6-2011

Search for Patterns in Sequences of Single-Photon Polarization Measurements

David Branning
Trinity College, david.branning@trincoll.edu

Adam Katcher
Trinity College

Wayne Strange
Trinity College

Mark P. Silverman
Trinity College, mark.silverman@trincoll.edu

Search for patterns in sequences of single-photon polarization measurements

David Branning,* Adam Katcher, Wayne Strange, and Mark P. Silverman

Department of Physics, Trinity College, Hartford, Connecticut 06106, USA
**Corresponding author: david.branning@trincoll.edu*

Received January 24, 2011; revised April 7, 2011; accepted April 8, 2011;
posted April 8, 2011 (Doc. ID 141602); published May 18, 2011

Sequences of random binary numbers created from polarization measurements of single photons were subjected to a comprehensive runs analysis. Photon pairs from a spontaneous parametric downconversion source were detected in coincidence, with one photon acting as a trigger while the other was analyzed for horizontal or vertical polarization. The resulting sequences of polarization measurements were tested for runs of consecutive vertical or horizontal outcomes against a theory of nonoverlapping runs, without numerical unbiasing. The sequences produced no statistically significant discrepancies with the predicted numbers of runs, even with multiphoton events retained.

OCIS codes: 270.0270, 270.5568, 270.5290, 030.5260.

1. INTRODUCTION

Single-photon sources of random numbers have become increasingly important in recent years due to their central role in quantum key distribution protocols for cryptography [1]. These protocols rely on the unpredictability of measurement outcomes from quantum superposition states for their security [2]. This unpredictability is also fundamental to quantum mechanics. For both of these reasons, experimental tests of quantum randomness have been performed on bit sequences derived from radioactive decays [3–5], from atomic fluorescence [6], and from single-photon detection times [7–11] or polarizations [12–15], or both [16].

Here we report on a new theoretical and experimental test, based on runs analysis, of the randomness of single-photon polarization measurement outcomes, using pairs of photons generated by cw-pumped spontaneous parametric downconversion [17]. One member of each pair was used as a detection trigger, while the other was put into a superposition state of horizontal (H) and vertical (V) polarization, and then measured in the H–V basis. Runs of consecutive H and V outcomes were counted, and these totals were compared with a theory of runs. Because this theory is valid for any ratio of H to V events, it was not necessary to perform any numerical unbiasing [18,19] on the sequences before tabulating the runs. In addition, time bins in which two or more polarization measurements occurred, which are typically discarded in the construction of quantum cryptographic keys, were included in the runs analysis to see if any effects could be observed.

2. SINGLE-PHOTON POLARIZATION MEASUREMENTS

The polarizations of single photons were measured as shown in Fig. 1 [15]. The apparatus was a "heralded" single-photon source [20] based on the process of spontaneous parametric downconversion, in which a photon from a cw "pump" laser is annihilated within a nonlinear optical medium to produce two lower-frequency photons, called the signal and the idler [21]. A cw 405 nm diode laser served as the pump, while a 3.0 mm nonlinear beta-barium borate crystal served as the parametric downconverter (PDC). The PDC was cut for Type I phase matching, so that the 810 nm signal and idler photons emerged with similar horizontal polarizations [22], and oriented so that they propagated away from the pump beam at an opening angle of 3°. The signal and idler beams were then directed to single-photon counting modules (A, B, B') using lenses and optical fibers. Within each fiber channel, long-pass filters (LP) absorbed wavelengths shorter than 780 nm to reduce background counts.

In cw-pumped downconversion, the signal and idler photons are emitted at irregular times, but they must be emitted together in order to conserve energy and momentum. This fact is expressed in the single-mode approximation for the quantum state of the light in the signal and idler modes [21]:

$$|\psi\rangle = \mathcal{M}|\mathrm{vac}\rangle + \eta|H\rangle_s|H\rangle_i + O(\eta^2)|2H\rangle_s|2H\rangle_i, \qquad (1)$$

where $\mathcal{M}$ is a normalization constant and η is a small number characterizing the size of the perturbation on the initial vacuum state. The second term, a product state of one signal and one idler photon, gives the "heralded" source its name: when a signal photon is detected, the idler photon must also be present, in a close approximation to a localized single-photon Fock state [23]. This is accomplished in practice using coincidence detection, in which the electronic signals from the signal and idler detectors are sent to an AND gate, and the resulting "coincidence count" indicates that a correlated photon pair was detected [24].

The higher-order terms in Eq. (1) express the possibility that more than one pair of photons can be generated within the coherence time of the downconverted light. In quantum key distribution systems, the presence of two or more photons in the same spatiotemporal mode, or even within the same data collection time, can introduce errors into the distributed

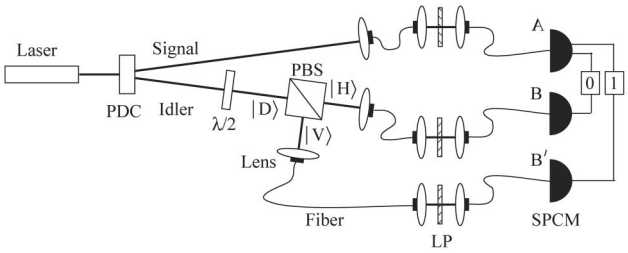

Fig. 1. Experimental arrangement for measuring single-photon polarizations. Signal and idler photon pairs are created in the PDC and counted in coincidence either at detectors AB or AB', depending on the measurement outcome for the diagonally polarized idler photon in the H–V basis. A binary sequence is created by assigning "0" to the coincidence events AB and "1" to the events AB'.

key and/or compromise its security; the probability of this is kept low by ensuring $\eta \ll 1$ [1,2].

