Canad. Math. Bull. Vol. **13** (4), 1970

ARITHMETICAL FUNCTIONS AND DISTRIBUTIVITY

BY
P. J. McCARTHY

1. **The general results.** In this note we shall present a result about incidence functions on a locally finite partially ordered set, a result which is related to theorems of Lambek [2] and Subbarao [6]. Our terminology and notation will be that of Smith [4, 5] and Rota [7].

Let $(L, \leq)$ be a partially ordered set which is locally finite in the sense that for all $x, y \in L$, the interval $[x, y]=\{z \mid x\leq z\leq y\}$ is finite. Denote by $A(L, \leq)$ the set of functions f from $L\times L$ into some field, which is fixed once and for all, such that $f(x, y)=0$ whenever $x \not\leq y$. The product fg and the convolution $f*g$ of functions $f, g \in A(L, \leq)$ are defined, respectively, by

$$(fg)(x, y) = f(x, y)g(x, y)$$

and

$$(f*g)(x, y) = \sum_{x\leq z\leq y} f(x, z)g(z, y)$$

for all $x, y \in L$, a sum over an empty set being equal to zero.

Our concern will be with the following question: under what conditions will a function $f\in A(L, \leq)$ have the property that $f(g*h)=fg*fh$ for all $g, h \in A(L, \leq)$? Lambek, in [2], and Subbarao, in [6], asked and answered an analogous question in two very special cases involving arithmetical functions. The answer to this question is very simple to obtain, and will be given in Theorem 1. In the next section we shall show how to specialize to arithmetical functions and obtain a result broad enough to include the theorems of Lambek and Subbarao. In the final section we shall look at still another special situation.

THEOREM 1. *If $f\in A(L, \leq)$ then $f(g*h)=fg*fh$ for all $g, h \in A(L, \leq)$ if and only if*

$$f(x, y) = f(x, z)f(z, y) \quad \textit{for all } x \leq z \leq y. \tag{1}$$

Proof. If (1) holds then for $x\leq y$,

$$\begin{aligned}(f(g*h))(x, y) &= \sum_{x\leq z\leq y} f(x, z)g(x, z)f(z, y)h(z, y)\\ &= (fg*fh)(x, y).\end{aligned}$$

Conversely, suppose that $f(g*h)=fg*fh$ for all $g, h \in A(L, \leq)$. For $x\leq y$, let δ_{xy} be any function in $A(L, \leq)$ such that

$$\delta_{xy}(x, z) = \begin{cases}1 & \text{if } z = y\\ 0 & \text{if } z \neq y\end{cases}, \qquad \delta_{xy}(z, y) = \begin{cases}1 & \text{if } z = x\\ 0 & \text{if } z \neq x\end{cases}.$$

Received by the editors April 20, 1970.

https://doi.org/10.4153/CMB-1970-089-8 Published online by Cambridge University Press

Then, if $x \leq z \leq y$,

$$\begin{aligned}(f(\delta_{xz} * \delta_{zy}))(x, y) &= f(x, y) \sum_{x \leq w \leq y} \delta_{xz}(x, w)\delta_{zy}(w, y) \\ &= f(x, y)\end{aligned}$$

is equal to

$$\begin{aligned}(f\delta_{xz} * f\delta_{zy})(x, y) &= \sum_{x \leq w \leq y} f(x, w)\delta_{xz}(x, w)f(w, y)\delta_{zy}(w, y) \\ &= f(x, z)f(z, y).\end{aligned}$$

Always, there exists such a function δ_{xy} whenever $x \leq y$; for example, set

$$\delta_{xy}(u, v) = \begin{cases} 1 & \text{if } u = x \quad \text{and } v = y \\ 0 & \text{otherwise.} \end{cases}$$

However, in certain special cases we shall want to choose δ_{xy} so that it has additional properties.

For the rest of this section we shall assume that $(L, \leq)$ is a locally distributive local lattice, i.e. every nonempty interval $[x, y]$ is a finite distributive lattice. If $x, y \in L$, then y is said to cover x if $[x, y]$ contains exactly two elements. By a result of Rota [7, p. 350] the Möbius function μ of $(L, \leq)$ is given by

$$\mu(x, y) = \begin{cases} 0 & \text{if } y \text{ is not the join of elements covering } x \\ (-1)^n & \text{if } y \text{ is the join of } n \text{ elements covering } x. \end{cases}$$

In [4], Smith introduced the notion of a factorable function in $A(L, \leq)$, and in [5, Lemma 3] he showed that an invertible function $f \in A(L, \leq)$ is factorable if f satisfies (1) and the following condition:

(2) $f(x \wedge y, x) = f(y, x \vee y)$ whenever x and y belong to an interval of $(L, \leq)$.

