On the Density of Sequences of Integers the Sum of No Two of Which is a Square II. General Sequences

J. C. Lagarias
A. M. Odlyzko
*J. B. Shearer**

AT&T Labs - Research
Murray Hill, NJ 07974

1. Introduction

P. Erdös and D. Silverman (see [4]) posed the problem of determining the maximal density attainable by a set $S = \{s_i\}$ of positive integers having the following property.

PROPERTY NS. $s_i + s_j$ *is not a perfect square for all* $i \neq j$.

J. P. Massias [8] observed that the set S_1 of integers consisting of all $x \equiv 1 \pmod 4$ together with all $x \equiv 14, 26, 30 \pmod{32}$ has property *NS* and density $\frac{11}{32}$. In a previous paper [6] we proved the following result. Let $d(S)$ denote the natural density of a sequence S.

Theorem A. Let S be a union of arithmetic progressions (mod N) having property NS. Then the density $d(S) \leq \frac{11}{32}$ *with equality possible only if* $32 | N$. *For all other N,* $d(S) \leq \frac{1}{3}$.

In this paper we bound the maximal upper asymptotic density

$$\overline{d}(S) = \limsup_{N \to \infty} \frac{1}{N} |S \cap [1,N]|$$

attainable for an arbitrary sequence S having property *NS*. It is easy to see that this density cannot exceed 1/2, for any square n^2 excludes ½ the positive integers smaller than n^2, since at most one element of each pair $(k, n^2 - k)$ can be in a set S having property *NS*, while for each $\varepsilon > 0$ there is a square between x and $(1+\varepsilon)x$ for all sufficiently large x.

Our main result applies to finite sets. Let S denote a finite set with all elements $\leq N$ which has property *NS*, and let

---

* Current address: University of California, Berkeley, CA 94720.

$$d(N) = \max_S \frac{|S|}{N} \tag{1.1}$$

denote the maximum density of such a set in $[1,N]$. Our main result is the following.

Theorem B. There exists an absolute constant N_0 such that for all $N \geq N_0$,

$$d(N) \leq .475. \tag{1.2}$$

Theorem B is proved using the Hardy-Littlewood circle method, based on an idea used in [6]. It immediately implies that the upper asymptotic density $\overline{d}(S)$ of an infinite sequence having property *NS* must satisfy

$$\overline{d}(S) \leq .475. \tag{1.3}$$

The bound (1.2) can be improved by extending the methods used in this paper, but we see no hope of attaining an upper bound near to $\frac{11}{32}$ without some new ideas. (In fact, it may well be that sequences with $\overline{d}(S) > \frac{11}{32}$ exist.)

The methods of this paper also apply to the analogous problem of bounding the maximal density attainable by a sequence $S = \{s_i\}$ of positive integers having the following property.

Property NP(k). $s_i + s_j$ is not a perfect k^{th} power for all $i \neq j$.

For $k = p-1$ where p is an odd prime the set $S_p = \{x : x \equiv i \text{ (mod p)}, 1 \leq i \leq \frac{p-1}{2}\}$ has property $NP(k)$, since $x^k \equiv 0$ or 1 (mod p) for all x. S_p has density $\frac{1}{2} - \frac{1}{2p}$. By an adaptation of the method of this paper it can be shown that for any sequence S with Property $NP(k)$,

$$\overline{d}(S) \leq \frac{1}{2} - c_0(k),$$

where $c_0(k)$ is a positive absolute constant depending on k.

It is interesting to note that the density behavior of sets having property *NS* differs completely from that of sets S having the following property

Property DS. $s_i - s_j$ is not a perfect square whenever $i \neq j$.

Sárközy [9] has shown that any sequence having property *DS* must have density zero; he shows the

number of elements $\le x$ in such a set is $O\left(\frac{x\ (\log\log\ x)^{2/3}}{(\log\ x)^{1/3}}\right)$.

In another related direction, Erdös [3] has proposed the following problem: Given a sequence $n_1 < n_2 <...$ of positive integers with $n_{i+1}/n_i \to 1$ as $i \to \infty$, and such that the n_i are uniformly distributed modulo d for every d, does it follow that if $S = \{s_i\}$ is an infinite sequence of positive integers for which $s_j + s_k \neq n_i$ for all i,j,k, then $\overline{d}(S) < \frac{1}{2}$?

2. Proof of the Main Theorem

In this section we prove Theorem B assuming certain results proved by the circle method in later sections.

Proof of Theorem B. Let S be a subset of $[1,N]$ having Property *NS*. We wish to bound $|S|$ from above. Let $G^*(N)$ denote the graph having N vertices labelled 1 through N, and in which $\{i,j\}$ is an edge if and only if

$$i + j = k^2 \tag{2.1}$$

for some integer k. Note that $G^*(N)$ contains loops at those vertices i with $i = \frac{1}{2}\ k^2$. If $\alpha^*(N)$ denotes the independence number of the graph $G^*(N)$ then

$$d(N) \le \frac{\alpha^*(N)}{N} + N^{-1/2}\ , \tag{2.2}$$

since if $S \subseteq [1,N]$ has Property NS, it consists of an independent set in $G^*(N)$ plus some integers j such that $2j = k^2$, and there can only be $\le N^{1/2}$ of those. Thus the problem is that of bounding the independence number of $G^*(N)$.