The polarization state of the idler photons was rotated from $|H\rangle_i$ to $|D\rangle_i = \frac{1}{\sqrt{2}}(|H\rangle_i + |V\rangle_i)$ by passage through a zero-order half-wave plate $(\lambda/2)$. The idler photons then were analyzed by a polarizing beam splitter (PBS), which transmitted H-polarized photons to detector B, and reflected V-polarized photons to detector B'. Thus, a coincidence count AB indicated a horizontal polarization outcome for the idler photon, while a coincidence event AB' represented a vertical outcome.

The numbers of coincidence counts occurring in a predetermined time bin were recorded repeatedly during the experiment. For a cw-pumped downconversion source, this number follows a Poisson distribution with a mean occupation number of μ counts per bin [20,23]. Two experiments were performed, with differing values of μ. In each case, the empty bins, in which no coincidence events occurred, were removed from consideration because neither a horizontal nor a vertical outcome was recorded. The remaining occupied bins were used to construct Sequence Lo-μ ($\mu = 0.0111$) and Sequence Hi-μ ($\mu = 0.364$). The characteristics of these sequences are shown in Table 1.

Because $\mu < 1$ for both sequences Lo-μ and Hi-μ, the majority of the occupied bins contained exactly one event, either AB or AB', corresponding to a horizontal or a vertical idler polarization measurement, respectively labeled "0" and "1." It is these singly occupied bins that form the random number sequences in polarization-based quantum random number generators; when multiphoton events (more than one coincidence count) are detected, they are typically not included in the random bit sequence because there is no way to unambiguously assign them as 0s or 1s [15]. However, it is possible to include these events in a runs analysis of the sequence, as shown in Section 4. Because the multiphoton events will inevitably cut short some runs that would have occurred without them, they are referred to as "interruptors" in the following analysis.

3. TESTS OF RANDOMNESS WITH RUNS

The utility of a statistical test of randomness resides in its generality, ease of implementation, and sensitivity to deviations from expected random behavior. In this regard, runs tests are among the most widely used and most effective (see Appendix A). In statistical parlance, a run is an unbroken sequence of similar events of a binary nature—e.g., outcomes of a stochastic process denotable by $(1, 0)$, $(+, -)$, (H, T), or any other set of two symbols. For example, a sequence of symbols *aabbbaa* comprises two runs of *a*s of length 2 and one run of *b*s of length 3. The tabulation of runs produced by a set of data can serve as a test of randomness of the process that generated the data. More precisely, it is a test of randomness in permutational ordering along a single dimension, either spatial or temporal. The expression "test of randomness" needs to be understood appropriately. No statistical test (runs or otherwise) can prove that a physical process is random. Rather, a theoretical model leading to the predicted probabilities of all outcomes is derived from an initial set of assumptions against which the actual frequencies of observed outcomes are compared.

The applicability of runs tests is more general than might be inferred at first glance from the above definition of a run, since the original data can be any discrete or continuous series of real numbers. This series can then be mapped to a set of binary elements in various ways. The different mappings generally produce different sets of frequencies of runs of specified length, independently mining the information inherent in the data.

One virtue of a runs test is that it is a distribution-free test, so called because no assumptions are required regarding the distribution of the sampled population (in contrast to classical statistical tests associated with particular distributions, usually the Gaussian) [25]. Runs tests are distribution free because they rely on ordinal or categorical relationships between the elements of the sequence, rather than on the exact magnitudes of the elements themselves. Nevertheless, to apply a runs test, one must know, or at least be able to approximate closely, the distribution of the chosen test statistic. In applying runs tests, the statistics of interest have traditionally been the total number of runs (of both types of symbols) and the frequency of longest runs. However, the data are much more effectively utilized by determining, for each run length t, the probability distribution $p_{n,t,k}$ for k runs to occur in n trials, and comparing this with the observed frequencies of all runs.

Table 1. Characteristics of the Polarization Measurement Sequences Lo-$\mu$and Hi-μ

	Sequence	
	Lo-μ	Hi-μ[a]
Mean # events per time bin, μ	0.0111 ± 0.0002	0.364 ± 0.002
Time bin duration	1 ms	0.1 ms
P (no event in a bin)	0.98920	0.694
P (one event in a bin)	0.01074	0.253
P (> 1 event in a bin) $= P$ (interruptor)	0.00006	0.053
Ratio of interruptors to nonzero events	0.0056	0.17
Without Interruptors		
Sequence length, n	8,919,341	16,797,012
Probability of a 1, p	0.47850	0.50037
Subsequences of length 8192, M	1088	2050
With Interruptors		
Sequence length n	8,969,641	20,258,816
Probability of a 1, p'	0.47582	0.41487
Subsequences of length 8192, M	1094	2473

[a]Sequence Hi-μ was previously subjected to another set of randomness tests (without interruptors) in [15].

