Von Neumann Normalisation and Symptoms of Randomness: An Application to Sequences of Quantum Random Bits

Alastair A. Abbott* and Cristian S. Calude**

Department of Computer Science, University of Auckland,
Private Bag 92019, Auckland, New Zealand
aabb009@aucklanduni.ac.nz, cristian@cs.auckland.ac.nz
www.cs.auckland.ac.nz

Abstract. Due to imperfections in measurement and hardware, the flow of bits generated by a quantum random number generator (QRNG) contains bias and correlation, two symptoms of non-randomness. There is no algorithmic method to eliminate correlation as this amounts to guaranteeing incomputability. However, bias can be mitigated: QRNGs use normalisation techniques such as von Neumann's method—the first and simplest technique for reducing bias—and other more efficient modifications.

In this paper we study von Neumann un-biasing normalisation for an ideal QRNG operating 'to infinity', i.e. producing an infinite bit-sequence. We show that, surprisingly, von Neumann un-biasing normalisation can both increase or *decrease* the (algorithmic) randomness of the generated sequences. The impact this has on the quality of incomputability of sequences of bits from QRNGs is discussed.

A successful application of von Neumann normalisation—in fact, any un-biasing transformation—does exactly what it promises, *un-biasing*, one (among infinitely many) symptoms of randomness; it will not produce 'true' randomness, a mathematically vacuous concept.

1 Introduction

The outcome of some individual quantum-mechanical events cannot in principle be predicted, so they are thought as ideal sources of random numbers. An incomplete list of quantum phenomena used for random number generation include nuclear decay radiation sources [24], the quantum mechanical noise in electronic circuits known as shot noise [25] or photons travelling through a semi-transparent mirror [15,19,23,26,27,29].

Due to imperfections in measurement and hardware, the flow of bits generated by a quantum random number generator (QRNG) contains bias and correlation, two symptoms of non-randomness [7]. In this paper we study the first and simplest technique for reducing bias: von Neumann normalisation [31]. We specifically investigate the effect this has on the quality of randomness of infinite

* AA was in part supported by the CDMTCS.
** CC was in part supported by the CDMTCS and UoA R&SL grant.

C.S. Calude et al. (Eds.): UC 2011, LNCS 6714, pp. 40–51, 2011.

sequences of quantum random bits. Although some of the mathematical results we present apply to any RNG, our approach is intimately motivated by the operation of photon-based QRNGs, more specifically, by their mechanisms [3] and the quality of randomness they produce [2].

Von Neumann's method considers pairs of bits, and takes one of three actions: a) pairs of equal bits are discarded; b) the pair 01 becomes 0; c) the pair 10 becomes 1. Contrary to wide spread claims, the technique works for some sources of bits, but not for all. The output produced by a source of independent and constantly biased bits is transformed into a flow of bits in which the frequency of 0's and 1's are equal: 50% for each.

Mathematically, the notion of 'true randomness' is vacuous, so we can investigate only symptoms of randomness. Mathematical arguments show that we have to study infinite sequences of bits: various forms of algorithmic randomness [10] are each defined by an infinity of conditions, some 'statistical' (like bias), some 'non-statistical' (like lack of computable correlations). The symptoms of 'randomness' often emphasised for the source of a QRNG are unpredictability and uniformity of distribution. In fact, here are three—out of an infinity of—symptoms of randomness which can be used to understand quantum randomness:

1) *Unpredictability*, which is a manifestation of the strong incomputability of the bits [9] (an infinite sequence is strongly incomputable if it is provable that no Turing machine or equivalent formalism can compute and certify more than finitely many scattered bits of the sequence). For quantum bits, no bit at all can be provably computed in advance [2]. This type of unpredictability is strong—it is not due to ignorance of the system but is a fundamental feature of the system.
2) *Uniform distribution* of the generated bits (not just of individual bits, but of all n-bit strings), a manifestation of the Borel normality of a sequence. Unlike strong incomputability, this is not known to be guaranteed for quantum bits, but as we shall see, under certain conditions the sequence is Borel normal with probability one[1].
3) *Lack of patterns*, a manifestation of algorithmic randomness (incompressibility) of a sequence of bits. As for normality, this is not known to be guaranteed for quantum bits, but again a measure-theoretical argument can show such sequences are algorithmically random with probability one if normalisation can be successfully conducted.

Mathematically, it is well known that 3) $\rightarrow$ 1) and 2), but the converse implications are false. Further, both implications 1) $\rightarrow$ 2) and 2) $\rightarrow$ 1) are false [7]. While computability implies predictability, unpredictability depends not just on incomputability, but the *strength* of incomputability. Further, no sequence is absent of all possible patterns so only computable patterns can be excluded. This is one of the reasons for the impossibility of 'true randomness'.

[1] It is important to note the subtle theoretical difference between a *probability-one* event and a *provably guaranteed* event in the probability space of infinite sequences: in contrast with a provably guaranteed event whose complement is empty, the complement of a probability-one event can be not only non-empty, but even infinite [11].