We may compare $G^*(N)$ with the graph $G(N)$ of [6], in which $\{i,j\}$ was an edge if and only if

$$i + j \equiv k^2 \qquad (\text{mod N}).$$

All edges of $G^*(N)$ are edges of $G(N)$, but $G^*(N)$ has $O(N^{3/2})$ edges, while for any $\varepsilon > 0$ and all $N > N_0(\varepsilon)$, $G(N)$ has at least $N^{2-\varepsilon}$ edges. In [6] we showed the independence number $\alpha(N)$ of $G(N)$ satisfies $\alpha(N) \le \frac{11}{32}N$. We may expect a weaker bound here since $G^*(N)$ has many fewer edges than $G(N)$ and hence, presumably, a larger independence number.

As in [6] we view the problem of calculating the independence number $\alpha(G)$ of a graph G as that of solving the following $0-1$ integer programming problem: Maximize

$$Z = \sum_{i=1}^{n} x_i \tag{2.3}$$

subject to

$$x_i + x_j \leq 1, \tag{2.4}$$

if $\{i,j\}$ is an edge of G. We will obtain an upper bound for (2.3) by first replacing the constraints (2.4) with a set of weaker constraints implied by (2.4), and second by treating the resulting program as a linear program with the added constraints

$$0 \leq x_i \leq 1 \ , \tag{2.5}$$

for all i.

The weaker constraints we consider are obtained as follows. If H is a subgraph of G the constraints (2.4) for G imply

$$\sum_{i \in V(H)} x_i \leq \alpha(H) \ , \tag{2.6}$$

where $V(H)$ is the set of vertices of H. For example, if H is a $(2s+1)$-cycle, then $\alpha(H) = s$. We will use a subset of the constraints

$$\sum_{i \in V(C_{2s+1})} x_i \leq s \ , \tag{2.7}$$

where C_{2s+1} is any $(2s+1)$-cycle in $G^*(N)$.

We can produce a large number of explicit $(2s+1)$-cycles in $G^*(N)$ using simple identities involving sums of squares. Let $y_0,\ldots,y_{2s}$ be $2s+1$ integers such that

$$\sum_{i=0}^{2s} y_i \equiv 0 \qquad (\text{mod } 2) \ . \tag{2.8}$$

For $0 \leq k \leq 2s$ set

$$2n_k = \sum_{i=0}^{2s} (-1)^i \ y_{k+i+1}^2 \tag{2.9}$$

where the subscripts on the y_{k+i+1} are interpreted (mod $2s+1$). The congruence (2.8) is a necessary and sufficient condition that all the n_k be integers. A calculation shows that

$$n_k + n_{k+1} = y_{k+1}^2 \tag{2.10}$$

for $0 \le k \le 2s-1$, and that

$$n_0 + n_{2s} = y_0^2 \ . \tag{2.11}$$

Consequently if all the n_k's are positive then $(n_0,n_1,\ldots,n_{2s})$ is a $(2s+1)$-cycle in $G^*(N)$. We label this cycle $C(y_0,y_1,\ldots,y_{2s})$. A sufficient condition to guarantee that all of $(n_0,n_1,\ldots,n_{2s})$ be positive is that all the y_i be nearly equal in size. Such a condition is given by

$$(1-\varepsilon)\ M \le y_i \le M, \quad 0 \le i \le 2s \ , \tag{2.12}$$

for any $M > 0$ and any ε with

$$0 < \varepsilon < \frac{1}{s+1} \ . \tag{2.13}$$

To see this, we note that (2.9), (2.12), and (2.13) imply

$$2n_k > (s+1)\ (1-\varepsilon)\ M - sM \ge 0 \ .$$

Next note that the constraint (2.7) corresponding to $C(y_0,y_1,\ldots,y_{2s})$ is

$$\sum_{k=0}^{2s} x_{n_k} \le s \ . \tag{2.14}$$

We now consider the linear program L_s having the objective function (2.3) and the constraints (2.5) and (2.14) for all $C(y_0,\ldots,y_{2s})$ satisfying (2.12), for a *fixed* value of s. Let $\mathbf{y} = (y_0,\ldots,y_{2s})$. If we add up the constraints $C(\mathbf{y})$ in (2.14) weighted with nonnegative weights $w(\mathbf{y})$ we obtain

$$\begin{aligned} \sum_{n=1}^{N} r(n)\ x_n &= \sum_{\mathbf{y}} w(\mathbf{y}) \left[\sum_{k=0}^{2s} x_{n_k} \right] \\ &\le s \left[\sum_{\mathbf{y}} w(\mathbf{y}) \right] \ , \end{aligned} \tag{2.15}$$

where

$$r(n) = \sum_{\mathbf{y}} m_n(\mathbf{y})\ w(\mathbf{y}) \ , \tag{2.16}$$

and $m_n(\mathbf{y})$ is the number of times n occurs as a component in the vector $(n_0,\ldots,n_{2s})$ corresponding to $\mathbf{y}$ via (2.9). Note that we have the identity

$$\sum_{n=1}^{N} r(n) = (2s+1) \sum_{\mathbf{y}} w(\mathbf{y}) \ , \tag{2.17}$$

since each $\mathbf{y}$ produces a vector of $2s+1$ n_j's. If we can find nonnegative weights $w(\mathbf{y})$ such that (2.16) gives

$$r(n) \geq 1, \qquad 1 \leq n \leq N, \tag{2.18}$$

then

$$\begin{aligned} Z &\leq \sum_{n=1}^{N} r(n)\ x_j \\ &\leq s(\sum_{y} w(\mathbf{y})) \\ &\leq \frac{s}{2s+1} \left[\sum_{n=1}^{N} r(n)\right] \end{aligned} \tag{2.19}$$

using (2.15) and (2.17). If furthermore

$$r(j) \leq \mu, \qquad 1 \leq j \leq N, \tag{2.20}$$

we obtain the upper bound

$$Z \leq \frac{s}{2s+1}\ \mu\ N\ , \tag{2.21}$$

i.e., $d(N) \leq \frac{s}{2s+1}\ \mu$. In linear programming terms the $w(\mathbf{y})$ are dual variables and (2.18) are the conditions that the $w(\mathbf{y})$'s be a dual feasible solution. Dual feasible solutions always provide an upper bound on the primal problem's objective function, which in this case is (2.19).