Table 2. Predicted and Observed Numbers of Runs of 1s for Sequence Lo-μ, With and Without Interruptors

Run Length t	N_{obs} no int.	$E(N)$	N_{obs} with int.	$E(N)$
2	1,381,157	$1,381,300 \pm 900$	1,375,944	$1,376,000 \pm 900$
3	572,187	$572,300 \pm 700$	567,578	$567,600 \pm 700$
4	257,254	$257,300 \pm 500$	253,947	$254,000 \pm 500$
5	119,840	$119,700 \pm 300$	117,665	$117,500 \pm 300$
6	56,511	$56,500 \pm 200$	55,200	$55,200 \pm 200$
7	26,863	$26,870 \pm 160$	26,044	$26,110 \pm 160$
8	12,878	$12,820 \pm 110$	12,443	$12,390 \pm 110$
9	6125	6120 ± 80	5887	5890 ± 80
10	2966	2930 ± 50	2850	2800 ± 50
11	1452	1400 ± 30	1384	1330 ± 40
12	730	670 ± 30	699	630 ± 30
13	365	321 ± 18	343	301 ± 17
14	157	153 ± 12	142	143 ± 12
15	69	73 ± 9	63	68 ± 8
16	32	35 ± 6	27	32 ± 6
17	16	17 ± 4	13	15 ± 4
18	9	8 ± 2	7	7 ± 2
19	7	3 ± 2	4	3.5 ± 1.9
20	4	1.8 ± 1.4	2	1.7 ± 1.3
21	2	0.9 ± 0.9	1	0.8 ± 0.9
22	2	0.4 ± 0.6	1	0.4 ± 0.6
23	1	0.2 ± 0.4	0	0.2 ± 0.4
24	1	0.1 ± 0.3	—	—
25	1	0.05 ± 0.21	—	—
26	0	0.02 ± 0.15	—	—

Broadly speaking, runs tests are of three types. The first type [26] is based on categorical relationships—e.g., a variate is assigned symbol a or b depending on whether it was greater or lesser than a specified threshold, e.g., the median. The null hypothesis, against which the resulting series containing n_a elements of one kind and n_b elements of another is compared, is that each of the

$$\binom{n_a + n_b}{n_a}$$

distinguishable arrangements is equally likely prior to sampling. This hypothesis implies that the probability of an element (a or b) is *constant*, no matter where in the series the element appears.

Table 3. Predicted and Observed Numbers of Runs of 1s for Sequence Hi-μ, With and Without Interruptors

Run Length t	N_{obs} no int.	$E(N)$	N_{obs} with int.	$E(N)$
2	2,802,820	$2,803,000 \pm 1300$	2,464,125	$2,464,000 \pm 1300$
3	1,202,758	$1,202,000 \pm 900$	911,663	$911,500 \pm 900$
4	561,638	$561,300 \pm 700$	361,732	$361,900 \pm 600$
5	271,694	$271,800 \pm 500$	147,779	$147,500 \pm 400$
6	133,684	$133,900 \pm 400$	60,917	$60,800 \pm 200$
7	66,255	$66,400 \pm 300$	25,164	$25,130 \pm 160$
8	33,002	$33,110 \pm 180$	10,473	$10,400 \pm 100$
9	16,568	$16,530 \pm 130$	4337	4320 ± 70
10	8219	8270 ± 90	1775	1790 ± 40
11	4047	4130 ± 60	725	740 ± 30
12	1987	2070 ± 50	273	308 ± 18
13	979	1030 ± 30	99	127 ± 11
14	493	520 ± 20	38	53 ± 8
15	237	259 ± 16	13	22 ± 5
16	119	130 ± 11	8	9 ± 3
17	63	65 ± 8	2	3.8 ± 1.9
18	34	32 ± 6	1	1.6 ± 1.3
19	19	16 ± 4	0	0.7 ± 0.8
20	9	8 ± 3	—	—
21	3	4 ± 2	—	—
22	1	2.0 ± 1.4	—	—
23	1	1.0 ± 1.0	—	—
24	1	0.5 ± 0.7	—	—
25	1	0.3 ± 0.5	—	—
26	1	0.1 ± 0.4	—	—
27	0	0.06 ± 0.25	—	—

The second type of runs analysis, based on ordinal relationships [27], defines an "up–down" run as an unbroken sequence of increasing or decreasing values. If n unequal numbers are generated by a random process, then each of the $n!$ distinguishable orderings has an equal *a priori* probability of being observed. A binary series can be constructed from an observed sequence of real numbers by taking first differences, i.e., the difference of each pair of contiguous elements, and assigning (let us say) the symbol "+" if the difference is positive and "–" otherwise. In this case, the probability of a "+" (or "–") is not constant within a run: the occurrence of each "+" (or "–") is less probable than the immediately preceding one. Both of these types—constant-probability runs and up–down runs—have been used by two of the authors (Silverman and Strange) to test the randomness of nuclear alpha, beta, and electron-capture decay processes [3].

Here we apply a third type of runs analysis, based on the theory of recurrent runs, which are defined as follows: a sequence of n symbols A and $\bar{A}$ (read as "not A") contains as many runs of length t as there are nonoverlapping uninterrupted successions of exactly t symbols A [28]. This definition leads to generating functions for determining the exact probability distribution and statistical moments of runs as a function of run length and length of the data series, in contrast to approximate or asymptotic expressions that are available in the statistics literature for the first two types of runs. Also, unlike the first two types of runs tests, the theory of recurrent events can be readily generalized to test other patterns besides straight binary runs of A or $\bar{A}$.

4. THEORY OF RECURRENT RUNS

In a sequence of n trials with binary outcomes 1 or 0, we denote the occurrence of a run of t consecutive 1s (with $t > 1$) as the event ε_t. Because the runs are nonoverlapping, a given trial can only be included in one run of a fixed length t. For example, the sequence 01110 contains only one event ε_2, because the middle bit cannot belong to two different ε_2 events. However, runs of each length are counted independently of the others, so that a given bit may belong to runs of different lengths. For example, the pattern 011110 contains one event ε_5, one event ε_4, one event ε_3, and two events ε_2.