Up until now, QRNGs have been given largely the same mathematical treatment used for pseudo-random number generators, focusing on producing uniformly distributed bits. For real devices this primarily entails the use of randomness extractors—which von Neumann's procedure is one of—to make the source as close as possible to the uniform distribution [30]. But as we have seen, uniformity does not imply unpredictability. Indeed, a device outputting successive bits of a predetermined Borel normal sequence will appear uniformly distributed. However, the strength of QRNGs is in the incomputability of the bits, and this requires computability analysis rather than probabilistic treatment. Until now, the unpredictability has been assumed an intrinsic feature of quantum bits and has escaped rigorous treatment [26]. A step in the right direction was made in [23], where violation of Bell inequalities was used to try and verify unpredictability. However, Bell tests, like the probabilistic treatment of the distribution, are unable to say anything about the computability of the bits [3].

Since uniformity of distribution is a necessary requirement for a good QRNG in addition to incomputability, techniques such as von Neumann's will need to be used for real devices where bias and correlation is inevitable. In this paper we study the effect of von Neumann normalisation on infinite sequences with a particular focus on the effect this has on the symptoms of randomness within the sequences. We focus on von Neumann normalisation because it is simple, easy to implement, and (along with the more efficient iterated version due to Peres [22] for which the results will also apply) is widely used by current proposals for QRNGs [19,20,13,26].

The main results of this paper are the following. In the 'ideal case', the von Neumann normalised output of an independent constantly biased QRNG is the probability space of the uniform distribution (un-biasing). We treat only the case of an infinite sequence of bits, but the corresponding result for finite strings also holds [1]. It is important to note that independence in the mathematical sense of multiplicity of probabilities is a model intended to correspond to the physical notion of independence of outcomes [16]. In order to study the theoretical behaviour of QRNGs, which are based on the *assumption of physical independence of measurements*, we must translate this appropriately into our formal model. In [1] we carefully defined independence of QRNGs to achieve this aim.

We then examine the effect von Neumann normalisation has on various properties of infinite sequences. In particular, Borel normality and (algorithmic) randomness are invariant under normalisation, but suprisingly for ε-random sequences with $0 < \varepsilon < 1$, normalisation can both decrease or increase the randomness of the source. Full proofs of all results presented in this paper can be found in [1].

2 Notation

We present the main notation used throughout the paper. By 2^X we denote the power set of X. By $|X|$ we denote the cardinality of the set of X. Let $B = \{0, 1\}$ and denote by B^* the set of all bit-strings (λ is the empty string). If $x \in B^*$

and $i \in B$ then $|x|$ is the length of x and $\#_i(x)$ represents the number of i's in x. By B^n we denote the finite set $\{x \in B^* \mid n = |x|\}$. The concatenation product of two subsets X, Y of B^* is defined by $XY = \{xy \mid x \in X, y \in Y\}$. If $X = \{x\}$ then we write xY instead of $\{x\}Y$. By B^ω we denote the set of all infinite binary sequences. For $\mathbf{x} \in B^\omega$ and natural n we denote by $\mathbf{x}(n)$ the prefix of $\mathbf{x}$ of length n. We write $w \sqsubset v$ or $w \sqsubset \mathbf{x}$ in case w is a prefix of the string v or the sequence $\mathbf{x}$.

A prefix-free (Turing) machine is a Turing machine whose domain is a prefix-free set of strings [7]. The prefix complexity of a string, $H_W(\sigma)$, induced by a prefix-free machine W is $H_W(\sigma) = \min\{|p| \ : \ W(p) = \sigma\}$. Fix a computable ε with $0 < \varepsilon \leq 1$. An ε–universal prefix-free machine U is a machine such that for every machine W there is a constant c (depending on U and W) such that $\varepsilon \cdot H_U(\sigma) \leq H_W(\sigma) + c$, for all $\sigma \in B^*$. If $\varepsilon = 1$ then U is simply called a universal prefix-free machine. A sequence $\mathbf{x} \in B^\omega$ is called ε–random if there exists a constant c such that $H_U(\mathbf{x}(n)) \geq \varepsilon \cdot n - c$, for all $n \geq 1$. Sequences that are 1–random are simply called random.

A sequence $\mathbf{x}$ is called Borel m–normal ($m \geq 1$) if for every $1 \leq i \leq 2^m$ one has: $\lim_{n\to\infty} N_i^m(\mathbf{x}(n))/\lfloor \frac{n}{m} \rfloor = \lim_{n\to\infty} \mathcal{N}_i^m(\mathbf{x}(n))/n = 2^{-m}$; here $N_i^m(y)$ ($\mathcal{N}_i^m(y)$) counts the number of non-overlapping (respectively, overlapping [18]) occurrences of the ith (in lexicographical order) binary string of length m in the string y. The sequence $\mathbf{x}$ is called Borel normal if it is Borel m–normal, for every natural $m \geq 1$.

A probability space is a measure space such that the measure of the whole space is equal to one [5]. More precisely, a (Kolmogorov) probability space is a triple consisting of a sample space Ω, a σ–algebra $\mathcal{F}$ on Ω, and a probability measure P, i.e. a countably additive function defined on $\mathcal{F}$ with values in $[0, 1]$ such that $P(\Omega) = 1$.

