MATH. SCAND. 66 (1990), 197–215

ON THE NUMBER OF SEMIGROUPS OF NATURAL NUMBERS

JÖRGEN BACKELIN

Introduction.

This paper consists of two parts. In part I two problems concerning subsemigroups S of $\mathbb{N}$ are treated:

- How many S with a given Frobenius number g (or a given conductor $c = g + 1$) are there?
- How many *maximal* S with a given Frobenius number g are there?

(For g odd, the maximal semigroups are precisely he symmetric semigroups.) The first question was raised by H. S. Wilf in [3]. The second question is considered in [2, proposition 5], where it is proved that (for g odd)

$$\#\,\text{symmetric } S \geq 2^{[g/8]}.$$

The answers given in the theorem below are, roughly: $C \cdot 2^{g/2}$ and $C' \cdot 2^{g/6}$, respectively, where C and C' vary within finite bounds. For the answer of the second question it was necessary to investigate a question of some interest in itself, namely:

- How many subsets X of $\{1, 2, \ldots, n\}$, such that there are at most q different sums of pairs of elements from X, are there?

We did not find any treatment of this question in the literature. A sufficiently good answer for our applications is given as a "main lemma". Part II of this paper is devoted to the proof of that lemma. (It is quite independent of part I.)

ACKNOWLEDGEMENTS. This work is inspired by and done in conjunction with [2], and I want to thank the authors of that paper for introducing me to these questions and (in particular Roland Häggkvist) for valuable discussions and contributions of ideas. My special thanks go to Calle Jacobsson, whose ideas I have employed in the formulation and the proof of the main lemma.

Received October 1, 1987; in revised form January 25, 1988.

I. Semigroups.

I.0. TERMINOLOGY. In this part, mainly the terminology of [2] is adopted:

N denotes the set of natural numbers (including 0).

A *semigroup* S will always denote a submonoid of (N, +), i.e. a subset of N which contains 0 and is closed under addition. Furthermore (discarding the trivial semigroups $\{0\}$ and N, and employing isomorphisms of monoid) we always assume that $\mathsf{N}\setminus S\,\{=n\in\mathsf{N}: n\notin S\})$ is a non-empty finite set.

If S is a semigroup, then the *Frobenius number* $g(S) := \max \mathsf{N}\setminus S$, while the *minimal generator* $m(S) := \min S\setminus\{0\}$.

If X is any subset of N, then $S\langle X\rangle$ is the minimal semigroup containing X, i.e. the set of all linear combinations of elements in X, with non-negative integer coefficients; while $2X := \{x + y: x, y \in X\}$.

If X is any finite set, then $|X|$ = number of elements in X.

If a is a real number, then $[a]$ = integer part of a; and if $a > 0$, $\ln a$ and $\lg a$ denote the logarithms of a with bases e and 2, respectively.

$\mathscr{S}_g := \{$semigroups S with $g(S) = g\}$, for $g = 1, 2, \ldots$. $\mathscr{S}_g$ is partially ordered by (set-theoretical) inclusion; let $\mathscr{M}_g$ be the set of the maximal elements in $\mathscr{S}_g$.

In [2] a number of equivalent conditions on elements $S \in \mathscr{S}_g$ are given, which are shown to be equivalent to the condition "S be maximal". They are slightly dependent on the parity of g. In particular, for g odd it is shown that $S \in \mathscr{S}_g$ is maximal iff S is *symmetric* in the sense that for any integer i we have that $i \in S$ iff $g - i \notin S$. (There are some more precise conditions on symmetric semigroups than on "even-case" maximal ones, like this: S is symmetric iff the semigroup ring $k[S]$ is Gorenstein (k some field). These conditions are of no concern in this article.)

Below we shall concentrate on achieving estimates for the quantities $f(g) := |\mathscr{S}_g|$ and $e(g) := |\mathscr{M}_g|$.

I.1. THE MAIN RESULTS. The main object of this article is to prove.

THEOREM. *With the terminology above,*

(i) $$0 < \liminf_{g\to\infty} 2^{-g/2}|\mathscr{S}_g| < \limsup_{g\to\infty} 2^{-g/2}|\mathscr{S}_g| < \infty, \text{ and}$$

(ii) $$0 < \liminf_{g\to\infty} 2^{-g/6}|\mathscr{M}_g| < \limsup_{g\to\infty} 2^{-g/6}|\mathscr{M}_g| < \infty.$$

In fact, we will get stronger results, like

(1) $$2^{[(g-1)/2]} \le |\mathscr{S}_g| < 4\cdot 2^{[(g-1)/2]} \text{ for all positive integers } g, \text{ and}$$

PROPOSITION 1. $\lim_{g \text{ odd}} 2^{-g/2}|\mathscr{S}_g|$ *and* $\lim_{g \text{ even}} 2^{-g/2}|\mathscr{S}_g|$ *exist, and likewise* $\lim_{g:g\equiv i \pmod 6} 2^{-g/6}|\mathscr{M}_g|$ *exists for* $i = 0, 1, 2, 3, 4, 5$.

The values of these limits are briefly discussed in section I.3. Furthermore, "almost all" S in $\mathscr{S}_g$ (in $\mathscr{M}_g$) have their minimal generators $m(S)$ "almost equal" to $g/2$ (to $g/3$, respectively), in the following strong sense:

PROPOSITION 2. *For any real number* $\varepsilon > 0$ *there is an integer* n_0 *such that for every positive integer* g *we have*

$$|\{S \in \mathscr{S}_g : |m(S) - g/2| > n_0\}| < \varepsilon \cdot 2^{g/2}, \text{ and} \tag{2}$$

$$|\{S \in \mathscr{M}_g : |m(S) - g/3| > n_0\}| < \varepsilon \cdot 2^{g/6}. \tag{3}$$

In the next section, the theorem and the propositions are proved, except for the "lim inf $\neq$ lim sup"-parts of the theorem, the proof of which is postponed to I.3. The proofs are mainly by subdivision into different cases, depending on $m(S)$.

I.2. PROOFS. It will turn out that the sets $A := \{n \in \mathrm{N} : g/2 < n < g\}$ and $B := \{n \in \mathrm{N} : g/3 < n < g/2\}$ are of fundamental interest for the counting arguments, and we shall compute in terms of 2^a and 2^b, where $a := |A|$ and $b := |B|$, rather than in terms of $2^{g/2}$ and $2^{g/6}$. (A, B, a and b are functions of g, strictly speaking.) Clearly $a = [(g-1)/2]$ and $b = [(g-1)/2] - [g/3]$, and for all g we have $|a - g/2| \le 1$ and $|b - g/6| \le 1$; the exact differences depend only on the residue classes of g modulo 2 and modulo 6, respectively. For any positive integers g and m, let $\mathscr{S}_{g,m} := \{S \in \mathscr{S}_g : m(S) = m\}$ and $\mathscr{M}_{g,m} := \{S \in \mathscr{M}_g : m(S) = m\}$. Furthermore, let $f(g,m) := |\mathscr{S}_{g,m}|$ and let $e(g,m) := |\mathscr{M}_{g,m}|$. Clearly,

$$\sum_m f(g,m) = f(g) \quad \text{and} \tag{4}$$

$$\sum_m e(g,m) = e(g). \tag{5}$$

LEMMA 1.