We assume the hypothesis that the trials are independent and random, with probability p of outcome 1 and $q = 1 - p$ of outcome 0. Then the mean interval between recurrence of events ε_t (the "wait time") can be shown to be [25]

$$\mu_t = \frac{1 - p^t}{qp^t}, \tag{2}$$

with variance

$$\sigma_t^2 = \frac{1}{(qp^t)^2} - \frac{2t+1}{qp^t} - \frac{p}{q^2}. \tag{3}$$

Let $N_{n,t}$ be the number of times ε_t occurs in a sequence of n trials. The expected value of $N_{n,t}$ can be shown to be [28]

$$E(N_{n,t}) = \frac{n+1}{\mu_t} + \frac{\sigma_t^2 - \mu_t(\mu_t + 1)}{2\mu_t^2}, \tag{4}$$

with variance

$$\mathrm{var}(N_{n,t}) = \frac{n\sigma_t^2}{\mu_t^3} + \frac{7\mu_t^2 + 2\mu_t^3 - \mu_t^4 + 2\mu_t\sigma_t^2(\mu_t - 1) - \sigma_t^4}{4\mu_t^4}. \tag{5}$$

In the limit of large n, the first terms dominate and the mean and variance approach the values

$$E(N_{n,t}) \cong \frac{n}{\mu_t}, \tag{6}$$

$$\mathrm{var}(N_{n,t}) \cong \frac{n}{\mu_t^3}\sigma_t^2. \tag{7}$$

Tables 2 and 3 show the observed numbers of runs of consecutive 1s for the sequences Lo-μ and Hi-μ, along with the expected numbers of these runs, both with and without interruptors. As expected, the sequences with interruptors included have fewer occurrences of runs, because a run of 1s can be halted either by the occurrence of a 0 or by the occurrence of an interruptor. The expected numbers of runs are calculated in this case by reducing p to a new empirically determined value p' for the sequence, calculated with all of the interruptors treated as 0 events.

The exact probability distribution for the occurrence of nonoverlapping runs may be derived by means of generating

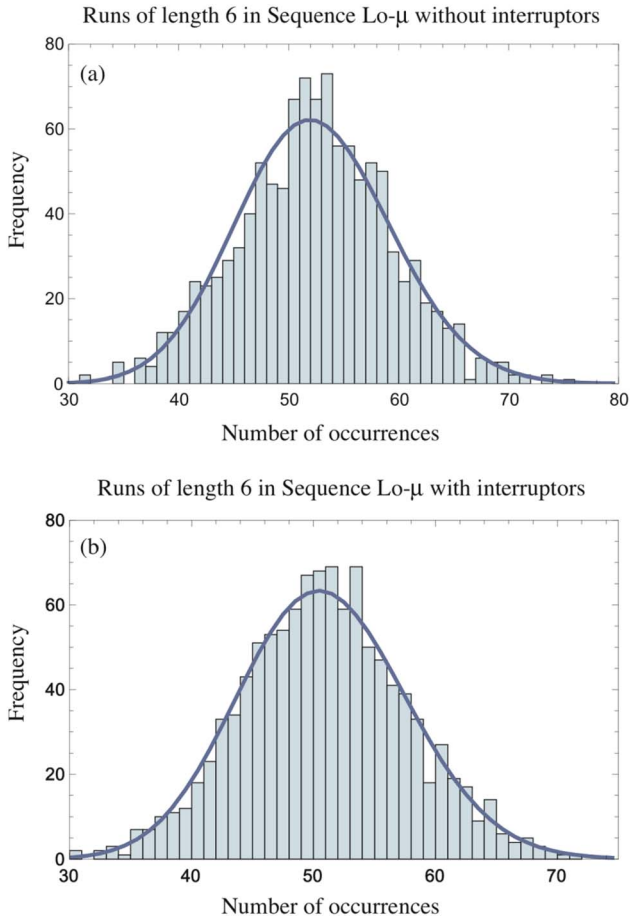

Fig. 2. (Color online) Observed frequencies of runs of 1s of length $t = 6$ occurring in M subsequences of Sequence Lo-μ of length 8192 bits, with interruptors (a) removed and (b) retained. The solid curves are the theoretical distributions, approximated by a concatenation method. The interruptors do not change the distribution appreciably because they occur in only 0.6% of the occupied time bins.

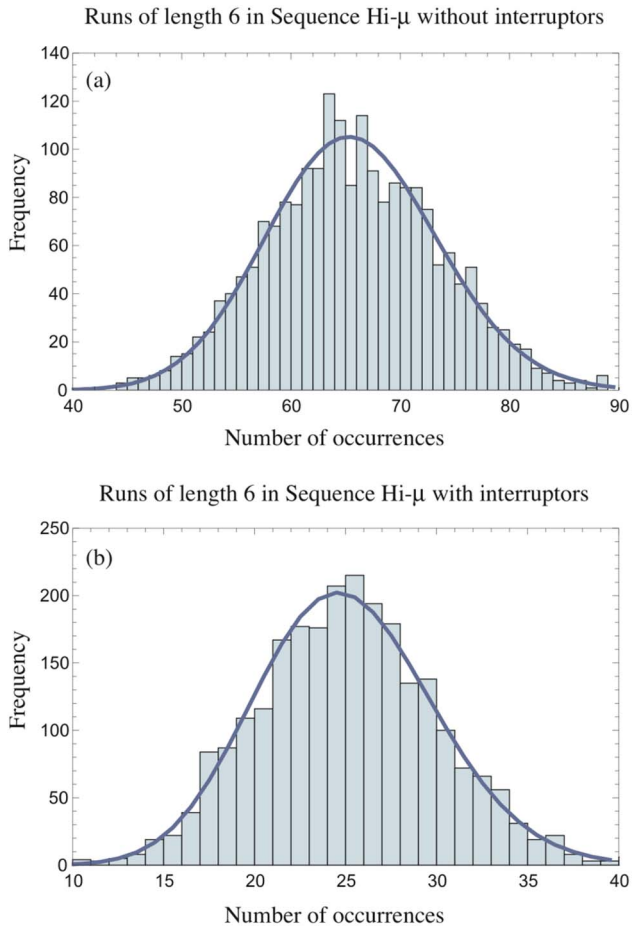

Fig. 3. (Color online) Observed frequencies of runs of length $t = 6$, for subsequences of Sequence Hi-μ with interruptors (a) removed and (b) retained. The solid curves are the theoretical distributions, approximated by a concatenation method. The interruptors, which constitute 17% of the occupied time bins, shift the distribution substantially by decreasing the frequency of occurrence of runs.

