THE SHNIREL'MAN-LINNIK APPROACH TO WARING'S PROBLEM

ALEXEY SPIRIDONOV

1. Introduction

In the late 18th century, Waring proposed a generalization of the four-squares theorem. This problem now bears his name. He conjectured that for any k, every natural number can be written as a sum of a uniformly bounded number of a_i^k, where $a_i \in \mathbb{N}_0$ (natural numbers with 0 added). Hilbert proved this fact in 1909 using hard techniques from analysis; several slightly simpler analytic proofs followed. In 1943, Yurij V. Linnik found an elementary (though involved) proof using Shnirel'man density. This paper will cover the main steps of his proof, with the exception of the upper bound on the representation function (counting how many ways there are of writing n as a sum of a fixed number of $f(x_i)$). We retell, with a few omissions, Chapter 11 of [1], modulo some attempts to improve the structure of the arguments.

2. Waring's Problem for Integer-Valued Polynomials

Linnik proved a generalization of Waring's problem; his result deals with arbitrary integer-valued polynomials, and not just x^k. An integer-valued polynomial is simply one that takes values from $\mathbb{Z}$ to $\mathbb{Z}$.

The coefficients of such a polynomial need not be integer. For instance, the binomial coefficient $\binom{x}{k}$ with $0 \leq k \leq x$ is a kth-degree polynomial $\frac{x(x-1)(x-2)...(x-k+1)}{k(k-1)(k-2)\cdots 3\cdot 2\cdot 1}$, with the leading coefficient $\frac{1}{k!}$. On the other hand, $\binom{x}{k}$ is the number of ways of choosing x items out of a labeled set of x, which is necessarily an integer. A useful fact (stated without proof) is that every integer-valued polynomial can be written as $\sum_{i=0}^{k} u_i \binom{x}{i}$ with u_i integer.

Given an integer-valued polynomial $f(x)$ with a positive leading coefficient, we consider its set of values $A(f) = \{f(n) | n \in N_0\}$. After some N, the highest-degree term dominates the others, and thereafter, for all $n \geq N$, $f(n)$ is a monotonically increasing sequence. Consider the polynomial $f_N(x) = f(x + N)$; it has the same degree and the same leading

coefficient (one sees this by expanding $(x+N)^k$). So, we can consider f_N instead of f, or simply assume that $\{f(n)\}_{i=0}^{\infty}$ is monotonically increasing.

Furthermore, suppose that $gcd(A(f)) \neq 1$, then we can divide through by it. Therefore, we assume without loss of generality that $gcd(A(f)) = 1$.

With these definitions, Waring's problem for polynomials asks if it is possible to write every natural number as the sum of at most $h(f)$ elements of $A(f)$, with $h(f)$ not dependent on n.

3. Shnirel'man Density and Bases

We want to establish a sufficient condition for being able to write every number in $\mathbb{N}$ as a sum of h numbers from smaller sets. This condition was discovered and proved by Shnirel'man, and, formulated informally, states: if a set has positive density in $\mathbb{N}$, then every $n \in \mathbb{N}$ is an h-term sum from this set (for some h). The rest of this section makes this statement precise, and then proves it.

Consider a set $A = \{a_i\}_{i=0}^{\infty} \subset \mathbb{Z}$. We will denote by $A(n)$ the number of elements of A that are natural numbers not exceeding n. We introduce two related concepts of density. The *Shnirel'man density* (density for short) is the least density of A within all of the sets $[1, n]$:

$$\sigma(A) = \inf\{\frac{A(n)}{n} : n \in \mathbb{N}\},$$

and the *lower asymptotic density* (lower density for short) is

$$d(A) = \liminf\{\frac{A(n)}{n} : n \in \mathbb{N}\}.$$

Both are clearly between 0 and 1. $\sigma(A)n \leq A(n)$ for any n, while $(d(A) - \epsilon)n \leq A(n)$ for any ϵ and large enough n. Note that in order to have positive density, a set must include 1, and contain a reasonably uniformly spaced subset of $\mathbb{N}$ (specifically, $\limsup a_{i+1} - a_i$ must be finite). The set of kth powers, which we would ultimately like to work with, quite clearly has zero density, as well as zero lower density. We handle this complication in §5.

