MATH. SCAND. 43 (1978), 11–25

NONCOVERING OF MULTIPLES

TORLEIV KLØVE

1.

In this paper we consider a combinatorial problem which arose in coding theory. Let $q>1$ be an integer. We define a partial ordering on the non-negative integers by m covers n if and only if each coefficient in the q-ary expansion of m is greater than or equal to the corresponding coefficient in the q-ary expansion of n. Our problem is to find how many of the integers less than q^m do not cover any multiple of b where b is some fixed integer dividing q^m-1. The number of such integers is the number of information symbols in some codes of length q^m-1 over GF (q), where q is a prime power. The codes are in a class of codes defined by Lin and Yiu [3]. We do not make use of this fact, however, and so we will treat the problem as a purely combinatorial problem.

2.

We will use the following notations:

The elements of an m-dimensional vector $\boldsymbol{u}$ will be denoted $u_0, u_1, \ldots, u_{m-1}$,

$$\boldsymbol{u} \leqq \boldsymbol{v} \text{ if and only if } u_i \leqq v_i \quad \text{for } i=0,1,\ldots,m-1 ,$$

$$|\boldsymbol{u}| = \sum_{i=0}^{m-1} u_i, \qquad \|\boldsymbol{u}\| = \sum_{i=0}^{m-1} u_i q^i .$$

The columns of an $n \times m$ matrix $\boldsymbol{E}$ will be denoted by $\boldsymbol{e}^0, \boldsymbol{e}^1, \ldots, \boldsymbol{e}^{m-1}$, the rows by $\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n$, and the elements by e_{ij}.

Let b be a positive integer which is prime to q and let $s=\operatorname{ord}_b(q)$, that is, s is the least positive integer such that $q^s \equiv 1 \pmod b$. Let

$$M = \{0,1,\ldots,q-1\} ,$$

$$\mathscr{L}(\lambda) = \{\boldsymbol{l} \in M^{\lambda s} \mid \text{ if } \boldsymbol{0}<\boldsymbol{u}\leqq \boldsymbol{l}, \text{ then } \|\boldsymbol{u}\| \not\equiv 0 \pmod b\} ,$$

$$P(\lambda) = \#\mathscr{L}(\lambda), \text{ that is number of elements in } \mathscr{L}(\lambda) .$$

Then $P(\lambda)$ is the number of integers $<q^{\lambda s}$ which do not cover any multiple of b.

Further let

Received August 18, 1977.

$$\mathscr{F} = \{\boldsymbol{f} \in \mathbf{N}^s \mid \text{ if } \mathbf{0}<\boldsymbol{g} \leqq \boldsymbol{f}, \text{ then } \|\boldsymbol{g}\| \not\equiv 0 \pmod b\}$$

$$\mathscr{E} = \left\{\boldsymbol{E} \in \mathbf{N}^{(q-1)\times s} \;\middle|\; \sum_{i=1}^{q-1} i\boldsymbol{e}_i \in \mathscr{F}\right\},$$

$$\Lambda_{\boldsymbol{E}}(\lambda) = \{\boldsymbol{l} \in M^{\lambda s} \mid \#\{\mu \mid l_\mu = i \;\&\; \mu \equiv j \pmod s\} = e_{ij}\},$$

$$\Lambda(\lambda) = \bigcup_{\boldsymbol{E}\in\mathscr{E}} \Lambda_{\boldsymbol{E}}(\lambda).$$

The multinomial coefficients are denoted by

$$\binom{c}{c_1, c_2, \ldots, c_m} = \frac{c!}{c_1!\,c_2!\ldots c_m!\,(c-\sum_{i=1}^m c_i)!} \quad \text{if } m>0,\ c_i \geqq 0 \text{ for all } i, \text{ and } \textstyle\sum c_i \leqq c,$$

$$= 1 \quad \text{if } m=0.$$

Note that

$$\binom{c}{c_1, c_2, \ldots, c_m} = \binom{\sum c_i}{c_1, c_2, \ldots, c_{m-1}}\binom{c}{\sum c_i}.$$

LEMMA 1. *We have* $\Lambda(\lambda) \subseteq \mathscr{L}(\lambda)$.

PROOF. Let $\boldsymbol{l} \in \Lambda(\lambda)$. Then $\boldsymbol{l} \in \Lambda_{\boldsymbol{E}}(\lambda)$ for some $\boldsymbol{E} \in \mathscr{E}$. Let $\mathbf{0}<\boldsymbol{u}\leqq\boldsymbol{l}$. Then

$$\|\boldsymbol{u}\| = \sum_{\sigma=0}^{\lambda-1}\sum_{\mu=0}^{s-1} q^{\sigma s+\mu} u_{\sigma s+\mu}$$
$$\equiv \sum_{\mu=0}^{s-1} q^\mu \sum_{\sigma=0}^{\lambda-1} u_{\sigma s+\mu} \pmod b.$$

Hence

$$\|\boldsymbol{u}\| \equiv \left\|\left(\sum_{\sigma=0}^{\lambda-1} u_{\sigma s}, \sum_{\sigma=0}^{\lambda-1} u_{\sigma s+1}, \ldots, \sum_{\sigma=0}^{\lambda-1} u_{\sigma s+s-1}\right)\right\| \pmod b.$$

Further

$$\sum_{\sigma=0}^{\lambda-1} u_{\sigma s+\mu} \leqq \sum_{\sigma=0}^{\lambda-1} l_{\sigma s+\mu} = \sum_{i=0}^{q-1} i e_{i\mu}.$$

By the definition of $\mathscr{E}$ it follows that $\|\boldsymbol{u}\| \not\equiv 0 \pmod b$. Therefore $\boldsymbol{l} \in \mathscr{L}(\lambda)$.

