ON ARITHMETIC CONVOLUTIONS

T. M. K. Davison

(received January 4, 1966)

1. Introduction. Let A be the set of all functions from N, the natural numbers, to C the field of complex numbers. The Dirichlet product of elements f, g of A is given by

$$f*g(n) = \sum_{d \mid n} f(d)\, g(nd^{-1}), \text{ for all } n \in N,$$

where the summation condition means sum over all positive integers d which divide n. The set A with the binary operation * (denoted by $\langle A, * \rangle$) is a semigroup with identity δ, where

$$\delta(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases},$$

(see e.g. [1]). The group of units of $\langle A, * \rangle$ is $\langle B, * \rangle$ where $B = \{f \mid f \in A,\ f(1) \neq 0\}$ (see [1]). The number theoretic result of most interest to us is that M, the set of multiplicative functions, is a subgroup of B. (Recall that $f \in B$ is multiplicative if, whenever m, n are relatively prime positive integers we have $f(mn) = f(m)f(n)$.)

In this paper we introduce a class of binary operations over A which includes the above product. Let X be the set of all ordered pairs of natural numbers such that $(m, n) \in X$ if, and only if, $n \mid m$. Let a be an arbitrary function from X to C, $(a: X \to C)$. The $\bar{a}$ - product of any pair f, g of elements of A is given by

$$f\bar{a}g(n) = \sum_{d \mid n} a(n, d) f(d)\, g(nd^{-1}), \text{ for all } n \in N.$$

We say that the function a determines the product $\bar{a}$. It is easy to see that distinct functions determine distinct products (c.f.

proof of Theorem 1). The function from X to C which is identically 1 determines the Dirichlet product.

The class of $\bar{a}$ - products includes the following products. The unitary product of Cohen [2], is determined by the function a, where

$$a(mn, n) = \begin{cases} 1 & \text{if } (m, n) = 1 \\ 0 & \text{otherwise} \end{cases} .$$

The convolutions of Narkiewicz [6], are determined by functions from X to C which take only the values 0, 1. (It will be realized that in this case the a(n, d) merely selects out "suitable" divisors.) Finally, the K-products of Subba Rao and Gioia [8], and Gioia [3], which are given by expressions of the form

$$f \times g(n) = \sum_{d|n} f(d) g(nd^{-1}) K((d, nd^{-1})),$$

(where (d, nd^{-1}) is the g.c.d. of d and nd^{-1}) are seen to be $\bar{a}$-products.

We now define some special types of $\bar{a}$-products, or equivalently, special types of determining functions. The function $a: X \to C$ is bounded if there is a $K > 0$ such that $|a(m, n)| < K$ for all pairs (m, n) in X. We say $a: X \to C$ is simple if

$$a(k\ell, \ell) = a((k, \ell)\ell, \ell) = a((k, \ell)\ell, (k, \ell))$$

for all $k, \ell \in N$ (note that (k, ℓ) denotes the g.c.d. of k and ℓ). The function $a: X \to C$ determines a convolution if, and only if, $< M, \bar{a} >$ is a group with identity δ. We note that the products of Dirichlet and Cohen are both bounded and simple, while the convolutions of Narkiewicz are bounded but not simple and the products of Subba Rao and Gioia are simple but not, in general, bounded.

In § 2 we state our main results which are then proved in § § 3, 4. Further examples of $\bar{a}$-products are given in § 5 (including a non-abelian product), and we indicate how the idea of the $\bar{a}$-product can be used to unify and extend some known results.

I am indebted to Professor J.H.H. Chalk for his help with the original version of these results which formed the substance of a chapter in my doctoral dissertation at the University of Toronto.

2. Statement of Results. The first theorem characterizes those functions which determine convolutions (c.f.[6, § 2]).

THEOREM 1. $< M, a >$ *is a group with identity* δ *if, and only if,* $a(m, n)$ *satisfies the following conditions:*

(i) $a(kmn, mn)\, a(mn, n) = a(kmn, n)\, a(km, m)$ *for all* $k, m, n, \in N$;

(ii) $a(rmsn, mn) = a(rm, m)\, a(sn, n)$ *whenever* $(rm, sn) = 1$;

(iii) $a(n, 1) = a(n, n) = 1$ *for all* $n \in N$.