Suppose that every natural number can be written as a sum of exactly h elements of A. Then, A a is basis of order h. A is a *basis (of finite order)* if there is some $h < \infty$ that makes A is a basis of order h. For instance, the four-squares theorem states that $\{i^2\}_{i=0}^{\infty}$ is a basis of order 4. Similarly, A is an *asymptotic basis of order* h if every sufficiently large natural number is a sum of h elements of A. An *asymptotic basis (of finite order)* is defined analogously.

If $d = \gcd(A) \neq 1$, A cannot be a basis (asymptotic or not); however, we can consider $A' = \frac{A}{d}$, which will still be a set of natural numbers. Then, A' is an (asymptotic) basis if, and only if, we can represent every (sufficiently large) number in $d\mathbb{N}$ as a sum of some h elements of A. Hence, we lose nothing by taking $d = 1$, and this is our assumption from now on.

We will often use the following notation: $A + B = \{a + b | a \in A, b \in B\}$; $hA = \underbrace{A + \cdots + A}_{h \text{ times}}$. For instance, "$A$ a basis of order h" is equivalent to $\mathbb{N} \in hA$.

4. Shnirel'man's Theorem

With the definitions of §3, we can precisely formulate the theorem we need:

Theorem 4.1. ***(Shnirel'man)*** *If A has positive density, and contains 0, it is a basis.*

We will spend the remainder of the section proving it; however, first we show a very useful consequence:

Corollary 4.2. *If B has positive lower density, and contains 0, it is an asymptotic basis.*

Proof. We know that for all $\epsilon > 0$, we have N such that for any $n > N$, the difference from the limiting density is small: $d(B) - \frac{B(n)}{n} < \epsilon$. We pick ϵ small, so that $d(B) > \epsilon$. The set $A = B \cup \{1\}$ therefore has positive density: for $n \leq N$, we have $\frac{A(n)}{n} \geq \frac{1}{N} > 0$, and otherwise, $\frac{A(n)}{n} > \frac{B(n)}{n} > d(B) - \epsilon > 0$.

By Shnirel'man's theorem, A is a basis of some order h; thus, every natural number is a sum of j ones and $h - j$ elements of B: $n = u + j$. Therefore, $u = n - j \in (h - j)B$, while the latter is in hB (since B contains 0). In other words, for every n, there is some $0 \leq j_n \leq h$ such that $n - j_n \in hB$.

$gcd(B) = 1$, so there is a finite subset B' with $gcd = 1$, and every large enough number (each $n > N$) can be written as a sum of elements of B'. In particular, the numbers $N, ..., N + h$ can all be written as a sum of at most h' elements of B'; hence they are in $h'B$. Suppose $n > N$; then, $n = N + j_{u_n} + u_n$, where $0 \leq j_{u_n} \leq h$, and so $N + j_{u_n} \in h'B$, while $u_n \in hB$ by construction. Putting the two together, $n \in (h + h')B$. □

The key step in proving Shnirel'man's theorem is showing a lower bound on the density of the sum of two sets.

Theorem 4.3. *If A and B contain 0, and have densities: $\sigma(A) = \alpha$, $\sigma(B) = \beta$, then*

$$\sigma(A + B) \geq \alpha + \beta - \alpha\beta.$$

Proof. Take the non-negative elements of A that do not exceed n, and order them so (there are $k = A(n)$ of them):

$$0 = a_0 < a_1 < a_2 < \cdots < a_{k-1} < a_k \leq n.$$

Analogously for B:

$$0 = b_0 < b_1 < b_2 < \cdots < b_{l-1} < b_l \leq n.$$

By abuse of notation, let $a_{k+1} = n + 1$; remember, however, that a_{k+1} needn't be in A or $A + B$. Now, consider the half-open interval $[a_i, a_{i+1})$, for $0 \leq i \leq k$. Of the elements of $A + B$ that fall in this gap, some have the form $a_i + b_j$. Of those, let $a_i + b_{r_i}$ be the largest sum that still lands in the interval. Observe that $r_i \geq 0$, because $b_0 = 0$. So, in all, we have (bold to emphasize the gaps):

$$\mathbf{a_0} \leq a_0+b_0 < a_0+b_1 < \cdots < a_0+b_{r_0} < \mathbf{a_1} \leq ... < \mathbf{a_k} \leq a_k+b_0 < \cdots < \mathbf{a_{k+1}}.$$

