can check that $|\mathcal{H}_N| = |\mathcal{H}''|$ by checking that it is true for each prime power $p^e$. We leave this computation to the reader. Then $\mathcal{H}_N$ is multiplicatively independent, and $\mathcal{H}''$ has the same multiplicative span as $\mathcal{H}_N$, so $\mathcal{H}''$ must also be multiplicatively independent.

Thus $\mathcal{H}''$ is a multiplicative basis for $\mathcal{G}$ and Theorem E is proven.

References


Received on 13.4.1988
and in revised form on 18.10.1988

An upper bound for the $h$-range of the postage stamp problem

by

Öystein J. Rødseth (Bergen)

Dedicated to Professor Ernst S. Selmer on the occasion of his 70th birthday

1. Introduction. For a positive integer $h$, the $h$-range $n(h, A_k)$ of an integer sequence

$$(1) \quad A_k: \ a_0 = 0 < a_1 < a_2 < \ldots < a_k$$

is the largest $n$ for which each of the integers $0, 1, \ldots, n$ can be written as a sum of $h$ elements of $A_k$, repetitions being allowed. The extremal $h$-range $n(h, k)$ is given by

$$n(h, k) = \max_{A_k} n(h, A_k).$$

The problem of calculating $n(h, k)$ is by some authors referred to as the `postage stamp problem’, due to a rather obvious combinatorial interpretation. In this note we consider $n(h, k)$ for $k \geq 1$ fixed and $h$ large.

By a simple combinatorial argument, Rohrbach [11] showed that

$$n(h, k) \leq \binom{n+h+k}{k},$$

so in particular

$$n(h, k) \leq \frac{k^{h-1}}{(k-1)!} \left( \frac{h}{k} \right)^n + O(h^{k-1}).$$

On the other hand we have $n(h, k) \geq \left( \frac{h}{k} \right)^n$ (Stöhr [13]).

For $k \leq 3$ we have

$$n(h, k) = c_k \left( \frac{h}{k} \right)^n + O(h^{k-1}),$$

where $c_1 = 1$ (trivial), $c_2 = 1$ (Stöhr [13]), $c_3 = 4/3$ (Hofmeister [4], Klotz [6]).

For $k \geq 4$, however, it is not even known if such a constant $c_k$ exists. Guy [13].
C12) suggests that for \( h \) large enough, \( n(h, k) \) is given by a finite set of polynomials in \( h \). If this is true, these polynomials must be of degree \( k \) in \( h \).

For \( k \geq 4 \), the only improvement of the bound (2) seems to be that of Klotz [6], who showed that

\[
n(h, k) \leq c \frac{k^{k-1}}{(k-1)!} \left( \frac{h^k}{k} \right) \quad \text{for } k \geq 2 \text{ and } h \text{ large},
\]

where \( c \) depends on \( k \) (but not on \( h \)) and lies in the interval \( 1 - 2^{-k} < c < 1 \).

(Thus \( c \to 1 \) as \( k \to \infty \)). The object of this note is to show that

\[
n(h, k) \leq \frac{(k-1)^{k-1}}{(k-1)!} \left( \frac{h^k}{k} \right) + O(h^{k-1}),
\]

(3)

thus improving (2) by a factor which tends to \( 1/e \) as \( k \to \infty \).

2. The Frobenius number. The Frobenius number \( g_{k+1} = g(b_0, b_1, \ldots, b_k) \) of \( k+1 \geq 2 \) relatively prime positive integers \( b_i \) is the largest non-zero integer which cannot be written as a sum of numbers \( b_0 \), repetitions being allowed. Put \( a_0 = 1 \), and

\[
a_k = \inf \left( \frac{g_{k+1} + b_0 + b_1 + \ldots + b_k}{b_0 b_1 \ldots b_k} \right) \quad \text{for } k \geq 1,
\]

the infimum being taken over all sequences \( b_0, b_1, \ldots, b_k \) of \( k+1 \) relatively prime positive integers. We now show that

\[
a_k \geq k!.
\]

(5)

Given \( k+1 \) relatively prime positive integers \( b_0, b_1, \ldots, b_k \), let \( L_r \) be the smallest integer \( \equiv r \pmod{b_0} \) with an integral representation

\[
L_r = b_1 x_1 + b_2 x_2 + \ldots + b_k x_k, \quad x_i \geq 1.
\]

Clearly, we then have (Brauer and Shockley [2])

\[
\max L_r = g_{k+1} + b_0 + b_1 + \ldots + b_k,
\]

the maximum being taken over a complete set of residues \( r \pmod{b_0} \).

For a positive real number \( x \), let \( M(x) \) denote the number of vectors \( (x_1, x_2, \ldots, x_k) \) with positive integer coordinates satisfying

\[
b_1 x_1 + b_2 x_2 + \ldots + b_k x_k \leq x.
\]

(6)

Then, for each \( L_r \) at least one such vector is counted in \( M(\max L_r) \).