(i) $f(g,m) = |\{X \subseteq \{m, m+1, \ldots, g-1\} : g \notin S\langle X\rangle \,\&\, m \in X\}|$ *for* $m < g$.

(ii) $e(g,m) = |\{X \subseteq \{m, m+1, \ldots, [(g-1)/2]\} : g \notin S\langle X\rangle \,\&\, m \in X\}|$ *for* $m < g/2$.

(iii) $\sum_{m \geq g} f(g,m) = f(g, g+1) = 1.$

(iv) $\sum_{m \geq [(g+1)/2]} e(g,m) = e(g, [(g+2)/2]) = 1.$

PROOF. If $S \in \mathscr{S}_{g,m}$ and $S \neq \{0, g+1, g+2, g+3, \ldots\}$, then $S \cap \{1, 2, \ldots, g-1\}$ is a set X fulfilling the conditions in (i). On the other hand, if X is such a set, then $\{0\} \cup X \cup \{g+1, g+2, \ldots\} \in \mathscr{S}_{g,m}$. (i) and (iii) follow.

(ii) and (iv) are proved similarily, using the following implicit facts from [2]: *If S is a maximal semigroup and n is any integer ($\neq g(S)/2$), then $n \in S \Leftrightarrow g(S) - n \notin S$; and if S is any semigroup, then there is exactly one maximal semigroup S_1 such that $S \subseteq S_1$ & $g(S) = g(S_1)$ & $S \cap \{1, 2, \ldots, [(g-1)/2]\} = S_1 \cap \{1, 2, \ldots, [(g-1)/2]\}$.*

If $X \subseteq A$ or $X \subseteq B$, then $g \notin S\langle X \rangle$. For $g \notin A$, while the sum of two or more elements in A is greater than $2 \cdot g/2 = g$; and likewise $g \notin B$, the sum of two elements in B is less than g, and the sum of three or more elements in B is greater than $3 \cdot g/3 = g$. Thus and by lemma 1,

(6) $$f(g, m) = 2^{g-m-1} \quad \text{if} \quad g/2 < m < g, \quad \text{and}$$

(7) $$e(g, m) = 2^{a-m} \quad \text{if} \quad g/3 < m < g/2; \quad \text{and furthermore,}$$

(8) $$\sum_{m > g/2} f(g, m) = 2^a \quad \text{and}$$

(9) $$\sum_{m > g/3} e(g, m) = 2^b.$$

(4), (8), (5) and (9) immediately prove the left inequalities of the theorem and of (1).

Of course, (8) is just a numerical consequence of the correspondence "S with 'upper' $m(S) \leftrightarrow$ subsets of A" (where "upper" obviously means "greater than $g(S)/2$"). The reason for analyzing it as a geometric sum by means of (6) is that this also yields the "upper case" part of (2). Similarly, the "upper case" of (3) follows from (7). (Here "upper" means: "greater than $g(S)/3$".)

With more effort we shall establish upper bounds on $f(g, m)$ and $e(g, m)$ for "lower" m, and thus be able to bound the sums of these with 2^a or 2^b times a geometrical sum, thus establishing both the right inequalities of the theorem and the rest of proposition 2.

From now on, fix g and always assume that $2 \leq m \leq a$. Let X be any subset of $D_m := \{m, m+1, \ldots, a\}$, such that $m \in X$. X is called *m-admissible* if there is an $S \in \mathscr{S}_{g,m}$, such that $X = S \cap D_m$. If X is m-admissible, then let $f(g, m, X) := |\{S \in \mathscr{S}_{g,m} : S \cap D_m = X\}|$.

LEMMA 2.

(i) *X is m-admissible iff $g \notin S\langle X \rangle$.*

(ii) $f(g, m) = \sum_{X\ m\text{-adm.}} f(g, m, X)$.

(iii) $e(g, m) = |\{m\text{-}admissible\ X\}|$.

This is just reformulations of the definitions and former results.

In order to get estimates for $f(g,m)$, we shall use different methods, depending on whether $m > g/4$ or not.

$f(g,m)$ for $m > g/4$: Fix an m with $g/4 < m < g/2$; we may exclude the trivial case $m = g/3$. Let $s := a + 1 - m$. Then we have:

$$|\{m\text{-admissible X}: |X| = k\}| \leq \binom{s-1}{k-1} \qquad (k = 1,\ldots,s). \tag{10}$$

Let $A := \{[g/2]+1,\ldots,g-1\}$ (as before). Fix an m-admissible X. Let $k := |X|$. We shall try to restrict the number of X-*admissible* sets Y, i.e. the subsets Y of A such that $S = \{0\} \cup X \cup Y \cup \{g+1, g+2,\ldots\} \in \mathscr{S}_{g,m}$. To begin with, we note that such a Y must fulfill three conditions:

(a) If $x \in X$, then $g - x \notin Y$ (since $x + (g-x) \notin S$);
(b) If $x_1, x_2 \in X$, then $x_1 + x_2 \in Y$; and
(c) If $y_1, y_2 \in A$ and $y_2 - y_1 \in X$, then none of y_1 and y_2, or both of them, or y_2 but not y_1 belong to Y
(since $y_1 \in Y \Rightarrow y_2 = y_1 + (y_2 - y_1) \in S \cap A = Y$).

On the other hand, when $m > g/3$ any $Y \subseteq A$ fulfilling (a), (b) and (c) indeed is X-admissible: (b) and (c) guarantee that $S\langle X \cup Y\rangle \cap A = Y$, whence (a) implies that $g \notin S\langle X \cup Y\rangle$. Thus indeed $S\langle X \cup Y\rangle = S \in \mathscr{S}_{g,m}$.

The elements $g - x$ of (a) and $x_1 + x_2$ of (b) (all of which indeed lie strictly between $g/2$ and g) form two disjoint sets $g - X$ and $2X$, respectively, for which there is no freedom of choice when constructing an X-admissible Y. Thus Y is determined by $Y \cap L$, where $L := A \setminus ((g - X) \cup 2X)$. Now $|N| = a$ and $|g - X| = k$, while $|2X| \geq 2k - 1$ by the following well-known argument (cf e.g. [1, 1.8] and note that $m = \min X$): $(m + X) \cup (X + \max X) \subseteq 2X$; and $|m + X| = |X + \max X| = k$, while $|(m + X) \cap (X + \max X)| = |\{m + \max X\}| = 1$, whence $|(m + X) \cup (X + \max X)| = 2k - 1$. Thus

$$|L| \leq a - 3k + 1. \tag{11}$$

The condition (c) may be reformulated thus: Let us turn A into a directed graph by introducing an arrow $y_1 \to y_2$ $(y_1, y_2 \in A)$ iff $y_2 - y_1 \in X$. Then any X-admissible Y does not contain any *tail* (i.e., arrow-start) without containing the corresponding *head* (arrow-end). In order to get a computable upper bound, let us confine ourselves to the *principal* arrows, i.e. to $y_1 \to y_2$ given by $y_2 - y_1 = m$. In the entire set A there are exactly $s - 1 = a - m$ (disjoint) principal arrows, namely $g - a \to g - s + 1, g - a + 1 \to g - s + 2, \ldots, g - m - 1 \to g - 1$. The other $a - 2(s-1)$ points in A be called *isolated*.