We can now compute the size of this subset of $A + B$, giving us a lower bound:

$$(A + B)(n) \geq \sum_{i=0}^{k}(1 + r_i) = A(n) + \sum_{i=0}^{k} r_i.$$

The r_i signify the number of b_j that are less than $a_{i+1} - a_i$, which we can write as $B(a_{i+1} - a_i - 1)$. Furthermore, we previously observed that $B(n) \geq \sigma(B)n = \beta n$; so, we have:

$$(A + B)(n) \geq A(n) + \sum_{i=0}^{k}(a_{i+1} - a_i - 1)\beta = A(n) - \beta k + \sum_{i=0}^{k}(a_{i+1} - a_i)\beta.$$

The sum telescopes, giving $A(n)(1 - \beta) + \beta(a_{k+1} - a_0) \geq \alpha n(1 - \beta) + \beta n$. Now we almost have the bound we want:

$$(A + B)(n) \geq \alpha n - \alpha\beta n + \beta n \Rightarrow \frac{(A + B)(n)}{n} \geq \alpha + \beta - \alpha\beta,$$

and it holds for all positive n. Finally, $\sigma(A + B) = \inf\{\frac{(A+B)}{n} | n \in \mathbb{N}\} \geq \alpha + \beta - \alpha\beta$, so we are done. □

Note that this theorem is equivalent to $1 - \sigma(A + B) \leq 1 - \alpha - \beta - \alpha\beta = (1 - \sigma(A))(1 - \sigma(B))$. This formulation of the result easily generalizes to multiple sums, since $A + B$ also contains 0.

Corollary 4.4. *Suppose that $A_1, \ldots, A_h$ are sets containing 0, with densities $\alpha_1, \ldots, \alpha_h$. Then,*

$$1 - \sigma(A_1 + \cdots + A_h) \leq \prod_{i=1}^{h}(1 - \alpha_i).$$

Proof. By induction on h; Theorem 4.3 gives the base case. Suppose the theorem holds for $h-1$; let $A = A_1 + \cdots + A_{h-1}$ and $B = A_h$. Then,

$$\begin{aligned} 1 - \sigma(A_1 + \cdots + A_h) = 1 - \sigma(A + B) &\leq (1 - \sigma(A))(1 - \alpha_h) \\ &\leq (1 - \alpha_h) \prod_{i=1}^{h-1}(1 - \alpha_i) = \prod_{i=1}^{h}(1 - \alpha_i). \end{aligned}$$

□

The lower bound we derived is not quite good enough – if we start with densities that are below 1, we have no chance of ever getting to 1. However, we can get as close to 1 as we like:

Lemma 4.5. *If A contains 0, and has positive density α, then for any $\epsilon > 0$ there exists h such that $1 - \sigma(hA) < \epsilon$.*

Proof. $1 - \sigma(hA) \leq \prod_{i=1}^{k}(1 - \alpha) = (1 - \alpha)^k$. By assumption, $1 - \alpha < 1$, and so, indeed, a desired h exists. □

To complete the proof of Schnirel'man's theorem, we will show that two sets of large densities (which we **can** get by the above) produce $\mathbb{N}$ when added together. We start with the following lemma.

