The Annals of Statistics
1992, Vol. 20, No. 1, 590–597

ITERATING VON NEUMANN'S PROCEDURE FOR EXTRACTING RANDOM BITS[1]

By Yuval Peres

Hebrew University, Jerusalem

Given a sequence of independent, identically distributed random biased bits, von Neumann's simple procedure extracts independent unbiased bits. In this note we show that the number of unbiased bits produced by iterating this procedure is arbitrarily close to the entropy bound.

1. Introduction. A source produces independent biased random bits $\{x_i\}_{i=1}^n$, with $p = \Pr[x_i = 0] \neq 1/2$, $q = \Pr[x_i = 1]$. We wish to extract from them as many as possible independent unbiased bits, without assuming prior knowledge of p. Von Neumann's procedure [8] consists of dividing the sequence $\{x_i\}_{i=1}^n$ into pairs, discarding pairs of equal bits, and replacing each 10 pair by a 0, each 01 pair by 1. From n biased bits, this procedure extracts approximately npq unbiased bits.

In [2], Elias exhibits extensions of the von Neumann procedure which produce unbiased bits at a rate arbitrarily close to the entropy bound (see Section 3). In this note we show that iterating the original von Neumann procedure on the information which it discards achieves the same end. The proof is based on a functional equation satisfied by the entropy function. In the last section we include an extension to exchangeable processes and discuss the relationship to the Keane–Smorodinsky finitary codes. It may be seen that the memory requirements of the procedures discussed here are substantially smaller than those of the Elias procedures.

Notation. Let $\Omega = \bigcup_{n=0}^{\infty}\{0,1\}^n$. Write $l(u)$ for length of strings $u \in \Omega$. For $u, v \in \Omega$, we write $u \leq v$ if u is a prefix of v and $u * v$ for the concatenation of u and v. By convention, the empty string is a prefix of any $v \in \Omega$.

Definition. By an *extraction procedure* we mean a mapping $\Psi\colon \Omega \to \Omega$ such that

$$u \leq v \Rightarrow \Psi(u) \leq \Psi(v),$$

with the property that for any $0 < p < 1$, if $x_1, \dots, x_n$ are (p,q) distributed independent random bits, then $\Psi(x_1, \dots, x_n)$ is uniformly distributed in $\{0,1\}^k$, given that $l(\Psi(x_1, \dots, x_n)) = k$.

Received March 1990; revised April 1991.

[1] Partially supported by a grant from the Landau Centre for Mathematical Analysis.

AMS 1980 *subject classifications*. Primary 94A17; secondary 60G09.

Key words and phrases. Random bits, entropy, functional equation, exchangeability.

Note that Ψ is *not* allowed to depend on p. The *rate* of an extraction procedure Ψ is the function

$$r(p) = \limsup_{n \to \infty} \frac{1}{n} E\left[l(\Psi(x_1, \ldots, x_n))\right],$$

where x_i are independent (p, q) distributed bits and E denotes expectation.

2. The iterated procedures. The von Neumann extraction procedure $\Psi_1 \colon \Omega \to \Omega$ is defined by

$$\Psi_1(x_1, x_2, \ldots, x_{2n+1}) = \Psi_1(x_1, \ldots, x_{2n}) = (y_1, \ldots, y_k),$$

where $y_i = x_{2m_i}$ and $m_1 < m_2 < \cdots < m_k$ are all the indices $m \leq n$ for which $x_{2m} \neq x_{2m-1}$.