We have now transformed the problem to that of finding a "good" choice of the nonnegative weights $w(\mathbf{y})$ so as to make all the $r(j)$ nearly equal as given by (2.18) and (2.20). Now the formula (2.16) for $r(j)$ shows that it is a weighted sum over those $\mathbf{y}$ such that

$$2n\ =\ \sum_{i=0}^{2s} (-1)^i\ y_i^2\ , \tag{2.22}$$

for some k, i.e., over representations of $2n$ by the indefinite diagonal quadratic form

$$Q(\mathbf{z})\ =\ \sum_{i=0}^{2s} (-1)^i\ z_i^2\ . \tag{2.23}$$

We can count the number of weighted integral representations of such a form satisfying certain side conditions using the Hardy-Littlewood circle method. Let $r^*_{M,\varepsilon}(2n)$ denote the number of ordered $(2s+1)$-triples of integers $\mathbf{z}\ =\ (z_0, z_1, \ldots, z_{2s})$ such that $2n\ =\ Q(\mathbf{z})$ and

$$(1-\varepsilon)M \leq z_i \leq M \tag{2.24}$$

for $0 \leq i \leq 2s$, and such that all the z_i are distinct. Using the circle method, in Section 3 we will prove the following result.

Theorem C. Let $s \geq 2$, and suppose $0 < \varepsilon < \frac{1}{4(s+1)}$. There is a constant $\delta' > 0$ such that

$$r^{*}_{M,\varepsilon}(2n) = M^{2s-1}\, G_s(2n)\, f(\frac{2n}{M^2}) + O(M^{2s-1-\delta'}) , \qquad (2.25)$$

where the O-constant depends on s and ε, but not on n and M. Here:

(i) *For all positive integers n, $G_s(2n)$ satisfies*

$$c_1(s) \geq G_s(2n) \geq c_0(s) \qquad (2.26)$$

for certain constants $c_1(s)$ and $c_0(s)$.

(ii) *$f(t)$ is a continuously differentiable function which is nonnegative and not identically zero. It vanishes outside the interval $I_{\varepsilon,s}$ given by*

$$1 - 2(s+1)\varepsilon + (s+1)\varepsilon^2 \leq t \leq 1 + 2s\varepsilon - s\varepsilon^2 . \qquad (2.27)$$

In this theorem $G_s(2n)$ is the *singular series*; it is defined by (3.18) below. The proof of Theorem C shows that we can take $\delta' = \frac{1}{12}$, a constant independent of M, s, and ε. In addition we note that the conditions on ε and s insure that

$$I_{\varepsilon,s} \subseteq [\frac{1}{2}, 2] .$$

The constant $c_0(s)$ is strictly positive for $s \geq 2$, as will be seen in Section 4.

We can use Theorem C to obtain weights $w(\mathbf{y})$ so as to obtain $r(n) \approx r_{M,\varepsilon}(2n)$. However $r_{M,\varepsilon}(n)$ fluctuates greatly in size in the interval $0 \leq n \leq N$ due to the term $f(\frac{n}{M^2})$. We damp out these fluctuations by choosing weights that involve a further averaging over the parameter M. We first set

$$w(\mathbf{y},M) = M^{-2s} \qquad (2.28)$$

provided that

$$M(1-\varepsilon) \leq y_i \leq M, \quad 0 \leq i \leq 2s, \qquad (2.29)$$

and that all the y_i are distinct. Otherwise we set $w(\mathbf{y},M) = 0$. Our choice of weights is

$$w(\mathbf{y}) = \sum_{M}{}' w(\mathbf{y},M) , \qquad (2.29)$$

where the prime in this and later summations indicates it is over all integers M in the range

$$\varepsilon \sqrt{N} < M < (3-\varepsilon) \sqrt{N}. \qquad (2.30)$$

Lemma 2.1. For $s \geq 2$ and the choice of weights $w(\mathbf{y})$ given by (2.29), (2,30), there are positive constants c_2 and δ'' such that

$$r(n) = c_2\ G_s(2n) + O(N^{-\delta''}) \tag{2.31}$$

for $\varepsilon N < n < (1-\varepsilon) N$. In any case

$$r(n) \leq c_2 G_s(2n) + O(N^{-\delta''}) \tag{2.32}$$

for $1 \leq n \leq N$. The O-symbol constants depend on s and ε, but not N.

