PACIFIC JOURNAL OF MATHEMATICS
Vol. 79, No. 2, 1978

A CONVOLUTION RELATED TO GOLOMB'S ROOT FUNCTION

E. E. GUERIN

The root function $\gamma(n)$ is defined by Golomb for $n>1$ as the number of distinct representations $n=a^b$ with positive integers a and b. In this paper we define a convolution ∇ such that γ is the ∇-analog of the (Dirichlet) divisor function τ. The structure of the ring of arithmetic functions under addition and ∇ is discussed. We compute and interpret ∇-analogs of the Moebius function and Euler's Φ-function. Formulas and an algorithm for computing the number of distinct representations of an integer $n\geqq 2$ in the form $n=a_1^{a_2^{\cdot^{\cdot^{\cdot^{a_k}}}}}$, with a_i a positive integer, $i=1,\cdots,k$, are given.

1. Introduction. Let Z denote the set of positive integers, let A denote the set of arithmetic functions (complex-valued functions with domain Z), and let F denote the set of elements of Z which are not kth powers of any positive integer for $k>1 (k\in Z)$. Note that $1\notin F$. The divisor function τ can be defined as $\tau=\nu_0 * \nu_0$, where $\nu_0\in A$, $\nu_0(n)=1$ for all $n\in Z$, and $*$ is the Dirichlet convolution defined for $\alpha,\beta\in A$ by $(\alpha*\beta)(n)=\sum_{d\mid n}\alpha(d)\beta(n/d)$.

Any integer $n\geqq 2$ having canonical form $n=p_1^{e_1}\cdots p_r^{e_r}$ is uniquely expressible as $n=m^g$, where $g=g.c.d.\ (e_1,\cdots,e_r)$ and $m\in F$. Golomb [1] defines the root function $\gamma(n)$ for $n\in Z, n>1$, as the number of distinct representations $n=a^b$ with $a,b\in Z$; and he notes that $\gamma(n)=\tau(g)$ for $n=m^g$, $m\in F$, $g\in Z$. We let $\gamma(1)=1$.

For $\alpha,\beta\in A, n=m^g$, with $m\in F, g\in Z$, we define the G-convolution ("Golomb" convolution), ∇, by

$$(\alpha\nabla\beta)(n)=\sum_{d\mid g}\alpha(m^d)\beta(m^{g/d})\ . \tag{1.1}$$

We define $(\alpha\nabla\beta)(1)=1$. This G-convolution is not of the Narkiewicz type [2, 4].

In § 2, we show that $\{A,+,\nabla\}$ (where $(\alpha+\beta)(n)=\alpha(n)+\beta(n)$, $n\in Z$) is a commutative ring with unity and we characterize the units and the divisors of zero. We define a G-multiplicative function and note that the set of G-multiplicative units in $\{A,+,\nabla\}$ forms an Abelian group under the operation ∇.

We choose to define ∇ as in (1.1) because then $(\nu_0\nabla\nu_0)(n)$ equals $\gamma(n)$, the number of distinct representations of n as a^b, $a,b\in Z$;

this is an analog of $\tau(n) = (\nu_0 * \nu_0)(n)$ which is the number of distinct representations of n as $a \cdot b$, $a, b \in Z$. In § 3, ∇-analogs of the Moebius function μ, the sum of divisors function σ, and Euler's ϕ-function are computed and interpreted.

In § 4, we state formulas and an algorithm for computing the number of distinct representations of an integer $n \geqq 2$ in the form

$$n = a_1^{a_2^{\cdot^{\cdot^{\cdot^{a_k}}}}} \tag{1.2}$$

with $a_i \in Z$, $i = 1, \cdots, k$.

2. The ring $\{A, +, \nabla\}$. First we state some properties related to the G-convolution.

THEOREM 2.1. (i) *The system $\{A, +, \nabla\}$ is a commutative ring with unity ε_∇ (where $\varepsilon_\nabla(n) = 1$ if $n=1$ or $n \in F$, $\varepsilon_\nabla(n)=0$ otherwise).*

(ii) *α is a unit in $\{A, +, \nabla\}$ if and only if $\alpha(1) \neq 0$ and $\alpha(m) \neq 0$ for all $m \in F$.*

(iii) *A nonzero arithmetic function α is a nonzerodivisor in $\{A, +, \nabla\}$ if and only if $\alpha(1) \neq 0$ and for each $m \in F$ there is a positive integer g such that $\alpha(m^g) \neq 0$.*

