## A stochastic interpretation of the Riemann zeta function

KENNETH S. ALEXANDER\*, KENNETH BACLAWSKI†, AND GIAN-CARLO ROTA‡

\*Department of Mathematics, University of Southern California, Los Angeles, CA 90089; †College of Computer Science, Northeastern University, Boston, MA 02115; and ‡Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139

Contributed by Gian-Carlo Rota, August 10, 1992

ABSTRACT We give a stochastic process for which the terms of the Riemann zeta function occur as the probability distributions of the elementary random variables of the process.

#### **Section 1. Introduction**

As in ref. 1 we use the term *process* for a probability space  $\Omega$  together with a parametrized family of random variables. The purpose of this paper is to exhibit a process  $(\Omega, Z_s)$  parametrized by integers s > 1 such that the probability distributions of the  $Z_s$  are the terms of the Riemann zeta function—i.e.,  $\Pr(Z_s = n) = n^{-s} \zeta(s)^{-1}$ .

#### Section 2. The Rédei Zeta Function of an Inverse System

Let  $(\{G_{\alpha}: \alpha \in L\}, \{\phi_{\beta,\alpha}: G_{\beta} \to G_{\alpha}\})$  be an inverse system of finite groups over a lattice L. We will write  $\hat{0}$  for the minimum element of L, and we will assume that  $G_{\hat{0}}$  is a one-element group. The profinite completion  $G = \lim_{\leftarrow} G_{\alpha}$  has a unique normalized Haar measure that we will denote Pr. We may then regard G as a probability space.

If, in addition, we assume that the structure homomorphisms  $\phi_{\beta,\alpha}$  are all surjective, then we can define a function  $\nu$  on pairs of elements  $(\alpha, \beta)$  in L such that  $\alpha \leq \beta$ , by the formula  $\nu(\alpha, \beta) = |\text{Coker}(\phi_{\beta,\alpha})|$ , which then satisfies the condition

for any triple 
$$\alpha \le \gamma \le \beta$$
,  $\nu(\alpha, \beta) = \nu(\alpha, \gamma)\nu(\gamma, \beta)$ .

A lattice with such a function is called a *lattice of Dirichlet type*, and  $\nu$  is called its *order function*. We abbreviate  $\nu(\hat{0}, \alpha)$  to  $\nu(\alpha) = |G_{\alpha}|$ .

Lattices of Dirichlet type were introduced in ref. 2, and for such lattices a formal Dirichlet series was introduced called the *Rédei zeta function*. This function is defined by

$$\rho(s; \mathbf{L}) = \sum_{\alpha \in \mathbf{L}} \mu(\hat{0}, \alpha) \nu(\alpha)^{-s},$$

where  $\mu$  is the Möbius function of L (see ref. 3).

It is easy to check that inverse limits preserve products. In particular, from the inverse system above one can form the kth power inverse system

$$(\{G_{\alpha}^k : \alpha \in \mathbf{L}\}, \, \{\phi_{\beta,\alpha}^{(k)} : G_{\beta}^k \to G_{\alpha}^k\}),$$

whose limit will be denoted  $G^k$ . The lattices of the kth power inverse systems are all isomorphic as lattices, but they differ from one another as lattices of Dirichlet type. Let  $\mathbf{L}^{(k)}$  be the lattice of Dirichlet type associated with the kth power inverse system. It is easy to check that

$$\rho(s; \mathbf{L}^{(k)}) = \rho(sk; \mathbf{L}), \quad \text{for every } k \ge 1.$$

The publication costs of this article were defrayed in part by page charge payment. This article must therefore be hereby marked "advertisement" in accordance with 18 U.S.C. §1734 solely to indicate this fact.

A lattice L with minimum element  $\hat{0}$  is said to be homogeneous if

for every 
$$\alpha \in L$$
,  $\{\beta \in L: \beta \ge \alpha\} \cong L$ .