We note that condition (ii) is that $a(m, n)$ be multiplicative in the sense of Vaidyanathaswamy [9]. Condition (i) gives necessary and sufficient conditions that the $\bar{a}$-product be associative, while (iii) gives the existence and uniqueness of the identity. It will be noted that inverses look after themselves (c.f. [6, (v)])! Before stating our next theorem we define some auxiliary functions. Let $a: X \to C$. For all $n \in N$, put

(2.1) $$u(n) = \sum_{k=1}^{n} a(kn, n),$$

(2.2) $$v(n) = \sum_{d \mid n} a(d^2, d)\, \mu(nd^{-1}),$$

and

(2.3) $$w(n) = \sum_{d \mid n} |v(d)|.$$

THEOREM 2. *Let* $a(m, n)$ *be bounded and simple. Let* $g \in A$ *satisfy* $g(n) = 0(1)$. *Then*

$$\sum_{n \leq x} g\bar{a}i(n) = \frac{x^2}{2} \sum_{1}^{\infty} g(m)u(m)m^{-3} + 0(x \sum_{k \leq x} w(k)k^{-1}),$$

where $i \in A$ *is given by* $i(n) = n$ *for all* $n \in N$.

In the special case when a determines the Dirichlet product this is a well-known result (see e.g.[10, p.9]); if, on the other hand, $a(m, n)$ determines the unitary product, then the result is due to Cohen [2, Th. 4.1].

3. Proof of Theorem 1. We shall prove the necessity of the conditions first. Assume then that $< M, \bar{a} >$ is a group with identity δ, so that $f\bar{a}\delta = f$; in other words $f(n) = a(n, n)f(n)$ for all $n \in N$ and all $f \in A$. From this, and a similar argument on the left, we deduce that $a(n, n) = a(n, 1) = 1$ for all $n \in N$.

https://doi.org/10.4153/CMB-1966-037-x Published online by Cambridge University Press

Next we note that the characteristic function of the divisors of a natural number is multiplicative. Now, given $m \in N$, $n \in N$ such that $(m, n) = 1$, and positive integers d and e where $d|m$, and $e|n$, construct f, g in M as follows:

$$f(k) = \begin{cases} 1 & \text{if } k|de \\ 0 & \text{otherwise,} \end{cases}$$

and

$$g(k) = \begin{cases} 1 & \text{if } k|mnd^{-1}e^{-1} \\ 0 & \text{otherwise} \end{cases}.$$

Then it is easy to verify that $f\bar{a}g(mn) = a(mn, de)$ and that $f\bar{a}g(m) = a(m, d)$, $f\bar{a}g(n) = a(n, e)$. But $f\bar{a}g \in M$ since M is a group; thus we have $a(mn, de) = a(m, d)a(n, e)$, which is equivalent to condition (ii). Since we have proved (ii) and (iii) we need only prove the validity of (i) on powers of a prime. Let p be any prime number, and α, β, γ be integers such that $\alpha \geq \beta \geq \gamma \geq 0$; then we have to show that $a(p^\alpha, p^\beta)\, a(p^\beta, p^\gamma) = a(p^\alpha, p^\gamma)\, a(p^{\alpha-\gamma}, p^{\beta-\gamma})$. Construct functions f, g, h in M as follows: put $f(1) = g(1) = h(1) = f(p^\gamma) = g(p^{\beta-\gamma}) = h(p^{\alpha-\beta}) = 1$, and put zero at all other arguments. Once again it is straightforward to verify that $f\bar{a}(g\bar{a}h)\,(p^\alpha) = a(p^\alpha, p^\gamma)\, a(p^{\alpha-\gamma}, p^{\beta-\gamma})$, and $(f\bar{a}g)\,\bar{a}\,h\,(p^\alpha) = a(p^\alpha, p^\beta)\, a(p^\beta, p^\gamma)$, which gives us the desired result.