LEMMA 2. *We have* $\mathscr{L}(\lambda) \subseteq \Lambda(\lambda)$.

PROOF. Let $\boldsymbol{l} \in \mathscr{L}(\lambda)$ and let

$$e_{ij} = \#\{\mu \mid l_\mu = i \;\&\; \mu \equiv j \pmod s\}.$$

Let $\boldsymbol{E}=(e_{ij})$. Then $\boldsymbol{l} \in \Lambda_{\boldsymbol{E}}(\lambda)$. We will show that $\boldsymbol{E} \in \mathscr{E}$. Let $\boldsymbol{0}<\boldsymbol{g} \leqq \sum_{i=1}^{q-1} i\boldsymbol{e}_i$. Then

$$g_\mu \leqq \sum_{i=1}^{q-1} ie_{i\mu} = \sum_{\sigma=0}^{\lambda-1} l_{\sigma s+\mu}\,.$$

For $\mu=0,1,\ldots,s-1$, let

$$\begin{aligned} k_\mu &= \max\left\{k \,\middle|\, g_\mu > \sum_{\sigma=0}^{k-1} l_{\sigma s+\mu}\right\} && \text{if } g_\mu>0\,. \\ &= -1 && \text{if } g_\mu=0\,. \end{aligned}$$

Then $-1 \leqq k_\mu \leqq \lambda-1$. Let

$$\begin{aligned} u_{\sigma s+\mu} &= l_{\sigma s+\mu} && \text{for } \sigma<k_\mu\,, \\ u_{k_\mu s+\mu} &= g_\mu - \sum_{\sigma=0}^{k_\mu-1} l_{\sigma s+\mu}\,, \\ u_{\sigma s+\mu} &= 0 && \text{for } \sigma>k_\mu\,. \end{aligned}$$

By the definition of k_μ, $0 \leqq u_{k_\mu s+\mu} \leqq l_{k_\mu s+\mu}$. Hence $\boldsymbol{0}<\boldsymbol{u}\leqq\boldsymbol{l}$ and so $\|\boldsymbol{u}\| \not\equiv 0 \pmod b$. Further

$$\|\boldsymbol{g}\| = \sum_{\mu=0}^{s-1} g_\mu q^\mu = \sum_{\mu=0}^{s-1}\sum_{\sigma=1}^{q-1} u_{\sigma s+\mu} q^\mu \equiv \|\boldsymbol{u}\| \not\equiv 0 \pmod b\,.$$

Therefore $\sum_{i=1}^{q-1} i\boldsymbol{e}_i \in \mathscr{F}$ and so $\boldsymbol{E} \in \mathscr{E}$.

LEMMA 3. *If* $\boldsymbol{E} \neq \boldsymbol{E}'$, *then* $\Lambda_{\boldsymbol{E}}(\lambda) \cap \Lambda_{\boldsymbol{E}'}(\lambda) = \varnothing$.

PROOF. Obvious.

LEMMA 4. *We have*

$$\#\Lambda_{\boldsymbol{E}}(\lambda) = \prod_{j=0}^{s-1} \binom{|\boldsymbol{e}^j|}{e_{1j}, e_{2j}, \ldots, e_{q-2,j}} \binom{\lambda}{|\boldsymbol{e}^j|}\,.$$

PROOF. For a given j there are

$$\binom{\lambda}{e_{1j}, e_{2j}, \ldots, e_{q-1,j}} = \binom{|\boldsymbol{e}^j|}{e_{1j}, e_{2j}, \ldots, e_{q-2,j}} \binom{\lambda}{|\boldsymbol{e}^j|}$$

ways to choose the elements $l_j, l_{s+j}, \ldots, l_{j+(\lambda-1)s}$ such that e_{ij} elements are equal to i for $i=1,2,\ldots,q-1$. Further, the choices for different j's are independent.

We can now prove our main theorem.

THEOREM 1. *We have*

$$P(\lambda) = \sum_{E\in\mathscr{E}} \prod_{j=0}^{s-1} \binom{|e^j|}{e_{1j}, e_{2j}, \ldots, e_{q-2,j}} \binom{\lambda}{|e^j|}$$

PROOF. By lemmata 1, 2 and 3

$$P(\lambda) = \#\mathscr{L}(\lambda) = \#\Lambda(\lambda) = \sum_{E\in\mathscr{E}} \#\Lambda_E(\lambda)$$

and so the theorem follows by lemma 4.

LEMMA 5 (Gould [2, identity no. 6. 44]).

$$\binom{\lambda}{m}\binom{\lambda}{n} = \sum_{j=0}^{\min(m,n)} \binom{n+m-j}{m-j, n-j}\binom{\lambda}{n+m-j}.$$

Using lemma 5 s times on each term in the sum in theorem 1 we get the next theorem.