Proof. Recall $Q(\mathbf{y}) = \sum_{i=0}^{s} (-1)^i y_i^2$ and let

$$\begin{aligned} w^*(2n) &= \sum_{\mathbf{y}}{}' \ w(\mathbf{y}) \\ &= \sum_{M}{}' \sum_{\substack{\mathbf{y} \\ Q(\mathbf{y})=2n}} w(y, M) \\ &= \sum_{M}{}' M^{-2s}\ r^*_{M,\varepsilon}\ (2n) \\ &= \sum_{M}{}' \{M^{-1}\ G_s(2n)\ f(\frac{2n}{M^2}) + O(M^{-1-\delta'})\} \\ &= \sum_{M}{}' M^{-1}\ G_s(2n)\ f(\frac{2n}{M^2}) + O((\varepsilon\sqrt{N})^{-\delta'}) \end{aligned} \tag{2,33}$$

using Theorem C. Since $\varepsilon > 0$ is fixed, we can replace the error term in (2.33) by $O(M^{-\frac{1}{2}\delta'})$. Now

$$\sum_{M}{}' M^{-1}\ f(\frac{2n}{M^2}) = \int_{\varepsilon\sqrt{N}}^{(3-\varepsilon)\sqrt{N}} t^{-1}\ f(\frac{2n}{t^2})\, dt + O(N^{-\frac{1}{2}}), \tag{2.34}$$

using

$$|f'(t)| \leq K_0(\varepsilon, s)\ , \quad t\ \varepsilon\ (-\infty, \infty)\ .$$

The change of variables $u = \frac{t}{\sqrt{2n}}$ yields

$$\sum_{M}{}' M^{-1}\ f(\frac{2n}{M^2}) = \int_{\varepsilon\sqrt{\frac{N}{2n}}}^{(3-\varepsilon)\sqrt{\frac{N}{2n}}} u^{-1}\ f(u^{-2})\, du + O(N^{-\frac{1}{2}}). \tag{2.35}$$

For $\varepsilon\ N \le n \le (1-\varepsilon)\ N$, the range of integration in (2.35) includes $[\frac{1}{2},\ 2]$, hence using Theorem C (ii) we have

$$\sum_M{}' M^{-1}\ f(\frac{2n}{M^2}) = c_3 + O(N^{-\frac{1}{2}}), \tag{2.36}$$

where

$$c_3 = \int_{1/2}^{2} u^{-1}\ f(u^{-2})\ du.$$

Then (2.33) and (2.36) yield

$$w^*(2n) = c_3\ G_s(2n) + O(M^{-\delta''}), \tag{2.37}$$

with $\delta'' = \min(\frac{1}{2}\delta',\ \frac{1}{2})$, for n in the range $\varepsilon\ N \le n \le (1-\varepsilon)\ N$, and

$$w^*(2n) \le c_3\ G_s(2n) + O(N^{-\delta''}) \tag{2.38}$$

for $1 \le n \le N$.

A counting argument now shows that

$$r(n) = (2s+1)\ w^*(2n)\ . \tag{2.39}$$

To prove (2.39), let σ_i be the cyclic permutation acting on y by

$$\sigma_i(y_j) = y_{i+j}\ ,$$

where subscripts are interpreted (mod $2s+1$). Note that the definitions (2.28)-(2.30) guarantee that

$$w(\sigma_i(\mathbf{y})) = w(\mathbf{y}) \tag{2.40}$$

for all σ_i, $0 \le i \le 2s$. The condition that $\mathbf{y}$ has distinct coordinates implies that

$$\sigma_i(\mathbf{y}) \ne \mathbf{y} \tag{2.41}$$

for $0 \le i \le 2s$. Now each $w(\mathbf{y})$ weights $2s+1$ n_i's, (see (2.9)) but only the weights corresponding to n_0's are counted in $w^*(n)$. The permutation σ_i sends $\mathbf{y}$ to $\sigma_i(\mathbf{y})$, and $n_0(\sigma_i(\mathbf{y})) = n_i(\mathbf{y})$. This gives a one-to-$(2s+1)$ weight-preserving map (by (2.40)) from the set $\{(\mathbf{y},\ n_0(\mathbf{y}))\ |\ \text{all } \mathbf{y}\}$ *onto* $\{(\mathbf{y},\ n_i(\mathbf{y}))\ |\ \text{all } \mathbf{y},\ 0 \le i \le 2s\}$, which proves (2.39).

The lemma follows from (2.37)-(2.39), with $c_2 = c_3(2s+1)$. □

Lemma 2.1 shows that the choice of weights (2.29) has eliminated almost all fluctuations in the resulting $r(n)$, except those due to the singular series. By increasing s we can reduce the fluctuations in the singular series given by (2.26). In Lemma 4.3 we prove that for $s = 7$ and all n,

$$1.0085 \geq G_7(n) \geq 0.9915. \tag{2.42}$$

Now choosing $s = 7$ and applying (2.42) with Lemma 2.1 and (2.19), we obtain

$$\begin{aligned} 0.9915\ c_2 Z &\leq \sum_{n=1}^{N} c_2\ G_7(2n)\ x_n \\ &\leq \sum_{n=1}^{N} r(n) x_n + 1.0085\ c_2(2\varepsilon N) + O(N^{1-\delta'}) \\ &\leq \frac{7}{15}\left[\sum_{n=1}^{N} r(n)\right] + 1.0085 c_2(2\varepsilon N) + O(N^{1-\delta'}) \\ &\leq \frac{7}{15}\ c_2\left[\sum_{n=1}^{N} G_7(2n)\right] + 2.017\ c_2\varepsilon N + O(N^{1-\delta'}) \\ &\leq c_2(1.0085)\left(\frac{7}{15} + 2\varepsilon\right)N + O(N^{1-\delta'}) \quad . \end{aligned} \tag{2.43}$$

