ON AN ARITHMETIC FUNCTION HAVING AN APPLICATION IN CODING THEORY

K_{n,q}(z)=

1965

SovietRxiv

Abstract

Full Text

CYBERNETICS AND CONTROL THEORY

R. R. VARSHAMOV

ON AN ARITHMETIC FUNCTION HAVING AN APPLICATION IN CODING THEORY

(Presented by Academician V. S. Kulebakin, 13 VII 1964)

Of great importance in coding theory and cybernetics is the study of the arithmetic function $K_{n,q}(z)$, defined by the equality

$$K_{n,q}(z) = \sum_{\substack{a_1+2a_2+\ldots+na_n \equiv z \pmod{n+1} \\ 0 \leqslant a_i \text{ integer } \leqslant q}} 1,$$

the nature of which has been poorly studied. Thus, for example, a connection has been established between the function $K_{n,q}(z)$ and the power of certain special, most effective, asymmetric error-correcting codes (^{2}).

In addition, of special interest (in connection with technical applications) is an a priori indication of at least one zero of the numerical function

$$V_{n,q}(z) = K_{n,q}(z) - \max_{\xi}\{K_{n,q}(\xi)\},$$

whose behavior is very irregular.

Denoting the variable quantity by x and expanding the product

$$P^n_{m,q}(x) = \prod_{k=m}^{n} (1 + x^k + \ldots + x^{kq})$$

as a sum in powers of x, we obtain

$$P^n_{m,q}(x) = \sum_{i=N(n,m)}^{N(n,m)} S^n_{m,q}(i) x^i.$$

The coefficients of x^i, in view of

$$P^n_{m,q}(x) = (1 + x^m + \ldots + x^{mq}) P^n_{m+1,q}(x)$$

(taking $P^m_{m+1,q}(x) = 1$), satisfy the recurrence equation

$$S^n_{m,q}(i) = \sum_{j=0}^{q} S^n_{m+1,q}(i - mj).$$

Hence, in particular, for any integer $\delta > 0$ we find

$$S^n_{1,q}(i) = \sum_{j=0}^{\frac{1}{2}q(\delta^2-\delta)} b_{\delta,q}(j) S^n_{\delta,q}(i - j).$$

The quantities $b_{\delta,q}(t)$*, connected by the relation

$$b_{\delta+1,q}(t) = \sum_{i=0}^{q} b_{\delta,q}(t - \delta i), \qquad \text{taking } b_{1,q}(k) = 0 \quad (k \neq 0), \tag{1}$$

possess a number of interesting properties and are closely connected with the classical additive functions $\lambda(n)$, $\bar{\mu}(n)$, etc. (^{1})**.

* Here and below it is assumed that the integer $t \geqslant 0$.

** Thus, for example, for any integer θ $(-\infty < \theta < n/2)$ the equality holds

$$b_{n-\theta,2}(n) = \lambda(n) - \sum_{i=0}^{\theta} \lambda(i).$$

An analogous formula can also be obtained for the function $\mu(n)$, etc.

Let

$$M_{\delta,q,h}(t) = \sum_{i=-\infty}^{\infty} b_{\delta,q}(t + ih).$$

Then:

Lemma 1. For any positive integers $\rho, H, \tau \mid q+1$ and

$$h(\delta, \rho, H, \tau) = (q+1)^{[\log_{q+1}(\delta-\rho)H\tau] - \log_{q+1} H}$$

the identity

$$M_{\delta,q,h}(t) \equiv (q+1)^{\delta-1-\log_{q+1} h(\delta,\rho,H,\tau)} \tag{2}$$

holds.

Proof. By the definition and by virtue of (1), we have

$$M_{\delta'+\rho,q,\tau\delta'}(t)=\sum_{i=-\infty}^{\infty}\sum_{v_1=0}^{q}\cdots\sum_{v_\rho=0}^{q} b_{\delta',q}\left(t+\tau\delta' i-\sum_{j=1}^{\rho}(\delta'+\rho-j)v_j\right),$$

whence, since $\rho>0$ and $\tau \mid q+1$, we obtain

$$M_{\delta'+\rho,q,\tau\delta'}(t)=\sum_{i=-\infty}^{\infty}\sum_{v_1=0}^{q}\cdots\sum_{v_{\rho-1}=0}^{q}\sum_{u=0}^{(q+1)\tau^{-1}-1}\sum_{v=0}^{\tau-1} b_{\delta',q}\left(t+\delta'(\tau i-v)-u\tau\delta'-\sum_{j=1}^{\rho-1}(\delta'+\rho-j)v_j\right),$$

$$M_{\delta'+\rho,q,\tau\delta'}(t)=\sum_{v_1=0}^{q}\cdots\sum_{v_{\rho-1}=0}^{q}\sum_{u=0}^{(q+1)\tau^{-1}-1} M_{\delta',q,\delta'}\left(t-\sum_{j=1}^{\rho-1}(\rho-j)v_j\right). \qquad (3)$$

It is clear, by virtue of (1), that $M_{1,q,1}(t)\equiv 1$, and this together with (3) convinces us of the validity of (2). The lemma is proved.