functions. Let $p_{n,t,k}$ be the probability that exactly k runs of length t occur in n trials. The moment generating function for this distribution is

$$P_{n,t}(z) = \sum_{k=0}^{\infty} p_{n,t,k} z^k. \tag{8}$$

In principle, $p_{n,t,k}$ can be obtained by evaluating the kth derivative of $P_{n,t}(z)$ with respect to z, and the distribution of run occurrences $p_{n,t,k}$ is obtained as k is varied. For any value of n, $P_{n,t}(z)$ can, in turn, be obtained from its own generating function, given by

$$H_t(z,s) = \sum_{n=1}^{\infty} P_{n,t}(z) s^n = \frac{1 - P_t(s)}{(1-s)(1 - zP_t(s))}, \tag{9}$$

where

$$P_t(s) = \frac{p^t s^t (1 - ps)}{1 - s + qp^t s^{t+1}}. \tag{10}$$

In principle, $P_{n,t}(z)$ is obtained by taking the nth derivative of $H_t(z,s)$ with respect to s.

For small sequence lengths ($n < 200$), the required derivatives of $H_t(z,s)$ and $P_{n,t}(z)$ can be readily evaluated using software such as Mathematica, but the evaluation time appears to grow nonlinearly with n and t, and quickly becomes impractical for the long sequences generated in these experiments (e.g., the distribution for $n = 8192$, $t = 6$ was successfully obtained after more than 550 h of computation). However, after $P_{n,t}(z)$ is calculated for small n, it can be used to approximate $P_{n,t}(z)$ for large n by treating the larger sequence as a concatenation of small ones, and applying a correction for the loss of runs at the boundaries [29]. For distributions analyzed here, using sequences of length 8192 trials, this method yielded values for $p_{n,t,k}$ that differed from the exact probabilities by a theoretical bound of no more than 10^{-6}. In cases where direct comparison was possible ($t = 2, 3, 4, 6$ for Sequence Lo-μ without interruptors), this discrepancy was never greater than 10^{-8}.

5. ANALYSIS OF THE POLARIZATION SEQUENCES

To compare the observed occurrences of runs with the theory, the sequences Lo-μ and Hi-μ were partitioned into M subsequences of length $n = 8192$ bits (the values of M are listed in Table 1). The number of occurrences of each run length from 2 to 13 within all the subsequences were compiled into histograms, such as those shown in Figs. 2–5. For each

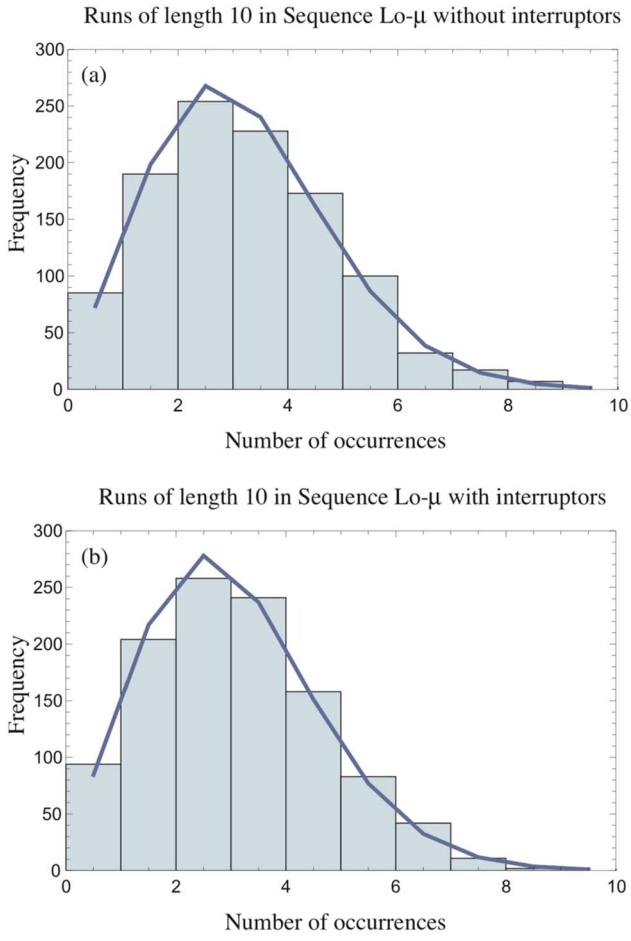

Fig. 4. (Color online) Observed frequencies of runs of length $t = 10$, for subsequences of Sequence Lo-μ with interruptors (a) removed and (b) retained. As in Fig. 2, the distributions are nearly identical because the interruptors are rare. Because the mean number of occurrences is low, the distributions for $t = 10$ are not well represented by the normal distribution, but can be closely approximated with the concatenation method (solid curves).

sequence, these 12 histograms of observed runs were tested against the theoretical distributions $N_{n,t,k} = M \cdot p_{n,t,k}$ with a χ^2 analysis [30]. The result of a χ^2 analysis is a p value, which is the probability that the observed $N_{n,t,k}$ will differ from the predicted $N_{n,t,k}$ by the observed amount or more, given that the null hypothesis of randomness is true. For an ideal random number generator, these p values are expected to be distributed uniformly on the interval $0 < p \leq 1$, so that one in every 100 sequences will have $p \leq 0.01$. Thus, on average, one in 100 sequences from an ideal random source will fail each test, by chance, at the significance level of 0.01. If more than 1% of the sequences fail at this level, the randomness of the source is suspect.