The term $2.017\ c_2\varepsilon N$ arises from n in the intervals $[0, \varepsilon N]$ and $[(1-\varepsilon)N, N]$ where (2.32) was used. Choosing $\varepsilon = .0001 < \frac{1}{4(s+1)}$ and dividing by c_2, we obtain

$$Z \leq .4747\ N + O(N^{1-\delta'}).$$

For sufficiently large $N > N_0$ it follows that

$$Z \leq .475\ N, \tag{2.44}$$

the desired result. □

Remark. There are a number of ways to improve the above bound. For example, it is easy to see that

$$\sum_{n=1}^{N} G_s(2n) = N + O(N).$$

If we used this in the inequalities leading to (2.43) instead of (2.42) we would obtain

$$Z < .4707\ N.$$

Further improvements are possible because $G_s(2n)$ depends largely on the residue classes of $2n$ modulo small prime powers, and so cannot be close to its lower bound too often. To get substantial improvements, however, we would need to take s much smaller than 7. (The circle method as we use it here works only for $s \geq 2$, but since we only need results that hold for most values of n, rather than all n, we could modify the method to work for $s=1$ as well.) For small s, however, the $G_s(2n)$ factors oscillate wildly, and to smooth out the oscillations we would need to consider weights $w(\mathbf{y},M)$ that depend on the congruence properties of $y_0,\ldots,y_{2s}$. This can be carried out (cf. [7]), but the proofs are quite cumbersome, and since it seems that they would not yield a bound close to $\frac{11}{32}\ N$, we have not pursued this subject further.

3. Application of the circle method

In this section we prove Theorem C following a version of the circle method incorporating improvements of I. M. Vinogradov, which is described in Davenport [2, pp. 9-48]. Since this proof is a relatively routine variant of the circle method, we shall only sketch the details.

Proof of Theorem C. We shall first estimate the number of representations $r_{M,\varepsilon}(n)$ of $(y_0,\ldots,y_{2s})$ of

$$n = \sum_{i=0}^{2s} (-1)^i y_i^2 \tag{3.1}$$

for which

$$(1-\varepsilon)M \leq y_i \leq M, \quad 0 \leq i \leq 2s, \tag{3.2}$$

where the y_i need not be distinct.

We suppose $s \geq 2$ and ε are fixed, $0 < \varepsilon < \frac{1}{4(s+1)}$. M will be a large variable integer, and we set $M_1 = [M(1-\varepsilon)]$.

The circle method involves study of the trigonometric sum

$$T(\alpha) = \sum_{x=M_1}^{M} e(\alpha x^2), \tag{3.3}$$

where

$$e(\alpha) = \exp(2\pi\alpha) .$$

Clearly we have

$$r_{M,\varepsilon}(n) = \int_0^1 T(\alpha)^{s+1} T(-\alpha)^s e(-n\alpha) d\alpha . \tag{3.4}$$

We estimate this integral by dividing the interval [0,1] into major and minor arcs. We take a parameter δ, to be chosen later, which satisfies $0 < \delta < \frac{1}{10}$, and define the major arcs $m_{a,q}$ to be the sets $m_{a,q}$ with $1 \le q \le M^{\delta}$ and $(a,q) = 1$, $1 \le a \le q$, where

$$m_{a,q} = \{\alpha: 0 \le \alpha < 1, \mid \alpha - \frac{a}{q} \mid < M^{-2+\delta}\} . \tag{3.5}$$

(We consider α modulo 1 here.) Let U denote the union of the major arcs and let V be its complement, the minor arcs.

We obtain the minor arcs estimate as in Davenport [2, p. 20]. (Note Davenport's s is our $2s+1$.)

Lemma 3.1. (Minor Arcs Estimate) We have

$$\int_V \mid T(\alpha) \mid^{s+1} \mid T(-\alpha)\mid^s d\alpha = O(M^{2s-1-\delta_1}), \tag{3.6}$$

for a fixed $\delta_1 > 0$ *depending on* δ.

An examination of Davenport's proof shows we may take $\delta_1 = \delta/2 + \eta$ for any fixed $\eta > 0$.

We next treat the major arcs. Analogously to [2, Lemma 4, p. 22] we obtain:

Lemma 3.2. Let $\alpha \in m_{a,q}$, *and set* $\beta = a/q - \alpha$. *We have*

$$T(\alpha) = q^{-1} S_{a,q} I(\beta) + O(M^{2\delta}) ,$$

where

$$S_{a,q} = \sum_{k=1}^{q} e(\frac{a}{q}k^2) \tag{3.7}$$

is a Gaussian sum, and where

$$I(\beta) = \int_{M_1}^{M} e(\beta t^2)\, dt.$$

Summing up over all the major arcs and making a change of variables leads to the following. (See [2, Lemma 5, p. 23])