$(*)$ The iterated procedures Ψ_ν, $\nu \geq 2$ are defined inductively. Given $x_1, \ldots, x_{2n}$, denote $u_j = x_{2j-1} \oplus x_{2j}$ ($\oplus$ is addition modulo 2) and $v_j = x_{2i_j}$, where $i_1 < i_2 < \cdots < i_{n-k}$ are all the indices $i \leq n$ for which $x_{2i} = x_{2i-1}$ and k is again the number of indices $m \leq n$ such that $x_{2m-1} \neq x_{2m}$. Let

$$\Psi_\nu(x_1, \ldots, x_{2n}) = \Psi_1(x_1, \ldots, x_{2n}) * \Psi_{\nu-1}(u_1, \ldots, u_n) * \Psi_{\nu-1}(v_1, \ldots, v_{n-k}).$$

Finally, define Ψ_ν for sequences of odd length by $\Psi_\nu(x_1, \ldots, x_{2n+1}) = \Psi_\nu(x_1, \ldots, x_{2n})$. To verify that the Ψ_ν are extraction procedures, it is convenient to extend the class of processes considered. Recall the notion of *exchangeable* random variables ([3], Section VII.4).

PROPOSITION 1. *If $x_1, \ldots, x_{2n}$ are exchangeable random bits and $\nu \geq 1$, then given that*

$$l(\Psi_\nu(x_1, \ldots, x_{2n})) = m,$$

the string $\Psi_\nu(x_1, \ldots, x_{2n})$ is uniformly distributed in $\{0,1\}^m$.

LEMMA. *Assume the random bits $x_1, \ldots, x_{2n}$ are exchangeable and $k \geq 0$. Then conditioning on the event $C_k = [l(\Psi_1(x_1, \ldots, x_{2n})) = k]$, we have:*

(i) *$\Psi_1(x_1, \ldots, x_{2n})$ is uniformly distributed in $\{0,1\}^k$.*

(ii) *The random bits $u_1, \ldots, u_n$ defined in $(*)$ by $u_j = x_{2j-1} \oplus x_{2j}$ are exchangeable [this implies that given C_k, the random string $(u_1, \ldots, u_n)$ is equidistributed among all $\binom{n}{k}$ strings in $\{0,1\}^n$ of Hamming weight k].*

(iii) *The random bits $v_1, \ldots, v_{n-k}$ defined in $(*)$ are exchangeable.*

(iv) *The three random vectors $\Psi_1(x_1, \ldots, x_{2n})$, $(u_1, \ldots, u_n)$ and $(v_1, \ldots, v_{n-k})$ are independent.*

(Note that we are *not* asserting that the u_i are independent of each other.)

PROOF OF THE LEMMA. (i) If $\{x_i\}$ are independent, this is the validity of the original von Neumann procedure. To obtain the general case, use the group of 2^n permutations generated by the n transpositions exchanging $2j-1$ and $2j$, $1 \leq j \leq n$, and exchangeability of the $\{x_i\}$.

(ii) This follows easily from the exchangeability of the $\{x_i\}$, as any permutation $\pi \in S_n$ of $(u_1, \dots, u_n)$ may be obtained from a corresponding permutation $\tilde{\pi} \in S_{2n}$ of $(x_1, \dots, x_{2n})$, where $\tilde{\pi}(2j - \delta) = 2\pi(j) - \delta$, $1 \le j \le n$, $\delta \in \{0, 1\}$.

(iii) Part (iii) is proved along the same lines as (ii).

(iv) What must be shown here, is that for any fixed string $c \in \{0, 1\}^{n-k}$, the probability

$$\mathbf{P}[\Psi_1(x_1, \dots, x_{2n}) = a, (u_1, \dots, u_n) = b, (v_1, \dots, v_{n-k}) = c | C_k]$$

does not depend on the strings $a \in \{0, 1\}^k$ and $b \in \{0, 1\}^n$ (where b has Hamming weight k). Indeed, let $a, a' \in \{0, 1\}^k$ and $b, b' \in \{0, 1\}^n$, where b, b' have Hamming weight k. Combining the tricks in parts (i) and (ii) above, one may construct a permutation $\sigma \in S_{2n}$ such that if a string $(x_1, \dots, x_{2n})$ satisfies $\Psi_1(x_1, \dots, x_{2n}) = a$, $(u_1, \dots, u_n) = b$ and $(v_1, \dots, v_{n-k}) = c$, then applying $(*)$ to $(x_{\sigma(1)}, \dots, x_{\sigma(2n)})$ generates

$$\Psi_1(x_{\sigma(1)}, \dots, x_{\sigma(2n)}) = a', \qquad (u'_1, \dots, u'_n) = b'$$

and

$$(v'_1, \dots, v'_{n-k}) = c.$$

By exchangeability of $\{x_i\}$, we are done. □

Proof of Proposition 1. We use induction on ν.