3 Von Neumann Normalisation

We define the mapping $F : B^2 \to B \cup \{\lambda\}$ as

$$F(x_1x_2) = \begin{cases} \lambda & \text{if } x_1 = x_2, \\ x_1 & \text{if } x_1 \neq x_2, \end{cases}$$

and $f : B \to B^2$ as $f(x) = x\bar{x}$, where $\bar{x} = 1 - x$. Note that for all $x \in B$ we have $F(f(x)) = x$ and, for all $x_1, x_2 \in B$ with $x_1 \neq x_2$, $f(F(x_1x_2)) = x_1x_2$.

For $m \leq \lfloor n/2 \rfloor$ we define the normalisation function $VN_{n,m} : B^n \to \left(\bigcup_{k\leq m} B^k\right) \cup \{\lambda\}$ as

$$VN_{n,m}(x_1 \dots x_n) = F(x_1x_2)F(x_3x_4) \cdots F\left(x_{(2\lfloor \frac{m}{2} \rfloor - 1)} x_{2\lfloor \frac{m}{2} \rfloor}\right).$$

Consider a string of n independent bits produced by a constantly biased QRNG. Let p_0, p_1 be the probability that a bit is 0 or 1, respectively, with $p_0 + p_1 = 1$, $p_0, p_1 \leq 1$.

The probability space of bit-strings produced by the QRNG is $(B^n, 2^{B^n}, P_n)$ where $P_n : 2^{B^n} \to [0,1]$ is defined by

$$P_n(X) = \sum_{x \in X} p_0^{\#_0(x)} p_1^{\#_1(x)}, \tag{1}$$

for all $X \subseteq B^n$.

The space $(B^n, 2^{B^n}, P_n)$ is just the n-fold product of the single bit probability space $(B, 2^B, P_1)$, and for this reason it is often called an 'independent identically-distributed bit source'. The outcome of successive context preparations and measurements (which photon-based QRNGs consist of) are postulated to be independent of previous and future outcomes [14]. This means there must be no causal link between one measurement and the next within the system (preparation and measurement devices included) so that the system has no memory of previous or future events. It is this physical understanding which is behind the modelling of QRNGs as independent bit sources.

The above assumption needs to be made clear as in high bit-rate experimental configurations to generate QRNs with photons, its validity may not always be clear. If the wave-functions of successive photons 'overlap' the assumption no longer holds and (anti)bunching phenomena may play a role. This is an issue that needs to be more seriously considered in QRNG design and will only become more relevant as the bit-rate of QRNGs is pushed higher and higher [3].

The von Neumann normalisation function $VN_{n,m}$ transforms the source probability space $(B^n, 2^{B^n}, P_n)$ into the target probability space $(B^m, 2^{B^m}, P_{n\to m})$. The target space of normalised bit-strings of length $1 < m \leq \lfloor n/2 \rfloor$ associated to the source probability space $(B^n, 2^{B^n}, P_n)$ is the space $(B^m, 2^{B^m}, P_{n\to m})$, where $P_{n\to m} : 2^{B^m} \to [0,1]$ is defined for all $Y \subseteq B^m$ by the formula:

$$P_{n\to m}(Y) = \frac{P_n\left(VN_{n,m}^{-1}(Y)\right)}{P_n\left(VN_{n,m}^{-1}(B^m)\right)}.$$

The von Neumann procedure transforms the source probability space with constant bias into the probability space with the uniform distribution over B^m, i.e. the target probability space $(B^m, 2^{B^m}, P_{n\to m})$ has $P_{n\to m} = U_m$, the uniform distribution. Simple examples show that independence and the constant bias of P_n are essential hypotheses in the following result.

Theorem 1 (von Neumann, [1,31]). *Assume that* $1 < m \leq \lfloor n/2 \rfloor$. *In the target probability space* $(B^m, 2^{B^m}, P_{n\to m})$ *associated to the source probability space* $(B^n, 2^{B^n}, P_n)$ *we have* $P_{n\to m}(Y) = U_m(Y) = |Y| \cdot 2^{-m}$, *for every* $Y \subseteq B^m$.

4 Infinite Von Neumann Normalisation

We extend von Neumann normalisation to infinite sequences of bits to study those produced by QRNGs. First, we extend the definition of the normalisation function $VN_{n,m}$ to sequences. We define $VN : B^\omega \to B^\omega \cup B^*$ as

$$VN(\mathbf{x} = x_1 \dots x_n \dots) = F(x_1x_2)F(x_3x_4) \cdots F(x_{2\lfloor \frac{n}{2} \rfloor - 1} x_{2\lfloor \frac{n}{2} \rfloor}) \cdots .$$

For convenience we also define $VN_n : B^\omega \to \left(\bigcup_{k\le n} B^k\right) \cup \{\lambda\}$ as

$$VN_n(\mathbf{x}) = F(x_1x_2)F(x_3x_4)\cdots F(x_{2\lfloor \frac{n}{2}\rfloor -1}x_{2\lfloor \frac{n}{2}\rfloor}) = VN_{n,n}(x_1\dots x_n).$$