Lemma 4.6. *If A and B contain 0, and satisfy $A(n) + B(n) \geq n$, then $n \in A + B$.*

Proof. If $n \in A \cup B$, we are done, since $0 \in A \cap B$. Otherwise, we may define the following new sets:

$$A' = \{n - a | 1 \leq a \leq n - 1, a \in A\}$$

$$B' = B \cap [1, n - 1]$$

All the $n - a$ entering A' are distinct, since $n \notin A$; therefore, $|A'| = A(n)$. Similarly, $|B'| = B(n)$. Both A and B are in the range $[1, n-1]$, but there are $|A'| + |B'| = A(n) + B(n) \geq n$ elements to go around. By Dirichlet's principle, the two sets have at least one common element, so $n - a = b$, with $a \in A$, $b \in B$, and hence $n = a + b \in A + B$. □

This has an immediate consequence in terms of densities:

Lemma 4.7. *If A and B contain 0, and have densities such that $\sigma(A) + \sigma(B) \geq 1$, then $\mathbb{N} \in A + B$.*

Proof. For $n \geq 1$,

$$A(n) + B(n) \geq (\sigma(A) + \sigma(B))n \geq n,$$

so, by Lemma 4.6, $n \in A + B$. Hence, $\mathbb{N} \in A + B$. □

We can now prove Shnirel'man's Theorem. Suppose that $0 \in A$ and $\sigma(A) > 0$. If we set $\epsilon < \frac{1}{2}$ in Lemma 4.5, we get h such that hA has density $> \frac{1}{2}$. Then, by Lemma 4.7, $hA + hA = 2hA$ has density 1, completing the proof.

5. Proving Waring's Theorem

We start with an integer-valued polynomial $f(x)$, as introduced in §2. It gives rise to $A(f) = \{f(i)\}_{i=0}^{\infty}$. We assume that $gcd(A(f)) = 1$. Our goal is to show that $A = A(f) \cup \{0\}$ is an asymptotic basis. To do this, we will use the corollary to Shnirel'man's theorem, and thus need to demonstrate that hA has positive lower density for some h.

The trick will be to produce a lower bound for $\frac{(hA)(n)}{n}$ by getting it to show up in an asymptotic expression of the form $X \ll Y \ll \frac{(hA)(n)}{n} X$. Then, the main questions are: what are the quantities X and Y, and how will we define h?

To answer the first question, we will be bounding so-called representation functions ("#" henceforth denotes the number of s-tuples that satisfy the corresponding equation):

$$r_{f,s}(n) = \#\{x_1, \ldots x_s \in N_0 | \sum_{i=1}^{s} f(x_i) = n\}$$

denoting the number of ways of representing n as a sum of at most s values of f. The cumulative number,

$$R_{f,s}(N) = \sum_{n=0}^{N} r_{f,s}(n),$$

is the quantity we will be estimating.

Lemma 5.1. *Suppose $f(x) = \sum_{i=0}^{k} a_i x^i$ is an integer-valued polynomial with $a_k > 0$. Define*

$$x^*(f) = \frac{2(|a_{k-1}| + |a_{k-2}| + \cdots + |a_0|)}{a_k}.$$

If $x > x^*(f)$ is an integer, then $f(x)$ is within 50% of the leading term:

$$\frac{a_k x^k}{2} < f(x) < \frac{3a_k x^k}{2}.$$

Proof. The condition we're trying to prove can be rewritten as $\left|\frac{f(x)}{a_k x^k} - 1\right| < \frac{1}{2}$. Writing out the left-hand side:

$$\left|\frac{f(x)}{a_k x^k} - 1\right| = \left|\frac{a_k x^k}{a_k x^k} + \frac{a_{k-1}x^{k-1}}{a_k x^k} + \frac{a_{k-2}x^{k-2}}{a_k x^k} + \cdots + \frac{a_0}{a_k x^k} - 1\right| =$$

$$= \left|\frac{a_{k-1}}{a_k x} + \frac{a_{k-2}}{a_k x^2} + \cdots + \frac{a_0}{a_k x^k}\right| \leq \sum_{i=1}^{k} \left|\frac{a_{k-i}}{a_k x^k}\right|.$$