As we saw above there are but three possibilities as for what part of a principal arrow may be contained in a given X-admissible Y; and for any isolated point there are two possibilities ("to belong or not to belong"). Thus only using (c) we get

$$f(g,m,X) \leq 3^{s-1} \cdot 2^{a-2(s-1)} = 2^a \cdot \left(\frac{3}{4}\right)^{s-1},$$

while (a) and (b) alone gave (11) and thus

$$f(g,m,X) \leq 2^{a-3k+1}.$$

Let us combine the results, by starting with (A, {principal arrows}) and removing the elements in $g - X$ and in $2X$ one by one, checking the effect of each step on the upper bound for the number of X-admissible sets!

The element $g - m$ is isolated, whence deleting it reduces the bound to 1/2 of its former value.

Deleting any other point in $g - X$ or in $\{y \in 2X: y > g - m\}$ means deleting either an isolated point or one of the points of a principal arrow (thus also deleting the arrow, turning its other end to a new isolated points). This reduces the bound to 1/2 or to 2/3 of the former value, respectively, and thus reduces it "at least" to 2/3 thereof.

Finally, deleting any remaining element $y \in 2X$ either deletes an isolated element or the tail of an arrow; in the latter case, however, we know that also $y + m \in Y$ for any X-admissible Y, whence *the whole arrow* (including both its points) may be deleted. Thus the reduction is at least $\max(1/2, 1/3) = 1/2$; and there are at least $|m + X| = k$ such Y.

Summing up, we find that

$$(12) \quad f(g,m,X) \leq 2^a \cdot \left(\frac{3}{4}\right)^{s-1} \cdot \left(\frac{1}{2}\right)^{k+1} \cdot \left(\frac{2}{3}\right)^{2k-2} = \frac{1}{4} \cdot 2^a \left(\frac{3}{4}\right)^{s-1} \cdot \left(\frac{2}{9}\right)^{k-1},$$

$$(k = |X| \text{ and } g/4 < m < g/2).$$

By (10), (12) and the binomial theorem we have:

$$(13) \qquad f(g,m) \leq \frac{1}{4} \cdot 2^a \cdot \left(\frac{11}{12}\right)^{s-1} \quad (\text{for } g/4 < m = a + 1 - s < g/2).$$

Thus indeed

$$(14) \qquad \sum_{g/4 < m < g/2} f(g,m) \leq \sum_{s=1}^{a-[g/4]} \frac{1}{4} \cdot 2^a \cdot \left(\frac{11}{12}\right)^{s-1} < 3 \cdot 2^a.$$

$f(g,m)$ for $m < g/4$: Fix an m with $1 < m < g/4$ and such that m does not divide g. Let $n := [g/m]$ and $r := g - mn$ (= the remainder of g modulo m). Thus $n \geqq 4$ and $r > 0$.

Consider $S \in \mathscr{S}_{g,m}$. We shall partition that "candidates" for elements in

$S \cap \{m+1,\ldots,g-1\}$ into residue classes modulo m, and employ the fact that if one element in a class belongs to S, then so do all higher elements in this class. (This corresponds to the "principal arrows" above.) Furthermore, the condition $g \notin S$ will turn out to impose heavy restrictions.

For any integer i, let $r_i := \{j \in \mathrm{N}: m < j < g \,\&\, j \equiv i (mod\, m)\}$, and let $s_i = s_i(S) := r_i \cap S$. Then we have:

$$s_0 = r_0, \text{ and}$$

$$s_r = \emptyset; \text{ whence}$$

$$S \cap \{m+1,\ldots,g-1\} = \Bigg(\bigcup_{\substack{0<i<m \\ i \neq r}} s_i \Bigg) \cup r_0.$$

Henceforth we only regard r_i and s_i for $i \not\equiv 0, r$. If $x \in s_i$ and $x < y \in r_i$, then $y \in s_i$. Thus s_i is completely determined by $|s_i| \in \{0,\ldots,|r_i|\}$. If $0 < i < r$ then $|r_i| = n$, while if $r < i < m$ then $|r_i| = n - 1$.

Let us call $r_1,\ldots,r_{r-1}$ and $r_{r+1},\ldots,r_{m-1}$ the *lower* and the *upper* classes, respectively. If $r_i \neq r_j$ and $i + j \equiv r$, then we shall call $\{r_i, r_j\}$ a *class couple*. Clearly, the classes of a couple either both will be lower or both will be upper, whence we may talk of *lower class couples* or *upper class couples*. If $2i \equiv r$, then r_i is called a (lower or upper) *class singleton*.

Fix a lower class couple $\{r_i, r_j\}$ with $0 < i < j < r$, and assume that $|s_i| + |s_j| \geq n + 2$. Then we have $i + j = r$; $r_i = \{m + i, 2m + i,\ldots, nm + i\}$; $r_j = \{m + j, 2m + j,\ldots, nm + j\}$; $s_i = \{\alpha m + i,\ldots, nm + i\}$ (where $\alpha = n + 1 - |s_i|$); and $s_j = \{\beta m + j,\ldots, nm + j\}$ (where $\beta = n + 1 - |s_j|$). By the assumption $\alpha + \beta = 2n + 2 - (|s_i| + |s_j|) \leq n$, whence

$$g = nm + i + j = (n - \alpha - \beta)m + (\alpha m + i) + (\beta m + j) \in S,$$

a contradiction. Thus, in fact

$$|s_i| + |s_j| \leq n + 1.$$

This together with the conditions $|s_i|$, $|s_j| \leq n$ yields: there are (at most) $(n^2 + 5n + 2)/2$ different possible pairs $(|s_i|, |s_j|)$ and thus different possible $s_i \cup s_j$.