The image of  $\gamma \in \{\beta : \beta \ge \alpha\}$  in L via this isomorphism will be written  $\gamma/\alpha$ .

A lattice L of Dirichlet type is said to be homogeneous if L is homogeneous as a lattice and if in addition

for every 
$$\alpha \le \beta$$
 in L,  $\nu(\beta/\alpha) = \nu(\beta)/\nu(\alpha)$ .

An inverse system  $(\{G_{\alpha}\}, \{\phi_{\beta,\alpha}\})$  is said to be homogeneous if the following conditions apply:

- (i) The lattice of the inverse system is homogeneous.
- (ii) For every  $\alpha \leq \beta$  in L,  $Ker(\phi_{\beta,\alpha}) \cong G_{\beta/\alpha}$ .
- (iii) The isomorphisms above commute with the structure homomorphisms of the inverse system.

It is easy to check that the lattice of a homogeneous inverse system is also homogeneous as a Dirichlet lattice.

#### Section 3. Möbius Inversion on an Infinite Lattice

We will use Möbius inversion on L, so it is useful to formalize the basic convergence result we need.

THEOREM 1. Let P be a locally finite poset. Let  $g:P \to C$  be a function such that  $\Sigma_{y \geq x} g(y)$  converges absolutely for every  $x \in P$ . Write f(x) for the sum  $\Sigma_{y \geq x} g(y)$ . If the double sum  $\Sigma_{w \geq x} \Sigma_{y \geq w} \mu(x, w) g(y)$  converges absolutely for every  $x \in P$ , then  $\Sigma_{y \geq x} \mu(x, y) f(y)$  converges absolutely to g(x) for every  $x \in P$ .

*Proof:* Absolutely convergent series are arbitrarily rearrangeable. Therefore

$$\sum_{w \geq x} \mu(x, w) \sum_{y \geq w} g(y) = \sum_{y \geq x} g(y) \sum_{y \geq w \geq x} \mu(x, w),$$

for every  $x \in P$ .

Now the left-hand side of the equation above is  $\sum_{w \ge x} \mu(x, w) f(w)$ , while the right-hand side is  $\sum_{y \ge x} g(y) \delta(x, y) = g(x)$ , by definition of the Möbius function on a locally finite poset. Absolute convergence clearly also holds.

We now give an example of the use of Möbius inversion in the setting of Section 2.

THEOREM 2. Let L be a homogeneous lattice of Dirichlet type with order function  $\nu$ . If

- (i)  $|\mu(\hat{0}, \alpha)|$  is bounded by a polynomial in  $\nu(\alpha)$  of degree  $k \ge 0$ , and
  - (ii)  $\sum_{\alpha \in L} \nu(\alpha)^{-s}$  converges absolutely for  $Re(s) > s_0$ ; then (i)  $\rho(s; L)$  converges absolutely for  $Re(s) > s_0 + k$ , and
  - (ii)  $\rho(s; \mathbf{L}) (\Sigma_{\alpha \in \mathbf{L}} \nu(\alpha)^{-s}) = 1$ , for  $Re(s) > s_0 + k$ .

**Proof:** We first check conclusion i. By condition i, we have that, for some constant C > 0,

$$\begin{split} \sum_{\alpha \in \mathbf{L}} |\mu(\hat{\mathbf{0}}, \, \alpha)| |\nu(\alpha)^{-s}| &\leq C \sum_{\alpha \in \mathbf{L}} \nu(\alpha)^k |\nu(\alpha)^{-s}| \\ &= \sum_{\alpha \in \mathbf{L}} \nu(\alpha)^{k - \operatorname{Re}(s)}. \end{split}$$

By condition ii, the last expression above is finite for  $Re(s) > s_0 + k$ . This gives conclusion i by the definition of  $\rho$ .