Since x is an integer, $x > x^*(f) \geq 0 \Rightarrow x \geq 1$. Thus, $a_k x^k \geq a_k x$, and we can bound the denominator in the sum as:

$$\frac{1}{a_k x} \sum_{i=1}^{k} |a_{k-i}|$$

Now we use $x^*(f) < x \Rightarrow a_k x > 2\sum_{i=1}^{k} |a_{k-i}|$, and the difference is bounded simply by $\frac{1}{2}$ as desired. □

Lemma 5.2. *With $f(x)$ as in the previous lemma, we can bound $R_{f,s}(N)$ from below for N sufficiently large:*

$$R_{f,s}(N) > \frac{1}{2}\left(\frac{2N}{3a_k s}\right)^{s/k}.$$

Proof. As this is a lower bound, we will only consider $x_1, \ldots, x_s > x^*(f)$; this enables us to use the previous lemma. We have for all i: $0 < \frac{1}{2}a_k x_i^k < f(x_i) < \frac{3}{2}a_k x_i^k$. We will force the $f(x_i)$ to sum to an integer not exceeding N by requiring $\frac{N}{s} \geq \frac{3}{2}a_k x_i^k \Rightarrow x_i \leq (\frac{2N}{3sa_k})^{1/k}$. To get our lower bound, it remains to estimate the number of integers in the range $x^*(f) < n \leq (\frac{2N}{3sa_k})^{1/k}$. The number of choices is at least $(\frac{2N}{3sa_k})^{1/k} - x^*(f) - 1$. Since the second term is invariant in N, we pick N large enough that the first term exceeds the second by more than a factor of two. Then, we make s independent choices of the x_i to get the bound in the statement: $R_{f,s}(N) > \frac{1}{2}\left(\frac{2N}{3a_k s}\right)^{s/k}$. □

Now that we have a lower bound on the cumulative number of representations, we see that there is a choice of $N(f)$ so that the upper bound cannot be too far off.

Lemma 5.3. *Suppose $f(x)$ is an integer-valued polynomial as before, with $A(f)$ nonnegative, monotonically increasing. x^* is as in Lemma 5.1; let*

$$N(f) = \frac{x^*(f)^k}{2(k!)},$$

If $N > N(f)$ and $\sum_{i=1}^{s} f(x_i) \leq N$, then the number of available x_i is of the same order in N as the lower bound:

$$0 \leq x_i \leq \big(2(k!)N\big)^{1/k}.$$

Proof. Suppose that some $x_i$violates this. Then, $x_i > \big(2(k!)N\big)^{1/k}$; we plug in $N(f)$ to get: $x_i > x^*(f)$; so, by Lemma 5.1, $f(x_i) > \frac{1}{2}a_k x_i^k \geq \frac{1}{2}a_k 2(k!)N$. An integer-valued polynomial cannot have $|a_k| < \frac{1}{k!}$, since the coefficient of x^k comes from the binomial $\binom{x}{k}$ with an integer coefficient. Thus, $f(x_i) > N$, a contradiction, because the other summands of $\sum_{i=1}^{s} f(x_i)$ are nonnegative. □

So far, we have avoided choosing s; the following subtle and technical result by Linnik tells us how to choose s so that $sA(f) = \{\sum_{i=1}^{s} f(x_i) : x_i \in \mathbb{N}_0\}$ will have positive lower density.

Theorem 5.4. ***(An application of Linnik's main theorem)*** *Define the sequence $\{s(k)\}_{k=1}^{\infty}$ recursively, as follows:*

$$s(1) = 1$$
$$s(k) = 8k2^{\log_2 s(k-1)} \quad \text{for } k \geq 2.$$

If we have an integer-valued polynomial $f(x) = \sum_{i=0}^{k} a_i x^i$, with $a_0 > 0$ and

$$|a_i| \leq cP^{k-i} \qquad 0 \leq i \leq k,$$

we get the following estimate on what is almost a representation function:

$$(1) \qquad \#\left\{ \begin{array}{ccc} |x_i| \leq cP & and & x_i \in \mathbb{Z} \\ for\ 1 \leq i \leq s(k) & : & \sum_{i=1}^{s(k)} f(x_i) = n \end{array} \right\} \ll_{k,c} P^{s(k)-k},$$

where the constant in the inequality depends on k and c.