For upper class couples $\{r_i, r_j\}$, lower class singletons r_l, and upper class singletons r_h, we similarly get the conditions

$$|s_i| + |s_j| \leq n,$$

$$|s_l| \leq [(n+1)/2], \quad \text{and}$$

$$|s_h| \leq [n/2],$$

yielding (at most) $(n^2 + 3n - 2)/2$, $[(n + 1)/2] + 1$, and $[n/2] + 1$ possibilities, respectively. Thus, if we count the numbers of the various couples and singletons (with due consideration to the parities of m and r), we get an upper bound for $f(g,m)$. To be precise,

$$f(g,m) \leq \left(\frac{n^2+5n+2}{2}\right)^{[\frac{1}{2}(r-1)]}\left(\frac{n^2+3n-2}{2}\right)^{[\frac{1}{2}(m-r-1)]}\cdot \tag{15}$$

$$\left[\frac{n+5}{2}\right]^{r-1-2[\frac{1}{2}(r-1)]}\left[\frac{n+4}{2}\right]^{m-r-1-2[\frac{1}{2}(m-r-1)]} \quad \text{(for } m < g/4).$$

The rest is an exercise in elementary calculus: Considering odd and even cases for $r-1$ and for $m-r-1$ separately, and using the assumption $n \geq 4$, we find that the right side of (15), and thus $f(g,m)$, is not greater than

$$4(13\sqrt{19})^{-1}(\tfrac{1}{2}(n^2+5n+2))^{\frac{1}{2}r}(\tfrac{1}{2}(n^2+3n-2))^{\frac{1}{2}(m-r)} <$$
$$0.071h(n+1)^{\frac{1}{2}r}h(n)^{\frac{1}{2}(m-r)}2^{-\frac{1}{2}m},$$

where $h(x) = x^2+3x-2$ (x real). Now $(h(n+1)^r \cdot h(n)^{m-r})^{1/m} = h(n+1)^w \cdot h(n)^{1-w}$ ($w := r/m$) is a weighted geometric mean of $h(x)$. Taking logarithms we pass to an *arithmetic* mean, and since

$$\frac{d^2}{dx^2}\ln h(x) < 0 \quad (x \geq 4),$$

we get

$$w \ln h(n+1) + (1-w)\ln h(n) < \ln h(n+w) = \ln h(g/m),$$

whence

$$f(g,m) < 0.071(\tfrac{1}{2}h(g/m))^{\frac{1}{2}m} = 0.071\left(\tfrac{1}{2}\left(\left(\frac{g}{m}\right)^2 + 3\frac{g}{m} - 2\right)\right)^{\frac{1}{2}m} \tag{16}$$

$$\text{for} \quad m < g/4.$$

Now $(\frac{1}{2}h(4))^{\frac{1}{2}g/4} = 13^{g/8} = 2^{g/2}\cdot 2^{-g(\lg(16/13))/8}$,

$$\frac{d}{dy}(\tfrac{1}{2}y\ln(\tfrac{1}{2}h(g/y)))|_{y=g/4} = \tfrac{1}{2}\ln 13 - 11/13 > 0.436, \quad \text{and}$$

$$\frac{d^2}{dy^2}(\tfrac{1}{2}y\ln(\tfrac{1}{2}h(g/y))) < 0 \quad \text{for} \quad 0 < y < g/4.$$

Thus $(\frac{1}{2}h(g/(m-1)))^{\frac{1}{2}(m-1)} < (\frac{1}{2}h(g/m))^{\frac{1}{2}m}\cdot e^{-0.436} < (\frac{1}{2}h(g/m))^{\frac{1}{2}m}2^{-0.628}$, for $2 \leq m \leq g/4$, and we get indeed

$$f(g,m) < 0.071\cdot 2^{g/2}\cdot(13/16)^{g/8}\cdot 2^{-0.628((g/4)-m)} \quad \text{for} \quad m < g/4 \tag{17}$$

and thus a way to express $\sum_{m<g/4} f(g,m)$ as a geometric sum. For uniformity, it may

be nicer to note that (since $(13/16)^{1/8} < (11/12)^{1/4}$ and $0.628 > \lg(12/11)$) we can extend (13) to the case $m < g/4$, too. That is, we have

$$f(g,m) \le \frac{1}{4}\cdot 2^a \cdot \left(\frac{11}{12}\right)^{a-m} \quad \text{for} \quad m = 2,3,\ldots,a(=[(g-1)/2]). \tag{18}$$

This (and (8)) yield the upper inequality of (1), whence indeed $\limsup_g 2^{-g/2} f(g) \leqq 4 < \infty$. Moreover, (6) and (8) imply the (2)-part of proposition 2.

Finally, we shall derive bounds for the $e(g,m)$ in a similar way; we are through if $m := m(S) > g/3$, and otherwise we divide the analysis into two parts, depending on whether $m > g/6$ or not. However, just copying the methods from the $\limsup f(g)$ – proof is not enough; indeed that yields $2^b \cdot$ (geometrical sums), but the bases of the terms of the power expressions are greater than rather than less than 1. We overcome this by using the following *Main lemma* (instead of the crude estimate $|2X| \ge 2|X| - 1$) which essentially tell us that *on the average* the cardinality of $2X$ is *much* bigger than the cardinality of X. The explicit lemma deals with the inverse problem: Given $|2X|$, there are few possible X, and thus in particular few possible X of large cardinality:

$$(\forall \varepsilon > 0)(\exists C)(\forall n, q \in \mathbf{N})(|\{X \subseteq \{1,2,\ldots,n\}: |2X| \le q\}| < C \cdot 2^{\varepsilon n + \frac{1}{2}q})$$

$e(g,m)$ for $m > g/6$: Fix m such that $g/6 < m < g/3$ (and $m \neq g/4, g/5$). Let $s := [(g+2)/3] - m$. This time, we shall only regard "small" m-admissible sets X, i.e. such that $m \in X \subseteq \{m,\ldots,[(g-1)/3]\}$ and $g \notin S\langle X\rangle$. Then

$$e(g,m) = \sum_X e(g,m,X), \tag{19}$$

where $e(g,m,X) := \# Y \subseteq B$, such that $g \notin S\langle X \cup Y\rangle$ and that $S\langle X \cup Y\rangle \cap B = Y$. (This clearly is equivalent to $X \cup Y$ being a *general* m-admissible set; cf. lemma 2 (iii).) Now, let $e(g,m,q) := \sum_{|2X|=q} e(g,m,X)$ for $q = 1,\ldots,2s-1$. Then

$$e(g,m) = \sum_{q=1}^{2s-1} e(g,m,q). \tag{20}$$

Let $\varepsilon > 0$, $\varepsilon < \lg(2/\sqrt{3}) = 1 - \frac{1}{2}\lg 3$ be given. By the main lemma there is a constant C such that for any fixed q we have

$$|\{\text{small } m\text{-admissible } X \text{ with } |2X| = q\}| \le$$
$$|\{\text{small } m\text{-admissible } X \text{ with } |2X| \le q\}| < C \cdot 2^{\varepsilon s} \cdot 2^{\frac{1}{2}q}.$$

Next, fix such an X (with $|2X| = q$) and let us estimate $e(g, m, X)$. The element m induces a structure of *undirected* graph on B, by the rule that there should be an edge between y and z ($y, z \in B$) iff $m + y + z = g$. These edges are disjoint. Their exact number depends on the residue class of g modulo 3 and on s, but there are not less than $(s-1)/2$ of them within B. They are unordered and 'antipathic', where the principal arrows analyzed above were ordered and 'sympathic': if $\{y, z\}$ forms an edge, then none or one but not both of y and z may be contained in a Y such that $g \notin S\langle X \cup Y\rangle$. Thus the effect of their presence is the same as for the principal arrows: they reduce the number of possibilities to $(3/4)^{\#\text{edges}}$ of the a priori number.