The case $\nu = 1$ is part (i) of the lemma. For the inductive step it suffices to check that for fixed m, the probability

$$\mathbf{P}[\Psi_\nu(x_1, \dots, x_{2n}) = s]$$

is the same for all $s \in \{0, 1\}^m$. By the lemma, this probability may be written as

$$\sum_{k=0}^{m} \mathbf{P}(C_k) \mathbf{P}[\Psi_1(x_1, \dots, x_{2n}) = (s_1, \dots, s_k) | C_k]$$
$$\times \sum_{r=0}^{m-k} \mathbf{P}[\Psi_{\nu-1}(u_1, \dots, u_n) = (s_{k+1}, \dots, s_{k+r}) | C_k]$$
$$\times \mathbf{P}[\Psi_{\nu-1}(v_1, \dots, v_{n-k}) = (s_{k+r+1}, \dots, s_m) | C_k].$$

By induction, this expression does not depend on s. □

In the construction $(*)$, note that when x_i are (p, q) distributed independently, then $u_i = x_{2i} \oplus x_{2i-1}$ are independent $(p^2 + q^2, 2pq)$ distributed bits and v_i (as defined there) are independent $(p^2/(p^2 + q^2), q^2/(p^2 + q^2))$ distributed bits. This allows a recursive computation of the rates of the procedures Ψ_ν.

PROPOSITION 2. *The rates $r_\nu(p)$ of the procedures Ψ_ν satisfy the recursion*

$$r_\nu(p) = pq + \frac{1}{2}r_{\nu-1}(p^2+q^2) + \frac{1}{2}(p^2+q^2)r_{\nu-1}\left(\frac{p^2}{p^2+q^2}\right) \quad \textit{for } \nu \geq 2,$$

where $r_1(p) = pq$. All these rates exist as a.e. limits: If $x_1, x_2, \ldots,$ are (p,q) distributed independent bits, then $r_\nu(p) = \lim_{n\to\infty}(1/n)l(\Psi_\nu(x_1,\ldots,x_n))$ a.e.

PROOF. Let $0 < p < 1$ and let $x_1, x_2, x_3, \ldots$ be independent (p,q) distributed random bits. Noting that

$$E[l(\Psi_1(x_1,\ldots,x_{2n}))] = \sum_{i=1}^{n} E(x_{2i} \oplus x_{2i-1}) = 2npq,$$

it follows that $r_1(p) = pq$.

By the strong law of large numbers, almost surely

$$\lim_{n\to\infty}\frac{1}{2n}l(\Psi_1(x_1,\ldots,x_{2n})) = \lim_{n\to\infty}\frac{1}{2n}\sum_{i=1}^{n}(x_{2i}\oplus x_{2i-1}) = pq = r_1(p).$$

(It is convenient, and clearly suffices, to compute the limit along even indices.) For the inductive step, assume the proposition holds for $\nu - 1$ in place of ν.