THEOREM 2. *There exist non-negative integers* $A_i = A_i(q, b)$ *such that*

$$P(\lambda) = \sum_{i\geqq 0} A_i\binom{\lambda}{i}.$$

We could, by theorem 1 and lemma 5, get explicit expressions for the A_i's. In general they will be very complicated however. In the remaining part of this

Table 1. $A_i(2, b)$

$i \backslash b$	3	5	7	9	11	13	15
1	2	8	6	26	150	336	14
2	2	20	24	144	1660	5160	146
3		16	48	324	5480	22176	896
4		4	45	414	8130	42504	3244
5			18	336	6810	46152	7464
6			3	168	3990	35616	11816
7				48	1760	22356	13696
8				6	530	10692	12012
9					100	3720	8008
10					10	912	4004
11						144	1456
12						12	364
13							56
14							4

paper we will give simpler expressions for the A_i's in special cases. In particular, we have computed all $A_i(2,b)$ for $b=3,5,\ldots,35$. The values for $b \leqq 15$ are given in table 1. Since $A_0(2,b)=1$ for all b this is omitted in the table. In the next section we prove that $A_i(2,b)=0$ for $i \geqq b$, these values are also omitted in the table.

3.

In this section we take a closer look at $\mathscr{F}$ to get more information about the $A_i(q,b)$'s.

DEFINITION. If $\boldsymbol{E}$ is an $n \times m$ matrix, then

$$\sigma \boldsymbol{E} = (\boldsymbol{e}^{m-1}, \boldsymbol{e}^0, \boldsymbol{e}^1, \ldots, \boldsymbol{e}^{m-2}) .$$

LEMMA 6. (i) *If* $\boldsymbol{u} \in N^s$, *then* $\|\sigma \boldsymbol{u}\| = q\|\boldsymbol{u}\| - u_{s-1}(q^s-1)$,
(ii) *if* $\boldsymbol{f} \in \mathscr{F}$, *then* $\sigma \boldsymbol{f} \in \mathscr{F}$,
(iii) *if* $\boldsymbol{E} \in \mathscr{E}$, *then* $\sigma \boldsymbol{E} \in \mathscr{E}$,
(iv) $\sharp \Lambda_{\sigma \boldsymbol{E}}(\lambda) = \sharp \Lambda_{\boldsymbol{E}}(\lambda)$.

PROOF. (i) We have

$$\|\sigma \boldsymbol{u}\| = u_{s-1} + \sum_{i=0}^{s-2} u_i q^{i+1} = u_{s-1} - u_{s-1} q^s + q \sum_{i=0}^{s-1} u_i q^i$$
$$= -u_{s-1}(q^s-1) + q\|\boldsymbol{u}\| .$$

(ii) If $\boldsymbol{u}' \leqq \sigma \boldsymbol{f}$, then $\boldsymbol{u} = \sigma^{-1}\boldsymbol{u}' \leqq \boldsymbol{f}$. Hence $\|\boldsymbol{u}\| \not\equiv 0 \pmod b$. Further by (i),

$$\|\boldsymbol{u}'\| = \|\sigma \boldsymbol{u}\| \equiv q\|\boldsymbol{u}\| \not\equiv 0 \pmod b$$

since $\gcd(q,b)=1$.
(iii) If $\boldsymbol{E} \in \mathscr{E}$, then $\sum_{i=1}^{q-1} i\boldsymbol{e}_i \in \mathscr{F}$. Hence

$$\sum_{i=1}^{q-1} i\sigma \boldsymbol{e}_i = \sigma \sum_{i=1}^{q-1} i\boldsymbol{e}_i \in \mathscr{F}$$

by (ii) and so $\sigma \boldsymbol{E} \in \mathscr{E}$.
(iv) This follows immediately from Lemma 4.

LEMMA 7 (Bovey, Erdös, and Niven [1]). *Let* $b>0$ *and* $k \geqq 0$ *be integers with* $b-2k \geqq 1$. *Given any* $n-k$ *integers* $a_1, a_2, \ldots, a_{n-k}$ *there is a non-empty subset of subscripts* I *such that* $\sum_{i \in I} a_i \equiv 0 \pmod b$ *if at most* $n-2k$ *of the integers lie in the same residue class modulo* b.

Putting $k=0$ in lemma 7, we see that any sequence of b (or more) integers has a subsequence with sum congruent to zero modulo b. Hence se get the following corollary.

COROLLARY. (i) *If* $f \in \mathscr{F}$, *then* $|f| \leqq b-1$,
(ii) $A_i(q,b)=0$ *for* $i \geqq b$.

By lemma 6 iv, to find $\#\Lambda_E(\lambda)$ it is enough to find $\#\Lambda_{\sigma^j E}(\lambda)$ for some j. We may for instance choose j such that if $\sigma^j E = (e'_{ij})$ then $\sum_i ie'_{i0} \geqq \sum_i ie'_{ik}$ for all k. This motivates the next definition.

DEFINITION.

$$\mathscr{F}_r = \{f \in \mathscr{F} \mid f_0 \geqq f_i \text{ for } i=1,2,\ldots,s-1 \ \& \ |f|=r\} .$$

DEFINITION. To each $f \in \mathscr{F}_r$ we associate the sequence $a_1, a_2, \ldots, a_r$ with f_0 1's followed by f_1 q_1's, f_2 q_2's etc. where $q_i \equiv q^i \pmod b$ and $0 \leqq q_i < b$. Then any subsequence has a sum $\not\equiv 0 \pmod b$.

LEMMA 8. *If* $k \leqq (b+1)/3$ *and* $f \in \mathscr{F}_{b-k}$, *then*

(i) $f_0 \geqq b-2k+1 \geqq (b+1)/3$,
(ii) $f_0 > \frac{1}{2}(b-k)$.