Let $D' := 2X \cap \{1, \ldots, a\}$, $D'' := g - (2X \setminus D')$. Then $D' \subseteq B$ (since $2m > g/3$), $D'' \subseteq B$, and for any Y as above, $D' \subseteq Y$ while $D'' \cap Y = \emptyset$. (In particular $D' \cap D'' = \emptyset$.) Thus Y is determined by $Y \cap C$ where $C := B \setminus (D' \cup D'')$; and as before we find that there are not less than $(s-1)/2 - |D' \cup D''| = (s-1)/2 - q$ edges in C. Thus

$$(21) \quad e(g,m,X) \leq 2^{|C|} \cdot \left(\frac{3}{4}\right)^{\frac{1}{2}(s-1)-q} = \sqrt{\frac{4}{3}} \cdot 2^b \cdot \left(\frac{2}{3}\right)^q \cdot \left(\frac{3}{4}\right)^{\frac{1}{2}s} \quad (m > g/6;\ |2X| = q).$$

Thus and by (20) and the main lemma

$$(22) \qquad e(g,m) < \left(\sum_{q \geq 1} \left(\frac{2}{3}\right)^q \cdot 2^{\frac{1}{2}q}\right) \cdot C \cdot 2^{\varepsilon s + \frac{1}{2}(\lg(3/4))s} \cdot 2^b,$$

where C only depends on ε. The sum over q is $C_1 := \sqrt{8}/(3 - \sqrt{8})$; and $C_2 := 2^{\varepsilon + \frac{1}{2}\lg(3/4)} < 1$ by the choice of ε. Thus indeed

$$(23) \qquad \sum_{(g/6) < m < (g/3)} e(g,m) < \sum_{s \geq 1} C_2^s \cdot C_1 C \cdot 2^b = C' \cdot 2^b$$

for some C' (which is independent of g).

$e(g,m)$ for $m < g/6$: Fix m; for $S \in \mathcal{M}_{g,m}$ let $X(S) := S \cap \{m, m+1, \ldots, 2m\}$; for $X \subset \{m, \ldots, 2m\}$ let $e'(g,m,X) := |\{S \in \mathcal{S}_{g,m} : X(S) = X\}|$; for $q = 3, 4, \ldots, 2m-1$ let $e(g,m,q) := \sum_{X : |2X| = q} e'(g,m,X)$; choose an ε with $0 < \varepsilon < 1 - 0.4 \lg 5$; and (by means of the main lemma) choose a C such that

$$(24) \qquad |\{X \subset \{m, \ldots, 2m\} : |2X| = q\}| < C \cdot 2^{\varepsilon m + \frac{1}{2}q} < C \cdot 2^{\varepsilon g/6 + \frac{1}{2}q}.$$

We have also

$$(25) \qquad e(g,m) = \sum_q e(g,m,q).$$

Fix q and X (with $|2X| = q$). We are trying to decide in how many ways we may extend $2X\setminus\{2m\}$ to a set $Z \subset \{2m+1,\ldots,a\}$ such that $g \notin S\langle X \cup Z\rangle$. Thus, let $r_i := \{j: 2m+1 \leq j \leq a \,\&\, j \equiv i(\operatorname{mod} m)\}$; $s_i := r_i \cap S$ (whenever S is chosen); $n := [g/m]\,(\geqq 6)$; and $r := g - mn$. As before, $r_1,\ldots,r_{r-1}$ and $r_{r+1},\ldots,r_{m-1}$ be the *lower* and the *upper* classes, respectively; and lower or upper class couples and singletons be as before.

If $\{r_i, r_j\}$ is a class couple, $x \in r_i$, and $y \in r_j$, then $x + y < g$ and $x + y \equiv g(\operatorname{mod} m)$; thus $x + y \notin S$. I.e., if $\{r_i, r_j\}$ is a class couple, then $s_i = \emptyset$ or $s_j = \emptyset$. Should e.g. $s_i \neq \emptyset$, then s_i is determined by $\min s_i \in r_i$. Thus

$$\#\,\text{possible}(s_i, s_j) \leq |r_i| + |r_j| + 1 = \begin{cases} n-2 & \text{if } \{r_i, r_j\} \text{ is lower} \\ n-3 & \text{if } \{r_i, r_j\} \text{ is upper} \end{cases}.$$

(If r_i is a singleton, then $s_i = \emptyset$.) Thus (ignoring the restrictions imposed by having fixed $2X$) we get an upper bound

$$(n-2)^{\frac{1}{2}r} \cdot (n-3)^{\frac{1}{2}(m-r)}$$

on $e'(g, m, X)$. Arguing as before (taking logarithms, etc.) yields

$$e'(g, m, X) \leq \left(\frac{g}{m} - 3\right)^{\frac{1}{2}m}.$$

The influence of the $2X$-elements may be estimated thus: Let $\{r_i, r_j\}$ be a class couple. Assume that $x \in 2X$ and that $x \equiv i(\operatorname{mod} m)$; then we must have $x = 2m + i$ or $x = 3m + i$. Thus $g/2 + m > 3m + i \in S$. If $y \in s_j$, then $g + m > y + 3m + i \equiv g(\operatorname{mod} m)$, whence $y \notin S$. Thus $s_j = \emptyset$ (even if $x \notin s_i$). Furthermore, if in addition $z \in 2X$ and $z \equiv j(\operatorname{mod} m)$, then we must have $x = 3m + i$, $z = 3m + j$, and $s_i = s_j = \emptyset$; while if $z \in 2X$, $z \equiv i(\operatorname{mod} m)$ and $z \neq x$, then $s_i = r_i$. To sum up, there are at most two $2X$-elements with remainders corresponding to a given class couple $\{r_i, r_j\}$, and *if* there are two such elemments, then they completely determine (s_i, s_j). If $\{r_i, r_j\}$ is a class couple with just one single element $x \in 2X$ which is congruent to i (and none congruent to j), then there may be one choice left: if $x > 3m$ then we may or we may may not have $x - m \in s_i$. There are at most four elements in $2X$ with zero or singleton remainders. Any other element will yield a reduction not "less" than $\max(2/(n-3), 1/2) \leq 2/3$, and we get

$$e'(g, m, X) < \left(\frac{2}{3}\right)^{q-4} \left(\frac{g}{m} - 3\right)^{\frac{1}{2}m},$$

whence by (24)

$$e(g, m, q) < \frac{81C}{16}\left(\frac{2\sqrt{2}}{3}\right)^{q} \cdot 2^{\varepsilon g/6} \cdot \left(\frac{g}{m} - 3\right)^{\frac{1}{2}m}.$$

Summing over q yields

$$e(g,m) < C''2^{\varepsilon g/6}\left(\frac{g}{m}-3\right)^{\frac{1}{2}m} \tag{26}$$

for some constant C''.