Again, let $\{x_i\}$ be independent (p,q) distributed random bits and consider the random variables

$$K(n) = l(\Psi_1(x_1,\ldots,x_{2n})).$$

We have

$$l(\Psi_\nu(x_1,\ldots,x_{2n})) = K(n) + l(\Psi_{\nu-1}(u_1,\ldots,u_n)) + l(\Psi_{\nu-1}(v_1,\ldots,v_{n-K(n)}))$$

and therefore

$$\begin{aligned}\frac{1}{2n}&l(\Psi_\nu(x_1,\ldots,x_{2n}))\\ &= \frac{K(n)}{2n} + \frac{1}{2n}l(\Psi_{\nu-1}(u_1,\ldots,u_n))\\ &\quad+\frac{n-K(n)}{2n}\frac{1}{n-K(n)}l(\Psi_{\nu-1}(v_1,\ldots,v_{n-K(n)})).\end{aligned}$$

From the discussion above $(K(n)/2n) \to pq$, and in particular $n - K(n) \to \infty$ as $n \to \infty$, with probability 1. Thus the last formula and the induction hypothesis imply that

$$\begin{aligned}\lim_{n\to\infty}&\frac{1}{2n}l(\Psi_\nu(x_1,\ldots,x_{2n}))\\ &= pq + \frac{1}{2}r_{\nu-1}(p^2+q^2) + \frac{1}{2}(p^2+q^2)r_{\nu-1}\left(\frac{p^2}{p^2+q^2}\right).\end{aligned}$$

Taking expectations and using the bounded convergence theorem, we get

$$\begin{aligned} r_\nu(p) &= \lim_{n\to\infty} \frac{1}{2n} E\big[l(\Psi_\nu(x_1,\dots,x_{2n}))\big] \\ &= pq + \frac{1}{2} r_{\nu-1}(p^2+q^2) + \frac{1}{2}(p^2+q^2) r_{\nu-1}\left(\frac{p^2}{p^2+q^2}\right). \end{aligned}$$

Comparing the last two formulas completes the proof of the proposition. □

3. The entropy bound. Denote $h(p) = -p\log_2 p - q\log_2 q$, where $q = 1-p$ for $0 < p < 1$ and let $h(0) = h(1) = 0$. Also denote by $H(Z)$ the entropy of any discrete random variable Z. For an extraction procedure Ψ with rate function r, the inequality $r(p) \le h(p)$ holds for all $0 < p < 1$. The reason for this well-known fact is that if $x_1,\dots,x_n$ are (p,q) distributed independent bits, then

$$\begin{aligned} nh(p) &= H(x_1,\dots,x_n) \ge H(\Psi(x_1,\dots,x_n)) \\ &= H\big(l(\Psi(x_1,\dots,x_n))\big) + H\big(\Psi(x_1,\dots,x_n) \big| l(\Psi(x_1,\dots,x_n))\big) \\ &\ge E\big(l(\Psi(x_1,\dots,x_n))\big). \end{aligned}$$

For details see, for instance, [2] or [5].

PROPOSITION 3.

$$\lim_{\nu\to\infty} r_\nu(p) = h(p) \quad \textit{uniformly in } p \in (0,1).$$

PROOF. Let

$$\mathscr{F} = \left\{ f\colon [0,1] \to \mathbf{R} \,\middle|\, \lim_{t\to 0} f(t) = 0 = \lim_{t\to 1} f(t) \right\}.$$

Consider the operator $T\colon \mathscr{F} \to \mathscr{F}$ defined by

$$(Tf)(p) = pq + \frac{1}{2} f(p^2+q^2) + \frac{1}{2}(p^2+q^2) f\left(\frac{p^2}{p^2+q^2}\right),$$

where $q = 1-p$. Define $r_0(p) = 0$ for $0 \le p \le 1$.

By Proposition 2, the functions $\{r_\nu\}_{\nu\ge 0}$ satisfy $r_\nu = Tr_{\nu-1}$ for all $\nu \ge 1$, and this, together with $r_0 \equiv 0$, is all we shall use to prove the proposition. (In particular, the general entropy bound is not utilized.)

One directly verifies that the entropy function h is a fixed point of T. Since T is a monotone operator and $r_0(p) \le h(p)$, it follows by induction that $r_\nu(p) \le h(p)$ for all $\nu \ge 0$.