PROOF. (i) By Lemma 7, if $f_0 \leqq b-2k$ then $f \notin \mathscr{F}$. Hence $f_0 \geqq b-2k+1 \geqq (b+1)/3$ when $k \leqq (b+1)/3$.
(ii) By (i),

$$2f_0-(b-k) \geqq 2b-4k+2-b+k = b+1-3k+1 \geqq 1 .$$

LEMMA 9. *If* $k \leqq (b+1)/3$ *and* $f \in \mathscr{F}_{b-k}$, *then* $\sum_{i=0}^{s-1} f_i q_i < b$.

PROOF. Let $a_1, a_2, \ldots, a_{b-k}$ be the sequence associated with f, and let A be the set of integers that appears in the sequence. Let $S=S_v$ denote the sum of some arbitrary subsequence with v elements, all >1.

The proof of the lemma is done in several steps.

(I) *If* $S \leqq \lambda b$, *then* $S \leqq \lambda b - f_0 - 1 \leqq (\lambda-1)b+2k-2$.

Suppose $S \geqq \lambda b - f_0$. Let $a_{i_1}, a_{i_2}, \ldots, a_{i_v}$ be the subsequence with sum S. Since $\lambda b - S \leqq f_0$,

$$a_1, a_2, \ldots, a_{\lambda b - S}, a_{i_1}, a_{i_2}, \ldots, a_{i_v}$$

is a subsequence also and it's sum is

$$(\lambda b - S)\cdot 1 + S = \lambda b \equiv 0 \pmod{b}.$$

This is a contradiction. Hence

$$S \leqq \lambda b - f_0 - 1 \leqq (\lambda - 1)b + 2k - 2$$

by lemma 8i.

(II) *If $a \in A$, then $a \leqq b - f_0 - 1$.*

Since $a < b$ this follows from (I).

(III) *If $S = S' + a$ where a is a summand of S, $a \leqq f_0 + 1$, and $S' \leqq \lambda b$, then $S \leqq \lambda b - f_0 - 1$.*

By (I), $S' \leqq \lambda b - f_0 - 1$ and so $S \leqq \lambda b - f_0 - 1 + f_0 + 1 = \lambda b$. Again by (I), $S \leqq \lambda b - f_0 - 1$.

(IV) $S_{2\lambda+1} \leqq \lambda b + b - f_0 - 1$.

We prove this by induction on λ. By (II) it is true for $\lambda = 0$. Suppose it is true for $\lambda - 1$. Then

$$\begin{aligned} S_{2\lambda+1} &= S_{2\lambda-1} + a + a' \leqq \lambda b - f_0 - 1 + 2(b - f_0 - 1) \\ &= \lambda b + b + b - 3f_0 - 1 \leqq \lambda b + b - 2 \end{aligned}$$

by the induction hypothesis, (I), and lemma 8i. By (I), $S_{2\lambda+1} \leqq \lambda b + b - f_0 - 1$.

(V) *The sequence $a_1, a_2, \ldots, a_{b-k}$ has at most one element in $[f_0, b/2]$.*

Suppose a, a' are two elements from the sequence which both are in $[f_0, b/2]$. Then $S_2 = a + a' \in [2f_0, b]$. By (I) $2f_0 \leqq S_2 \leqq b - f_0 - 1$ and so $3f_0 \leqq b - 1$. This is a contradiction to lemma 8i.

(VI) *If $a \in A$, then $a \leqq b/2$.*

First we notice that if $a > b/2$, then $a \geqq (b+1)/2$. Let

$$\begin{aligned} \alpha &= \text{number of elements of } (a_i) \text{ in } [(b+1)/2, b), \\ \beta &= \text{number of elements of } (a_i) \text{ in } [f_0, b/2], \\ \gamma &= [(\alpha - 1)/2] \text{ (the integer value)}, \\ \delta &= \alpha - 1 - 2\gamma. \end{aligned}$$

Suppose $\alpha > 0$. Let $a_{i_1}, a_{i_2}, \ldots, a_{i_{2\gamma+1}}$ be the $2\gamma + 1$ largest elements of (a_i) and let

$$U = \sum_{j=1}^{2\gamma+1} \{a_{i_j} - (b+1)/2\}, \quad V = \sum_{a_i \in [2, f_0 - 1]} a_i, \quad W = \sum_{j=1}^{2\gamma+1} a_{i_j},$$

$$T = \sum_{a_i=1} 1+V+W = f_0+V+W.$$

First we show that $U+1 \geqq \beta+\delta$. By (IV), $\beta \leqq 1$, and by definition $\delta \leqq 1$. Suppose $U+1<\beta+\delta$. Then $\beta=\delta=1$ and $U<1$. We will show that this gives a contradiction. Since $\beta=1$, there exists an $a \in A \cap [f_0, b/2]$. We consider the cases b even and b odd separately. First b even. Then $U<1$ implies $U=1/2$, $a_{i_1} = b/2+1$, and $\gamma=0$. If $a<b/2$, then $a \leqq b/2-1$ and $b/2-1-a \leqq b/2-1-f_0<f_0$. Hence

$$S = (b/2-1-a)\cdot 1+a+a_{i_1} = b \equiv 0 \pmod{b},$$

a contradiction. If $a=b/2$, then the elements of $A \cap [f_0, b)$ are $a=b/2$ and $c = b/2+1$; a appear once in A and c twice since $\delta=1$. Since $a+2c<2b$, $a+2c+V \leqq 2b-f_0-1$ by (III) and induction. Therefore

$$V \leqq 2b-a-2c-f_0-1 = b/2-f_0-3 .$$

Since $\alpha=2$ and $\beta=1$,

$$V \geqq 2(b-k-f_0-\alpha-\beta) = 2(b-k-f_0-3) .$$

Combining we get $b/2-f_0-3 \geqq 2b-2k-2f_0-6$ and so

$$f_0 \geqq 3b/2-2k-3 \geqq 3b/2-2(b+1)/3-3 = (b/2-2)+(b-5)/3 .$$

Therefore, if $b \geqq 5$, then $f_0 \geqq b/2-2$ and so

$$S = (b/2-2)\cdot 1+a+2c = 2b \equiv 0 \pmod{b}$$

a contradiction. For $b=2$ and $b=4$ it is obvious that $\alpha=0$, and in particular $\delta=0$ and we have a contradiction. The case b odd is similar to the first subcase since $a \leqq (b-1)/2<b/2$. We omit the details.