To show conclusion ii, one proceeds as in the proof of *Theorem 1*. Form the following double sum:

$$\sum_{\alpha,\beta\in L} \mu(\hat{0},\,\beta)\nu(\beta)^{-s}\nu(\alpha)^{-s}.$$

We first show that this double sum converges absolutely for  $Re(s) > s_0 + k$  by using the following bounds:

$$\begin{split} \sum_{\alpha,\beta\in\mathbf{L}} |\mu(\hat{0},\,\beta)| |\nu(\beta)^{-s}| |\nu(\alpha)^{-s}| &\leq C \sum_{\alpha,\beta} |\nu(\beta)^k \nu(\beta)^{-\operatorname{Re}(s)} \nu(\alpha)^{-\operatorname{Re}(s)} \\ &\leq C \sum_{\alpha} |\nu(\alpha)^{-\operatorname{Re}(s)} \sum_{\beta} |\nu(\beta)^{k-\operatorname{Re}(s)} \\ &< \infty, \quad \text{for } \operatorname{Re}(s) > s_0 + k. \end{split}$$

The last bound above follows from the fact that both of the series converge in the specified region by condition *ii* and conclusion *i*. It follows that the double sum above may be rearranged in any order. In particular, it follows that:

$$\sum_{\alpha,\beta\in\mathbf{L}}\mu(\hat{0},\,\beta)\nu(\beta)^{-s}\nu(\alpha)^{-s} = \sum_{\beta}\mu(\hat{0},\,\beta)\nu(\beta)^{-s}\sum_{\alpha}\nu(\alpha)^{-s}$$
$$= \rho(s;\,\mathbf{L})\Biggl(\sum_{\alpha}\nu(\alpha)^{-s}\Biggr),$$
for Re(s) > s<sub>0</sub> + k.

On the other hand, by homogeneity of L, for each pair  $\alpha, \beta \in$  L, there is a unique  $\gamma \in$  L such that  $\gamma/\beta = \alpha$ . Moreover, for this  $\gamma$  we have  $\nu(\alpha)\nu(\beta) = \nu(\gamma)$ . For a fixed  $\beta$ , a sum over all  $\alpha \in$  L is then equivalent to a sum over  $\gamma \ge \beta$ . Thus the double sum can also be rearranged as follows:

$$\sum_{\alpha,\beta \in \mathbf{L}} \mu(\hat{0}, \beta) \nu(\beta)^{-s} \nu(\alpha)^{-s} = \sum_{\beta} \mu(\hat{0}, \beta) \sum_{\gamma \geq \beta} \nu(\gamma)^{-s}$$

$$= \sum_{\gamma} \left( \sum_{0 \leq \beta \leq \gamma} \mu(\hat{0}, \beta) \right) \nu(\gamma)^{-s}$$

$$= \delta(\hat{0}, \gamma) \nu(\gamma)^{-s}$$

$$= \nu(\hat{0})^{-s}$$

$$= 1, \quad \text{for } \operatorname{Re}(s) > s_0 + k.$$

The theorem now follows.

# Section 4. A Stochastic Interpretation of the Rédei Zeta Function

Let  $(G_{\alpha})$ ,  $\{\phi_{\beta,\alpha}\}$ ) be an inverse system as in Section 2 with profinite completion G. Let Y be the random variable on G with values in  $L \cup \{\infty\}$  given by

$$Y(x) = \begin{cases} \sup\{\alpha \in \mathbf{L}: \mathbf{x}_{\alpha} = e\}, \\ \text{if the supremum exists in } \mathbf{L}, \text{ and} \\ \infty, \text{ otherwise,} \end{cases}$$

where e denotes the identity element of the group  $G_{\alpha}$ . Similarly, let  $Y^{(t)}$  for  $t \ge 1$  be the corresponding random variable on the tth power inverse system of  $(\{G_{\alpha}\}, \{\phi_{\beta,\alpha}\})$ . This sequence of random variables gives the following stochastic interpretation of the Rédei zeta function:

Theorem 3. Let G be the profinite limit of a homogeneous inverse system over a lattice L, having associated random variables  $Y^{(t)}$ , where t>0 is an integer. If L satisfies the hypotheses of Theorem 2 and if  $Pr(Y^{(t)}=\hat{0})>0$ , for  $t>t_0$ , then

$$Pr(\mathbf{Y}^{(t)} = \alpha | \mathbf{Y}^{(t)} \neq \infty) = \nu(\alpha)^{-t} \rho(t; \mathbf{L}), \text{ for } t > \max(t_0, s_0 + \mathbf{k}),$$

where k and s<sub>0</sub> are specified by condition ii of Theorem 2. Proof: By homogeneity, we know that

$$Pr(Y^{(t)} = \alpha) = \nu(\alpha)^{-t}Pr(Y^{(t)} = \hat{0}).$$

Hence

$$Pr(Y^{(t)} \neq \infty) = \sum_{\alpha \in L} Pr(Y^{(t)} = \alpha)$$
$$= Pr(Y^{(t)} = \hat{0}) \sum_{\alpha \in L} \nu(\alpha)^{-t}.$$

If  $t > t_0$ , then  $\Pr(Y^{(t)} = \hat{0}) > 0$  and hence also  $\Pr(Y^{(t)} \neq \infty) > 0$ . So in this case we have

$$\Pr(Y^{(t)} = \hat{0}|Y^{(t)} \neq \infty) \sum_{\alpha \in \mathbb{I}} \nu(\alpha)^{-t} = 1, \quad \text{for } t > t_0.$$

By Theorem 2 we may then conclude that

$$\Pr(Y^{(t)} = \hat{0}|Y^{(t)} \neq \infty) = \rho(t; L), \quad \text{for } t > \max(t_0, s_0 + k).$$

Finally, using homogeneity once more, we obtain the result in general.

The random variables  $Y^{(r)}$  have the desired probability distributions, but they are on different probability spaces. We would like a single probability space that supports all of these random variables in a natural way.

For an inverse system  $(\{G_{\alpha}\}, \{\phi_{\beta,\alpha}\})$  with profinite completion G, let  $G^{\infty}$  denote the product of countably many copies of G, i.e.,  $\prod_{i=1}^{\infty}G$ . For every positive integer t, let  $\pi_{[1,t]}:G^{\infty} \to G^t$  denote the projection onto the first t components of  $G^{\infty}$ . Finally, let  $Z_t:G^{\infty} \to \mathbb{C}$  be the composition  $Y^{(t)} \circ \pi_{[1,t]}$ . Because the probability measure on  $G^{\infty}$  is Haar measure, and hence the product measure, it follows that  $Y^{(t)}$  and  $Z_t$  have the same distribution.

We summarize these considerations in the following:

COROLLARY 1. Given the hypotheses of Theorem 3, there is a probability space  $G^{\infty}$  and sequence of random variables  $Z_t$ , for integers  $t > t_0$ , with values in L such that

$$Pr(Z_t = \alpha | Z_t \neq \infty) = \nu(\alpha)^{-t} \rho(t; L), \text{ for } t > max(t_0, s_0 + k).$$

### Section 5. The Riemann Zeta Function

We now specialize to the following classical situation. Let L = N be the lattice of positive integers ordered by divisibility. The groups  $G_n$  are the cyclic groups  $\mathbf{Z}/n\mathbf{Z}$ , and the order function is given by  $\nu(n) = n$ . The profinite completion is known to be  $\hat{\mathbf{Z}} \cong \Pi_p$  prime  $\mathbf{Z}_p$ , where  $\mathbf{Z}_p$  is the ring of p-adic integers. Note that the minimum element of N is  $\hat{\mathbf{0}} = 1$ . The random variable  $Y^{(t)}$  on  $\hat{\mathbf{Z}}^t$  takes values in  $\mathbf{N} \cup \{\infty\}$  and is defined by

$$Y^{(t)}(x) = \begin{cases} \sup\{n: x_n^{(1)} = x_n^{(2)} = \cdots = x_n^{(t)} = e\}, \\ \text{if this supremum exists, and} \\ \infty, \text{ otherwise.} \end{cases}$$

We then have the following stochastic interpretation of the Riemann zeta function:

THEOREM 4. For every integer s > 1, we have

$$Pr(Y^{(s)} = n) = n^{-s} \zeta(s)^{-1}$$
.