We turn now to the sufficiency of the conditions. Assume (i). Let f, g, h be any three elements of M, and n any positive integer. Then, we have

$$\begin{aligned}(f\bar{a}g)\,\bar{a}\,h(n) &= \sum_{d|n} a(n, d)\, f\bar{a}g(d)\, h(nd^{-1}) \\ &= \sum_{d|n} a(n, d) \sum_{e|d} a(d, e)f(e)g(de^{-1})h(nd^{-1}) \\ &= \sum_{d|n} \sum_{e|d} a(n, d)a(d, e)f(e)g(de^{-1})h(nd^{-1}).\end{aligned}$$

But $a(n, d)a(d, e) = a(n, e)a(ne^{-1}, de^{-1})$ by (i), so that

$$(f\bar{a}g)\,\bar{a}\,h(n) = \sum_{d|n} \sum_{e|d} a(n, e)a(ne^{-1}, de^{-1})\, f(e)g(de^{-1})h(nd^{-1})$$

https://doi.org/10.4153/CMB-1966-037-x Published online by Cambridge University Press

$$= \sum_{e|n} a(n,e) f(e) \sum_{de^{-1}|ne^{-1}} a(ne^{-1}, de^{-1}) g(de^{-1}) h(nd^{-1})$$

$$= \sum_{e|n} a(n,e) f(e)\ g\bar{a}h(ne^{-1})$$

$$= f\ \bar{a}\ (g\bar{a}h)(n).$$

Thus we have shown that $\bar{a}$ is associative. Next, let f, g be any elements in M, and m, n any pair of relatively prime positive integers. Then

$$f\bar{a}g(mn) = \sum_{d|mn} a(mn, d)\ f(d)\ g(mnd^{-1})$$

$$= \sum_{k|m} \sum_{e|n} a(mn, ke)\ f(ke)\ g(mnk^{-1}e^{-1}).$$

By (ii) we have $a(mn, ke) = a(m,k)\ a(n,e)$, so that the previous sum splits into a product of sums and we deduce that $f\bar{a}g(mn) = f\bar{a}g(m)\ f\bar{a}g(n)$. (Note that the fact that f and g are multiplicative is crucial in this splitting.) It is trivial to deduce from (iii) that δ is the identity for M. It remains to show that every element in M has an inverse in M. In fact it suffices to prove that every element in M has a left inverse, since the two sided-ness follows from the existence of the identity (2-sided) δ; and the fact that the inverse, if it exists, must lie in M can be shown as follows. Suppose that $f \in M$ and that $g\bar{a}f = \delta$. Define

$\bar{g} \in M$ by specifying $\bar{g}$ on prime powers by $\bar{g}(p^{\alpha}) = g(p^{\alpha})$ and extending $\bar{g}$ to all of N in the obvious fashion to make it multiplicative. Then clearly

$$\bar{g}\ \bar{a}\ f(n) = \prod_{p^{\alpha}|n} \bar{g}\ \bar{a}\ f(p^{\alpha}) = \prod_{p^{\alpha}|n} g\ \bar{a}\ f(p^{\alpha}) = \prod_{p^{\alpha}|n} \delta(p^{\alpha})$$

$$= \delta(n).$$

We now have to construct a left inverse of an arbitrary element $f \in M$. Put $f^{-1}(1) = 1$, and assume that $f^{-1}(k)$ has been defined for all integers less than n, where $n \geq 2$. Define f^{-1} at n by

$$f^{-1}(n) = -\sum_{d|n,\ d<n} a(n,d)\ f^{-1}(d)\ f(nd^{-1}).$$

It is then easy to check that $f^{-1}\bar{a}\ f(n) = \delta(n)$ for all n. Thus

$< M, \bar{a} >$ is a group.

4. Proof of Theorem 2. In the proof of the theorem we use a pair of lemmas in which it is assumed that $a: X \to C$ is simple. The functions u, v, w are defined by equations 2.1, 2.2, 2.3. We note that $u = v*i$, since (a is simple!)

