can check that $|\mathscr{H}_0| = |\mathscr{H}''|$ by checking that it is true for each prime power p^α. We leave this computation to the reader. Then $\mathscr{H}_0$ is multiplicatively independent, and $\mathscr{H}''$ has the same multiplicative span as $\mathscr{H}_0$, so $\mathscr{H}''$ must also be multiplicatively independent.

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

References

[1] Bruce C. Berndt, Anthony J. F. Biagioli and James M. Purtilo, *Ramanujan's modular equations of "large" prime degree*, J. Indian Math. Soc. 51(1987).

[2] J. G. Conway and S. P. Norton, *Monstrous Moonshine*, Bull. London Math. Soc. 11 (1979), 308–339.

[3] Victor G. Kac, *Infinite dimensional Lie algebras*, 2nd ed., Cambridge University Press, Cambridge 1985.

[4] Marvin I. Knopp, *Modular functions in analytic number theory*, Markham Publishing Company, 1985.

[5] Marvin Knopp, Joseph Lehner and Morris Newman, *A bounded automorphic form of dimension zero is constant*, Duke Math. J. 32 (3) (1965), 457–460.

[6] Morris Newman, *Construction and application of a certain class of modular functions*, Proc. London Math. Soc., (3), 7 (1956), 334–350.

[7] — *Construction and application of a certain class of modular functions II*, ibid. 9 (1959), 373–387.

[8] W. H. H. Petersson, *Über Thetareihen zu grossen Untergruppen der rationale Modulgruppe*, Springer-Verlag, Berlin 1972.

[9] Hans Rademacher, *Topics in analytic number theory*, Springer-Verlag, New York 1972.

[10] Bruno Schoeneberg, *Elliptic modular functions, an introduction*, Springer-Verlag, Berlin 1972.

DEPARTMENT OF MATHEMATICS AND STATISTICS
THE UNIVERSITY OF MISSOURI AT ROLLA
Rolla, MO 65401-0249
U.S.A.

Received on 13.4.1988
and in revised form on 18.10.1988 (1812)

ACTA ARITHMETICA
LIV (1990)

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

by

ÖYSTEIN J. RÖDSETH (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

$$A_k\colon\ a_0 = 0 < 1 = a_1 < a_2 < \ldots < a_k \tag{1}$$

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 $k \geqslant 1$ fixed and h large.

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

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

so in particular

$$n(h, k) \leqslant \frac{k^{k-1}}{(k-1)!}\left(\frac{h}{k}\right)^k + O(h^{k-1}). \tag{2}$$

On the other hand we have $n(h, k) \geqslant (h/k)^k$ (Stöhr [13]).

For $k \leqslant 3$ we have

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

where $c_1 = 1$ (trivial), $c_2 = 1$ (Stöhr [13]), $c_3 = 4/3$ (Hofmeister [4], Klotz [6]). For $k \geqslant 4$, however, it is not even known if such a constant c_k exists. Guy ([3], 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 $k \geqslant 4$, the only improvement of the bound (2) seems to be that of Klotz [6], who showed that

$$n(h, k) \leqslant c\frac{k^{k-1}}{(k-1)!}\left(\frac{h}{k}\right)^k \quad \text{for } k \geqslant 2 \text{ and } h \text{ large},$$

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

$$n(h, k) \leqslant \frac{(k-1)^{k-1}}{(k-1)!}\left(\frac{h}{k}\right)^k + O(h^{k-1}), \tag{3}$$

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 $k+1 \geqslant 2$ relatively prime positive integers b_i is the largest non-zero integer which cannot be written as a sum of numbers b_i, repetitions being allowed.

Put $\sigma_0 = 1$, and

$$\sigma_k = \inf \frac{(g_{k+1}+b_0+b_1+\ldots+b_k)^k}{b_0 b_1 \ldots b_k} \quad \text{for } k \geqslant 1, \tag{4}$$

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

$$\sigma_k \geqslant k!. \tag{5}$$

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

$$L_r = b_1 x_1 + b_2 x_2 + \ldots + b_k x_k, \quad x_i \geqslant 1.$$

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

$$b_1 x_1 + b_2 x_2 + \ldots + b_k x_k \leqslant x. \tag{6}$$

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

Hence

$$b_0 \leqslant M(g_{k+1} + b_0 + b_1 + \ldots + b_k),$$

and (5) is a consequence of the inequality

$$M(x) \leqslant \frac{x^k}{k!\, b_1 b_2 \ldots b_k},$$

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

3. The h-range. We now show that

$$n(h, k) \leqslant \frac{(k-1)^{k-1}}{\sigma_{k-1}}\left(\frac{h}{k}\right)^k + O(h^{k-1}), \tag{7}$$