**Proof:** First apply **Theorem 3.** Since the inverse system defined above is obviously homogeneous, we must check that the hypotheses of **Theorem 2** hold and also that  $Pr(Y^{(s)} = \hat{0}) > 0$  for s > 1. Now the Möbius function of N takes values  $\pm 1$  and 0, so the first hypothesis holds with k = 0. The sum

 $\Sigma_{\alpha \in L} \nu(\alpha)^{-s}$  is, in this case, the sum defining the Riemann zeta function  $\zeta(s) = \Sigma_{n=1}^{\infty} n^{-s}$ . This is known to converge for Re(s)  $> s_0 = 1$ .

To check that  $\Pr(Y^{(s)} = 1) > 0$ , we introduce the random variables  $X_p^{(t)}$  on  $\hat{\mathbf{Z}}_p^t$  by  $X_p^{(t)}(x) = x_p \in (\mathbf{Z}/p\mathbf{Z})^t$ , for every prime p. Since  $\hat{\mathbf{Z}}' \cong \prod_p \text{prime } \mathbf{Z}_p^t$ , and since  $\Pr$  is a Haar measure, the  $X_p$  are independent random variables. Now  $Y^{(s)}$  has value  $\hat{\mathbf{0}} = 1$  if and only if every  $X_p^{(s)}$  is not the identity element of  $(\mathbf{Z}/p\mathbf{Z})^s$ . Hence

$$Pr(Y^{(s)} = 1) = \prod_{p} Pr(X_{p}^{(s)} \neq e)$$

$$= \prod_{p} (1 - p^{-s})$$

$$= \zeta(s)^{-1}, \quad \text{for } s > 1,$$

by a well-known product expansion for  $\zeta(s)$  valid for Re(s) > 1.

Therefore, by *Theorem 3*, we have that

$$\Pr(Y^{(s)} = n | Y^{(s)} \neq \infty) = n^{-s} \zeta(s)^{-1}, \quad \text{for } s > 1.$$

On the other hand, setting n=1 in the formula above and comparing it with the earlier unconditional probability computed above yields the fact that  $\Pr(Y^{(s)} \neq \infty) = 1$ . The result then follows.

We remark that one can show

$$\Pr(Y^{(s)} \neq \infty) = \begin{cases} 0, & \text{if } s = 1, \text{ and} \\ 1, & \text{if } s > 1. \end{cases}$$

This is consistent with the fact that  $(Y^{(s)} = \infty)$  is a "tail event."

As in Corollary 1 of Section 4, we can restate Theorem 4 in terms of a process on a probability space. This gives the result stated in Section 1:

COROLLARY 2. There is a probability measure on  $\hat{\mathbf{Z}}^{\infty}$ , and a sequence of random variables  $Z_s$  on  $\hat{\mathbf{Z}}^{\infty}$ , for s>1, such that

$$Pr(Z_s = n) = n^{-s}\zeta(s)^{-1}$$
, for every  $s > 1$ .

This research was supported by National Science Foundation Grants DMS-90006395 to K.S.A., MCS-7903029 to K.B., and MCS-7308445 to G.-C.R.

- 1. Baclawski, K., Cerasoli, M. & Rota, G.-C. (1984) Introduction to Probability and Random Processes (Unione Matematica Italiana, Bologna, Italy) (published in Italy under the title Introduzione alla Probabilità).
- Kung, J., Murty, M. & Rota, G.-C. (1980) J. Number Theory 12, 421–436.
- 3. Rota, G.-C. (1964) Z. Wahrsch. Verw. Gebiete 2, 340-368.