Now the continuous function $h(y) = \left(\frac{g}{y}-3\right)^{\frac{1}{2}y}$, $0 \leqq y \leqq g/6$, has a negative second derivative in the whole interval, and its firstderivative changes sign within the interval; thus h has a unique maximum, which in fact is attained for some y_0 such that $g/7.98 < y_0 < g/7.97$. In particular,

$$\left(\frac{g}{m}-3\right)^{\frac{1}{2}m} < \left(\frac{g}{g/8}-3\right)^{\frac{1}{2}g/7.5} = 5^{g/15} = 2^{(g/6)\cdot 0.4\lg 5}. \tag{27}$$

Thus and by (26)

$$\sum_{m<g/6} e(g,m) < \frac{C''g}{6}\cdot 2^{-C_3 g}\cdot 2^{g/6},$$

where $C_3 := \frac{1}{6}(1-0.4\lg 5-\varepsilon) > 0$, whence $\lim_{g\to\infty} g2^{-C_3 g} = 0$. Proposition 2 and the last inequality of the theorem follow.

PROOF OF PROPOSITION 1: By proposition 2, as g tends to infinity it is enough to investigate $f(g,m)$ and $e(g,m)$ for m being close to $g/2$ and to $g/3$, respectively. In particular, we may confine ourselves to $m > g/3$ and to $m > g/4$, respectively. For concreteness, consider

$$C(g) := \sum_{m>g/3} f(g,m)\cdot 2^{-g/2}, \quad g \text{ even},$$

as g tends to infinity. By lemma 1, the "upper" part of the sum (i.e. the "$m > \frac{1}{2}g$"-part) equals $2^{a-\frac{1}{2}g} = 2^{-1}$. In the "lower" cases, we found that for each m-admissible set X we had three conditions (a), (b), (c), which were translatable to a graph structure on a certain subset of A; and this graph structure completely determined the quantity $f(g,m,X)$. Now since $m > g/3$, all elements in $g - X$ are strictly smaller than the elements in $2X$. Therefore, if we put $g' := g+2$, $m' := m+1$, and $X' := X+1$, then the graph corresponding to $f(g',m',X')$ will be isomorphic to the graph corresponding to $f(g,m,X)$ *with one isolated vertex added*. Thus $f(g',m',X') = 2f(g,m,X)$, whence $f(g',m')\cdot 2^{-g'/2} = f(g,m)\cdot 2^{-g/2}$ and (using proposition 2) the existence of $\lim C(g)$ follows.

The case g odd and the $e(g)$-cases are similar. In the latter cases the graph-structures depend on $g \pmod 3$, while $b - g/6$ depends on $g \pmod 6$.

I.3. APPROXIMATE VALUES OF THE LIMITS. We have established the existence of the limits of proposition 1. In this section we consider the less important question: what might these limits be? Let us reformulate proposition 1 in terms of 2^a and 2^b, where as before

$$a = a(g) = [(g-1)/2], \quad \text{and}$$
$$b = b(g) = [(g-1)/2] - [g/3].$$

The proof of the proposition yields:

There are constants C_0, C_1, D_0, D_1 and D_2 such that

(28) $$\lim_{g \equiv i (\mathrm{mod}\ 2)} 2^{-a} f(g) = C_i \quad (i = 0, 1) \quad \textit{and}$$

(29) $$\lim_{g \equiv i (\mathrm{mod}\ 3)} 2^{-b} e(g) = D_i \quad (i = 0, 1, 2).$$

We also get methods for computing arbiitrarily good approximations for these constants:

(30) $$C_i = 1 + \sum_{s=1}^{\infty} c_{i,s}, \text{ and}$$

(31) $$D_i = 1 + \sum_{s=1}^{\infty} d_{i,s},$$

where $c_{i,s} = f(g, [(g+1)/2] - s) \cdot 2^{-a}$ for any g such that $(g/3) < [(g+1)/2] - s$ and that $g \equiv i (\mathrm{mod}\ 2)$, and $d_{i,s} = e(g, [(g+2)/3] - s) \cdot 2^{-b}$ for any g such that $(g/4) < [(g+2)/3] - s$ and that $g \equiv i (\mathrm{mod}\ 3)$.

Fixing i and s we may calculate $c_{i,s}$ as follows: Pick appropriate g and $m (= [g+1)/2] - s)$ with $c_{i,s} = f(g,m)2^{-a} = \sum_X f(g,m,X)$ (sum over m-admissible X). For any subset $T \subseteq \{1, \ldots, s-1\}$, let $X = X(T) := \{[(g+1)/2] - k: k \in T \cup \{s\}\}$; and let the directed graph $L = L(T) := A \setminus ((g - X) \cup 2X)$ with the arrows as introduced in section I.2. If (y_1, y_2) is an arrow in L we have $y_1 < g - [(g+1)/2] + s = [g/2] + s < 2([(g+1)/2] - s) < y_2$. Hence all elements in $g - X$ and all tails are $\leq g - m$, while all elements in $2X$ and all heads are $\geq 2m\,(g - m)$. Thus L consists of a bipartite graph $L' = L'(T)$ in disjoint union with $3m - g - 1 = a - 3s + i$ isolated vertices, where L' (up to isomorphisms) is independent of the choice of g; and we get:

$$f(g, m, X(T))2^{-a} = |\{\text{independent subsets of } L'\}| \cdot 2^{-3s+i}, \text{ whence}$$

$$c_{i,s} = \sum_T |\{\text{independent subsets of } L'(T)\}| \cdot 2^{-3s+i}.$$

By (13), $c_{i,s} \leq \frac{1}{4} \cdot \left(\frac{11}{12}\right)^{s-1}$. Thus, if we calculate $c_{i,1}, \ldots, c_{i,n}$ for some n, we find that

$$1 + \sum_{s=1}^{n} c_{i,s} < C_i \le 1 + \sum_{s=1}^{n} c_{i,s} + 3 \cdot \left(\frac{11}{12}\right)^n.$$

Choosing $n = 15$ and calculating (by computer) gave

$$\sum_{s}^{15} c_{0,s} = 1.472\ldots; \sum_{s}^{15} c_{1,s} = 1.502\ldots; \ 3 \cdot \left(\frac{11}{12}\right)^{15} = 0.813\ldots;$$

thus

(32) $$2.47 < c_0 < 3.3; \ 2.5 < c_1 < 3.32.$$

In particular,

$$\lim_{g \text{ even}} (S_g| \cdot 2^{-\frac{1}{2}g}) = \tfrac{1}{2} \cdot C_0 < \sqrt{\tfrac{1}{2}}\, C_1 = \lim_{g \text{ odd}} (|S_g| \cdot 2^{-\frac{1}{2}g}),$$

(Actually, we may get sharper results without increasing n, by employing non-principal arrows and more precise results than the crude inequality $|2X| \ge 2|X| - 1$. In this manner we may deduce that the value of the constants lie "fairly" close to the lower estimates given in (32).)

