VINOGRADOV'S INVERSION THEOREM FOR GENERALIZED ARITHMETICAL FUNCTIONS

Pentti Haukkanen
University of Tampere, SF-33101 Tampere, Finland
(Submitted September 1988)

1. Introduction

In this paper we introduce the Vinogradov [8] inversion theorem for functions defined on a finite partially ordered set. Our inversion theorem reduces to that by Vinogradov in the case of positive integers. For material relating to Vinogradov's inversion theorem, we refer to [2], [3], and [4].

As an example of our generalized Vinogradov inversion theorem we consider an inversion theorem relating to arithmetical functions and regular convolutions. As applications, we give expressions for certain restricted sums of Fibonacci and Lucas numbers. Special cases of the applications can be found in [4].

2. A Generalized Vinogradov Inversion Theorem

Let $(P, \subseteq)$ be a locally finite partially ordered set. A complex-valued function f on $P \times P$ is said to be an incidence function of $(P, \subseteq)$ if $f(x, y) = 0$ unless $x \subseteq y$. We denote by $I(\subseteq, P)$ the set of all incidence functions of $(P, \subseteq)$. The convolution of $f, g \in I(\subseteq, P)$ is defined by

$$(f \circ g)(x, y) = \sum_{x \subseteq z \subseteq y} f(x, z)g(z, y).$$

The inverse of $f \in I(\subseteq, P)$ is defined by

$$f \circ f^{-1} = f^{-1} \circ f = \delta,$$

where $\delta(x, x) = 1$ and $\delta(x, y) = 0$ if $x \neq y$. The inverse of ζ, defined by $\zeta(x, y) = 1$ whenever $x \subseteq y$, is denoted by μ and is called the Möbius function of $(P, \subseteq)$.

Now we are able to give our generalized Vinogradov inversion theorem. The original Vinogradov inversion theorem is reproduced in the remark of Theorem 2 in Section 3.

Theorem 1: Suppose $(P, \subseteq)$ and $(P, \leq)$ are locally finite partially ordered sets. Let f_x be a complex-valued function of $x \in P$ and let d_x be a function of $x \in P$ into P. Then, for all $a, b \in P$,

$$\sum_{\substack{a \leq x \leq b \\ d_x = a}} f_x = \sum_{a \subseteq z} \mu(a, z) \sum_{\substack{a \leq x \leq b \\ z \subseteq d_x}} f_x,$$

where μ is the Möbius function of $(P, \subseteq)$.

Proof: We have

$$\sum_{\substack{a \leq x \leq b \\ d_x = a}} f_x = \sum_{a \leq x \leq b} f_x \delta(a, d_x) = \sum_{a \leq x \leq b} f_x \sum_{a \subseteq z \subseteq d_x} \mu(a, z) = \sum_{a \subseteq z} \mu(a, z) \sum_{\substack{a \leq x \leq b \\ z \subseteq d_x}} f_x,$$

which was required.

Remark: We note that Theorem 1 implies the classical inversion theorem for incidence functions of $(P, \subseteq)$ stating that if, for all $a, b \in P$,

$$g(a, b) = \sum_{a \subseteq z \subseteq b} f(z, b),$$

then

$$f(a, b) = \sum_{a \subseteq z \subseteq b} \mu(a, z) g(z, b);$$

that is

$$f(a, b) = \sum_{a \subseteq z \subseteq b} \mu(a, z) \sum_{z \subseteq y \subseteq b} f(y, b). \tag{1}$$