$$u(n) = \sum_{k \leq n} a(kn, n) = \sum_{k \leq n} a((k, n)n, n) = \sum_{d|n} a(dn, n)\, \emptyset(nd^{-1})$$

$$= \sum_{d|n} a(d^2, d)\, \emptyset(nd^{-1}), \quad \text{for all } n \in N.$$

After putting $b(m) = a(m^2, m)$ for all $m \in N$, we have $u = b*\emptyset = b*(\mu*i) = (b*\mu)*i$; but $v = b*\mu$ by definition, so $u = v*i$ as stated. The proof of Lemma 1 below uses the following well-known result (see e.g. [5, p.91 prob. 3]): If $\Phi(x, n)$ is the number of positive integers less than or equal to x and prime to n, then

$$\Phi(x, n) = \sum_{d|n} \mu(d)\, [xd^{-1}].$$

LEMMA 1. Put $F(x, n) = \sum_{k \leq x} a(kn, n)$ for all $x \geq 0$ and all $n \in N$. Then, we have

$$F(x, n) = \sum_{d|n} v(d)\, [xd^{-1}].$$

Proof. $$\sum_{k \leq x} a(kn, n) = \sum_{d|n} a(d^2, d)\, \Phi(xd^{-1}, nd^{-1})$$

$$= \sum_{d|n} a(d^2, d) \sum_{m|nd^{-1}} \mu(m)[xd^{-1}m^{-1}].$$

Putting $s = dm$ and rearranging the summation, we obtain

$$F(x, n) = \sum_{s|n} [xs^{-1}] \sum_{d|s} a(d^2, d)\, \mu(sd^{-1});$$

but the inner sum is just $v(s)$, whence the result follows.

COROLLARY. $F(x, n) = u(n)n^{-1}x + 0(w(n))$.

Proof. $$\sum_{d|n} v(d)[xd^{-1}] = xn^{-1}\Big(\sum_{d|n} v(d)nd^{-1}\Big) + 0\Big(\sum_{d|n} |v(d)|\Big),$$

https://doi.org/10.4153/CMB-1966-037-x Published online by Cambridge University Press

$$= xn^{-1} \; v * i(n) + O(w(n))$$

$$= xn^{-1} \; u(n) + O(w(n)).$$

LEMMA 2. *Put* $F^*(x, n) = \sum_{k \le x} k \; a(kn, n)$ *for all* $x \ge 0$ *and* $n \in N$. *Then we have*

$$F^*(x, n) = \frac{u(n)}{2n} x^2 + O(x \; w(n)).$$

Proof. By partial summation we see that

$$F^*(x, n) = [x+1] \; F(x, n) - \sum_{k \le x} F(k, n)$$

$$= S_1 - S_2, \text{ say.}$$

Now

$$S_1 = u(n)n^{-1} x^2 + O(x|u(n)n^{-1}|) + O(x \; w(n)),$$

and

$$S_2 = \frac{1}{2} u(n)n^{-1} x^2 + O(x|u(n)n^{-1}|) + O(x \; w(n))$$

by the corollary; but $|u(n)n^{-1}| = |\sum_{d|n} v(d)d^{-1}| = O(w(n))$, so that $S_1 - S_2 = \frac{1}{2} u(n)n^{-1} x^2 + O(x \; w(n))$ as stated.

We can now proceed to the proof of the theorem.

$$\sum_{n \le x} g \; \bar{a} \; i(n) = \sum_{n \le x} \sum_{de=n} a(de, d) \; g(d)e$$

$$= \sum_{d \le x} g(d) \; F^* \; (xd^{-1}, d).$$

We use our estimate of F^* and the hypothesis that $g(n) = O(1)$ to obtain

$$\sum_{d \le x} g(d) \; F^*(xd^{-1}, d) = \frac{1}{2} x^2 \sum_{d \le x} g(d)u(d)d^{-3} + O(x \sum_{d \le x} w(d)d^{-1}).$$

Now $u(n) = O(n)$ since a is bounded. Thus $g(n) \; u(n) \; n^{-3} = O(n^{-2})$, and so we can write

$$\sum_{d \le x} g(d)u(d)d^{-3} = \sum_{1}^{\infty} g(m)u(m) \; m^{-3} + O(x^{-1}).$$

https://doi.org/10.4153/CMB-1966-037-x Published online by Cambridge University Press

It is clear that $w(n) \geq 1$ for all n, and the theorem is proved.

5. Examples and further results. Our first example is constructed so that the product of completely multiplicative functions is itself completely multiplicative. It is given by

$$a(p^m, p^n) = \binom{m}{n} = \frac{m!}{n!(m-n)!}, \quad p \text{ prime}, \ m \geq n \geq 0,$$

and is extended to all of X using multiplicativity. In fact this a determines a convolution, as the reader can easily prove.