For example, a multiplicative congruential generator (MCG) is a deterministic algorithm for producing pseudorandom number sequences, such as the following:

$$\{Z_i = AZ_{i-1}(\mathrm{mod} 2^{31} - 1); i = 1, 2, \ldots\}, \tag{11}$$

where Z_0 is the (arbitrarily chosen) seed and A is the (constant) multiplier. If Z_i is less than $2^{31}/2$, the output is a 0, otherwise it is a 1. A previous analysis of this MCG employing four tests of randomness for 16 values of A found no deficiencies in these generators [31]. We used each of these generators to produce 10,000 sequences of length 200,000 bits, which were then subjected to our recurrent runs analysis for the run length $t = 2$. A given sequence was said to fail if the number of runs exceeded the expected value at the 0.01 significance level. For the multiplier $A = 2,139,391,393$, the number of failing sequences, with $p \leq 0.01$, was 128. This exceeded the expected number of 100 failures at this level by 2.8 standard deviations, indicating that this MCG with this

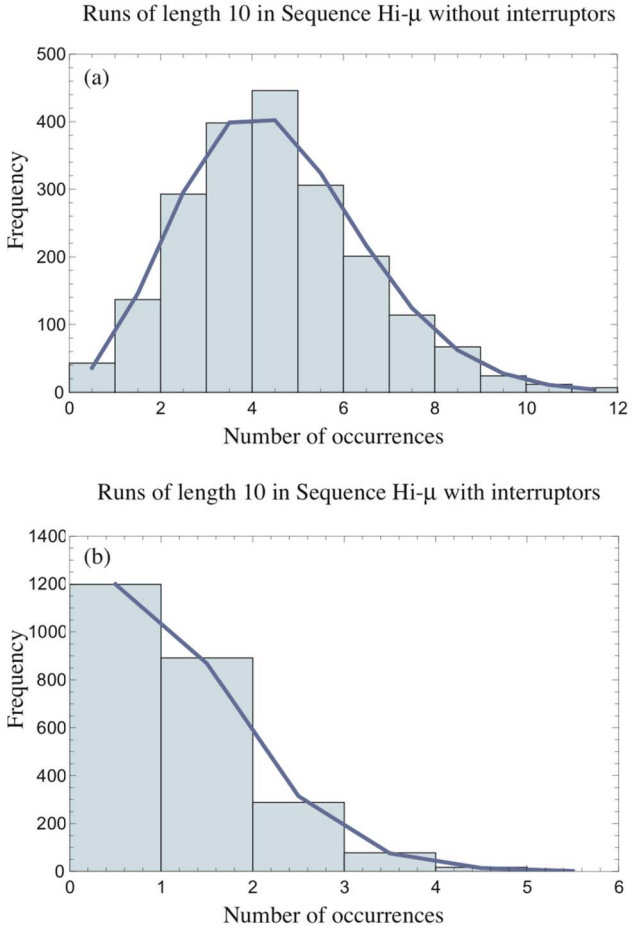

Fig. 5. (Color online) Observed frequencies of runs of length $t = 10$, for subsequences of Sequence Hi-μ with interruptors (a) removed and (b) retained. As in Fig. 3, the interruptors shift the distribution substantially in favor of lower numbers, and the concatenation method allows the theoretical distribution to be well approximated (solid curves) even where the Gaussian approximation fails.

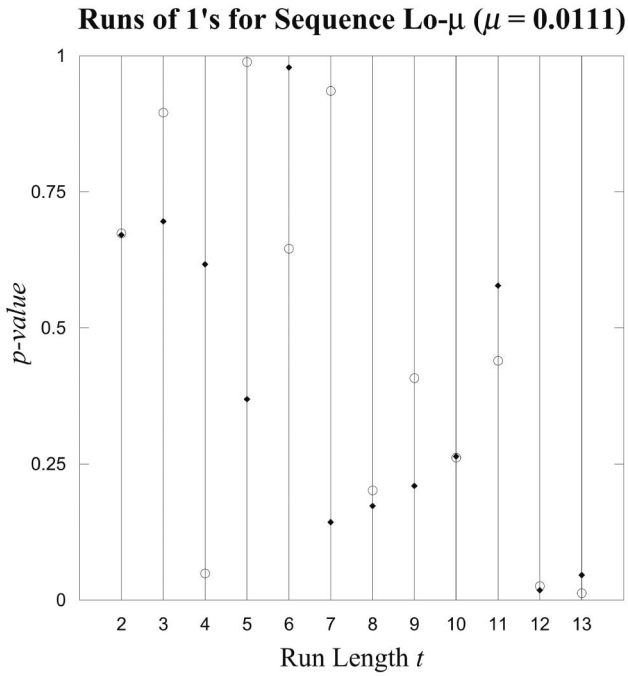

Fig. 6. P values from χ^2 tests of Sequence Lo-μ with interruptors retained (solid diamonds) and removed (open circles) for run lengths 2–13.