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

Given the sequence (1), put

$$A_i\colon a_0 = 0 < 1 = a_1 < a_2 < \ldots < a_i, \quad 1 \leqslant i < k.$$

We use induction on i to prove that

$$n(h, A_i) \leqslant \frac{(i-1)^{i-1}}{\sigma_{i-1}}\left(\frac{h}{i}\right)^i + O(h^{i-1}), \quad 1 \leqslant i \leqslant k. \tag{8}$$

Since $n(h, A_1) = h$, (8) holds for $i = 1$. Suppose that (8) holds for $1 \leqslant i < K$, for some K in the interval $1 < K \leqslant k$. Then

$$n(h, A_i) = O(h^i), \quad 1 \leqslant i < K.$$

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

$$a_{i+1} \leqslant n(h, A_i) + 1, \quad 1 \leqslant i < K, \tag{9}$$

so in particular

$$a_{i+1} = O(h^i), \quad 1 \leqslant i < K. \tag{10}$$

Now consider an integer N in the interval

$$h a_K - n(h, A_K) \leqslant N < h a_K - n(h, A_K) + a_K. \tag{11}$$

By (9), we then have

$$0 \leqslant n(h, A_{K-1}) - a_K + 1 \leqslant n(h, A_K) - a_K + 1,$$

so that

$$0 \leqslant h a_K - N \leqslant n(h, A_K).$$

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

$$N = \sum_{i=0}^{K-1} (a_K - a_i) x_i, \quad x_i \geqslant 0,$$

and by adding multiples of a_K, we see that so does every integer $\geqslant h a_K - n(h, A_K)$.

Thus we have (cf. [10], §2)

$$g(a_K, a_K-a_1,\dots,a_K-a_{K-1}) \leqslant ha_K-n(h, A_K)-1.$$

Using (4), we further get

$$n(h, A_K) \leqslant ha_K-(\sigma_{K-1}a_K)^{1/(K-1)}(a_K-a_{K-1})+Ka_K,$$

so that, by (10),

$$n(h, A_K) \leqslant ha_K-(\sigma_{K-1}a_K^K)^{1/(K-1)}+O(h^{K-1}),$$

and maximizing the real function

$$f(x) = hx-(\sigma_{K-1}x^K)^{1/(K-1)}, \quad x \geqslant 0,$$

we see that (8) also holds for $i = K$.

4. Concluding remarks. As a direct consequence of the well-known formula $g_2 = b_0b_1-b_0-b_1$, we have $\sigma_1 = 1$. 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 $k+1 \geqslant 3$ relatively prime positive integers $b_0, b_1,\dots,b_k$, put

$$d = \gcd(b_1, b_2,\dots,b_k).$$

For $L_r = L_r(b_0, b_1,\dots,b_k)$ defined as in Section 2, we then have

$$L_{dr}(b_0, b_1,\dots,b_k) = d\cdot L_r\left(b_0, \frac{b_1}{d},\dots,\frac{b_k}{d}\right),$$

so that (Brauer and Shockley [2])

$$g(b_0, b_1,\dots,b_k) = d\cdot g\left(b_0, \frac{b_1}{d},\dots,\frac{b_k}{d}\right)+b_0(d-1).$$

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

For $\gcd(b_1, b_2) = 1$, we showed in [9] that

$$g_3+b_0+b_1+b_2 = b_0\alpha+b_1\delta-x, \quad x = \min(b_0\beta, b_1\gamma) \tag{12}$$

for certain integers α, β, γ, δ satisfying

$$\alpha\delta-\beta\gamma = b_2, \quad 0 \leqslant \beta < \alpha \leqslant b_2, \quad 0 \leqslant \gamma < \delta \leqslant b_2. \tag{13}$$

Using (12), the arithmetic-geometric mean inequality, and (13), we get

$$\begin{aligned} g_3+b_0+b_1+b_2 &\geqslant 2(b_0\alpha\cdot b_1\delta)^{1/2}-x \\ &= 2(b_0\beta\cdot b_1\gamma+b_0b_1b_2)^{1/2}-x \geqslant 2(x^2+b_0b_1b_2)^{1/2}-x, \end{aligned}$$

and minimizing this last expression for x considered as a real variable, we get

$$g_3+b_0+b_1+b_2 \geqslant \sqrt{3b_0b_1b_2}. \tag{14}$$

Hence $\sigma_2 \geqslant 3$.