Proof. (i) The associativity of ∇ follows from (1.1) and the associativity of the Dirichlet convolution $*$. The commutativity of ∇ and the distributivity of ∇ over $+$ follow directly from the definition of the G-convolution. If $n = m^g$, $g \in Z$, $m \in F$, then $(\varepsilon_\nabla \nabla \alpha)(n) = \sum_{d \mid g} \varepsilon_\nabla(m^d)\alpha(m^{g/d}) = \alpha(m^g) = \alpha(n)$; $(\varepsilon_\nabla \nabla \alpha)(1) = \alpha(1)$. Therefore, ε_∇ is the unity element in $\{A, +, \nabla\}$.

(ii) An element β in A such that $\alpha \nabla \beta = \varepsilon_\nabla$ is defined if and only if $\alpha(1)\beta(1)=1$, $\alpha(m)\beta(m)=1$ for $m \in F$, and $\sum_{d \mid g} \alpha(m^d)\beta(m^{g/d})=0$ for $m \in F$, $g \in Z$, $g > 1$. Thus, $\alpha(1) \neq 0$, $\alpha(m) \neq 0$ for $m \in F$, if and only if α is a unit in $\{A, +, \nabla\}$.

(iii) If $\alpha(1) = 0$, define $\beta \in A$ by $\beta(1) = 1$, $\beta(n) = 0$ if $n>1$. Then $(\alpha \nabla \beta)(n) = 0$ for every $n \in Z$ and α is a divisor of zero. If there exists an $m \in F$ such that $\alpha(m^g) = 0$ for every $g \in Z$, define $\beta \in A$ by $\beta(m) = 1$, $\beta(n) = 0$ for $n \in Z$, $n \neq m$. Then $(\alpha \nabla \beta)(n) = 0$ for all $n \in Z$ and α is a divisor of zero.

Assume that α is a zero divisor in $\{A, +, \nabla\}$. Then there is some $\beta \in A$, $\beta \neq \bar{O}$ (where $\bar{O}(n)=0$ for all $n \in Z$), such that $\alpha \nabla \beta = \bar{O}$. (1) If $\beta(1) \neq 0$ then $\alpha \nabla \beta = \bar{O}$ implies that $\alpha(1)\beta(1) = 0$ and that $\alpha(1) = 0$. (2) If $\beta(1) = 0$, let n be the smallest positive integer such that $\beta(n) \neq 0$; if $n = m^v$, $m \in F$, $v \in Z$, we show that $\alpha(m^w) = 0$ for all $w \in Z$. First, $(\alpha \nabla \beta)(m^v) = \sum_{d \mid v} \alpha(m^d)\beta(m^{v/d}) = 0$ implies that

$\alpha(m)\beta(m^v) = 0$ and that $\alpha(m) = 0$. And $(\alpha\nabla\beta)(m^{2v}) = 0$ implies that $\alpha(m)\beta(m^{2v}) + \alpha(m^2)\beta(m^v) = 0$ and so $\alpha(m^2) = 0$. Assume that $\alpha(m^t) = 0$, $1 \leqq t < r$. Then $(\alpha\nabla\beta)(m^{rv}) = \sum_{d|rv} \alpha(m^d)\beta(m^{rv/d}) = 0$ implies that $\alpha(m^r)\beta(m^v) = 0$ and $\alpha(m^r) = 0$. Therefore, $\alpha(m^w) = 0$ for all $w \in Z$ by induction. This completes the proof of the theorem.

We define $\alpha \in A$ to be G-multiplicative if $\alpha(1) = 1$, and whenever $(a, b) = 1$ and $m \in F$, $\alpha(m^{ab}) = \alpha(m^a)\alpha(m^b)$.

THEOREM 2.2. *The set of G-multiplicative functions which are units in $\{A, +, \nabla\}$ form an abelian group under ∇.*

Proof. If α and β are G-multiplicative, then $\alpha\nabla\beta$ is also; the proof is similar to that of the multiplicativity of $\alpha*\beta$ given that α and β are multiplicative [3, p. 93]. It is then easy to verify the required group properties.

3. The functions $\sigma_\nabla, \mu_\nabla, \phi_\nabla$. As noted earlier, $\gamma = \nu_0\nabla\nu_0$ is the ∇-analog of $\tau = \nu_0*\nu_0$. For example, $\gamma(64) = \gamma(2^6) = \tau(6) = 4$, and 64 can be represented in the form a^b for $a, b \in Z$ in four ways: $(2^1)^6 = 2^6$, $(2^2)^3 = 4^3$, $(2^3)^2 = 8^2$, and $(2^6)^1 = 64^1$.