Lemma 3.3. (Major Arcs Estimate). We have

$$\int_U T(\alpha)^{s+1}\ T(-\alpha)^s\ e(-n\alpha)\,d\alpha = M^{2s-1}\ G(n,\ M^\delta)\ J(n,M^\delta) + O(M^{2s-1-\delta_2})\ , \tag{3.8}$$

where $\delta_2 = 1-5\delta > 0$*, and where*

$$G(n,\ M^\delta) = \sum_{q\le M^\delta}\ \sum_{\substack{a=1\\(a,q)=1}}^{q} q^{-2s-1}\ |S_{a,q}|^{2s}\ S_{a,q}\ e(-\frac{na}{q}) \tag{3.9}$$

and

$$J(n,M^\delta) = \int_{|\gamma|<M^\delta} H(\gamma)^{s+1}\ H(-\gamma)^s\ e(-\frac{n\gamma}{M^2})\ d\gamma\ , \tag{3.10}$$

where

$$H(\gamma) = \int_{1-\varepsilon}^{1} e(\gamma t^2)\,dt\ . \tag{3.11}$$

We next approximate $J(n,M^\delta)$. We define

$$f(u) = \int_{-\infty}^{\infty} H(\gamma)^{s+1}\ H(-\gamma)^s\ e(-\gamma u)\ d\gamma\ . \tag{3.12}$$

This integral converges, since we have

$$H(\gamma) = O(|\gamma|^{-1}) \tag{3.13}$$

as $\gamma\to\infty$, a fact checked by letting $x = t^2$ in (3.11) and integrating by parts. Comparing (3.12) and (3.11) using the bound (3.13), absolute value estimates yield

$$J(n,\ M^\delta) = f(\frac{n}{M^2}) + O(M^{-2\delta s})\ . \tag{3.14}$$

We claim $f(u)$ is a real-valued nonnegative function which vanishes outside the interval $I = I_{s,\varepsilon}$ defined by

$$1-2(s+1)\varepsilon + (s+1)\varepsilon^2 \le u \le 1 + 2s\varepsilon - s\varepsilon^2\ . \tag{3.15}$$

To see this, we note using (3.11) that $H(\gamma)$ is the Fourier integral transform

$$H(\gamma) = \int_{-\infty}^{\infty} h(u)\ e(\gamma u)\ du$$

of

$$h(u) = \begin{cases} \frac{1}{2} u^{-\frac{1}{2}} & (1-\varepsilon)^2 \le u \le 1, \\ 0 & \text{elsewhere}, \end{cases} \tag{3.16}$$

and $H(-\gamma)$ the Fourier integral transform of $h^*(u) = h(-u)$. But (3.12) says $f(u)$ is the inverse Fourier integral transform of $H(\gamma)^{s+1} H(-\gamma)^s$, which implies that $f(u)$ is given by the repeated convolution

$$f(u) = [h_1(u) * \ldots * h_{s+1}(u)] * [h_{s+2}(u) * \ldots * h_{2s+1}(u)] , \tag{3.17}$$

where

$$h_i(u) = \begin{cases} h(u) & 1 \le i \le s+1, \\ h^*(u) & s+2 \le i \le 2s+1. \end{cases}$$

Using the definitions of $h(u)$ and $h^*(u)$, the expression (3.17) shows $f(u)$ is real and nonnegative, and that it vanishes outside the interval (3.15). The fact that $s \ge 2$ shows that $f(u)$ in (3.17) is continuously differentiable, since $h(u)$ and $h^*(u)$ are piecewise continuous.

We next approximate $G(n, M^{\delta})$ by the singular series $G_s(n)$ defined by

$$G_s(n) = \sum_{q=1}^{\infty} q^{-2s-1} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} |S_{a,q}|^{2s} S_{a,q} \, e(-\frac{na}{q}) , \tag{3.18}$$

provided this sum converges absolutely. Since $S_{a,q}$ is a Gaussian sum, we have

$$S_{a,q} = (\frac{a}{q}) S_{1,q}, \tag{3.19}$$

where $(\frac{a}{q})$ is the Jacobi symbol, and we can rewrite $G_s(n)$ as

$$G_s(n) = \sum_{q=1}^{\infty} q^{-2s} \, |S_{1,q}|^{2s} \, A_q(n), \tag{3.20}$$

where

$$A_q(n) = q^{-1} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} S_{a,q} \, e(-\frac{na}{q}) . \tag{3.21}$$

The quadratic Gaussian sum is explicitly evaluated to be (e.g., [1, Theorem 4.15]):

$$S_{1,q} = \begin{cases} (1+i)\sqrt{q} & q \equiv 0 \pmod 4, \\ \sqrt{q} & q \equiv 1 \pmod 4, \\ 0 & q \equiv 2 \pmod 4, \\ i\sqrt{q} & q \equiv 3 \pmod 4. \end{cases} \tag{3.22}$$

Hence

$$|S_{a,q}| \leq \sqrt{2q}.$$

Absolute value estimates show that

$$|A_q(n)| < \sqrt{2q}.$$

and hence that (3.18) converges for $s \geq 2$, and that for all n

$$|G_s(n)| < c_1(s) = 2^{s+1}\ \zeta(s - \frac{1}{2})\ . \tag{3.23}$$

Similar absolute value estimates give

$$G_s(n, M^{\delta}) = G_s(n) + O(2^{s+1} M^{-\delta(s-\frac{3}{2})})\ . \tag{3.24}$$

Combining lemmas 3.2 and 3.3 with (3.14), (3.23) and (3.24) we obtain for $s \geq 2$ that

$$r_{M,\varepsilon}(n) = M^{2s-1}\ G_s(n)\ f(\frac{n}{M^2}) + O(M^{2s-1-\delta'}), \tag{3.25}$$

where $\delta' = \min[2\delta s,\ \delta(s - \frac{3}{2}) + \eta,\ 1 - 5\delta,\ \frac{\delta}{2} + \eta]$ for any $\eta > 0$. We can choose $\delta' = \frac{1}{12}$ by taking δ slightly exceeding $\frac{1}{6}$. Here $G_s(n)$ and $f(x)$ satisfy (i), (ii) of Theorem C, by (3.15) and an earlier remark.