In [5], Smith considered local lattices for which the following holds:

(3) Every nonempty interval is a direct product of a finite number of chains.

It follows from a general result in lattice theory [8, p. 200] that such a direct decomposition is unique except for trivial factors and the order of the factors. If $(L, \leq)$ satisfies (3), then the functions in $A(L, \leq)$ behave very much like arithmetical functions, and the factorable functions behave like multiplicative functions, as we see from the following result.

THEOREM 2. *Assume that* $(L, \leq)$ *satisfies* (3) *and that* f *is an invertible function in* $A(L, \leq)$ *which satisfies* (1) *and* (2). *If* $x \leq y$ *and if* $[x, y]$ *is the direct product of chains* $[x_{i0}, x_{ik_i}]$, $i = 1, \ldots, n$, *then*

$$f(x, y) = \prod_{i=1}^{n} f(x_{i0}, x_{ik_i}).$$

https://doi.org/10.4153/CMB-1970-089-8 Published online by Cambridge University Press

Proof. The proof we shall give was suggested by an argument given by Lambek [2, p. 971]. Define $\delta \in A(L, \leq)$ by $\delta(x, x)=1$ for all $x \in L$ and $\delta(x, y)=0$ if $x \neq y$. Recall that, by definition, f is invertible if there exists $f' \in A(L, \leq)$ such that $f * f' = \delta$. This is the case if and only if $f(x, x) \neq 0$ for all $x \in L$ [4, Proposition 1]: if, in addition, f satisfies (1), then $f(x, x)=1$ for all $x \in L$.

Now assume that f is invertible and does satisfy (1) and (2). Define $g \in A(L, \leq)$ as follows: if $x \nleq y$ then $g(x, y)=0$, and if $x \leq y$ and $[x, y]$ is the direct product of chains $[x_{i0}, x_{ik_i}]$, $i=1, \ldots, n$, then

$$g(x, y) = \prod_{i=1}^{n} f(x_{i0}, x_{ik_i}).$$

It is clear that g satisfies (1), and it follows from (2) that $g\mu = f\mu$. To show this we note that $(g\mu)(x, y)=0=(f\mu)(x, y)$ if y is not the join of elements covering x, so we assume that y is the join of n elements covering x, say $x_1, \ldots, x_n$. Then $[x, y]$ is the direct product of the intervals $[x, x_i]$, $i=1, \ldots, n$. If we use (1) and (2), and the fact that the lattice $[x, y]$ is distributive, we obtain $(f\mu)(x, y)=(-1)^n f(x, x_1) \ldots f(x, x_n)$, which is equal to $(g\mu)(x, y)$. Furthermore, $f\mu * f = \delta = g * g\mu$. Therefore, $f = \delta * f = g * g\mu * f = g * f\mu * f = g * \delta = g$.

2. **Regular arithmetical convolutions.** By an arithmetical convolution we mean a mapping C from the set N of positive integers into the set of subsets of N such that for each $n \in N$, $C(n)$ consists entirely of divisors of n. If f and g are arithmetical functions, their C-convolution $f * g$ is defined by

$$(f * g)(n) = \sum_{d \in C(n)} f(d)g(n/d).$$

Following Narkiewicz [3], we shall call an arithmetical convolution C regular if

(a) the set of arithmetical functions is a commutative ring with unity with respect to addition, defined by $(f+g)(n)=f(n)+g(n)$ for all $n \in N$, and C-convolution,

(b) the C-convolution of multiplicative functions is multiplicative, and

(c) the function e defined by $e(n)=1$ for all $n \in N$ has an inverse μ_C with respect to C-convolution, and $\mu_C(n)=0$ or -1 whenever n is a prime power.

Narkiewicz showed [3, pp. 82–85] that C is regular if and only if it satisfies the following conditions (which are not independent of one another):

(i) The statements "$d \in C(m)$ and $m \in C(n)$" and "$d \in C(n)$ and $m/d \in C(n/d)$" are equivalent.

(ii) $d \in C(n)$ implies $n/d \in C(n)$.

(iii) $1, n \in C(n)$ for all $n \in N$.

(iv) If $(m, n)=1$ then $C(mn)=\{de \mid d \in C(m), e \in C(n)\}$.