By (IV), $W \leqq \gamma b+b-f_0-1$. Hence by (III) and induction we get $V+W \leqq \gamma b+b-f_0-1$, and so $T \leqq \gamma b+b-1$. On the other hand,

$$\begin{aligned} T &\geqq \sum_{a_i \in [1, f_0-1]} 1+U+(2\gamma+1)(b+1)/2 \\ &= (b-k-2\gamma-1-\delta-\beta)+U+\gamma b+\gamma+(b+1)/2 \\ &\geqq \gamma b+b-1+(b+1)/2-\gamma-k-1 . \end{aligned}$$

Combining the two inequalities involving T we get

$$\gamma \geqq (b+1)/2-k-1 .$$

Further

$$(2\gamma+1)(b+1)/2 \leqq W \leqq \gamma b+b-f_0-1 \leqq \gamma b+2k-2$$

and so

$$\gamma \leqq 2k-2-(b+1)/2 .$$

Combining the two inequalities involving γ we get $3k \geqq b+2$ contradicting our assumption that $k \leqq (b+1)/3$. Hence $\alpha = 0$ and the proof of (VI) is complete.

(VII) $S_{b-k-f_0} \leqq b - f_0 - 1$.

By (VI) there are no elements $> b/2$ and at most one element $\geqq f_0$ in the sequence (a_i). Let S_v be the sum of the v largest elements in (a_i). Then $S_1 \leqq b/2$ and by (III) and induction $S_v \leqq b - f_0 - 1$ for $v = 1, 2, \ldots, b-k-f_0$. Note that S_{b-k-f_0} is the sum of all the elements > 1.

Hence

$$\sum_{i=1}^{b-k} a_i = f_0 \cdot 1 + S_{b-k-f_0} \leqq b-1$$

by (VII) and the proof of lemma 9 is complete.

THEOREM 3. *Let $k \leqq (b+1)/3$. Then $\mathscr{F}_{b-k}$ can be characterized as follows: Let $q_i \equiv q^i \pmod b$, $0 < q_i < b$. Then $(f_0, f_1, \ldots, f_{s-1}) \in \mathscr{F}_{b-k}$ if and only if $\sum_{i=1}^{s-1} f_i(q_i - 1) < k$ and $\sum_{i=0}^{s-1} f_i = b-k$.*

PROOF. By lemma 9, if $(f_0, f_1, \ldots, f_{s-1}) \in \mathscr{F}_{b-k}$, then

$$\sum_{i=0}^{s-1} f_i = b-k \quad \text{and} \quad \sum_{i=0}^{s-1} f_i q_i < b\,.$$

Hence

$$k > \sum_{i=0}^{s-1} f_i(q_i - 1) = \sum_{i=1}^{s-1} f_i(q_i - 1)$$

since $q_0 = 1$. On the other hand, if $\sum_{i=1}^{s-1} f_i(q_i-1) < k$ and $\sum_{i=0}^{s-1} f_i = b-k$ then $\sum_{i=0}^{s-1} f_i q_i < b$. If $\mathbf{0} < \boldsymbol{u} \leqq \boldsymbol{f}$, then $0 < \sum u_i q_i \leqq \sum f_i q_i < b$ and so

$$\|\boldsymbol{u}\| \equiv \sum u_i q_i \not\equiv 0 \pmod b\,.$$

Hence $\boldsymbol{f} \in \mathscr{F}$. Further

$$k-1 \geqq \sum_{i=1}^{s-1} f_i(q_i - 1) \geqq \sum_{i=1}^{s-1} f_i = b-k-f_0$$

and so $f_0 \geqq b - 2k + 1 > (b-k)/2$. Therefore $f_0 > f_i$ for $i = 1, 2, \ldots, s-1$ and $\boldsymbol{f} \in \mathscr{F}_{b-k}$.

Theorem 3 gives a very simple method to find the elements of $\mathscr{F}_{b-k}$. To illustrate this we give the leading coefficients of $P(\lambda)$ for $q=2$. We notice that if $q=2$, then $\mathscr{E} = \mathscr{F}$.

THEOREM 4. *If* $b \geqq 3$, *then* $A_{b-1}(2,b)=s$.
If $b \geqq 5$, *then* $A_{b-2}(2,b)=s(b-1)$.
If $b \geqq 7$, *then*

$$A_{b-3}(2,b) = s\left\{\binom{b-1}{2}+b-3\right\} \quad \textit{if } 2^i \equiv 3 \pmod b \textit{ is solvable },$$
$$= s\binom{b-1}{2} \quad \textit{otherwise }.$$

If $b \geqq 9$, *then*

$$A_{b-4}(2,b) = s\left\{\binom{b-1}{3}+2\binom{b-4}{2}+2(b-4)\right\} \quad \textit{if } 2^i \equiv 3 \pmod b \textit{ is solvable },$$
$$= s\binom{b-1}{3} \quad \textit{otherwise }.$$

PROOF. From the proof of theorem 2 it follows that only those f for which $|f| \geqq b-k$ will contribute to $A_{b-k}(2,q)$.