Theorem C will be proved if we show that for $s \geq 2$,

$$r^{*}_{M,\varepsilon}(n) = r_{M,\varepsilon}(n) + O(M^{2s-2+1/10}). \tag{3.26}$$

Let $r_{ij}(n)$ denote the number of solutions to (3.1), (3.2) with $y_i = y_j$, so that

$$r_{M,\varepsilon}(n) - r^{*}_{M,\varepsilon}(n) \leq \sum_{i=0}^{2s} \sum_{j \neq i} r_{ij}(n). \tag{3.27}$$

But $r_{ij}(n)$ is exactly the number of solutions to

$$Q_{ij}(\mathbf{y}) = n,$$

where Q_{ij} is a diagonal quadratic form in either $2s$ or $2s-1$ variables and all the variables satisfy

$$M(1-\varepsilon) \leq y_i \leq M.$$

If we now fix all but 2 of the variables, we will have $O(M^{\eta})$ solutions for each $\eta > 0$, which yields the desired result. □

4. The Singular Series

In this section we evaluate the singular series $G_s(n)$ in Theorem C, in order to obtain the bound (2.44). Again the method is standard, as in [2].

We first examine the expressions $A_q(n)$ given in (3.21).

Lemma 4.1. We have

$$A_q(n) = \frac{\phi(q)}{q} \sum_{x=1}^{q} \frac{\mu(\frac{q}{(q,x^2-n)})}{\phi(\frac{q}{(q,x^2-n)})} . \tag{4.1}$$

Moreover, $A_{q_1 q_2}(n) = A_{q_1}(n) A_{q_2}(n)$ *if* $(q_1, q_2) = 1$.

Proof. From (3.21) we obtain

$$\begin{aligned} A_q(n) &= q^{-1} \sum_{k=1}^{q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e(\frac{a}{q}(k^2-n)) \\ &= q^{-1} \sum_{k=1}^{q} c_q(k^2-n), \end{aligned} \tag{4.2}$$

where $c_q(m)$ is Ramanujan's sum. This sum can be evaluated explicitly [5, Theorem 272] as

$$c_q(m) = \mu(\frac{q}{d}) \frac{\phi(q)}{\phi(\frac{q}{d})}, \tag{4.3}$$

where $d = (q,m)$. This proves (4.1). The multiplicativity of $A_q(n)$ follows from the multiplicativity of $\mu(k)$ and $\phi(k)$. □

We can now represent $G_s(n)$ as an Euler product, using (3.20) and noting that $q^{-2s} \mid S_{1,q} \mid^{2s}$ is multiplicative. We obtain

$$G_s(n) = \prod_{p} (1 + \xi_p(n)) , \tag{4.4}$$

where the product is over all primes p, and where by (3.22) we find for odd p that

$$\xi_p(n) = \sum_{k=1}^{\infty} p^{-ks} A_{p^k}(n), \tag{4.5}$$

and that

$$\xi_2(n) = \sum_{k=1}^{\infty} 2^{-(k-1)s} A_{2^k}(n) .$$

The next step is to evaluate explicitly all the $A_{p^k}(n)$.

Lemma 4.2. If p is an odd prime then $A_p(n) = (\frac{n}{p})$ *and for* $k \geq 1$,

$$A_{p^{2k+1}}(n) = \begin{cases} \left(\frac{n/p^{2k}}{p}\right) p^k & \text{if} \quad p^{2k} | n, \\ 0 & \textit{otherwise}, \end{cases}$$

$$A_{p^{2k}}(n) = \begin{cases} p^{k-1}(p-1) & \text{if} \quad p^{2k} | n, \\ -p^{k-1} & \text{if} \quad (p^{2k}-1) \| n, \\ 0 & \textit{otherwise.} \end{cases}$$

If $p = 2$ *then* $A_2(n) = 0$ *and for* $k \geq 1$

$$A_{2^{2k+1}}(n) = \begin{cases} 2^k & \text{if} \quad n \equiv 2^{2k-2} \pmod{2^{2k+1}}, \\ -2^k & \text{if} \quad n \equiv 2^{2k} + 2^{2k-2} \pmod{2^{2k+1}}, \\ 0 & \textit{otherwise}, \end{cases}$$

$$A_{2^{2k}}(n) = \begin{cases} 2^{k-1} & \text{if} \quad n \equiv 0,\ 2^{2k-2} \pmod{2^{2k}}, \\ -2^{k-1} & \text{if} \quad n \equiv 2^{2k-1},\ 3.2^{2k-2} \pmod{2^{2k}}, \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. These are derived from (4.1). The only nonzero contributions to $A_q(n)$ for $q = p^k$ come from those x with $(q, x^2 - q) = q$ and $(q,\ x^2 - q) = p^{k-1}$, and so

$$A_{p^k}(n) = p^{-1}\{p\, A'_{p^k}(n) - A''_{p^k}(n)\}, \tag{4.6}$$

where

$$A_{p^k}'(n) = |\{x : 1 \le x \le p^k \ , \ x^2 \equiv n \ (mod \ p^k)\}|$$

$$A_{p^k}''(n) = |\{x : 1 \le x \le p^k \ , \ x^2 \equiv n \ (mod \ p^{k-1})\}|$$