The next example, also defined on prime power pairs and extended by multiplicativity, gives a class of non-abelian convolutions. Let $k \in N$ be at least 2. Put

$$a(p^m, p^n) = \begin{cases} 1 & \text{if } m = n \text{ or } n \equiv 0 \pmod{k} \\ 0 & \text{otherwise}. \end{cases}$$

To show that a is non-abelian evaluate

$$f\bar{a}g(p^{k+1}) = g(p^{k+1}) + f(p^{k+1}) + f(p^k)\, g(p),$$

which is, in general, distinct from $g\bar{a}f$.

Our final example is defined by

$$a(mn, n) = \begin{cases} 1, & m \text{ odd} \\ (-1)^{n-1}, & m \text{ even} \end{cases},$$

and is taken from an article of Rankin [7, form 33], who obtains the formula

$$P_{20}(n) = \frac{8}{31}\Big(\sum_{\substack{d|n \\ nd^{-1} \text{ odd}}} d^9 - \sum_{\substack{d|n \\ nd^{-1} \text{ even}}} (-1)^d d^9 \Big).$$

Using the above $\bar{a}$-product this can be written

$$P_{20} = \frac{8}{31}\, i^9 \,\bar{a}\, 1, \text{ where } i^9(n) = n^9 \text{ and } 1(n) = 1 \text{ for all } n \in N.$$

We turn now to the consideration of further applications of a-products. We define the $\bar{a}$-analogue μ_a of the Möbius function μ by

$$1 \,\bar{a}\, \mu_a = \mu_a \,\bar{a}\, 1 = \delta .$$

When a determines the Dirichlet product (resp. unitary product) μ_a is μ(resp. μ^* of Cohen). The μ_a of our first example above is λ, where $\lambda(n) = (-1)^p$, p being the total number of prime factors of n (see e.g. [4, Thm. 300]). We can use the "generalized" Möbius functions to define "generalized" $\emptyset$ functions, and, of course many other arithmetic functions. We can also give analogues of the Ramanujan sum ([4, Ch. 5.6]). First we define $a' : N \times N \to C$ by

$$a'(n, m) = \sum_{d \mid (m, n)} a(n, d)\, \mu_a(d),$$

and then we set

$$c_a(r, s) = \sum_{1 \leq k \leq s} a'(s, k)\, e(rks^{-1}),$$

where $r \geq 0$, $s \geq 1$, and $e(t) = \exp(2\pi i t)$. It is a straightforward exercise to verify that in the Dirichlet case c_a is c, the Ramanujan function, and in the unitary case c_a is the c^* of Cohen [2]. More generally it can be shown that our c_a is multiplicative, i.e. whenever $(s, t) = 1$, we have

$$c_a(r, st) = c_a(r, s)\, c_a(r, t).$$

REFERENCES

1. E.D. Cashwell and C.J. Everett, The ring of number theoretic functions. Pacific J. Math., 9(1959) 975-985.

2. E. Cohen, Arithmetical functions associated with the unitary divisors of an integer, Math. Zeit., 74 (1960), 66-80.

3. A.A. Gioia, The K-product of arithmetic functions. Canadian Journal of Math., XVII (1965) 970-976.

4. G.H. Hardy and E.M. Wright, An introduction to the theory of numbers, (Oxford, 3rd edition, 1954).

5. W.J. Le Veque, Topics in number theory I. (Reading, Addison-Wesley, 1956).

6. W. Narkiewicz, On a class of arithmetical convolutions, Colloq. Math., 10 (1963), 81-94.

7. R.A. Rankin, On the representation of a number as the sum of any number of squares, and in particular of twenty, Acta. Arith., 7(1962) 399-407.

8. M.V. Subba Rao and A.A. Gioia, Generalized Dirichlet products of arithmetic functions (abstract), Amer. Math. Soc. Notices 10 (1963) No. 7, p. 661.

9. R. Vaidyanathaswamy, The theory of multiplicative arithmetical functions, Trans. Amer. Math. Soc., 33 (1931) 579-662.

10. A. Wintner, Eratosthenian averages, (Privately printed, Baltimore, 1943).

University of Waterloo

https://doi.org/10.4153/CMB-1966-037-x Published online by Cambridge University Press