Hence

\[
b_0 \leq M(g_{k+1} + b_0 + b_1 + \ldots + b_k),
\]

and (5) is a consequence of the inequality

\[
M(x) \leq \frac{x^k}{k! b_1 b_2 \ldots b_k},
\]

which holds since the right hand side is the volume of the simplex determined by (6) and the inequalities \( x_i \geq 0 \), for the \( x_i \) considered as real variables.

3. The \( h \)-range. We now show that

\[
n(h, k) \leq \frac{(k-1)^{k-1}}{(k-1)!} \left( \frac{h^k}{k} \right) + O(h^{k-1}),
\]

which, by (5), proves (3).

Given the sequence (1), put

\[
A_i: a_0 = 0 < 1 = a_1 < a_2 < \ldots < a_i, \quad 1 \leq i \leq k.
\]

We use induction on \( i \) to prove that

\[
n(h, A_i) \leq \frac{(i-1)^{i-1}}{i!} \left( \frac{h^i}{i} \right) + O(h^{i-1}), \quad 1 \leq i \leq k.
\]

(8)

Since \( n(h, A_i) = h, (8) \) holds for \( i = 1 \). Suppose that (8) holds for \( 1 \leq i < K \), for some \( K \) in the interval \( 1 < K \leq k \). Then

\[
n(h, A_i) = O(h^i), \quad 1 \leq i < K.
\]

If \( a_{i+1} > n(h, A_i) + 1 \) for some \( i \) in the interval \( 1 \leq i < K \), then \( n(h, A_K) = n(h, A_i) \), and (8) holds for \( i = K \). Therefore suppose that

\[
a_{i+1} \leq n(h, A_i) + 1, \quad 1 \leq i < K,
\]

so in particular

\[
a_{i+1} = O(h^i), \quad 1 \leq i < K.
\]

(10)

Now consider an integer \( N \) in the interval

\[
h a_K - n(h, A_K) \leq N < h a_K - n(h, A_K) + a_K.
\]

(11)

By (9), we then have

\[
0 \leq n(h, A_{K-1}) - a_K + 1 \leq n(h, A_K) - a_K + 1,
\]

so that

\[
0 \leq h a_K - N \leq n(h, A_K).
\]

Thus there are non-negative integers \( x_i \) such that

\[
h a_K - N = \sum_{i=0}^{K} a_i x_i, \quad \sum_{i=0}^{K} x_i = h.
\]

Hence each integer \( N \) in the interval (11) has an integral representation

\[
N = \sum_{i=0}^{K} (a_K - a_i) x_i, \quad x_i \geq 0,
\]

and by adding multiples of \( a_K \), we see that so does every integer \( \geq h a_K - n(h, A_K) \).
Thus we have (cf. [10], §2)
\[ g(a_K, a_K-a_1, \ldots, a_K-a_{K-1}) \leq h a_K - n(h, A_K) - 1. \]

Using (4), we further get
\[ n(h, A_K) \leq h a_K - (a_K-a_{K-1})^{1/(K-1)}(a_K-a_{K-1}) + K a_K, \]
so that, by (10),
\[ n(h, A_K) \leq h a_K - (a_K-a_{K-1})^{1/(K-1)} + O(h^{-1}), \]
and maximizing the real function
\[ f(x) = h x - (a_K-a_{K-1})^{1/(K-1)}, \quad x \geq 0, \]
we see that (8) also holds for \( i = K. \)

4. Concluding Remarks. As a direct consequence of the well-known formula
\[ g_2 = b_0 b_1 - b_0 - b_1, \]
we have \( g_2 = 1. \) Also, for \( k = 2 \) we have that (3) is valid with equality, or more precisely (Stöhr [13])
\[ n(h, 2) = \left\lfloor \frac{h^2 + 6h + 1}{4} \right\rfloor. \]

Given \( k+1 \geq 3 \) relatively prime positive integers \( b_0, b_1, \ldots, b_k, \) put
\[ d = \gcd(b_1, b_2, \ldots, b_k). \]

For \( L_r = L_r(b_0, b_1, \ldots, b_k) \) defined as in Section 2, we then have
\[ L_r(b_0, b_1, \ldots, b_k) = d \cdot L_r\left(\frac{b_0}{d}, \frac{b_1}{d}, \ldots, \frac{b_k}{d}\right), \]
so that (Brauer and Shockley [2])
\[ g(b_0, b_1, \ldots, b_k) = d \cdot g\left(\frac{b_0}{d}, \frac{b_1}{d}, \ldots, \frac{b_k}{d}\right) + b_0(d-1). \]

Hence, in (4) it suffices to take the infimum over all sequences of positive integers \( b_0, b_1, \ldots, b_k \) satisfying \( \gcd(b_1, b_2, \ldots, b_k) = 1. \)

For \( \gcd(b_1, b_2) = 1, \) we showed in [9] that
\[ g_3 + b_0 + b_1 + b_2 = b_0 \alpha + b_1 \beta - x, \quad x = \min(b_0 \beta, b_1 \gamma), \]
for certain integers \( \alpha, \beta, \gamma, \delta \) satisfying
\[ \alpha \beta - \beta \gamma = b_2, \quad 0 \leq \beta < \alpha \leq b_2, \quad 0 \leq \gamma \leq \delta \leq b_2. \]