For the D_i's, the situation is slightly "better", but much "worse". "Better" in the sense that we may show the remaining middle inequality in the theorem directly, just by noting that the quantities $b(g) - g/6$ depend *strictly* on the residue class of g modulo 6, while D_* only depends on $g \pmod 3$. Thus e.g. $b(6g') - 6g'/6 = -1$, while $b(6g' + 3) - (6g' + 3)/6 = -\frac{1}{2}$, whence

$$\lim_{g \equiv 0 \pmod 6} 2^{-g/6} |\mathcal{M}_g| = \tfrac{1}{2} D_0 < \sqrt{\tfrac{1}{2}}\, D_0 = \lim_{g \equiv 3 \pmod 6} 2^{-g/6} |\mathcal{M}_g|.$$

On the other hand, although we may calculate any $d_{i,s}$ in a manner corresponding to the method above, and thus calculate any partial sum $\sum_{1}^{n} d_{i,s}$ of the sum in (31), we have no good estimate for the "tail" $\sum_{s=n+1}^{\infty} d_{i,s}$ of that sum. Indeed, we used the main lemma in order to ensure the convergence in (31); and, while realizations of the sought constants of that lemma may be deduced from its proof presented below, these yield ridicuously bad estimates for the *rate* of convergence in (32).

A computer calculation of $d_{0,s}$ for $s = 1, \ldots, 21$ is given in Table 1. It shows that $9.36 < D_0$. The marked diffferences between the odd and the even cases are due to the "extra" forbidden elements $g/6 + s/2$ for s even. Inspecting the table (taking this into account) makes it seem less likely that D_0 would not be less than (say) 15.

TABLE 1.

s	$d_{0,s}$ (exact)	$d_{0,s}$ ($\approx$)	accumulated sum
1	2/4	0.5	0.5
2	5/16	0.3125	0.8125
3	37/64	0.578125	1.390625
4	100/256	0.390625	1.78125
5	615/1024	0.60058593	2.3818359
6	1491/4096	0.36401367	2.7458496
7	10058/16384	0.61389160	3.3597412
8	25080/65536	0.38269042	3.7424316
9	154485/262144	0.58931350	4.3317451
10	347956/1048576	0.33183670	4.6635818
11	2275341/4194304	0.54248356	5.2060654
12	5617059/16777216	0.33480280	5.5408682
13	32932169/67108864	0.49072755	6.0315957
14	74146540/268435456	0.27621738	6.3078131
15	459815105/1073741824	0.42823618	6.7360493
16	1101432174/4294967296	0.25644716	6.9924964
17	6466239450/17179869184	0.37638467	7.3688811
18	14383614901/68719476736	0.20930914	7.5781903
19	88513143507/274877906944	0.32200893	7.9001992
20	205912251644/1099511627776	0.18727610	8.0874754
21	1202802586025/4398046511104	0.27348564	8.3609610

II. The main lemma.

II.1. STATEMENT. Recall that if A is a set then $|A|$ = number of elements in A; if A and B are sets of integers and c is an integer, then $A + B = \{a + b : a \in A \,\&\, b \in B\}$, $A + c = \{a + c : a \in A\}$, and $2A = A + A$; and if x is a real number, then $[x]$ denotes the integer part of x.

MAIN LEMMA. *Let ε be any given positive real number. Then there is a constant C such that for any positive integers n and q we have*

(33) $$K(n,q) := |\{X \subseteq \{1,2,\ldots,n\} : |2X| \leq q\}| < C \cdot 2^{\varepsilon n + \frac{1}{2}q}.$$

II.2. REMARKS.

1. We could as well have formulated the lemma for subsets of *any* fixed arithmetic sequence $\alpha + \beta, \alpha + 2\beta, \ldots, \alpha + n\beta$ of length n, by means of obvious

mappings; and, in fact, in this paper the lemma is indeed applied with this apparent generalization tacitly understood.

2. In some respects this lemma is close to optimal. Loosely spoken, if we fix n and let q vary (over $1,\ldots,2n-1$), then for any q we have that there are at least $2^{\frac{1}{2}q}$ subsets X of $\{1,\ldots,[(q+1)/2]\}$ (and of any other arithmetic subsequence of this length), and $|2X| \leq q$ for each such X. (Thus in particular $\sup_{n,q}(K(n,q)/2^{\varepsilon n+cq}) = \infty$ for $c < c + 2\varepsilon < \frac{1}{2}$.) On the other hand, for any given degree d we may fix a $q \geq \binom{d+2}{2}$ and let n grow; then, since if $|X| \leq d+1$ then $|2X| \leq \binom{d+2}{2}$, we get

$$K(n,q) > \binom{n}{d+1},$$

whence $K(n,q)$ grows faster than polynomially in n.

3. It would be very interesting to find explicit formulas or good approximations for the quantities

$$K(n,k,q) := |\{X \subseteq \{1,\ldots,n\} : |X| = k \;\&\; |2X| = q\}|.$$

(E.g. for $q < 3k-3$ fairly good results can be obtained by means of [1, thm. 1.9]; perhaps the weaker but quite general "fundamental theorem" [1, thm. 2.8] may yield good results in general.)

II.3. Proof. The lemma will be proved in the following, apparently weaker, formulation:

For any given positive ε there is a polynomial $p(x)$ (with real coefficients) such that for any positive integers n and q we have

$$K(n,q) \leq p(n)\cdot 2^{\varepsilon n + \frac{1}{2}q}. \tag{34}$$

Actually (33) for $\varepsilon = \varepsilon_1 > 0$ follows from (34), applied on some $\varepsilon = \varepsilon_2$, where $0 < \varepsilon_2 < \varepsilon_1$. Choose an $\varepsilon > 0$. For a while, fix an integer $m \geq 3/\varepsilon$. For any set A of integers, and for $i = 1, 2, \ldots, m$, let $A_i := \{j \in A : j \equiv i \pmod{m}\}$. We shall find upper bounds for the quantities

$$K^m(n,q) := |\{X \subseteq \{1,\ldots,n\} : |2X| \leq q \;\&\; X_i \neq \emptyset \quad \text{for} \quad i = 1,\ldots,m\}|.$$

$K^m(n,q) = 0$ if $m > n$, whence we subsequently assume $m \leq n$. Let α vary over the set of $2m$-tuples $(a_1, a_2, \ldots, a_m, b_1, \ldots, b_m)$ such that $a_i \equiv b_i \equiv i$ and $1 \leq a_i \leq b_i \leq n$ for $i = 1,\ldots,m$. There are less than n^{2m} such α; and clearly

$$K^m(n,q) = \left|\bigcup_{\alpha} \mathscr{V}(n,q,m,\alpha)\right|, \text{ where} \tag{35}$$