If $k \leqq (b+1)/3$, then $f_0 > f_i$ for $i=1,2,\ldots,s-1$ by lemma 8 (ii). Hence $f, \sigma f, \ldots, \sigma^{s-1} f$ are all distinct and by lemma 6(iv) give the same contribution to

Table 2.

k	β_1	β_2	β_3	β_4	γ_1	γ_2	γ_3	γ_4
1	$b-1$	0	0	0	1	0	0	0
2	$b-2$	0	0	0	0	1	0	0
	$b-3$	1	0	0	0	$b-2$	$b-3$	0
3	$b-3$	0	0	0	0	0	1	0
	$b-4$	1	0	0	0	0	$b-3$	$b-4$
	$b-5$	2	0	0	0	0	$\binom{b-3}{2}$	$(b-4)(b-5)$
	$b-4$	0	1	0	0	0	$b-3$	$b-4$
4	$b-4$	0	0	0	0	0	0	1
	$b-5$	1	0	0	0	0	0	$b-4$
	$b-6$	2	0	0	0	0	0	$\binom{b-4}{2}$
	$b-5$	0	1	0	0	0	0	$b-4$
	$b-7$	3	0	0	0	0	0	$\binom{b-4}{3}$
	$b-6$	1	1	0	0	0	0	$(b-4)(b-5)$
	$b-5$	0	0	1	0	0	0	$b-4$

A_{b-k}. Hence to find A_{b-k} for $k \leqq (b+1)/3$ it is enough to find the contribution from $f \in \mathscr{F}_{b-k}$ and multiply by s. Further the elements of $\mathscr{F}_{b-k}$ are found by theorem 3. In table 2 we give the possible elements of $\mathscr{F}_{b-k}$ for $k \leqq 4$ and we list their contributions to A_{b-k}. In the table, β_i is the number of i's in the sequence associated with f and γ_j is the contribution to A_{b-j}.

Adding up the contributions we get theorem 4 for $b \leqq 3k-1$. The remaining cases, $k=3$ and $b=7$, $k=4$ and $b=9$ are true by table 1.

By the same method we can get expressions for $A_i(2,b)$ for $i=b-5$, $b-6$, etc. By a similar method we can also find $A_i(q,b)$ for $q>2$. We notice that if $q \equiv q'$ $(\mathrm{mod}\, b)$ and $q>b$, $q'>b$ then $A_i(q,b)=A_i(q',b)$. We will use this fact in section 5 to find explicit formulae for $P(\lambda)$ when $q \equiv \pm 1 \pmod b$.

4.

In lemma 6 iv we proved that $\# \Lambda_{\sigma E}(\lambda) = \# \Lambda_E(\lambda)$. Therefore there are several equal terms in the sum in theorem 1 and we may bring them together. Formally, let

$$\boldsymbol{E} \text{ eqv } \boldsymbol{E}' \text{ if and only if } \boldsymbol{E} = \sigma^i \boldsymbol{E}' \text{ for some } i\,.$$

Then eqv is an equivalence relation. Let $\bar{\mathscr{E}}$ denote the set of equivalence classes and $\langle \bar{\boldsymbol{E}} \rangle$ the number of elements in the class $\bar{\boldsymbol{E}}$. Then we can restate theorem 1 as follows.

THEOREM 5. *We have*

$$P(\lambda) = \sum_{\bar{\boldsymbol{E}} \in \bar{\mathscr{E}}} \langle \bar{\boldsymbol{E}} \rangle \prod_{j=0}^{s-1} \binom{|e^j|}{e_{1j}, e_{2j}, \ldots, e_{q-2,j}} \binom{\lambda}{|e^j|}\,.$$

The advantage of theorem 5 over theorem 1 is that in some cases we may be able to give a characterization of one member in an equivalence class which is simpler than the definition of $\mathscr{E}$. For instance in theorem 3 we showed that if $q=2$ and $|\boldsymbol{f}| \geqq b-(b+1)/3$ then the equivalence class of $\boldsymbol{f}$ contains a member $\boldsymbol{f}'$ such that $\sum_{i=0}^{s-1} f_i q_i < b$. In the remainder of this section we consider the case $q=2$ and $b=2^s-1$. The reason is twofold. The case is interesting from a coding theory point of view and we can show that each equivalence class contains a member $\boldsymbol{f}$ such that $\|\boldsymbol{f}\| < b$.

DEFINITION. For $i=0,1,\ldots,s-2$ let ϱ_i be defined by

$$\begin{aligned}\varrho_i(f_0, f_1, \ldots, f_i, f_{i+1}, \ldots, f_{s-1}) \\ &= (f_0, f_1, \ldots, f_i - 2d_i, f_{i+1} + d_i, \ldots, f_n)\end{aligned}$$

where $d_i = [(f_i - 1)/2]$.

Then ϱ_i will leave 1 (if f_i is odd) or 2 (if f_i is even) at position i and carry the exceeding to position $i+1$ where half of it is added.

LEMMA 10. *For* $i=0,1,\ldots,s-1$ *we have*

(i) $\|\varrho_i \boldsymbol{f}\| = \|\boldsymbol{f}\|$ *for all* $\boldsymbol{f}$,
(ii) *if* $\boldsymbol{f} \in \mathscr{F}$, *then* $\varrho_i \boldsymbol{f} \in \mathscr{F}$.