Secondly, we introduce the probability space of infinite sequences as in [7]. Let $A_Q = \{a_1, \dots, a_Q\}$, $Q \ge 2$ be an alphabet with Q elements. We let $\mathcal{P} = \{xA_Q^\omega \mid x \in A_Q^*\} \cup \{\emptyset\}$ and $\mathcal{C}$ be the class of all finite mutually disjoint unions of sets in $\mathcal{P}$; the class $\mathcal{P}$ can be readily shown to generate a σ-algebra $\mathcal{M}$. Using Theorem 1.7 from [7], the probabilities on $\mathcal{M}$ are characterised by the functions $h : A_Q^* \to [0,1]$ satisfying the following two conditions: 1. $h(\lambda) = 1$, 2. $h(x) = h(x_{a_1}) + \cdots + h(x_{a_Q})$, for all $x \in A_Q^*$.

If $Q = 2$ so $A_2 = B$, and for $x \in B^n$ we take $h(x) = P_n(\{x\})$ with P_n as defined in (1), then the above conditions are satisfied. This induces our probability measure μ_P on $\mathcal{M}$, which satisfies $\mu_P(XB^\omega) = P_n(X)$ for $X \subseteq B^n$. Hence the suitable extension of the finite case probability space to infinite generated sequences is the space $(B^\omega, \mathcal{M}, \mu_P)$. In the special case when $p_0 = p_1$ we get the Lebesgue probability $\mu_{P_L}(XB^\omega) = \sum_{x\in X} 2^{-|x|}$.

In general, if $Q \ge 2$, $p_i \ge 0$ for $i = 1, \dots, Q$ are reals in [0,1] such that $\sum_{i=1}^{Q} p_i = 1$, we can take $h_Q(x) = p_1^{\#_{a_1}(x)} \dots p_Q^{\#_{a_Q}(x)}$ to obtain the probability space $(A_Q^\omega, \mathcal{M}, \mu_{P_Q})$ in which $\mu_{P_Q}(xA_Q^\omega) = h_Q(x)$, for all $x \in A_Q^*$.

Theorem 2. *For every string $y \in B^*$ there exists an uncountable set $R \subset B^\omega$ of μ_P measure zero such that for all $\mathbf{x} \in R$, $VN(\mathbf{x}) = y$.*

Proof. Let $y = y_1 \dots y_n \in B^*$ and $D = \{00, 11\}$, the two-bit blocks which are deleted by von Neumann normalisation and $y' = f(y_1) \dots f(y_n)$. Then every sequence $\mathbf{x} \in y'D^\omega$ satisfies $VN(\mathbf{x}) = VN_{2n}(\mathbf{x})VN(x_{2n+1}x_{2n+2}\dots) = y$ since $VN_{2n}(\mathbf{x}) = VN_{2n,2n}(y') = y$ and for all $\mathbf{z} \in D^\omega$ we have $VN(\mathbf{z}) = \lambda$. Obviously, the set $R = y'D^\omega$ is uncountable and has μ_P measure zero as the set of Borel normal sequences has measure one [7]. □

Corollary 1. *The set $Q = \{\mathbf{x} \in B^\omega \mid VN(x) \in B^*\}$ has μ_P measure zero.*

It is interesting to note that the 'collapse' in the generated sequence produced by von Neumann normalisation in Theorem 2 is not due to computability properties of the sequence. In particular, there are random sequences that collapse to any string, so to strings which are not Borel normal (see [7] for the definition of normality for strings).

In the following we need a measure-theoretic characterisation of random sequences, so we present a few facts from constructive topology and probability.

Consider the compact topological space (A_Q^ω, τ) in which the basic open sets are the sets wA_Q^ω, with $w \in A_Q^*$. Accordingly, an open set $G \subset A_Q^\omega$ is of the form $G = VA_Q^\omega$, where $V \subset A_Q^*$.

From now on we assume that the reals $p_i, 1 \le i \le Q$ which define the probability μ_{P_Q} are all computable. A constructively open set $G \subset A_Q^\omega$ is an open set $G = VA_Q^\omega$ for which $V \subset A_Q^*$ is computably enumerable (c.e.). A constructive sequence of constructively open sets, c.s.c.o. sets for short, is a sequence

$(G_m)_{m\geq 1}$ of constructively open sets $G_m = V_m A_Q^\omega$ such that there exists a c.e. set $X \subset A_Q^* \times \mathbf{N}$ with $V_m = \{x \in A_Q^* \mid (x,m) \in X\}$, for all natural $m \geq 1$. A constructively null set $S \subset A_Q^\omega$ is a set for which there exists a c.s.c.o. sets $(G_m)_{m\geq 1}$ with $S \subset \bigcap_{m\geq 1} G_m$, $\mu_{P_Q}(G_m) \leq 2^{-m}$. A sequence $\mathbf{x} \in A_Q^\omega$ is random in the probability space $(A_Q^\omega, \mathcal{M}, \mu_{P_Q})$ if $\mathbf{x}$ is not contained in any constructively null set in $(A_Q^\omega, \mathcal{M}, \mu_{P_Q})$. For the case of the Lebesgue probability μ_{P_L} the measure-theoretic characterisation of random sequences holds true: $\mathbf{x}$ is random if and only if $\mathbf{x}$ is not contained in any constructively null set of $(A_Q^\omega, \mathcal{M}, \mu_{P_L})$ [7,21].