Let σ,ρ be nonnegative integers, and let $a_0,a_1,\dots,a_{n-1}$ be real numbers. Denote by $J^n_{\sigma,\rho,t}(a)$ the sum

$$J^n_{\sigma,\rho,t}(a)=\sum_{i=0}^{n-1}\sum_{j=0}^{\sigma} a_i\left(a_{\varepsilon^n(i-\rho j)}-a_{\varepsilon^n(i-\rho j+t)}\right),$$

where $\varepsilon^n(z)$ is the least positive residue of z modulo n.

Lemma 2. Whatever the numbers $a_0,a_1,\dots,a_{2\rho-1}$,

$$J^{2\rho}_{\sigma,\rho,t}(a)\geq 0. \qquad (4)$$

Proof. Setting $\sigma'=[(\sigma+2)/2]$ and $\sigma''=[(\sigma+1)/2]$, write

$$J^{2\rho}_{\sigma,\rho,t}(a)=\sigma'\sum_{i=0}^{2\rho-1} a_i\left(a_i-a_{\varepsilon^{2\rho}(i+t)}\right)+\sigma''\sum_{i=0}^{2\rho-1} a_i\left(a_{\varepsilon^{2\rho}(i-\rho)}-a_{\varepsilon^{2\rho}(i-\rho+t)}\right).$$

Hence, denoting $A_i=a_{\varepsilon^{2\rho}(i)}+a_{\varepsilon^{2\rho}(i+\rho)}$ and taking into account that $A_i=A_{i+\rho}$, we obtain

$$J^{2\rho}_{\sigma,\rho,t}(a)=\sigma''\sum_{i=0}^{\rho-1} A_i(A_i-A_{i+t})+(\sigma'-\sigma'')\sum_{i=0}^{2\rho-1} a_i\left(a_i-a_{\varepsilon^{2\rho}(i+t)}\right),$$

or, equivalently,

$$J^{2\rho}_{\sigma,\rho,t}(a) = \sigma'' J^{\rho}_{0,0,t}(A) + (\sigma' - \sigma'') J^{2\rho}_{0,0,t}(a). \tag{5}$$

We shall show that for any numerical sequence $\xi_0, \xi_1, \dots, \xi_{c-1}$,

$$J_{c,t}(\xi) = J^{c}_{0,0,t}(\xi) \geq 0.$$

Indeed, let $d = (c, t)$ and

$$\Delta_{i,j} = \xi_{\varepsilon^c(i+jt)} - \xi_{\varepsilon^c(i+(j-1)t)} \quad (i = 0, 1, \dots, d-1;\ j = 1, 2, \dots, cd^{-1}).$$

Then the expression $J_{c,t}(\xi)$ can be written in the form

$$J_{c,t}(\xi) = -\sum_{i=0}^{d-1} \sum_{j=1}^{cd^{-1}} \xi_{\varepsilon^c(i+(j-1)t)} \Delta_{i,j},$$

but, since

$$\zeta_{\varepsilon^c(i+(j-1)t)} = \zeta_i + \sum_{v=1}^{j-1} \Delta_{i,v}, \qquad \Delta_{i,cd^{-1}} = -\sum_{v=1}^{cd^{-1}-1} \Delta_{i,v},$$

we have

$$\begin{aligned} J_{c,t}(\zeta) &= -\sum_{i=0}^{d-1} \left(\sum_{j=1}^{cd^{-1}-1} \left(\zeta_i + \sum_{v=0}^{j-1} \Delta_{i,v} \right) \Delta_{i,j} + \left(\zeta_i + \sum_{v=1}^{cd^{-1}-1} \Delta_{i,v} \right) \Delta_{i,cd^{-1}} \right) \\ &= \sum_{i=0}^{d-1} \left(- \sum_{j_1<j_2<cd^{-1}} \Delta_{i,j_1} \Delta_{i,j_2} + \left(\sum_{v=1}^{cd^{-1}-1} \Delta_{i,v} \right)^2 \right) \\ &= \sum_{i=0}^{d-1} \left(\sum_{j_1<j_2<cd^{-1}} \Delta_{i,j_1} \Delta_{i,j_2} + \sum_{v=1}^{cd^{-1}-1} \Delta^2_{i,v} \right), \end{aligned}$$

i.e.

$$2J_{c,t}(\zeta) = \sum_{i=0}^{d-1} \left(\left(\sum_{v=1}^{cd^{-1}-1} \Delta_{i,v} \right)^2 + \sum_{v=1}^{cd^{-1}-1} \Delta^2_{i,v} \right),$$

$$J_{c,t}(\zeta) \geqslant 0. \tag{6}$$

From (5) and (6), in view of $\sigma'' \geqslant 0$, $\sigma' - \sigma'' \geqslant 0$, (4) follows. The lemma is proved.