PROOF. (i) We have

$$\|\varrho_i \boldsymbol{f}\| = \sum_{j=0}^{s-1} f_j 2^j - 2d_i \cdot 2^i + d_i \cdot 2^{i+1} = \|\boldsymbol{f}\| .$$

(ii) Suppose $\boldsymbol{u} \leqq \varrho_i \boldsymbol{f}$. Let $\boldsymbol{u}'$ be defined by

$$\begin{aligned} u_j' &= u_j && \text{if } j \neq i,\ i+1 , \\ u_i' &= u_i + 2d_i && \text{if } u_{i+1} \geqq d_i , \\ &= u_i + 2u_{i+1} && \text{if } u_{i+1} < d_i , \\ u_{i+1}' &= u_{i+1} - d_i && \text{if } u_{i+1} \geqq d_i , \\ &= 0 && \text{if } u_{i+1} < d_i . \end{aligned}$$

Then $\boldsymbol{u}' \leqq \boldsymbol{f}$ and so $\|\boldsymbol{u}'\| \not\equiv 0 \pmod b$. Further $\|\boldsymbol{u}\| = \|\boldsymbol{u}'\|$. Hence $\|\boldsymbol{u}\| \not\equiv 0 \pmod b$. Therefore $\varrho_i \boldsymbol{f} \in \mathscr{F}$.

DEFINITION. Let $\boldsymbol{f} \in N^s$, $f_{s-1}=0$, and let $j_1, j_2, \ldots, j_r = s-1$ be the subscripts of the elements of $\boldsymbol{f}$ which are zero, i.e., $f_j=0$ for $j=j_1, j_2, \ldots, j_r$, $f_j \neq 0$ otherwise. Let

$$\nu[\boldsymbol{f} \mid i] = \varrho_{j_i-1} \circ \varrho_{j_i-2} \circ \cdots \circ \varrho_{j_{i-1}+1}$$

for $i=1,2,\ldots,r$, where $j_0+1=0$,

$$\nu[\boldsymbol{f}] = \nu[\boldsymbol{f} \mid 1] \circ \nu[\boldsymbol{f} \mid 2] \circ \ldots \circ \nu[\boldsymbol{f} \mid r] .$$

LEMMA 11. *If* $f_j=0$, *then* $\nu[\sigma^{s-1-j}\boldsymbol{f}] \circ \sigma^{s-1-j}\boldsymbol{f} = \sigma^{s-1-j} \circ \nu[\boldsymbol{f}]\boldsymbol{f}$.

PROOF. First we note that the last element of $\sigma^{s-1-j}\boldsymbol{f}$ is $f_j=0$ so that $\nu[\sigma^{s-1-j}\boldsymbol{f}]$ is defined. Let $\boldsymbol{f} = (\boldsymbol{F}_1, \boldsymbol{F}_2, \ldots, \boldsymbol{F}_r)$ where $\boldsymbol{F}_1, \boldsymbol{F}_2, \ldots, \boldsymbol{F}_r$ are blocks of elements, the last element in each block being 0, that is, $\boldsymbol{F}_i = (f_{j_{i-1}}, \ldots, f_{j_i})$. If $j=j_i$ then

$$\nu[\boldsymbol{f}]\boldsymbol{f} = (\boldsymbol{F}_1', \boldsymbol{F}_2', \ldots, \boldsymbol{F}_r')$$

and

$$\sigma^{s-1-j}(\nu[\boldsymbol{f}]\boldsymbol{f}) = (\boldsymbol{F}_{i+1}', \ldots, \boldsymbol{F}_r', \boldsymbol{F}_1', \ldots, \boldsymbol{F}_i') .$$

On the other hand

$$\sigma^{s-1-j}f = (F_{i+j},\ldots,F_r,F_1,\ldots,F_i)$$

and so

$$\nu[\sigma^{s-1-j}f]\circ\sigma^{s-1-j}f = (F'_{i+1},\ldots,F'_r,F'_1,\ldots,F'_1)\,.$$

LEMMA 12. *If* $\|f\| \leqq \|\sigma f\|$ *and* $\|f\| < b$, *then* $f_{s-1} = 0$.

PROOF. By lemma 6i

$$\|f\| \leqq \|\sigma f\| = 2\|f\| - f_{s-1}(2^s - 1) = \|f\| + \|f\| - f_{s-1}b\,.$$

Hence $f_{s-1} \leqq \|f\|/b < 1$ and so $f_{s-1} = 0$.

THEOREM 6. *Let* $q=2$ *and* $b=2^{s-1}$. *If* $f \in \mathscr{F}$, *then* $\|\sigma^i f\| < b$ *for some* i.

PROOF. The proof is by induction on $r = \#\{j \mid f_j = 0\}$. Since $\|(1,1,\ldots,1)\| = b$, $r \geqq 1$ for all $f \in \mathscr{F}$. Therefore, the basis $r=0$ for the induction is empty. Let $r \geqq 1$ and suppose that the theorem is true for all lower values. We may assume that $f_{s-1} = 0$ since otherwise we could use σ repeatedly until the last element is 0. Let $f_j = 0$ for $j = j_1, j_2, \ldots, j_r = s-1$. From lemma 10i it follows that $\|\nu[f]f\| = \|f\|$. From the definition of $\nu[f]$ it follows that the elements of $\nu[f]f$ are 1 or 2 except possibly those with subscripts $j_1, j_2, \ldots, j_r$.