By (7), we thus have

$$n(h, 3) \leqslant \frac{4}{3}\left(\frac{h}{3}\right)^3+O(h^2). \tag{15}$$

Using the simple Hilfssatz 1 of Hofmeister [4], bases A_3 for which

$$n(h, A_3) \geqslant \frac{4}{3}\left(\frac{h}{3}\right)^3+O(h^2)$$

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 $h \geqslant 200$, and the remaining values of $n(h, 3)$ have been computed by Mossige [7]. In particular, the conjecture of Guy ([3], C12) (or see Alter and Barnett [1]) holds true.

For the sequence

$$b_0 = k+1, \quad b_i = a(k+1)+i \quad \text{for } 1 \leqslant i \leqslant k, \tag{16}$$

we have $g_{k+1} = a(k+1)-1$. By taking a large, we get

$$\sigma_k \leqslant (k+1)^{k-1}.$$

This bound is also a consequence of (7) and the result

$$n(h, k) \geqslant \frac{(k-1)^{k-1}}{k^{k-2}}\left(\frac{h}{k}\right)^k+O(h^{k-1})$$

of Klotz [6].

It was pointed out by Selmer ([12], Chap. VI) that for $k = 2$, the sequence (16) satisfies

$$g_3+b_0+b_1+b_2 = \lceil \sqrt{3b_0b_1b_2}\, \rceil,$$

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 σ_3?

Mossige [8] has shown that

$$n(h, 4) \geqslant 2.008\left(\frac{h}{4}\right)^4+O(h^3).$$

Hence, by (5) and (7), $6 \leqslant \sigma_3 < 13.45$.

Finally, someone interested in the problems considered in this paper, could do no better than consulting Selmer's research monograph [12].

References

[1] R. Alter and J. A. Barnett, *A postage stamp problem*, Amer. Math. Monthly 87 (1980), 206–210.
[2] A. Brauer and J. E. Shockley, *On a problem of Frobenius*, J. Reine Angew. Math. 211 (1962), 215–220.
[3] R. K. Guy, *Unsolved problems in number theory*, Springer-Verlag, New York 1981.
[4] G. Hofmeister, *Asymptotische Abschätzungen für dreielementige Extremalbasen in natürlichen Zahlen*, J. Reine Angew. Math. 232 (1968), 77–101.
[5] — *Die dreielementigen Extremalbasen*, ibid. 339 (1983), 207–214.
[6] W. Klotz, *Extremalbasen mit fester Elementeanzahl*, ibid. 237 (1969), 194–220.
[7] S. Mossige, *Algorithms for computing the h-range of the postage stamp problem*, Math. Comp. 36 (1981), 575–582.
[8] — *On extremal h-bases A_4*, Math. Scand. 61 (1987), 5–16.
[9] Ö. J. Rödseth, *On a linear Diophantine problem of Frobenius*, J. Reine Angew. Math. 301 (1978), 171–178.
[10] — *On h-bases for n*, Math. Scand. 48 (1981), 165–183.
[11] H. Rohrbach, *Ein Beitrag zur additiven Zahlentheorie*, Math. Z. 42 (1937), 1–30.
[12] E. S. Selmer, *The local postage stamp problem, I, II*, Research monograph (available on request), Dept. of Math., University of Bergen 1986.
[13] A. Stöhr, *Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe. I*, J. Reine Angew. Math. 194 (1955), 40–65.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF BERGEN
Allégt. 55
N-5007 Bergen
Norway

Received on 18.4.1988 (1814)

ACTA ARITHMETICA
LIV (1990)

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 ralationships 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 $F_{q^n}^*$ denote the multiplicative group of nonzero elements and let $F_{q^n}^k$ 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 $f\colon F_{q^n}^k \to F_{q^n}$ can be uniquely realized as a polynomial in $F_{q^n}[x_1, \ldots, x_k]$ of degree at most $q^n - 1$ 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 $q^{n(k-1)}$ solutions in $F_{q^n}^k$ 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.