Suppose p is odd. Then $A_p'(n) = 1,\ 2$ or 0 according as $p|n$, n is a quadratic residue (mod p), or n is a quadratic nonresidue (mod p), respectively. On the other hand $A_p''(n) = p$ in all cases. Hence $A_p(n) = (\frac{n}{p})$ using (4.6). We next treat $A_{p^2}(n)$. Here $A_{p^2}'(n) = p,0,2,0$ in the four cases $p^2|n$, $p||n$, $p\nmid n$ and $(\frac{n}{p}) = 1$, $p\nmid n$ and $(\frac{n}{p}) = -1$, respectively. Similarly $A_{p^3}''(n) = p,p,2p,0$. If $p^2 \nmid n$ then $A_{p^k}'(n) = A_{p^k}''(n) = 0$. If $p^2|n$, however, then

$$A_{p^k}'(n) = p\ A_{p^{k-1}}'(\frac{n}{p^2}),$$

$$A_{p^k}''(n) = p\ A_{p^{k-2}}'(\frac{n}{p^2}).$$

The lemma follows for odd p. The analysis for $q = 2^k$ is similar and is omitted. □

We now estimate $G_7(n)$. (Note that somewhat better estimates can be obtained by bounding $\xi_p(n)$ from above and below, instead of estimating $|\xi_p(n)|$)

Lemma 4.3. For all n,

$$1.0085 \ge G_7(n) \ge 0.9915. \tag{4.7}$$

Proof. Using Lemma 4.2, we have for odd p that

$$|A_{p^k}(n)| \le \begin{cases} p^{\frac{k}{2}-\frac{1}{2}} & \text{if } 2\nmid k, \\ p^{\frac{k}{2}} & \text{if } 2|k. \end{cases}$$

Applying this when $s = 7$ in (4.5) we obtain

$$|\xi_p(n)| \le \sum_{k=1}^{\infty} p^{-7(2k-1)+(k-1)} + \sum_{k=1}^{\infty} p^{-7(2k)+k}$$
$$= \frac{p^{-7}}{1-p^{-13}} + \frac{p^{-13}}{1-p^{-13}} = \frac{p^6 + 1}{p^{13} - 1}. \tag{4.8}$$

Also from Lemma 4.2,

$$A_{2^k}(n) \le \begin{cases} 2^{\frac{k}{2} - \frac{1}{2}} & \text{if } 2 \nmid k, \\ 2^{\frac{k}{2} - 1} & \text{if } 2 \mid k. \end{cases}$$

Hence using $A_2(n) = 0$ we obtain

$$|\xi_2(n)| \le \sum_{k=1}^{\infty} 2^{-7(2k)+k} + \sum_{k=1}^{\infty} p^{-7(2k-1)+(k-1)}$$
$$\le \frac{2^{-13}}{1-2^{-13}} + \frac{2^{-7}}{1-2^{-13}}$$
$$\le \frac{2^6+1}{2^{13}-1} . \tag{4.9}$$

Hence

$$G(n) \le \frac{8260}{8195} \prod_{\substack{p \\ p \ge 3}} \left[1 + \frac{p^6+1}{p^{13}-1}\right] \le 1.0085 ,$$

$$G(n) \ge \frac{8130}{8195} \prod_{\substack{p \\ p \ge 3}} \left[1 - \frac{p^6+1}{p^{13}-1}\right] \ge 0.9915 . \qquad (sq$$

References

[1] R. Ayoub, *An Introduction to the Analytic Theory of Numbers*, Mathematical Surveys No. 10, American Mathematical Society, Providence, R.I., 1965.

[2] H. Davenport, *Analytic methods for Diophantine equations and Diophantine inequalities,* Ann Arbor Press, Ann Arbor, Michigan 1962.

[3] P. Erdös, Problem 268, Problems from West Coast Number Theory Conferences, (R. Guy, Ed.).

[4] P. Erdös and R. L. Graham, *Old and New Problems and Results in Combinatorial Number Theory,* Monographie de l'Enseignement Mathematique No. 28, 1980.

[5] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers* (4th Edition), Oxford University Press 1960.

[6] J. C. Lagarias, A. M. Odlyzko and J. B. Shearer, On the density of sequences of integers no two of which sum to a square I. Arithmetic progressions. J. Combinatorial Theory, Series A, to appear.

[7] A. V. Malyshev, On the representation of integers by positive quadratic form (Russian), Trudy Mat. Inst. Steklov. *65* (1962), 212 pp.

[8] J. P. Massias, Sur les suites dont les sommes des termes 2 a 2 m sont par des carres, to be published.

[9] A. Sárközy, On difference sets of sequences of integers I. Acta Math. Acad. Sci. Hungar. *31* (1978), 125-149.

On the Density of Sequences of Integers the Sum of No Two of Which is a Square II. General Sequences

J. C. Lagarias
A. M. Odlyzko
*J. B. Shearer**

AT&T Labs - Research
Murray Hill, NJ 07974

ABSTRACT

This paper studies the maximal density attainable by a sequence S of positive integers having the property that the sum of any two distinct elements of S is never a square. It shows there is a constant N_0 such that for all $N \geq N_0$ any set $S \subseteq [1,N]$ having this property must have $|S| < .475N$. The proof uses the Hardy-Littlewood circle method.

* Current address: University of California, Berkeley, CA 94720.