(v) For every prime power $p^a > 1$ there is a divisor $t=\tau_C(p^a)$ of a, called the type of p^a, such that $C(p^a)=\{1, p^t, p^{2t}, \ldots, p^{rt}\}$, $rt=a$, and $p^t \in C(p^{2t})$, $p^{2t} \in C(p^{3t})$, etc.

https://doi.org/10.4153/CMB-1970-089-8 Published online by Cambridge University Press

We note that the Dirichlet convolution D, where $D(n)$ is the set of all positive divisors of n, and the unitary convolution U, where $U(n)$ is the set of all positive divisors d of n such that $(d, n/d)=1$, are regular.

Suppose that C is a regular arithmetical convolution. If we define a relation on N by $m \leq_c n$ if $m \in C(n)$, then $(N, \leq_c)$ is a locally distributive local lattice which satisfies (3). This follows immediately from the characterization of regular arithmetical convolutions which is stated above. If f is an arithmetical function, then we can associate with f a function $f' \in A(N, \leq_c)$ defined by $f'(m, n)=0$ if $m \notin C(n)$ and $f'(m, n)=f(n/m)$ if $m \in C(n)$. The function f' is factorable if f is multiplicative. On the other hand, if $g \in A(N, \leq_c)$ and if $g(m, n)$ depends only on the ratio n/m whenever $m \in C(n)$, then we can associate with g an arithmetical function g' defined by $g'(n)=g(1, n)$. Not every function in $A(N, \leq_c)$ corresponds to an arithmetical function under this correspondence. However, if we can choose δ_{xy} in the proof of Theorem 1 in such a way that it does correspond to an arithmetical function, then our next result can be proved the same way as Theorem 1, and may be considered rightly as a corollary to Theorems 1 and 2. If $m \in C(n)$ define δ_{mn} by

$$\delta_{mn}(r, s) = \begin{cases} 1 & \text{if } r \in C(s) \text{ and } s/r = n/m \\ 0 & \text{otherwise.} \end{cases}$$

THEOREM 3. *Let C be a regular arithmetical convolution. If f is an arithmetical function, then $f(g * h)=fg * fh$ for all arithmetical functions g and h, if and only if for every positive integer $n=p_1^{a_1} \ldots p_k^{a_k}$, where the p_i are distinct primes and every $a_i \geq 1$, we have*

$$f(n) = \prod_{i=1}^{k} f(p_i^{t_i})^{a_i/t_i},$$

where

$$t_i = \tau_C(p_i^{a_i}) \quad \textit{for } i = 1, \ldots, k.$$

Note that if the function in $A(N, \leq_c)$ corresponding to f satisfies (1) and (2), then f is multiplicative by Theorem 2. On the other hand, if f satisfies that condition of Theorem 3, then f is multiplicative.

The special cases of Theorem 3 when $C=D$ and when $C=U$ are due to Lambek [2, Theorem 1] and to Subbarao [6, p. 986, Lemma], respectively.

In general, the C-convolution of arithmetical functions which satisfy the condition of Theorem 3 does not satisfy that condition. Hence, we cannot expect that for such functions will we have $(f * g)(h * k)$ equal to $fh * fk * gh * gk$. The relation between these two expressions was obtained by Lambek in the case when $C=D$ [2, Theorem 2], and by Subbarao in the case when $C=U$ [6, Theorem 2]. We shall now prove a theorem which contains both of these results.

THEOREM 4. *Let C be a regular arithmetical convolution. If f, g, h, and k are arithmetical functions which satisfy the condition of Theorem 3, then*

$$fh * fk * gh * gk = (f * g)(h * k) * u,$$

https://doi.org/10.4153/CMB-1970-089-8 Published online by Cambridge University Press

where u is a multiplicative function such that for every prime power $p^a > 1$, *with* $t = \tau_C(p^a)$,

$$u(p^a) = \begin{cases} f(p^{a/2})g(p^{a/2})h(p^{a/2})k(p^{a/2}) & \textit{if } a/t \textit{ is even,} \\ 0 & \textit{if } a/t \textit{ is odd.} \end{cases}$$

Proof. It is enough to show that the two functions are equal at every prime power $p^a > 1$. Let $C(p^a) = \{1, p^t, \ldots, p^{rt}\}$, $rt = a$. Then

$$\begin{aligned} ((f*g)(h*k)*u)(p^a) &= \sum_{b+2c=r} (f*g)(h*k)(p^{bt})u(p^{2ct}) \\ &= \sum_{b+2c=r} \sum_{w+x=b} \sum_{y+z=b} f(p^{(w+c)t})g(p^{(x+c)t})h(p^{(y+c)t})k(p^{(z+c)t}) \end{aligned}$$

and

$$(fh*fk*gh*gk)(p^a) = \sum_{b+c+d+e=r} f(p^{(b+c)t})g(p^{(d+e)t})h(p^{(b+d)t})k(p^{(c+e)t}).$$

The equality of these sums follows from a lemma due to Lambek [2, p. 972], when it is applied to the integers p^bp^c, p^dp^e, p^bp^d, and p^cp^e, and the result is interpreted in terms of the exponents.