Similarly, from $r_0(p) = 0 \le pq = r_1(p)$ for $0 \le p \le 1$, it follows that $r_{\nu-1}(p) \le r_\nu(p)$ for all $v \ge 1$ and $p \in [0,1]$. Thus for each p, the limit $f(p) = \lim_{\nu\to\infty} r_\nu(p)$ exists.

The function f satisfies $0 \le f(p) \le h(p)$, and therefore also $f \in \mathscr{F}$ and $Tf = f$. Thus the difference $g = h - f$ satisfies $g \in \mathscr{F}$, $g \ge 0$, and $g(p) = g(p^2 + q^2)/2 + (p^2 + q^2)g(p^2/(p^2 + q^2))/2$.

Let

$$M = \sup_{p \in (0,1)} g(p).$$

Assume that $M > 0$. Since $g \in \mathscr{F}$, there exists $\varepsilon > 0$ such that

$$M = \sup_{p \in [\varepsilon, 1-\varepsilon]} g(p).$$

However for all $p \in [\varepsilon, 1 - \varepsilon]$, we have

$$g(p) \le M/2 + \left[\varepsilon^2 + (1 - \varepsilon)^2\right] M/2 < M.$$

This contradiction forces $M = 0$ and therefore $f = h$. Since the convergence $r_\nu \to h$ is monotone, Dini's theorem guarantees that it is uniform on $[0, 1]$. □

4. Remarks.

Remark 1. As in [2], the output of a finite state Markov chain can be converted to several sequences of biased coin flips without losing entropy, and then one may apply the extraction procedures discussed above. Compare also [1].

Remark 2. Also following [2], one can use the diagonal method to construct from the procedures $\{\Psi_\nu\}_{\nu \ge 1}$ an extraction procedure with rate function precisely $h(p)$.

Remark 3. Often when an extraction procedure Ψ is utilized, the number m of unbiased bits to be generated is predetermined, while the number of biased (p, q) distributed bits used is not. One's natural inclination in this situation is to generate $\Psi(x_1, \dots, x_\tau)$, where τ is the stopping time:

$$\tau = \min\{n | l(\Psi(x_1, \dots, x_n)) = m\}.$$

We stress that if Ψ is any of the iterated von Neumann procedures, or the Elias procedure, the resulting string $(a_1, \dots, a_m) = \Psi(x_1, \dots, x_\tau)$ is *not* uniformly distributed in $\{0, 1\}^m$.

A way to bypass this difficulty is to fix a block length $b \ge 2$ and to generate

$$(**) \qquad \Psi(x_1, \dots, x_b) * \Psi(x_{b+1}, \dots, x_{2b}) * \cdots * \Psi(x_{tb-b+1}, \dots, x_{tb}),$$

where t is the minimal integer for which the number of unbiased bits so produced is at least m.

It is easy to see that the string in $(**)$ is composed of independent unbiased bits.

5. Exchangeable processes. Let $Y = \{Y_j\}_{j=1}^{\infty}$ be an *infinite* sequence of exchangeable, 0-1 valued random variables. The entropy of Y as a stationary process is

$$h(Y) \doteq \lim_{n\to\infty} \frac{1}{n} H(Y_1,\dots,Y_n).$$

The extraction procedures Ψ_ν may be applied to Y, and by Proposition 1 they generate independent unbiased bits. With a slight abuse of notation, let

$$r_\nu(Y) = \limsup_{n\to\infty} \frac{1}{n} E\left[l(\Psi_\nu(Y_1,\dots,Y_n))\right].$$

(We shall see in the proof below that actually the limit exists.)