We continue with another instance in which von Neumann normalisation decreases randomness.

Proposition 1. *There exist (continuously many) infinite ε-random sequences $\mathbf{x} \in B^\omega$ such that $VN(\mathbf{x}) = 000\ldots00\ldots$ for any computable $0 < \varepsilon < 1$.*

We follow this with instances for which the converse is true: von Neumann normalisation conservers or increases randomness.

Proposition 2. *There exist (continuously many) infinite ε-random sequences $\mathbf{x} \in B^\omega$ such that $VN(\mathbf{x})$ is random for any computable $0 < \varepsilon < 1$.*

Theorem 3. *Let $\mathbf{x} \in B^\omega$ be Borel normal in $(B^\omega, \mathcal{M}, \mu_{P_L})$. Then $VN(\mathbf{x})$ is also Borel normal in $(B^\omega, \mathcal{M}, \mu_{P_L})$.*

Proof. Note that $VN(\mathbf{x}) \in B^\omega$ because $\mathbf{x}$ contains infinitely many occurrences of 01 on even/odd positions. Let $D = \{00, 11\}$, $\mathbf{x}^*(n) = VN_{n,n}(\mathbf{x}(n))$, $n' = |\mathbf{x}^*(n)|$. We have

$$\lim_{n'\to\infty} \frac{N_i^m(\mathbf{x}^*(n))}{n'} = \lim_{n'\to\infty} \left(\frac{n}{n'}\right)\left(\frac{N_i^m(\mathbf{x}^*(n))}{n}\right),$$

but as $n \to \infty$, $n' \to \infty$. We thus have $\lim_{n'\to\infty} \frac{n'}{n} = 2^{-1}$, by the normality of $\mathbf{x}$. The number of occurrences of each $i = i_1 \ldots i_m \in B^m$ in $\mathbf{x}^*(n)$ is the number of occurrences of $i' = f(i_1)y_1 f(i_2)\ldots y_{m-1}f(i_m)$ in $\mathbf{x}(n)$, summed over all $y_1, \ldots, y_{m-1} \in D^*$. Viewing i' as a string over B^2 we have:

$$\lim_{n'\to\infty} \frac{N_i^m(\mathbf{x}^*(n))}{n} = \lim_{n\to\infty} \frac{\sum_{y_1,\ldots,y_{m-1}} N_{i'}^{|i'|}(\mathbf{x}(n))}{n} = 2^{-(m+1)}.$$

Hence, both limits exist and we have

$$\lim_{n'\to\infty} \frac{N_i^m(\mathbf{x}^*(n))}{n'} = \lim_{n'\to\infty} \left(\frac{n}{n'}\right)\left(\frac{N_i^m(\mathbf{x}^*(n))}{n}\right) = 2^{-m}.$$

Since this holds for all m, i, we have that $VN(\mathbf{x})$ is Borel normal. □

Let $A_Q = \{a_1, \ldots, a_Q\}$, $Q \geq 3$. Let $\sum_{i=1}^Q p_i = 1$ where $p_i \geq 0$ for $i = 1, \ldots, Q$ and $(A_Q^\omega, \mathcal{M}, \mu_{P_Q})$ be the probability space defined by the probabilities p_i. Let

$A_{Q-1} = \{a_1, \ldots, a_{Q-1}\}$ and $(A^\omega_{Q-1}, \mathcal{M}, \mu_{P^T_{Q-1}})$ be the probability space defined by the probabilities

$$p^T_i = p_i \left(1 + \frac{p_Q}{\sum_{j=1}^{Q-1} p_j}\right) = \frac{p_i}{1 - p_Q},$$

with $1 \leq i \leq Q-1$. Let $T : A^*_Q \to A^*_{Q-1}$ be the monoid morphism defined by $T(a_i) = a_i$ for $1 \leq i \leq Q-1$, $T(a_Q) = \lambda$; $T(x) = T(x_1)T(x_2)\cdots T(x_n)$ for $x \in A^n_Q$. As T is prefix-increasing we naturally extend T to sequences to obtain the function $T : A^\omega_Q \to A^\omega_{Q-1}$ given by $T(\mathbf{x}) = \lim_{n\to\infty} T(\mathbf{x}(n))$ for $\mathbf{x} \in A^\omega_Q$.

