1986) Shuffling Cards and Stopping Times. *The American Mathematical Monthly*, **93**, 333-348. <https://doi.org/10.1080/00029890.1986.11971821>
- [5] Sanz, A., Sanz-Sanz, C., Gonzalez-Lezana, T., Roncero, O. and Miret-Artes, S. (2012) Quantum Zeno Effect: Quantum Shuffling and Markovianity. *Annals of Physics*, **327**, 1277-1289. <https://doi.org/10.1016/j.aop.2011.12.012>
- [6] Knuth, D.E. (1998) Seminumerical Algorithms. In: *The Art of Computer Programming*, Vol. 2, 3rd Edition, Addison-Wesley, Boston, 12-15, 145-146.
- [7] Wikipedia (2019) Fisher-Yates Shuffle. http://en.wikipedia.org/wiki/Fisher%E2%80%93Yates_shuffle#cite_note-knuth3-4
- [8] Kolata, G. (1990) In Shuffling Cards, 7 Is a Winning Number. *New York Times*, 9 January 1990, 1.
- [9] Peterson, I. (2000) Disorder in the Deck. *Science News Online*, 21 October 2000. <http://sciencenews.org/articles/20001021/mathtrek.asp>
- [10] McGinty, J.C. (2018) The Trick behind Properly Shuffling Cards: Casual Players Don't Typically Randomize the Deck, but a Perfect "Riffle" Also Doesn't Work. *Wall Street Journal*, 11 May 2018. <http://www.wsj.com/articles/the-trick-behind-properly-shuffling-cards-1526043600>
- [11] Rehmeyer, J. (2008) Shuffling the Cards: Math Does the Trick. *Science News Online*, 7 November 2008. <http://www.sciencenews.org/article/shuffling-cards-math-does-trick>
- [12] Silverman, M.P., Strange, W., Silverman, C.R. and Lipscombe, T.C. (1999) Tests of Alpha-, Beta-, and Electron Capture Decays for Randomness. *Physics Letters A*, **262**, 265-273. [https://doi.org/10.1016/S0375-9601\(99\)00668-4](https://doi.org/10.1016/S0375-9601(99)00668-4)
- [13] Silverman, M.P., Strange, W., Silverman, C. and Lipscombe, T.C. (2000) Tests for

- Randomness of Spontaneous Quantum Decay. *Physical Review A*, **61**, Article ID: 042106. <https://doi.org/10.1103/PhysRevA.61.042106>
- [14] Silverman, M.P. and Strange, W. (2000) Experimental Tests for Randomness of Quantum Decay Examined as a Markov Process. *Physics Letters A*, **272**, 1-9. [https://doi.org/10.1016/S0375-9601\(00\)00374-1](https://doi.org/10.1016/S0375-9601(00)00374-1)
 - [15] Silverman, M.P. (2014) A Certain Uncertainty: Nature's Random Ways. Cambridge University Press, Cambridge. <https://doi.org/10.1017/CBO9781139507370>
 - [16] Weaver, W. (1963) Lady Luck: The Theory of Probability. Doubleday & Company, Garden City, 324-348.
 - [17] Bernstein, P.L. (1998) Against the Gods: The Remarkable Story of Risk. Wiley, New York, 12-14.
 - [18] McLeod, J. (2006) Playing-Card Games. International Playing Card Society. <https://i-p-c-s.org/faq/games.php>
 - [19] Parlett, D. (1991) A History of Card Games. Oxford University Press, Oxford.
 - [20] Diaconis, P., Graham, R.L. and Kanton, W.M. (1983) The Mathematics of Perfect Shuffles. *Advances in Applied Mathematics*, **4**, 175-196. [https://doi.org/10.1016/0196-8858\(83\)90009-X](https://doi.org/10.1016/0196-8858(83)90009-X)
 - [21] Diaconis, P., McGrath, M. and Pitman, J.W. (1995) Riffle Shuffles, Cycles and Descents. *Combinatorica*, **15**, 11-29. <https://doi.org/10.1007/BF01294457>
 - [22] Shannon, C.E. and Weaver, W. (1964) The Mathematical Theory of Communication. University of Illinois Press, Urbana.