If we define σ_∇ by $\sigma_\nabla = \nu_0\nabla\nu_1$, then for $n = m^g$, $m \in F$, $g \in Z$, $\sigma_\nabla(n) = \sum_{d|g} m^d$. So $\sigma_\nabla(n)$ is the sum of the a's such that $a^b = n$, whereas $\sigma(n) = (\nu_0*\nu_1)(n)$ is the sum of the a's such that $a \cdot b = n (a, b \in Z)$.

An analog μ_∇ of the Moebius function μ (where μ satisfies $\nu_0*\mu = \varepsilon$ with $\varepsilon(1) = 1$, $\varepsilon(n) = 0$ otherwise) is defined by $\nu_0\nabla\mu_\nabla = \varepsilon_\nabla$. Then $\mu_\nabla(n) = 1$ if $n = 1$, $\mu_\nabla(n) = \mu(g)$ if $n = m^g$, $m \in F$, $g \in Z$.

Euler's ϕ-function, which satisfies $\phi = \mu*\nu_1$ (where $\nu_1(n) = n$ for all $n \in Z$), has an analog ϕ_∇ with $\phi_\nabla(1) = 1$, $\phi_\nabla(n) = (\mu_\nabla\nabla\nu_1)(n) = \sum_{d|g} \mu(d)m^{g/d}$ for $n = m^g$, $m \in F$, $g \in Z$. Thus, $\phi_\nabla(m) = m$ for $m \notin F$ and $\phi_\nabla(m^p) = m^p - m$ for $m \in F$, p prime. If $n = m^g$, $m \in F$, $g \in Z$, then $\phi_\nabla(n)$ is n minus the number of positive integers less than or equal to n which are expressible as r^d, $r \in Z$, $d | g$, $d > 1$. Here, n and r^d have a common power $d > 1$ (since $n = a^d$ with $a = m^{g/d}$); this corresponds, in the computation of $\phi(n)$, to nonrelativity-prime n and m having a common divisor $d > 1$. To illustrate, $\phi_\nabla(64) = 2^6 - 2^3 - 2^2 + 2^1 = 64 - 10 = 54$. The ten integers of the form r^d, $r \in Z$, $d | 6$, $d > 1$, $r^d \leqq 64$, are

$$1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2 = 4^3 = 2^6, 2^3, 3^3 .$$

And, for example, 3^2 and $n = 8^2$ have common power 2, while 2^3 and $n = 4^3$ have common power 3.

It can be verified that $\gamma, \varepsilon_\nabla, \nu_0$, and μ_∇ are G-multiplicative functions whereas ν_1, σ_∇, and ϕ_∇ are not.

If $n = m^g$, $m \in F$, $g \in Z$, then $\sigma_{\nabla}(n) = 2n$ has no solutions. But if we define a G-perfect number $n = m^g$, $m \in F$, $g \in Z$, as one such that $\prod_{d \mid g} m^d = n^2$, then n is G-perfect if and only if g is perfect if and only if $(\nu_0 * \nu_1)(g) = 2g$.

4. Power representations of n. If $n = m^g$, $m \in F$, $g \in Z$, define $\rho \in A$ by $\rho(n) = g$; define $\rho(1) = 1$. Then $\gamma(n) = \tau(\rho(n)) = (\nu_0 \nabla \nu_0)(n) = ((\nu_0 * \nu_0) \circ \rho)(n)$ (where $(\alpha \circ \beta)(n) = \alpha(\beta(n))$). We note that $\mu_{\nabla}(n) = \mu(\rho(n))$ and $\varepsilon_{,}(n) = \varepsilon(\rho(n))$.