Lemma 1. *The transformation T is $(\mu_{P_Q}, \mu_{P^T_{Q-1}})$–preserving, i.e. for all $w \in A^*_{Q-1}$ we have $\mu_{P_Q}\left(T^{-1}(wA^\omega_{Q-1})\right) = \mu_{P^T_{Q-1}}\left(wA^\omega_{Q-1}\right)$.*

Proof. Take $w = w_1 \ldots w_m \in A^\omega_{Q-1}$. We have:

$$\mu_{P_Q}\left(T^{-1}(wA^\omega_{Q-1})\right) = \mu_{P_Q}\left(\{\mathbf{x} \in A^\omega_Q \mid w \sqsubset T(\mathbf{x})\}\right) = \mu_{P^T_{Q-1}}\left(wA^\omega_{Q-1}\right). \qquad \square$$

Proposition 3. *If $\mathbf{x} \in A^\omega_Q$ is random in $(A^\omega_Q, \mathcal{M}, \mu_{P_Q})$ and T is the transformation defined above, then $T(\mathbf{x})$ is random in $(A^\omega_{Q-1}, \mathcal{M}, \mu_{P^T_{Q-1}})$.*

Proof. We generalise a result in [8] stating that, for the Lebesgue probability, measure-preserving transformations preserve randomness. Assume that $\mathbf{x}$ is random in $(A^\omega_Q, \mathcal{M}, \mu_{P_Q})$ but $T(\mathbf{x})$ is not random in in $(A^\omega_{Q-1}, \mathcal{M}, \mu_{P^T_{Q-1}})$, i.e. there is a constructive null set $R = (G_m)_{m\geq 1}$ containing $T(\mathbf{x})$. Assume that $G_m = X_m A^\omega_{Q-1}$, where $X_m \subset A^\omega_{Q-1}$ is c.e. and has the measure $\mu_{P^T_{Q-1}}(X_m A^\omega_{Q-1})$ smaller than 2^{-m}. Define $S_m = T^{-1}(X_m A^\omega_{Q-1}) \subset A^\omega_Q$ and note that S_m is open because it is equal to $\bigcup_{w\in X_m} V_w A^\omega_Q$ with $V_w = \{v \in A^\omega_Q \mid w \sqsubset T(v)\}$ and, using Lemma 1, has the measure smaller than 2^{-m}:

$$\mu_{P_Q}(S_m) = \mu_{P_Q}\left(\bigcup_{w\in X_m} V_w A^\omega_Q\right) \leq 2^{-m}.$$

We have proved that $\mathbf{x}$ is not random in $(A^\omega_Q, \mathcal{M}, \mu_{P_Q})$, a contradiction. $\square$

Let us define $VN^{-1} : 2^{B^*} \to 2^{B^*}$ for $x = x_1 \ldots x_m \in B^m$ as

$$\begin{aligned} VN^{-1}(x) &= \{y \mid y = u_1 f(x_1) u_2 \ldots u_m f(x_m) u_{m+1} v \text{ and} \\ &\qquad u_i \in \{00, 11\}^* \text{ for } 1 \leq i \leq m, v \in B \cup \{\lambda\}\} \\ &= \bigcup_{n=0}^{\infty} VN^{-1}_{n+2m,m}(x), \end{aligned}$$

and for $X \subseteq B^*$ as

$$VN^{-1}(X) = \bigcup_{x\in X} VN^{-1}(x).$$

For all $x \in B^*$ and $\mathbf{y} \in VN^{-1}(x)B^\omega$ we then have $x \sqsubset VN(\mathbf{y})$.

For the cases that $VN(\mathbf{x}) \in B^\omega$, the probability space $(B^\omega, \mathcal{M}, \mu_{P_{VN}})$ induced by von Neumann normalisation is endowed with the measure $\mu_{P_{VN}}$. The measure $\mu_{P_{VN}}$ is defined on the sets xB^ω with $x \in B^*$ by

$$\mu_{P_{VN}}(xB^\omega) = \frac{\mu_P(VN^{-1}(x)B^\omega)}{\mu_P(VN^{-1}(B^{|x|})B^\omega)}.$$

By noting that $VN^{-1}(B^{|x|}) \subset VN^{-1}(B^*)$ it is clear that $\mu_{P_{VN}}$ satisfies the Kolmogorov axioms for a probability measure. While the set $VN^{-1}(B^{|x|})$ contains sequences for which normalisation produces a finite string, from Corollary 1 we know that the set of such sequences has measure zero, so the definition of $\mu_{P_{VN}}$ is a good model of the target probability space.

Scolium 1. *Let $\mathbf{x} \in B^\omega$ be random in $(B^\omega, \mathcal{M}, \mu_P)$. Then $VN(\mathbf{x}) \in B^\omega$ is also random in $(B^\omega, \mathcal{M}, \mu_{P_{VN}})$.*

Corollary 2. *If $\mathbf{x} \in B^\omega$ is random in $(B^\omega, \mathcal{M}, \mu_P)$ then $VN(\mathbf{x})$ is Borel normal in $(B^\omega, \mathcal{M}, \mu_{P_{VN}})$.*

Theorem 4. *The probability space $(B^\omega, \mathcal{M}, \mu_{P_{VN}})$ induced by von Neumann normalisation is the uniform distribution $(B^\omega, \mathcal{M}, \mu_{P_L})$, where μ_{P_L} is the Lebesgue measure.*