In fact, let $a, b \in P$ with $a \subseteq b$. We assume $x \subseteq y \Rightarrow x \le y$ for all $x, y \in P$ and denote

$$\{x \in P: a \subseteq x \subseteq b\} = \{x_1(=a), x_2, \ldots, x_m(=b)\},$$

$$\{x \in P: a \le x \le b\} = \{y_1(=a), y_2, \ldots, y_n(=b)\}, \; m \le n.$$

Then we take

$$d_{y_1} = a, \; d_{y_2} = x_2, \; \ldots, \; d_{y_m} = b, \; d_{y_{m+1}} = \cdots = d_{y_n} = c,$$

where $c \not\subseteq b$, and $f_x = f(d_x, b)$. (If there does not exist an element $c \in P$ such that $c \not\subseteq b$, then we consider the set $P \cup \{c\}$.) In this case,

$$\sum_{\substack{a \le x \le b \\ d_x = a}} f_x = \sum_{\substack{a \le x \le b \\ d_x = a}} f(d_x, b) = f(a, b)$$

and

$$\sum_{a \subseteq z} \mu(a, z) \sum_{\substack{a \le x \le b \\ z \subseteq d_x}} f_x = \sum_{a \subseteq z} \mu(a, z) \sum_{\substack{a \le x \le b \\ z \subseteq d_x}} f(d_x, b) = \sum_{a \subseteq z} \mu(a, z) \sum_{z \subseteq y \subseteq b} f(y, b).$$

Thus, by Theorem 1, we arrive at (1).

3. Regular Arithmetical Convolutions

Let A be a mapping from the set $\mathbb{N}$ of positive integers to the set of subsets of $\mathbb{N}$ such that, for each $n \in \mathbb{N}$, $A(n)$ is a subset of the set of positive divisors of n. Then the A-convolution of two arithmetical functions f and g is defined by

$$(f \circ_A g)(n) = \sum_{d \in A(n)} f(d) g(n/d).$$

Narkiewicz [6] defined an A-convolution to be regular if:

(a) the set of arithmetical functions forms a commutative ring with unity with respect to the ordinary addition and the A-convolution;
(b) the A-convolution of multiplicative functions is multiplicative;
(c) the function E, defined by $E(n) = 1$ for all $n \in \mathbb{N}$, has an inverse μ_A with respect to the A-convolution, and $\mu_A(n) = 0$ or -1 whenever n is a prime power.

The inverse of an arithmetical function f such that $f(1) \ne 0$ with respect to the A-convolution is defined by

$$f \circ_A f^{-1} = f^{-1} \circ_A f = E_0,$$

where $E_0(1) = 1$ and $E_0(n) = 0$ for $n > 1$.

It can be proved (see [6]) that an A-convolution is regular if and only if

(i) $A(mn) = \{de : d \in A(m), e \in A(n)\}$ whenever $(m, n) = 1$,
(ii) for each prime power $p^a > 1$ there exists a divisor $t = t_A(p^a)$ of a such that

$$A(p^a) = \{1, p^t, p^{2t}, \ldots, p^{rt}\},$$

where $rt = a$, and

$$A(p^{it}) = \{1, p^t, p^{2t}, \ldots, p^{it}\}, \; 0 \le i < r.$$

For example, the Dirichlet convolution D, where $D(n)$ is the set of all positive divisors of n, and the unitary convolution U, where

$$U(n) = \{d > 0 : d \mid n,\ (d,\ n/d) = 1\},$$

are regular (see [1]). In this paper we confine ourselves to regular convolutions.

A positive integer n is said to be A-primitive if $A(n) = \{1,\ n\}$. The generalized Möbius function μ_A is the multiplicative function given by (see [6])

$$\mu_A(p^a) = \begin{cases} -1 & \text{if } p^a\ (>1) \text{ is } A\text{-primitive,} \\ 0 & \text{if } p^a \text{ is non-}A\text{-primitive.} \end{cases}$$

For a positive integer k, we define

$$A_k(n) = \{d > 0 : d^k \in A(n^k)\}.$$

It is known [7] that the A_k-convolution is regular whenever the A-convolution is regular. The symbol $(a, b)_{A,k}$ denotes the greatest k^{th} power divisor of a which belongs to $A(b)$. In particular, denote $(a, b)_{A,1} = (a, b)_A$. Then

$$(a,\ b)_D = (a,\ b),$$

the greatest common divisor of a and b.