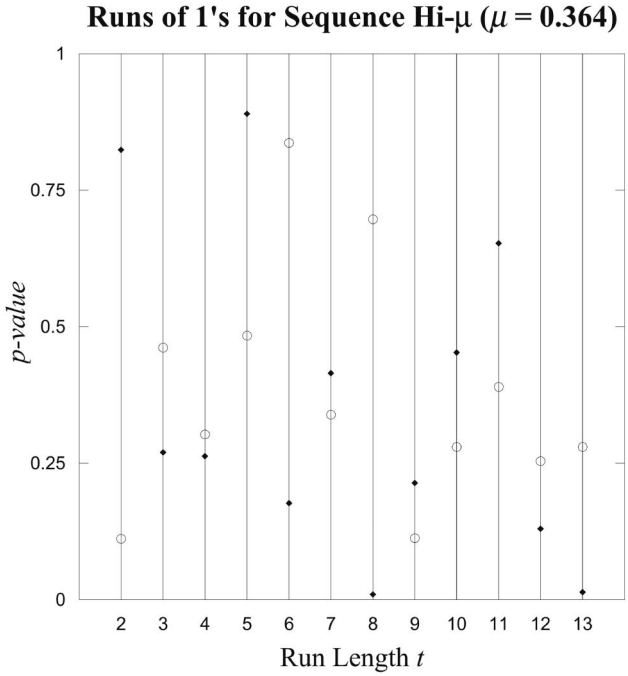

Fig. 7. P values from χ^2 tests of Sequence Hi-μ, with interruptors retained (solid diamonds) and removed (open circles) for run lengths 2–13.

particular multiplier is not consistent with the null hypothesis of randomness.

Returning to the analysis of our data, the p values for sequences Lo-μ and Hi-μ are shown in Figs. 6 and 7, respectively. There are no frequent occurrences of extremely low p values, either with or without interruptors, which would signal a disagreement with the hypothesis of randomness. Furthermore, the presence or absence of interruptors does not appear to systematically shift the p values higher or lower. This is true even for Sequence Hi-μ (Fig. 7), where interruptors account for more than 1/6 of all the events.

Finally, the preceding analysis was also applied to runs of horizontal polarization outcomes (0s) for both sequences, with interruptors both rejected and retained. The results were similar to those presented here, and revealed no statistically significant evidence of any deviations from randomness.

6. CONCLUSION

We have performed a new analysis of the quantum randomness of single-photon polarization measurements, based on a general theory of recurrent runs that is more comprehensive than our previous analysis based on the National Institute of Standards and Technology (NIST) Test Suite [15]. Because it can be applied directly to sequences of any bias, without requiring numerical unbiasing procedures, this new analysis can be generalized to include multiphoton events (interruptors), which are usually discarded in polarization-based quantum random number generators. The randomness of single-photon polarization sequences appears to be unaffected by the removal of these events.

The method presented here can be generalized to examine the recurrence of any arbitrary patterns of 1s and 0s in binary random sequences: one future direction that this implies is to search for signatures of detector dead time and/or afterpulsing effects in photonically generated random number sequences [32]. These effects may only become apparent for much shorter data collection time bins, of the order of the dead time of the single-photon detectors; to this end, we are increasing the data transfer rates in our coincidence-counting electronics [33]. We also intend to go beyond the limits of this stationary test to look for time-dependent or spectral correlations in the polarization measurements, which might arise from thermal changes in the phase-matching conditions within the PDC [22]. Finally, we intend to examine further applications of the concatenation method of approximation for $P_{n,t}(z)$ [29], which may enable the rapid calculation of other computationally intensive generating functions appearing in a wide array of statistical problems.

APPENDIX A: COMPARISON OF RUNS TESTS WITH OTHER TESTS OF RANDOMNESS

The null hypothesis tested in our experiment is that there is no underlying predictive ordering to the measurement outcomes for single photons prepared in a quantum superposition state of horizontal and vertical polarization. Conventionally, the sensitivity of a statistical test is gauged by its power, which is defined as the probability of *not* making a Type II error —i.e., of not wrongly accepting the null hypothesis when it is false [34]. (A Type I error is to wrongly reject the null hypothesis when it is true.) There is no simple formula for calculating the power of a runs test under general circumstances. In general, the power of a statistical test may depend on the circumstances of each situation. Nevertheless, there are reasons to believe that runs tests are particularly effective in comparison with other tests that could have been employed.

For example, NIST tested three pseudorandom number generators with five statistical tests at a level of significance of 1%. Each generator was used to generate 300 series of 1 million elements each. The relative effectiveness of the statistical tests was dependent on the generator, but runs tests were shown to be the most sensitive in all of the published graphical summaries [35].

Another basis for tests of randomness is entropy, which in statistical physics is related to order and in communications science is related to information. Power calculations of one such test, which measured the deviation of the estimated entropy of a data set of length n from the theoretical maximum of a random series of the same length, led to the conclusion that the test is more powerful than a runs test for low n, but less powerful than a runs test for large n [36]. The lengths of the data series in our experiment are very large, in which case runs tests would be preferred over the entropy test. Moreover, the entropy test yields a single statistic, whereas runs tests yield a statistic for each run length.

Finally, in tests carried out by one of the authors (Silverman) on the randomness of first differences of closing stock prices of more than 20 listed companies of the New York Stock Exchange, the resulting series passed tests of randomness based on autocorrelation, periodicity (by means of power spectra), and entropy, but failed runs tests (against distributions of $p_{n,t,k}$) for nearly all values of run length t [37].

ACKNOWLEDGMENTS

We thank Matt Bermudez for help with the data collection, and Jared Zimmerman for help with the analysis.