Proof. By Lemma 1 von Neumann normalisation is measure preserving, so for $x \in B^*$ we have $\mu_{P_{VN}}(xB^\omega) = \mu_P(VN^{-1}(x)B^\omega) = p_0^{|x|}p_1^{|x|}\sum_{d_i \in D^*} p_0^{\#_0(d_1 \ldots d_{|x|})}p_1^{\#_1(d_1 \ldots d_{|x|})}$. The key point is that this only depends on $|x|$ not x itself. By using the fact that for any n, $\sum_{x \in B^n} \mu_{P_{VN}}(xB^\omega) = 1$, we have $\mu_{P_{VN}}(xB^\omega) = 2^{-|x|}$, for all $x \in B^*$, and hence $\mu_{P_{VN}} = \mu_{P_L}$, the Lebesgue measure. □

Theorem 5. *The set $\{\mathbf{x} \in B^\omega \mid VN(\mathbf{x}) \in B^* \text{ or } VN(\mathbf{x}) \in B^\omega \text{ is computable}\}$ has measure zero with respect to the probability space $(B^\omega, \mathcal{M}, \mu_P)$.*

Both unpredictability and uniformity of distribution are independent symptoms of randomness, and it is important that any method to remove bias and ensure uniformity does not decrease unpredictability. Von Neumann's method preserves randomness and Borel normality, but fails to preserve incomputability in general. It is not known whether sequences of bits from a QRNG are random or even Borel normal with respect to the space $(B^\omega, \mathcal{M}, \mu_P)$, so it follows that such sequences may well lose unpredictability when normalised since only strong incomputability is known to be guaranteed. Fortunately, this 'damage' is limited in measure: it holds only with probability zero. However, it remains an open question to determine if strong computability is preserved. Even if it isn't, it may still be the case that the preservation of unpredictability can be guaranteed, but further theoretical characterisation of such sequences is needed to examine such issues.

5 Role of Probability Spaces for QRNGs

The treatment of QRNGs as entirely probabilistic devices is grounded purely on the probabilistic treatment of measurement in quantum mechanics which originated with Born's decision to 'give up determinism in the world of atoms' [6], a viewpoint which has become a core part of our understanding of quantum mechanics. This is formalised by the Born rule, but the probabilistic nature of *individual* measurement is nonetheless postulated and tells us nothing about *how* the probability arises. Along with the assumption of independence this allows us to predict the probability of *successive* events, as we have done.

No-go theorems such as the Kochen-Specker Theorem [17] tell us something stronger: if we assume non-contextuality (i.e. that the result of an observation is independent of the compatible observables are co-measured alongside it [4,12]) then there can, in general, be no pre-existing definite values prescribable to certain sets of measurement outcomes in dimension three or greater Hilbert space. In other words, the unpredictability is not due to ignorance of the system being measured; indeed, since there are in general no definite values associated with the measured observable it is surprising there is an outcome at all [28]. While this does not answer the question as to where the unpredictability arises from, it does tell us something stronger than the Born Rule does. In [9] it is shown that every infinite sequence produced by a QRNG is (strongly) incomputable. In particular, this implies that it is *impossible* for a QRNG to output a computable sequence. The set of computable numbers has measure zero with respect to the probability space of the QRNG, but the impossibility of producing such a sequence is much stronger than, although not in contradiction with, the probabilistic results.

In the finite case every string is, of course, obtainable, and we would expect the distribution to be that predicted by the probability space derived from the Born Rule. However, the infinite case has something to say here too. We can view any finite string produced by a QRNG as the initial segment of an infinite sequence the QRNG would produce if left to run indefinitely. For any infinite sequence produced by the QRNG, it is impossible to compute the value of *any bit* before it is measured [2]; in the finite case this means there is no way to provably compute the value of the next bit before it is measured. In light of value indefiniteness this is not unexpected, but nonetheless gives mathematical grounding to the postulated unpredictability of each individual measurement, as well as the independence of successive measurements—indeed we can rule out any computable causal link within the system which may give rise to the measurement outcome.

6 Conclusions

The analysis developed in this paper involves the probability spaces of the source and output of a QRNG and the effect von Neumann normalisation has on these spaces. In the 'ideal case', the von Neumann normalised output of an independent constantly biased QRNG is the probability space of the uniform distribution

(un-biasing). This result is true for both for finite strings and for the infinite sequences produced by QRNGs (the QRNG runs indefinitely in the second case). We have also examined the effect von Neumann normalisation has on various properties of infinite sequences. In particular, Borel normality and (algorithmic) randomness are invariant under normalisation, but for ε-random sequences with $0 < \varepsilon < 1$, normalisation can both decrease or increase the randomness of the source. Further results of this form are necessary in order to be assured that normalisation techniques preserve the strong incomputability of bits produced by QRNGs. Finally, we reiterate that a successful application of von Neumann normalisation—in, fact, any un-biasing transformation—does exactly what it promises, *un-biasing*, one (among infinitely many) symptoms of randomness; it will not produce 'true' randomness.

Acknowledgments

We thank Karl Svozil and Marius Zimand for many discussions and suggestions, and Tania Roblot and the anonymous referees for comments which helped improve the paper.