Let A be a regular arithmetical convolution. Then we define the relation $\subseteq$ on the set $\mathbb{N}$ of positive integers by

$$m \subseteq n \Leftrightarrow m \in A(n)$$

and denote by $\mathbb{N}_A$ the resulting locally finite partially ordered set.

Let f be an arithmetical function, that is, a complex-valued function on $\mathbb{N}$. Then we can associate with f an incidence function f' of $\mathbb{N}_A$ defined by

$$f'(m,\ n) = \begin{cases} f(n/m) & \text{if } m \in A(n), \\ 0 & \text{if } m \notin A(n). \end{cases}$$

The mapping $f \to f'$ is one-one and

(2) $$(f' \circ g')(m,\ n) = (f \circ_A g)'(m,\ n)$$

(see [5], Ch. 7). Plainly

$$(E_0)'(m,\ n) = \delta(m,\ n),\ E'(m,\ n) = \zeta(m,\ n).$$

Therefore, by (2),

$$(\mu_A)'(m,\ n) = \mu(m,\ n).$$

Now we are in a position to state Theorem 1 for regular convolutions. Letting $\le$ be the natural ordering on $\mathbb{N}$, we can write

Theorem 2: Let f_i be a complex-valued function of $i \in \mathbb{N}$ and let d_i be a function of $i \in \mathbb{N}$ into $\mathbb{N}$. Then, for all $n \in \mathbb{N}$,

$$\sum_{\substack{i=1 \\ d_i = 1}}^{n} f_i = \sum_{d \ge 1} \mu_A(d) \sum_{\substack{i=1 \\ d \in A(d_i)}}^{n} f_i.$$

Remark: If $A = D$ in Theorem 2, we obtain the original Vinogradov inversion theorem.

Corollary: Let f_i be a complex-valued function of $i \in \mathbb{N}$. Then

$$\sum_{\substack{i=1 \\ (i,\, n^k)_{A,k} = 1}}^{n} f_i = \sum_{d \in A_k(n)} \mu_{A_k}(d) \sum_{\substack{i=1 \\ d^k \mid i}}^{n} f_i.$$

Proof: Replace A by A_k and take $d_i = ((i,\ n^k)_{A,k})^{1/k}$ in Theorem 2. Since $d \in A_k(((i,\ n^k)_{A,k})^{1/k})$ if and only if $d \in A_k(n)$, $d^k \mid i$, we obtain the Corollary.

4. Applications to Fibonacci and Lucas Numbers

Let F_i be the i^{th} Fibonacci number, that is, $F_1 = 1$, $F_2 = 1$, $F_n = F_{n-1} + F_{n-2}$ $(n \geq 3)$, and let L_i be the i^{th} Lucas number, that is, $L_1 = 1$, $L_2 = 3$, $L_n = L_{n-1} + L_{n-2}$ $(n \geq 3)$.

Theorem 3: Let A be a regular convolution and $k \in \mathbb{N}$. Then, for each $n \in \mathbb{N}$,

$$(3) \qquad \sum_{\substack{i=1 \\ (i,n^k)_{A,k}=1}}^{n} F_i = \sum_{d \in A_k(n)} \mu_{A_k}(d) \frac{F_{md^k+d^k} - (-1)^{d^k} F_{md^k} - F_{d^k}}{L_{d^k} - (-1)^{d^k} - 1},$$

$$(4) \qquad \sum_{\substack{i=1 \\ (i,n^k)_{A,k}=1}}^{n} L_i = \sum_{d \in A_k(n)} \mu_{A_k}(d) \frac{L_{md^k+d^k} - (-1)^{d^k} L_{md^k} - L_{d^k} + 2(-1)^{d^k}}{L_{d^k} - (-1)^{d^k} - 1},$$

where $m = [n/d^k]$, the greatest integer in n/d^k.