3. **The Lucas convolution.** Let p be a prime, fixed throughout this section. For $m, n \in N' = N \cup \{0\}$, we set $m \le_p n$ if $p \nmid \binom{n}{m}$, where $\binom{n}{m} = 0$ when m is larger than n in the usual ordering of the integers. Then $(N', \le_p)$ is a locally distributive local lattice which satisfies (3). If f and g are arithmetical functions, then their Lucas convolution $f*g$ is defined by

$$(f*g)(n) = \sum_{m \le_p n} f(m)g(n-m).$$

This type of convolution was discussed in [1], [4, §7], and [5, §2]. There is a correspondence between the arithmetical functions and those functions $f \in A(N', \le_p)$ such that $f(m, n)$ depends only on $n-m$ whenever $m \le_p n$. If we make use of this correspondence, and if we use in the proof of Theorem 1 the function δ_{mn} defined for $m \le_p n$ by

$$\delta_{mn}(r, s) = \begin{cases} 1 & \text{if } r \le_p s \text{ and } s-r = n-m \\ 0 & \text{otherwise,} \end{cases}$$

then we obtain the following result as a corollary to Theorems 1 and 2.

THEOREM 5. *Let f be an arithmetical function. Then* $f(g*h) = fg*fh$ *for all arithmetical functions g and h, if and only if for every positive integer* $n = a_0 + a_1p + a_2p^2 + \cdots + a_kp^k$, *where* $0 \le a_i \le p-1$ *for* $i = 0, 1, \ldots, k$, *we have*

$$f(n) = \prod_{i=0}^{k} a_i f(p^i).$$

Note that the condition of this theorem implies that f is factorable in the sense

https://doi.org/10.4153/CMB-1970-089-8 Published online by Cambridge University Press

of Carlitz [1, p. 589]. On the other hand, if f is factorable in the sense of Carlitz, then the corresponding function in $A(N', \leq_p)$ is factorable in the sense of Smith.

Finally, we have the following analogue of Theorem 4.

THEOREM 6. *Let f, g, h, and k be arithmetical functions which satisfy the condition of Theorem 5. Then*

$$fh*fk*gh*gk = (f*g)(h*k)*u,$$

where u is a factorable function such that for all nonnegative integers t and all integers r with $0 \leq r \leq p-1$,

$$u(rp^t) = \begin{cases} f((r/2)p^t)g((r/2)p^t)h((r/2)p^t)k((r/2)p^t) & \text{if } r \text{ is even} \\ 0 & \text{otherwise.} \end{cases}$$

If we calculate both sides of the asserted equality at rp^t, we see that this theorem also follows from Lambek's lemma cited above.

REFERENCES

1. L. Carlitz, *Arithmetic functions in an unusual setting*, Amer. Math. Monthly **73** (1966), 582–590.

2. J. Lambek, *Arithmetical functions and distributivity*, Amer. Math. Monthly **73** (1966), 969–973.

3. W. Narkiewicz, *On a class of arithmetical convolutions*, Colloq. Math. **10** (1963), 81–94.

4. David Smith, *Incidence functions as generalized arithmetic functions*, I, Duke Math. J. **36** (1967), 617–634.

5. ———, *Incidence functions as generalized arithmetic functions*, III, Duke Math. J. **36** (1969), 353–368.

6. M. V. Subbarao, *Arithmetic functions and distributivity*, Amer. Math. Monthly **75** (1968), 984–989.

7. Gian-Carlo Rota, *On the foundations of combinatorial theory*, I, Theory of Möbius functions, Z. Wahrsch. **2** (1964), 340–368.

8. Gabor Szász, *Introduction to lattice theory*, Academic Press, New York, 1963.

UNIVERSITY OF KANSAS,
LAWRENCE, KANSAS

https://doi.org/10.4153/CMB-1970-089-8 Published online by Cambridge University Press