Using (12), the arithmetic-geometric mean inequality, and (13), we get
\[ g_3 + b_0 + b_1 + b_2 \geq 2(b_0 \alpha \cdot b_1 \beta)^{1/2} - x \]
\[ = 2(b_0 \beta \cdot b_1 \gamma + b_0 b_1 b_2)^{1/2} - x \geq 2(x^2 + b_0 b_1 b_2)^{1/2} - x, \]
and minimizing this last expression for \( x \) considered as a real variable, we get
\[ g_3 + b_0 + b_1 + b_2 \geq \sqrt{3b_0 b_1 b_2}. \]

Hence \( \sigma_2 \geq 3. \)

By (7), we thus have
\[ n(h, 3) \geq \frac{3h^3}{4} + O(h^2). \]

Using the simple Hilfssatz 1 of Hofmeister [4], bases \( A_3 \) for which
\[ n(h, A_3) \geq \frac{3h^3}{4} + O(h^2) \]
are easily constructed. Thus we have that (15) is valid with equality, as shown by Hofmeister [4], and independently by Klotz [6]. Hofmeister also gives the precise form of the error term for \( h \) large. More recently, Hofmeister [5] has shown that the results on \( n(h, 3) \) in [4] are valid for \( h \geq 200, \) and the remaining values of \( n(h, 3) \) have been computed by Mossige [7]. In particular, the conjecture of Guy [13, C12] (or see Alter and Barnett [1]) holds true.

For the sequence
\[ b_i = k+1, \quad b_i = a(k+1) + 1 \quad \text{for} \quad 1 \leq i \leq k, \]
we have \( g_{k+1} = a(k+1) - 1. \) By taking \( a \) large, we get
\[ \sigma_k \leq (k+1)^{-1}. \]

This bound is also a consequence of (7) and the result
\[ n(h, k) \geq \frac{(k-1)^{k-1}}{k^{-1}} \left(\frac{h^k}{k}\right) + O(h^{k-1}) \]
of Klotz [6].

It was pointed out by Selmer ([12, Chap. VI]) that for \( k = 2, \) the sequence (16) satisfies
\[ g_3 + b_0 + b_1 + b_2 = \lceil \sqrt{3b_0 b_1 b_2} \rceil, \]
which shows that the bound (14) is 'sharp'.

The bound (5) is probably not particularly good, and we do believe that an improvement is possible. As we have seen, we have \( \sigma_1 = 1 \) and \( \sigma_2 = 3. \) So what about \( \sigma_3? \)

Mossige [8] has shown that
\[ n(h, 4) \geq \frac{2.008 h^4}{4} + O(h^3). \]

Hence, by (5) and (7), \( 6 \leq \sigma_3 < 13.45. \)
Finally, someone interested in the problems considered in this paper, could do no better than consulting Selmer's research monograph [12].

References


Subfield permutation polynomials and orthogonal subfield systems in finite fields

by

STEPHAN J. SUCHOWER* (University Park, Pa.)

1. Introduction. In [5] Niederreiter developed the concepts of permutation polynomials in several variables over a finite field and orthogonal systems of polynomials over a finite field. In this paper we generalize these notions by allowing the image spaces of the polynomials to be arbitrary subfields of the finite field. Several properties of permutation polynomials and orthogonal systems are preserved and new relationships are exhibited. For a development of the basic properties of permutation polynomials and orthogonal systems, see [1], Ch. 7, Sec. 5.

In [3] Mullen demonstrated an application of the theory of permutation polynomials and orthogonal systems to the construction of complete sets of mutually orthogonal frequency squares of prime power order. Although Mullen's construction generated previously known designs, his algebraic approach was completely different than previous methods which were based upon statistical design theory. In a similar manner, we will show in a follow-up article how to use the theory developed in this paper to construct additional complete sets of frequency squares, rectangles and hyper-rectangles, as well as build orthogonal arrays of various strengths.

Let $F_q^n$ denote the finite field of order $q^n$ where $q$ is a power of a prime $p$ and $n$ is a positive integer. Let $F_q^*$ denote the multiplicative group of nonzero elements and let $F_q^{k,n}$ denote the product of $k$ copies of $F_q^n$, $k \geq 1$. The ring of polynomials in $k$ variables over $F_q^n$ will be denoted by $F_q^n[x_1, \ldots, x_k]$. Unless otherwise specified, two polynomials $f, g \in F_q^n[x_1, \ldots, x_k]$ are equal if they are equal as functions. Recall that every function $f: F_q^n \rightarrow F_q^n$ can be uniquely realized as a polynomial in $F_q^n[x_1, \ldots, x_k]$ of degree at most $q^k-1$ in each variable.

Following Niederreiter in [5], a polynomial $f \in F_q^n[x_1, \ldots, x_k]$ is called a permutation polynomial over $F_q^n$ if the equation $f(x_1, \ldots, x_k) = a$ has exactly $q^k-1$ solutions in $F_q^n$ for each $a \in F_q^n$. In addition, a system of polynomials

---

* This work is part of the author's Ph.D. dissertation at PSU under the direction of Professor G. L. Mullen.