$\mathscr{V}(n,q,m,\alpha) := \{X \subseteq \{1,\ldots,n\} : |2X| \leq q \,\&\, (\min X_i = a_i \,\&\, \max X_i = b_i \text{ for } i = 1, \ldots, m)\}$. Fix such an $\alpha = (a_1,\ldots,b_m)$. Since $|2X| = \sum_{r=1}^{m} |(2X)_r|$, we have

$$\mathscr{V} := \mathscr{V}(n,q,m,\alpha) = \bigcup_{r=1}^{m} \mathscr{V}^r, \tag{36}$$

where $\mathscr{V}^r := \{X \in \mathscr{V} : |(2X)_r| \leq q/m\}$. Fix an $r \in \{1,\ldots,m\}$. Note that for any $i,j \in \{1,\ldots,m\}$ such that $i + j \equiv r \pmod m$ and for any $X \in \mathscr{V}^r$ we have

$$A_i(X) := (a_i + X_j) \cup (X_i + b_j) \subseteq X_i + X_j \subseteq (2X)_r.$$

Conversely, given such an $A_i(X) \subseteq (2X)_r$ we may reclaim X_j and X_i, since then $X_j = \{x - a_i : a_i + b_j \geq x \in A_i(X)\}$ and $X_i = \{x - b_j : a_i + b_j \leq x \in A_i(X)\}$. The set $\{1,\ldots,m\}$ may be partitioned into c pairs $p_\mu := (i_\mu, j_\mu)$ with $i_\mu < j_\mu$ and $i_\mu + j_\mu \equiv r$, and d "singletons" s_ν with $2s_\nu \equiv r$. By construction, $2c + d = m$. Furthermore, the family

$$\mathscr{F}(X) := (A_{i_1}(X), A_{i_2}(X), \ldots, A_{i_c}(X), A_{s_1}(X), \ldots, A_{s_d}(X))$$

is completely determined by and completely determines X.

Let $B(X) := \bigcup_{A \in \mathscr{F}(X)} A$; then $B(X) \subseteq (2X)_r \subseteq \{2,\ldots,2n-1\}_r$; and $|B(X)| \leq q/m$. Thus there are less than $2^{(2n/m)+1} \leq 2^{3n/m} \leq 2^{\varepsilon n}$ possible different sets $B = B(X)$. Fix such a B. For each $\mu = 1,\ldots,c$ there are less than $2^{q/m}$ possible different $A_{i_\mu}(X)$. Furthermore, if $k \in \{1,\ldots,m\}$ is a singleton, then let

$$D_k := \begin{cases} \{x \in B : x > a_k + b_k\} & \text{if this set has less than } q/2m \text{ elements} \\ \{x \in B : x < a_k + b_k\} & \text{else} \end{cases}.$$

Clearly $A_k(X) \cap D_k$ completely determines $X_k(X)$. Thus, for each $\nu = 1,\ldots,d$ there are at most $2^{|D_{j^\nu}|} < 2^{q/2m}$ possible $A_{j^\nu}(X)$ (with $B(X) = B$). Thus # possible $\mathscr{F}(X)$ where $B(X) = B$ is less than $2^{c \cdot q/m + d \cdot q/2m} = 2^{\frac{1}{2}q}$. Summing over the different possible $B(X)$ we get

$$|\mathscr{V}^r| = \#\,\text{possible } \mathscr{F}(X) < 2^{\varepsilon n + \frac{1}{2}q}. \tag{37}$$

Thus and by (35) and (36) we get

$$K^m(n,q) < n^{2m} \cdot m \cdot 2^{\varepsilon n + \frac{1}{2}q} \leqq n^{2m+1} \cdot 2^{\varepsilon n + \frac{1}{2}q}. \tag{38}$$

Next, as is well known, we may choose a finite number of pairwise relatively prime integers (e.g. primes) $m_1,\ldots,m_t$, say, such that $m_i \geqq 3/\varepsilon$ for $i = 1,\ldots,t$, and that

$$c := \prod_{i=1}^{t} \frac{m_i - 1}{m_i} \leqq \varepsilon. \tag{39}$$

We may choose them in such a way that $m_1 = \max_i m_i$. Furthermore, let

$$D := \prod_{i=1}^{t} m_i.$$

Fix n and q. For any $X \subseteq \{1, \ldots, n\}$ such that $|2X| \leq q$ one of the following statements must hold:

(A) *There is an m_i such that there are elements of X in all residue classes modulo m_i*;

or

(B) *There is a family $\mathcal{g} = (g_i)_{i=1}^{t}$ of integers, such that for $i = 1, \ldots, t$ we have $1 \leq g_i \leq m_i$ and $x \not\equiv g_i \pmod{m_i}$ for all $x \in X$.*

Clearly, the number of sets X fulfilling (A) does not exceed $\sum_i^t K^{m_i}(n, q) < t \cdot n^{2m_1+1} \cdot 2^{\varepsilon n + \frac{1}{2}q}$. Thus it is sufficient to get a good upper bound for the number of sets fulfilling (B). We shall do this for *all* subsets X of $\{1, \ldots, n\}$, relaxing the condition on $|2X|$.

For any family $\mathcal{g}$ as above, let

$$\mathcal{E}(\mathcal{g}) := \{X \subseteq \{1, \ldots, n\} : (\forall x \in X)(\forall i \in \{1, \ldots, t\})(x \not\equiv g_i \pmod{m_i})\}.$$

Then the number of X fulfilling (B) does not exceed $\sum_{\mathcal{g}} |\mathcal{E}(\mathcal{g})|$. There are D different families $\mathcal{g}$ of this kind. For any fixed $\mathcal{g}$ and any sequence $S = \{u + 1, u + 2, \ldots, u + D\}$ of D successive integers there are exactly cD elements $s \in S$ such that $s \not\equiv g_i \pmod{m_i}$ for all i. Hence

$$|\{s \in \{1, \ldots, n\} : (\forall i)(s \not\equiv g_i \pmod{m_i})\}| < cn + D \leq \varepsilon n + D,$$

whence $\sum_{\mathcal{g}} |\mathcal{E}(\mathcal{g})| < D \cdot 2^D \cdot 2^{\varepsilon n}$.

To sum up: For all n and q

$$I(n, q) < (t \cdot n^{2m_1+1} + D \cdot 2^D) \cdot 2^{\varepsilon n + \frac{1}{2}q}, \tag{40}$$

where t, m_1 and D are independent of n and q. (34) and thus the main lemma follow.

REFERENCES

1. G. A. Freĭman, *Foundations of a Structural Theory of Set Addition*, Transl. Math. Monographs 37, AMS, 1973.

2. R. Fröberg, C. Gottlieb, R. Häggkvist, *On numerical semigroups*, Semigroup Forum 35 (1987), 63–83.
3. H. S. Wilf, *Circle-of-lights algorithm for money-changing problem*, Amer. Math. Monthly 85 (1978), 562–565.

MATEMATISKA INSTITUTIONEN
STOCKHOLMS UNIVERSITET
BOX 6701
S-11385 STOCKHOLM
SWEDEN