Let $R_k(n)$ denote the number of distinct representations of $n = m^g$, $m \in F$, $g \in Z$, in the form given in (1.2). (Assume that $R_k(1) = 1$ for all $k \in Z$.) We have the following formulas.

$$R_1(n) = 1 .$$

$$R_2(n) = \gamma(n) = \tau(\rho(n)) = (\nu_0 \nabla \nu_0)(n) .$$

$$\begin{aligned} R_3(n) &= \sum_{d \mid g} \gamma(d) = \sum_{d \mid \rho(n)} \tau(\rho(d)) = (\nu_0 * (\tau \circ \rho))(\rho(n)) \\ &= ((\nu_0 * (\nu_0 \nabla \nu_0)) \circ \rho)(n) . \end{aligned}$$

$$\begin{aligned} R_4(n) &= \sum_{d \mid g} \sum_{r \mid \rho(d)} \gamma(r) = \sum_{d \mid \rho(n)} \sum_{r \mid \rho(d)} \tau(\rho(r)) = (\nu_0 * ((\nu_0 * (\tau \circ \rho)) \circ \rho))(\rho(n)) \\ &= ((\nu_0 * ((\nu_0 * (\nu_0 \nabla \nu_0)) \circ \rho)) \circ \rho)(n) . \end{aligned}$$

Similar formulas can be written for $R_k(n)$ for any $k \in Z$.

If $n > 1$, then $R_k(n)$ can be computed as follows. List d_1 such that $d_1 \mid g$, list $\rho(d_1)$, list d_2 such that $d_2 \mid \rho(d_1)$, list $\rho(d_2), \cdots$, list d_{k-2} such that $d_{k-2} \mid \rho(d_{k-3})$, list $\rho(d_{k-2})$; and $R_k(n)$ is the sum of the number of divisors of the entries in the final list.

For example, if $n = 20^{400}$, $g = \rho(n) = 2^4 \cdot 5^2$. For $d_1 \mid g$, $d_2 \mid \rho(d_1)$, $d_3 \mid \rho(d_2)$, we have these lists.

$$\begin{aligned} d_1 &= 1, 2, 4, 8, 16, 1\cdot 5, 2\cdot 5, 4\cdot 5, 8\cdot 5, 16\cdot 5, 1\cdot 5^5, 2\cdot 5^2, 4\cdot 5^2, 8\cdot 5^2, 16\cdot 5^2 \\ \rho(d_1) &= 1, 1, 2, 3, 4, \qquad 1, 1, 1, 1, 1, 2, \quad 1, \quad 2, \quad 1, 2 \\ d_2 &= 1, 1, 1, 2, 1, 3, 1, 2, 4, \quad 1, 1, 1, 1, 1, 1, 2, 1, 1, 2, 1, 1, 2 \\ \rho(d_2) &= 1, 1, 1, 1, 1, 1, 1, 1, 2, \quad 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1 \\ d_3 &= 1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1 \\ \rho(d_3) &= 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1 \end{aligned}$$

Then $R_3(20^{400}) = 2\tau(1) + \tau(2) + \tau(3) + \tau(4) + 5\tau(1) + \tau(2) + \tau(1) + \tau(2) + \tau(1) + \tau(2) = 22$. And $R_4(20^{400}) = 23$, $R_5(20^{400}) = 23$; in fact, $R_k(20^{400}) = 23$ for $k \geqq 4$. There are four representations of $n = 20^{400}$ in the form given in (1.2) for $k = 4$ which correspond to $d_1 = 16$ (since $\tau(1) + \tau(1) + \tau(2) = 4$). They are

$$a^{16^{1^{1}}}, \quad a^{4^{2^{1}}}, \quad a^{2^{4^{1}}}, \quad a^{2^{2^{2}}},$$

where $a = 335, 544, 320, 000, 000, 000, 000, 000, 000, 000, 000$ (which is 20^{25} in expanded form). In only one of these representations is $a_i \neq 1, i = 1, \cdots, 4$. In general, the number of distinct representations of $n = m^g, m \in F, g \in Z$, in the form given in (1.2) with the additional requirement that $a_i \neq 1, i = 1, \cdots, k$, is the sum of the number of divisors less one of the entries in the final list (for $\rho(d_{k-2})$).

REFERENCES

1. S. W. Golomb, *A new arithmetic function of combinatorial significance*, J. Number Theory, **5** (1973), 218–223.
2. W. Narkiewicz, *On a class of arithmetical convolutions*, Colloq. Math., **10** (1963), 81–94.
3. I. Niven and H. Zuckerman, *An Introduction to the Theory of Numbers*, 3rd ed., New York, John Wiley Sons, 1972.
4. M. V. Subbarao, *On Some Arithmetic Convolutions in The Theory of Arithmetic Functions*, Lecture Notes #251, New York, Springer-Verlag, 1972.

Received October 3, 1977

SETON HALL UNIVERSITY
SOUTH ORANGE, NJ 07079