Proof: Plainly,

$$\sum_{\substack{i=1 \\ d^k|i}}^{n} F_i = \sum_{1 \leq i \leq n/d^k} F_{id^k}.$$

Then, using the formulas

$$F_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n), \quad L_n = \alpha^n + \beta^n,$$

where

$$\alpha = \frac{1}{2}(1 + \sqrt{5}), \quad \beta = \frac{1}{2}(1 - \sqrt{5}),$$

we obtain, after some computations,

$$\sum_{\substack{i=1 \\ d^k|i}}^{n} F_i = \frac{F_{md^k+d^k} - (-1)^{d^k} F_{md^k} - F_{d^k}}{L_{d^k} - (-1)^{d^k} - 1}.$$

Thus, applying the Corollary of Theorem 2, we get (3). The proof of (4) goes through in a manner similar to that of (3).

Corollary: Let A be a regular convolution. Then, for each $n \in \mathbb{N}$,

$$\sum_{\substack{i=1 \\ (i,n)_A=1}}^{n} F_i = \sum_{d \in A(n)} \mu_A(d) \frac{F_{n+d} - (-1)^d F_n - F_d}{L_d - (-1)^d - 1},$$

$$\sum_{\substack{i=1 \\ (i,n)_A=1}}^{n} L_i = \sum_{d \in A(n)} \mu_A(d) \frac{L_{n+d} - (-1)^d L_n - L_d + 2(-1)^d}{L_d - (-1)^d - 1}.$$

Theorem 4: Let A be a regular convolution and $k \in \mathbb{N}$. Then, for each $n \in \mathbb{N}$,

$$(5) \qquad \sum_{\substack{i=1 \\ (i,n^k)_{A,k}>1}}^{n} F_i = F_{n+2} - \sum_{d \in A_k(n)} \mu_{A_k}(d) \frac{F_{md^k+d^k} - (-1)^{d^k} F_{md^k} - F_{d^k}}{L_{d^k} - (-1)^{d^k} - 1} - 1,$$

$$(6) \qquad \sum_{\substack{i=1 \\ (i,n^k)_{A,k}>1}}^{n} L_i = L_{n+2} - \sum_{d \in A_k(n)} \mu_{A_k}(d) \frac{L_{md^k+d^k} - (-1)^{d^k} L_{md^k} - L_{d^k} + 2(-1)^{d^k}}{L_{d^k} - (-1)^{d^k} - 1} - 3,$$

where $m = [n/d^k]$.

Proof: We have

$$\sum_{\substack{i=1 \\ (i,n^k)_{A,k} > 1}}^{n} F_i = \sum_{i=1}^{n} F_i - \sum_{\substack{i=1 \\ (i,n^k)_{A,k} = 1}}^{n} F_i .$$

Therefore, applying (3) and the identity

$$\sum_{i=1}^{n} F_i = F_{n+2} - 1,$$

we obtain (5). Similarly, applying (4) and the identity

$$\sum_{i=1}^{n} L_i = L_{n+2} - 3,$$

we get (6).

References

1. E. Cohen. "Arithmetical Functions Associated with the Unitary Divisors of an Integer." *Math. Z.* *74* (1960):66-80.
2. R. T. Hansen. "Applications of the General Möbius Inversion Formula." *New Zealand Math. Mag.* *3* (1976):136-42.
3. R. T. Hansen. "Arithmetic Inversion Formulas." *J. Natur. Sci. Math.* *20* (1980):141-50.
4. R. T. Hansen & L. G. Swanson. "Vinogradov's Möbius Inversion Theorem." *Nieuw Arch. Wiskd.* *28* (1980):1-11.
5. P. J. McCarthy. *Introduction to Arithmetical Functions*. New York: Springer-Verlag, 1986.
6. W. Narkiewicz. "On a Class of Arithmetical Convolutions." *Colloq. Math.* *10* (1963):81-94.
7. V. Sita Ramaiah. "Arithmetical Sums in Regular Convolutions." *J. Reine Angew. Math.* *303/304* (1978):265-83.
8. I. M. Vinogradov. *Elements of Number Theory*. New York: Dover, 1954.

*****