References

1. Abbott, A.A., Calude, C.S.: Von Neumann normalisation of a quantum random number generator. Report CDMTCS-392, Centre for Discrete Mathematics and Theoretical Computer Science, University of Auckland, Auckland, New Zealand (2010)
2. Abbott, A.A., Calude, C.S., Svozil, K.: Unpublished work on the incomputability of quantum randomness (in preparation)
3. Abbott, A.A., Calude, C.S., Svozil, K.: A quantum random number generator certified by value indefiniteness. CDMTCS Research Report, 396 (2010)
4. Bell, J.S.: On the problem of hidden variables in quantum mechanics. Reviews of Modern Physics 38(3), 447–452 (1966)
5. Billingsley, P.: Probability and Measure. John Wiley & Sons, New York (1979)
6. Born, M.: Quantenmechanik der Stoßvorgänge. Zeitschrift für Physik 38, 803–837 (1926); English translation by Wheeler, J. A., Zurek, W.H.: Quantum Theory and Measurement, ch. I.2. Princeton University Press, Princeton (1983)
7. Calude, C.S.: Information and Randomness: An Algorithmic Perspective, 2nd edn. Springer, Berlin (2002)
8. Calude, C.S., Hertling, P., Jürgensen, H., Weihrauch, K.: Randomness on full shift spaces. Chaos, Solutions & Fractals 12(3), 491–503 (2001)
9. Calude, C.S., Svozil, K.: Quantum randomness and value indefiniteness. Advanced Science Letters 1, 165–168 (2008)
10. Downey, R., Hirschfeldt, D.: Algorithmic Randomness and Complexity. Theory and Applications of Computability. Springer, Heidelberg (2010)
11. Halmos, P.R.: Measure Theory. Springer, New York (1974)
12. Heywood, P., Redhead, M.L.G.: Nonlocality and the Kochen-Specker paradox. Foundations of Physics 13(5), 481–499 (1983)

13. id Quantique. Quantis—quantum random number generators (12/08/2009), http://idquantique.com/products/quantis.htm
14. Jauch, J.M.: Foundations of Quantum Mechanics. Addison-Wesley, Reading (1968)
15. Jennewein, T., Achleitner, U., Weihs, G., Weinfurter, H., Zeilinger, A.: A fast and compact quantum random number generator. Review of Scientific Instruments 71, 1675–1680 (2000)
16. Kac, M.: Statistical Independence in Probability, Analysis and Number Theory. The Carus Mathematical Monographs. The Mathematical Association of America (1959)
17. Kochen, S., Specker, E.: The problem of hidden variables in quantum mechanics. Journal of Mathematics and Mechanics 17, 59–87 (1967); Reprinted in Specker, E.: Selecta. Brikhäuser, Basel (1990)
18. Kuipers, L., Niederreiter, H.: Uniform Distribution of Sequences. John Wiley & Sons, New York (1974)
19. Kwon, O., Cho, Y., Kim, Y.: Quantum random number generator using photon-number path entanglement. Applied Optics 48(9), 1774–1778 (2009)
20. Ma, H., Wang, S., Zhang, D., Change, J., Ji, L., Hou, Y., Wu, L.: A random-number generator based on quantum entangled photon pairs. Chinese Physics Letters 21(19), 1961–1964 (2004)
21. Martin-Löf, P.: The definition of random sequences. Information and Control 9(6), 602–619 (1966)
22. Peres, Y.: Iterating von Neumann's procedure for extracting random bits. The Annals of Statistics 20(1), 590–597 (1992)
23. Pironio, S., Acín, A., Massar, S., de la Giroday, A.B., Matsukevich, D.N., Maunz, P., Olmchenk, S., Hayes, D., Luo, L., Manning, T.A., Monroe, C.: Random numbers certified by Bell's theorem. Nature 464(09008) (2010)
24. Schmidt, H.: Quantum-mechanical random-number generator. Journal of Applied Physics 41(2), 462–468 (1970)
25. Shen, Y., Tian, L., Zou, H.: Practical quantum random number generator based on measuring the shot noise of vacuum states. Physical Review A 81(063814) (2010)
26. Stefanov, A., Gisin, N., Guinnard, O., Guinnard, L., Zbinden, H.: Optical quantum random number generator. Journal of Modern Optics 47(4), 595–598 (2000)
27. Svozil, K.: The quantum coin toss – testing microphysical undecidability. Physics Letters A 143(9), 433–437 (1990)
28. Svozil, K.: Quantum information via state partitions and the context translation principle. Journal of Modern Optics 51, 811–819 (2004)
29. Svozil, K.: Three criteria for quantum random-number generators based on beam splitteres. Physical Review A 79(5), 054306 (2009)
30. Vadhan, S.: Pseudorandomness. Foundations and Trends in Theoretical Computer Science. Now publishers (to appear, 2011)
31. von Neumann, J.: Various techniques used in connection with random digits. National Bureau of Standards Applied Math Series 12, 36–38 (1951); In: Traub, A.H. (ed.) John von Neumann, Collected Works, pp. 768–770. MacMillan, New York (1963)