REFERENCES

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145–195 (2002).
2. V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys. **81**, 1301–1350 (2009).
3. M. P. Silverman, W. Strange, C. R. Silverman, and T. C. Lipscombe, "Tests of alpha-, beta-, and electron capture decays for randomness," Phys. Lett. A **262**, 265–273 (1999).
4. M. P. Silverman and W. Strange, "Experimental tests for randomness of quantum decay examined as a Markov process," Phys. Lett. A **272**, 1–9 (2000).
5. M. P. Silverman, W. Strange, C. R. Silverman, and T. C. Lipscombe, "Tests for randomness of spontaneous quantum decay," Phys. Rev. A **61**, 042106 (2000).
6. T. Erber, "Testing the randomness of quantum mechanics: nature's ultimate cryptogram?," Ann. N.Y. Acad. Sci. **755**, 748–756 (1995).
7. A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, "Optical quantum random number generator," J. Mod. Opt. **47**, 595–598 (2000).
8. H.-Q. Ma, Y. Xie, and L.-A. Wu, "Random number generation based on the time of arrival of single photons," Appl. Opt. **44**, 7760–7763 (2005).
9. M. Stipcevic and B. Medved Rogina, "Quantum random number generator based on photonic emission in semiconductors," Rev. Sci. Instrum. **78**, 045104 (2007).

10. J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, "A high speed, postprocessing free, quantum random number generator," Appl. Phys. Lett. **93**, 031109 (2008).
11. M. Furst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, "High speed optical quantum random number generation," Opt. Express **18**, 13029 (2010).
12. H.-Q. Ma, S.-M. Wang, D. Zhang, J.-T. Chang, L.-L. Ji, Y.-X. Hou, and L.-A. Wu, "A random number generator based on quantum entangled photon pairs," Chin. Phys. Lett. **21**, 1961–1964 (2004).
13. M. Fiorentino, C. Santori, S. M. Spillane, and R. G. Beausoleil, "Secure self-calibrating quantum random-bit generator," Phys. Rev. A **75**, 032334 (2007).
14. I. J. Owens, R. J. Hughes, and J. E. Nordholt, "Entangled quantum-key-distribution randomness," Phys. Rev. A **78**, 022307 (2008).
15. D. Branning and M. V. Bermudez, "Testing quantum randomness of single-photon polarization measurements with the NIST test suite," J. Opt. Soc. Am. B **27**, 1594–1602 (2010).
16. T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact random number generator," Rev. Sci. Instrum. **71**, 1675–1680 (2000).
17. D. C. Burnham and D. L. Weinberg, "Observation of simultaneity in parametric production of optical photon pairs," Phys. Rev. Lett. **25**, 84–87 (1970).
18. J. Von Neumann, "Various techniques used in connection with random digits," in *Monte Carlo Method*, Vol. 12 of National Bureau of Standards Applied Mathematics Series (1951), pp. 36–38.
19. Y. Peres, "Iterating von Neumann's procedure for extracting random bits," Ann. Stat. **20**, 590–597 (1992).
20. S. Scheel, "Single-photon sources—an introduction," J. Mod. Opt. **56**, 141–160 (2009).
21. L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics* (Cambridge Univ. Press, 1995).
22. A. Migdall, "Polarization directions of noncollinear phase-matched optical parametric downconversion output," J. Opt. Soc. Am. B **14**, 1093–1098 (1997).
23. C. K. Hong and L. Mandel, "Experimental realization of a localized one-photon state," Phys. Rev. Lett. **56**, 58–60 (1986).
24. D. Branning, S. Bhandari, and M. Beck, "Low-cost coincidence-counting electronics for undergraduate quantum optics," Am. J. Phys. **77**, 667–670 (2009).
25. J. V. Bradley, *Distribution-Free Statistical Tests* (Prentice-Hall, 1968); for more information on runs tests, see pp. 250–282.
26. A. M. Mood, "The distribution theory of runs," Ann. Math. Stat. **11**, 367–392 (1940).
27. H. Levene and J. Wolfowitz, "The covariance matrix of runs up and down," Ann. Math. Stat. **15**, 58–69 (1944).
28. W. Feller, *An Introduction to Probability Theory and its Applications* (Wiley, 1950), Vol. 1, pp. 299–300.
29. D. Branning, A. Katcher, and M. P. Silverman are preparing a manuscript to be called "Concatenation method for approximating distributions of nonoverlapping recurrent events."
30. P. R. Bevington and D. K. Robertson, *Data Reduction and Error Analysis* (McGraw-Hill, 2003).
31. G. S. Fishman and L. R. Moore, "A statistical evaluation of multiplicative congruential random number generators with modulus $2^{31}-1$," J. Am. Stat. Assoc. **77**, 129–136 (1982).
32. S. Cova, M. Ghioni, A. Lacaita, C. Samori, and F. Zappa, Appl. Opt. **35**, 1956–1976 (1996).
33. D. Branning, S. Khanal, Y. H. Shin, B. Clary, and M. Beck, "Scalable multi-photon coincidence-counting electronics," Rev. Sci. Instrum. **82**, 016102 (2011).
34. M. G. Kendall and A. Stuart, *The Advanced Theory of Statistics* (Griffin 1961), Vol. 2, pp. 164–165.
35. J. Soto, "Statistical testing of random number generators," *Proceedings of the 22nd National Information Systems Security Conference* (National Institute of Standards and Technology, 1999), csrc.nist.gov/groups/ST/toolkit/rng/documents/nissc-paper.pdf.
36. S. Chatterjee, M. R. Yilmaz, M. Habibuliah, and M. Laudato, Commun. Stat. Theory Methods **29**, 655–675 (2000).
37. M. P. Silverman is preparing a manuscript to be called "A certain uncertainty—physical insights from random events."