COROLLARY 4. *For any exchangeable* 0-1 *valued process* Y, *the sequence* $r_\nu(Y)$ *is increasing and*

$$\lim_{\nu\to\infty} r_\nu(Y) = h(Y).$$

PROOF. By de Finetti's theorem (see [3], Section VII.4) Y is a mixture of i.i.d. processes, that is, there exists a Borel probability measure μ on $[0,1]$ such that if $(s_1,\dots,s_n)$ is a string of bits of Hamming weight k, then

$$\mathbf{P}\left[Y_j = s_j, 1 \le j \le n\right] = \int_0^1 p^{n-k}(1-p)^k \, d\mu(p).$$

Since the entropy of a mixture is the corresponding average of entropies ([6], Theorem 9.8), we have

$$h(Y) = \int_0^1 h(p)\, d\mu(p).$$

Here $h(p)$ is the entropy of (p,q) distributed independent random bits and is given by the formula in Section 3. Also, by conditioning on p we get

$$E\left[l(\Psi_\nu(Y_1,\dots,Y_n))\right] = \int_0^1 E_p\left[l(\Psi_\nu(x_1,\dots,x_n))\right] d\mu(p)$$

[here E_p means that the x_i are taken as independent (p,q) distributed bits].

Dividing by n and taking the limit, the bounded convergence theorem gives

$$r_\nu(Y) = \lim_{n\to\infty} \frac{1}{n} E\left[l(\Psi_\nu(Y_1,\dots,Y_n))\right] = \int_0^1 r_\nu(p)\, d\mu(p).$$

Since $r_\nu(p)$ increases as $\nu \to \infty$ to $h(p)$ and the convergence is uniform,

$$\lim_{\nu\to\infty} r_\nu(Y) = \int_0^1 \lim_{\nu\to\infty} r_\nu(p)\, d\mu(p) = h(Y)$$

as claimed. □

It would be interesting to obtain a direct proof of the corollary, without invoking de Finetti's theorem.

As a final remark, note that the finitary homomorphism theorem of Keane and Smorodinsky [4] may be used to extract unbiased independent random bits from an i.i.d. process $X = \{X_n\}_{-\infty}^{\infty}$.

Indeed if (c/d) is a positive rational number smaller than the entropy $h(X)$, then an extraction rate (c/d) may be achieved by partitioning $\{X_n\}_{-\infty}^{\infty}$ into blocks of length d (i.e., considering the dth power of the shift) and mapping the resulting system [which has entropy $dh(X)$] by a finitary factor map onto the full shift on 2^c symbols. The codes of [4], unlike the procedures Ψ_ν, commute with the shift. However, they must be tailor-made to fit a *particular* process X, while the procedures Ψ_ν work for all exchangeable processes simultaneously.

It would be interesting to devise a coding which combines, to some extent, both features.

Acknowledgments. I am grateful to Moshe Dubiner for helpful discussions and to the referees for a substantial improvement of the exposition.

REFERENCES

[1] BLUM, M. (1984). Independent unbiased coin flips from a correlated biased source: A finite state Markov chain. In *Proceedings of the 25th IEEE Symposium on Foundations of Computer Science* 425–433. IEEE Computer Society Press, Silver Spring, Md.

[2] ELIAS, P. (1972). The efficient construction of an unbiased random sequence. *Ann. Math. Statist.* **43** 865–870.

[3] FELLER, W. (1966). *An Introduction to Probability Theory and Its Applications* **2**. Wiley, New York.

[4] KEANE, M. and SMORODINSKY, M. (1977). A class of finitary codes. *Israel J. Math.* **26** 352–371.

[5] MCELIECE, R. J. (1977). *The Theory of Information and Coding. Encyclopedia of Mathematics and Its Applications* **3**. Addison-Wesley, Reading, Mass.

[6] ROHKLIN, V. A. (1967). Lectures on the entropy theory of measure preserving transformations. *Russian Math. Surveys* **22** 1–52.

[7] STOUT, Q.R. and WARREN, B. (1984). Tree algorithms for unbiased coin tossing with a biased coin. *Ann. Probab.* **12** 212–222.

[8] VON NEUMANN, J. (1951). Various techniques used in connection with random digits. *National Bureau of Standards Applied Mathematics Series* **12** 36–38.

DEPARTMENT OF MATHEMATICS
YALE UNIVERSITY
NEW HAVEN, CONNECTICUT 06520