Proof. See Chapter 12 in [1]. □

The following theorem shows how the above choice of s precipitates $d(sA(f)) > 0$, and thus proves the result we wanted.

Theorem 5.5. ***(Waring's Problem for Polynomials)*** *Suppose we are given an integer-valued polynomial $f(x) = \sum_{i=0}^{k} a_i x^i$ with $a_k > 0$ and $gcd(A(f)) = 1$. Then, $A(f)$ is an asymptotic basis.*

Proof. We take $N(f)$ as in Lemma 5.3, and s as in Theorem 5.4. We will write $W = sA(f)$, and denote its counting function by $W(N)$.

In order to apply Theorem 5.4, we have to choose particular c and P. The requirements are:

(1) We want to force x_i into the range $[-cP, cP]$ used in Theorem 5.4, so that (1) can be used as an upper bound for $r_{s,f}(N)$. Lemma 5.3 gives us control over x_i for large enough N. Therefore, we want $x_i \leq (2(k!)N)^{1/k} \leq cP$. The form of the expression suggests this natural split: $c \geq (2(k!))^{1/k}$ (inequality, since we need $c \geq a_k$ also) and $P = N^{1/k}$.
(2) $|a_i| \leq cP^{k-i}$, as per hypothesis. To satisfy this, we just have to choose N large enough – the polynomial is fixed.

With these choices we can use Theorem 5.4 to write:

$$\begin{aligned} r_{f,s}(n) &= \#\{x_i \in \mathbb{N}_0 : \sum_{i=1}^{s} f(x_i) = n\} \\ &\leq \#\{x_i \in \mathbb{Z}, |x_i| \leq cP : \sum_{i=1}^{s} f(x_i) = n\} \\ &\ll_{k,c} P^{s-k}, \end{aligned}$$

for any $0 \leq n \leq N$. Now, we derive an upper bound for the cumulative function:

$$\begin{aligned} R_{f,s}(N) = \sum_{n=0}^{N} r_{f,s}(n) &= \sum_{\substack{n=0 \\ r_{f,s}(n)\geq 1}}^{N} r_{f,s}(n) \\ \ll_{k,c} P^{s-k} \sum_{\substack{n=0 \\ r_{f,s}(n)\geq 1}}^{N} 1 &= W(N)P^{s-k} \\ = W(N)\frac{P^s}{\left(N^{1/k}\right)^k} &= \frac{W(N)}{N}P^s. \end{aligned}$$

Recall the upper bound for $R_{f,s}(N)$ from Lemma 5.2 (also valid only when N sufficiently large):

$$R_{s,f}(N) > \frac{1}{2}\left(\frac{2N}{3a_k s}\right)^{s/k} \geq \frac{1}{2}\left(\frac{2}{3cs}\right)^{s/k}\left(N^{1/k}\right)^s \gg_{k,c} P^s$$

As promised, we get (for large enough N):

$$P^s \ll_{k,c} R_{f,s}(N) \ll_{k,c} \frac{W(N)}{N} P^s$$

$$\Rightarrow \frac{W(N)}{N} \gg_{k,c} 1.$$

So, $d(W) > 0$, and Corollary 4.2 gives us the asymptotic basis. □

From this theorem we get the following two results for free:

Corollary 5.6. *If we have $f(x)$ as in Theorem 5.5, and also assume $1 \in A(f)$, then $A(f)$ is a basis of finite order.*

Proof. Theorem 5.5 tells us that $A(f)$ is an asymptotic basis, so every $n > N$ is a sum of at most h elements of $A(f)$. But, all smaller n are a sum of at most N ones. So, $A(f)$ is a basis of order $\max(N, h)$. □

Corollary 5.7. ***(Waring's Problem; Hilbert 1909)*** *For every $k \geq 1$, the set $\{x^k : x \in \mathbb{N}_0\}$ is a basis.*

Proof. This follows trivially from Corollary 5.6. □

References

[1] M. Nathanson, "Elementary Methods in Number Theory", Springer-Verlag, New York, 1991