CASE 1. $\nu[f]f$ has r elements which are 0. These are then the elements with subscripts $j_1, j_2, \ldots, j_r = s-1$. Hence

$$\|\nu[f]f\| \leqq 2(1+2+2^2+\ldots+2^{s-2}) = b-1$$

and so $\|f\| < b$ in this case.

CASE 2. $\nu[f]f$ has less than r elements which are 0. By the induction hypothesis $\|\sigma^{i_0}(\nu[f]f)\| < b$ for some i_0 and by lemma 12 we may assume that the last element of $\sigma^{i_0}(\nu[f]f)$ is 0. Then $i_0 = s-1-j_i$ for some i, $1 \leqq i \leqq r$. By lemmata 10i and 11 we get

$$\|\sigma^{i_0}f\| = \|\nu[\sigma^{i_0}f](\sigma^{i_0}f)\| = \|\sigma^{i_0}(\nu[f])f\| < b$$

and the proof of theorem 6 is complete.

Combining theorems 5 and 6 it is simple to find $P(\lambda)$ for $q=2$ and $b=2^s-1$.

5.

In this section we give explicit expressions for $P(\lambda)$ in the cases when $q \equiv \pm 1 \pmod b$, $q > b$.

THEOREM 7. *If* $q\equiv 1 \pmod b$, *then* $P(\lambda)=\binom{\lambda+b-1}{b-1}$.

PROOF. Since $q\equiv 1 \pmod b$ we have $\|\boldsymbol{l}\|\equiv|\boldsymbol{l}| \pmod b$. Hence $\boldsymbol{l}\in\mathscr{L}(\lambda)$ if and only if $|\boldsymbol{l}|\leqq b-1$. The number of vectors $\boldsymbol{l}\in\mathscr{L}(\lambda)$ such that $|\boldsymbol{l}|=i$ for $0\leqq i\leqq b-1$ is equal to the number of ways i objects can be placed into λ boxes, i.e. $\binom{\lambda+i-1}{\lambda-1}$. Hence

$$P(\lambda) = \sum_{i=0}^{b-1}\binom{\lambda+i-1}{\lambda-1} = \binom{\lambda+b-1}{\lambda} = \binom{\lambda+b-1}{b-1}.$$

THEOREM 8. *If* $q\equiv -1 \pmod b$ *and* $q>b$, *then*

$$P(\lambda)=2\binom{\lambda+b-1}{b-1}-1\,.$$

PROOF. We have $s=2$ and

$$\|\boldsymbol{l}\| \equiv \sum_{i=0}^{\lambda-1} l_{2i}-\sum_{i=0}^{\lambda-1} l_{2i+1} \pmod b\,.$$

If $\boldsymbol{l}$ has two non-zero elements with subscripts j_1, j_2 of opposite parity and $u_{j_1}=u_{j_2}=1$, $u_i=0$ otherwise, then $\boldsymbol{u}\leqq\boldsymbol{l}$ and $\|\boldsymbol{u}\|\equiv 0 \pmod b$. Hence $\boldsymbol{l}\notin\mathscr{L}(\lambda)$. Therefore

$$\begin{aligned}\mathscr{L}(\lambda) &= \{(l_0,0,l_2,0,\ldots,l_{2\lambda-2},0)\mid 0\leqq\textstyle\sum l_i\leqq b-1\}\\ &\cup\ \{(0,l_1,0,l_3,\ldots,0,l_{2\lambda-1})\mid 0<\textstyle\sum l_i\leqq b-1\}\,.\end{aligned}$$

Comparing with the proof of theorem 7 we see that

$$P(\lambda) = 1+2\sum_{i=1}^{b-1}\binom{\lambda+i-1}{\lambda-1} = 2\binom{\lambda+b-1}{b-1}-1\,.$$

By [2] identity 3.20 we can rewrite theorem 7 as follows:

$$P(\lambda) = \sum_{m=0}^{b-1}\binom{b-1}{m}\binom{\lambda}{m}.$$

By theorem 1

$$P(\lambda) = \sum_{\sum ie_i<b}\binom{|\boldsymbol{e}|}{e_1,e_2,\ldots,e_{q-1}}\binom{\lambda}{|\boldsymbol{e}|}.$$

Comparing the coefficients of $\binom{\lambda}{m}$ we get the following identity:

COROLLARY. *If* $q\equiv 1 \pmod b$ *and* $m\leqq b-1$, *then*

$$\sum \binom{m}{e_1, e_2, \ldots, e_{q-2}} = \binom{b-1}{m}$$

where the summation is over those $(q-1)$*-tuples* $(e_1, e_2, \ldots, e_{q-1})$ *of non-negative integers for which* $\sum_{i=1}^{q-1} e_i = m$ *and* $\sum_{i=1}^{q-1} ie_i \leqq b-1$.

Finally I thank Shu Lin who put my attention to the main problem considered in this paper.

REFERENCES

1. J. D. Bovey, P. Erdös, and I. Niven, *Conditions for a zero sum modulo n*, Canad. Math. Bull. 18 (1975), 27–29.
2. H. W. Gould, *Cobinatorial Identities*, Morgantown, W. Va., 1972.
3. Shu Lin and Kai-Ping Yiu, *An improvement to multifold Euclidean geometry codes*, Information and Control 28 (1975), 221–265.

MATEMATISK INSTITUTT
ALLÉGATEN 53–55
N-5014 BERGEN — UNIVERSITETET
NORWAY