Consider the expression

$$\sum_{i=\overline{N}(n,m)}^{N(n,m)} S_{m,q}^{n}(i) x^{\varepsilon^{n+1}(i)} = \sum_{i=0}^{n} \overline{S}_{m,q}^{n}(i) x^{i}. \tag{7}$$

It is easy to observe that the coefficients of the unknown x^i on the right-hand side of equality (7) are the numbers of distinct solutions of the congruence

$$\sum_{v=m}^{n} v\alpha_v \equiv i \pmod{n+1},$$

where $0 \leqslant \alpha_v$ are integers, $\leqslant q$ (so that $\overline{S}_{1,q}^{n}(t) = K_{n,q}(t)$), and they satisfy the recurrence equation

$$\overline{S}_{m,q}^{n}(i) = \sum_{j=0}^{q} \overline{S}_{m+1,q}^{n}(\varepsilon^{n+1}(i - mj)). \tag{8}$$

From (8), analogously to the preceding, for any integer $\delta > 0$, taking $\overline{S}_{\delta,q}^{n}(\varepsilon^{n+1}(t)) = \overline{S}_{\delta,q}^{n}(t)$ and $a_{\delta,q}(\varepsilon^{n+1}(t)) = a_{\delta,q}(t)$, it is not difficult to obtain the formula

$$\overline{S}_{1,q}^{n}(t) = \sum_{i=0}^{m} a_{\delta,q}(i) \overline{S}_{\delta,q}^{n}(t - i), \tag{9}$$

as well as the recurrence relation

$$a_{\delta+1,q}(t) = \sum_{i=0}^{q} a_{\delta,q}(t - i\delta)* \tag{10}$$

Theorem 1. Let the integer $n = (q+1)^{|t| - \log_{q+1} H} - 1$ $(H > 0)$; then

$$K_{n,q}(t) \equiv (q+1)^{n - \log_{q+1}(n+1)}.$$

Proof. One may show that $a_{n+1,q}(t) = M_{n+1,q,n+1}(t)$ and, moreover, in view of (9), $a_{n+1,q}(t) = \overline{S}_{1,q}^{n}(t)$. Meanwhile, $\overline{S}_{1,q}^{n}(t) = K_{n,q}(t)$; therefore $K_{n,q}(t) = M_{n+1,q,n+1}(t)$, and, by virtue of Lemma 1 ($\delta = h(\delta, \rho, H, \tau) = n + 1$),

$$K_{n,q}(t) \equiv (q+1)^{n - \log_{q+1}(n+1)}.$$

The theorem is proved.

* The formulas given make it possible to obtain a comparatively convenient method of recurrent computation of the values of the function $K_{n,q}(t)$.

Corollary. The function $V_{n,q}(t)$ is identically equal to zero if and only if $n = h(n+1, \rho, H, \tau) - 1$.

Theorem 2. For any integer ξ—a root of the congruence $z \equiv 0 \pmod{n+1}$—the equality

$$V_{n,q}(\xi) = 0$$

holds.

Proof. From (8), (9), and (10) one can obtain the formula

$$a_{n+1,q}(t) = \sum_{i=0}^{n} a_{\delta,q}(i)\, a_{n+2-\delta,q}(t+i)$$

or, putting $\delta = [(n+2)/2] > 0$,

$$a_{n+1,q}(t) = \sum_{i=0}^{n} a_{(n+2)/2,q}(i)\, a_{[(n+3)/2],q}(t+i). \tag{11}$$

If $n = 2(p-1)$, then $[(n+2)/2] = [(n+3)/2] = p$,

$$a_{n+1,q}(t) = \sum_{i=0}^{n} a_{p,q}(i)\, a_{p,q}(t-i),$$

and, by virtue of (6) ($a_{p,q}(i) = \xi_i$),

$$a_{n+1,q}(0) - a_{n+1,q}(t) = J^{*}_{n+1,t}(a_{p,q}(\cdot)) \geq 0. \tag{12}$$

If $n = 2p-1$, then $[(n+2)/2] = p$, $[(n+3)/2] = p+1$, and, by virtue of (10), (11), as well as (4),

$$a_{n+1,q}(t) = \sum_{i=0}^{2p-1} \sum_{j=0}^{q} a_{p,q}(i)\, a_{p,q}(t+i-pj),$$

$$a_{n+1,q}(0) - a_{n+1,q}(t) = J^{2p}_{q,p,t}(a_{p,q}(\cdot)) \geq 0. \tag{13}$$

Inequalities (12) and (13) make it possible to write the relation

$$a_{n+1,q}(0) - a_{n+1,q}(t) \geq 0,$$

valid for any $n > 0$. Hence, in view of $a_{n+1,q}(t) = K_{n,q}(t)$, and also the periodicity of the numerical function $a_{n+1,q}(t)$, we find

$$V_{n,q}(\xi) = 0.$$

The theorem is proved.

Corollary. For any pair of positive integers n and q,

$$K_{n,q}(0) \geq (q+1)^{\,n-\log_{q+1}(n+1)}.$$

Institute of Automation and Telemechanics
(Technical Cybernetics)

Received
10 VII 1964

REFERENCES

1. B. A. Venkov, *Elementary Number Theory*, Moscow-Leningrad, 1937.
2. G. G. Varshamov, G. M. Tenengolts, *Automation and Telemechanics*, **26**, No. 2 (1965).

Note: Figure translations are in progress. See original paper for figures.

Source: Math-Net.Ru and CyberLeninka. Machine translation. Verify with the original.