 - [23] Kullback, S. (1968) Information Theory and Statistics. Dover Publications, Mineola.
 - [24] Stark, D., Ganesh, A. and O'Connell, N. (2002) Information Loss in Riffle Shuffling. *Combinatorics, Probability and Computing*, **11**, 79-95. <https://doi.org/10.1017/S0963548301004990>
 - [25] Brillouin, L. (1962) Science and Information Theory. 2nd Edition, Academic Press, New York, 11-22. <https://doi.org/10.1063/1.3057866>
 - [26] Gilbert, E.W. (1955) Theory of Shuffling. Bell Laboratories Technical Memorandum, Murray Hill.
 - [27] Reeds, J. (1981) Unpublished Manuscript. https://en.wikipedia.org/wiki/Gilbert%E2%80%93Shannon%E2%80%93Reeds_model
 - [28] Diaconis, P., Fulman, J. and Holmes, S. (2013) Analysis of Casino Shelf Shuffling Machines. *The Annals of Applied Probability*, **4**, 1692-1720. <https://doi.org/10.1214/12-AAP884>
 - [29] Hald, A. (1952) Statistical Theory with Engineering Applications. Wiley, New York, 342-359.
 - [30] Wald, A. and Wolfowitz, J. (1940) On a Test Whether Two Samples Are from the Same Population. *The Annals of Mathematical Statistics*, **11**, 147-162. <https://doi.org/10.1214/aoms/1177731909>
 - [31] Mood, A.M. (1940) The Distribution Theory of Runs. *The Annals of Mathematical Statistics*, **11**, 367-392. <https://doi.org/10.1214/aoms/1177731825>
 - [32] Silverman, M.P., Strange, W., Silverman, C.R. and Lipscombe, T.C. (1999) On the Run: Unexpected Outcomes of Random Events. *The Physics Teacher*, **37**, 218-225. <https://doi.org/10.1119/1.880232>
 - [33] Kendall, M.G. and Stuart, A. (1961) The Advanced Theory of Statistics. Vol. 2, Inference and Relationship. Hafner, New York, 474-483. <https://doi.org/10.2307/3538355>

- [34] Altman, D.G. (1991) Practical Statistics for Medical Research. Chapman & Hall/CRC, New York, 296-298.
- [35] Walpole, R.E. and Myers, R.H. (1978) Probability and Statistics for Engineers and Scientists. 2nd Edition, Macmillan, New York, 492-495.
<https://doi.org/10.2307/2530629>
- [36] Wald, A. and Wolfowitz, J. (1943) An Exact Test for Randomness in the Non-Parametric Case Based on Serial Correlation. *The Annals of Mathematical Statistics*, **14**, 378-388. <https://doi.org/10.1214/aoms/1177731358>
- [37] Hoel, P.G. (1947) Introduction to Mathematical Statistics. Wiley & Sons, New York, 182-183.
- [38] Brown, K. (no date) Eulerian Numbers.
<http://www.mathpages.com/home/kmath012/kmath012.htm>
- [39] Mann, B. (1994) How Many Times Should You Shuffle a Deck of Cards? *UMAP Journal*, **15**, 303-331.
http://www.dartmouth.edu/~chance/teaching_aids/Mann.pdf
- [40] Knuth, D.E. (1993) Johann Faulhaber and Sums of Powers. *Mathematics of Computation*, **61**, 277-294. <https://doi.org/10.1090/S0025-5718-1993-1197512-7>
- [41] Arfken, G.B. and Weber, H.J. (2005) Mathematical Methods for Physicists. Academic Press, New York, 376-379, 473-474.
- [42] Jaynes, E.T. (1957) Information Theory and Statistical Mechanics. *The Physical Review*, **106**, 620-630. <https://doi.org/10.1103/PhysRev.106.620>
- [43] Rozanov, Y.A. (1969) Introductory Probability Theory. Prentice-Hall, Englewood Cliffs, 115-120.
- [44] Ball, P. (2000) Shuffling: What's the Deal? *Nature*.
<https://doi.org/10.1038/news001005-8>
<http://www.nature.com/news/1998/001005/full/news001005-8.html>