Product Bases for the Rationals

P. Berrizbeitia and P. D. T. A. Elliott

Abstract. A sequence of positive rationals generates a subgroup of finite index in the multiplicative positive rationals, and group product representations by the sequence need only a bounded number of terms, if and only if certain related sequences have densities uniformly bounded from below.

In 1930 Schnirelmann introduced on the positive integers the density now named after him, and employed it to show that every integer greater than 1 could be expressed as a sum of primes, with a uniformly bounded number of summands. This was a first step towards the conjectures of Goldbach. It was important that once positive, Schnirelmann's density is increased by adding a sequence to itself.

It is tantalising to try and extend Schnirelmann's ideas to the multiplicative generation of rationals. There are obstacles.

Let Q^* denote the multiplicative group of positive rationals, Γ the subgroup generated by the members, a_n, of a sequence of rationals, G the quotient group, Q^*/Γ.

A sequence of rationals may generate a proper subgroup of Q^*. Unlike the situation for an integer sequence of positive Schnirelmann density, further multiplication will avail us naught; Q^* is not cyclic; there is no multiplicative element corresponding to 1.

Whether a positive integer may be expressed as a sum of elements taken from some sequence of distinct positive integers may be decided in a finite number of steps. Not surprisingly, Schnirelmann's arguments are local in nature. However, the word problem for denumerable abelian groups has no (finite recursive) decision procedure. Since Q^* is free on denumerably many generators, and factoring by Γ plays the rôle of adjoining relations, the nature of G cannot be determined, locally or not, without particular knowledge of the a_n in Γ. What should this knowledge be?

The following result throws a little light on this problem.

For each positive integer t, S_t will denote the members of Γ representable by a group product using at most t terms from the sequence (a_n), repetition allowed.

For a set of rationals, E, define the lower density

$$d(E) = \liminf_{x \to \infty} x^{-1} \sum_{n \le x, n \in E} 1,$$

the sum counting only positive integers. Clearly $0 \le d(E) \le 1$ and the density of a union of disjoint sets E and F is at least as large as the sum of their individual densities. $d(E)$ will be the classical asymptotic density if the infimum may be removed.

γE will denote the set of products of the elements in E by the rational γ.

Theorem   *The following propositions are equivalent:*

(i)   *G is finite and $\Gamma = S_t$ for some t.*
(ii)   *There is a k such that $d(m^{-1}S_k) \geq c_1 > 0$ uniformly for all positive integers m.*
(iii)   *There is a w such that $d(\gamma S_w) \geq c_2 > 0$ uniformly for all positive rationals γ.*

Moreover, t can be given explicitly in terms of k and c_1, or w and c_2.

In part, proposition (i) of the theorem asserts the existence of a t, so that if a rational belongs to Γ, then at most t members of the sequence (a_n) are needed in its product representation. Nothing is said concerning the realisation of such a representation.

That (ii) implies (i) could be obtained by adapting the short argument in Elliott [2], but t would not then be computable.

Combined with results from number theory, a careful variant of the argument given here shows that any rational representable as a product of shifted primes $p + 1$, has such a representation with exactly 19 terms [1].

We present a cyclic proof of the theorem. That (iii) implies (ii) is clear.

Proof that (ii) implies (i)   Let the integer h exceed c_1^{-1}. Let m be a positive integer. The sets S_k, $m^{-j}S_k$ $0 \leq j \leq h - 1$, cannot be mutually disjoint, otherwise the density of their union will exceed 1. There are integers u, v, $0 \leq u < v \leq h - 1$ so that m^{v-u} belongs to S_{2k}. The group G has bounded order.

If $\gamma = ab^{-1}$, with integers a, b, and b^z belongs to S_{2k}, then the coset $\gamma\Gamma$ contains the integer representative ab^{z-1}.

Let $m_1, \ldots, m_f$ be integer representatives for distinct cosets of Γ. The sets $m_j^{-1}S_k$, $1 \leq j \leq f$ are mutually disjoint. Their union has density at least $c_1 f$. The group G is bounded, of order at most c_1^{-1}.

That Γ is some S_t costs a little more. We use the fact that if $S_{r+1} = S_r$, then $\Gamma = S_r$.

$E - F$ will denote the set of elements in E but not F.

Let γ belong to $S_{r+1} - S_r$, $r \geq 3k$. If $\gamma = ab^{-1}$, as before, with b^z in S_{2k}, then $S_{r+1+2k} - S_{r-2k}$ contains the integer ab^{z-1}.

Moreover, if $S_{r+1} - S_r$ contains a rational, then so do each of $S_{j+1} - S_j$, $3k \leq j \leq r$. We can find an integer in each set $S_{j+1+2k} - S_{j-2k}$, $3k \leq j \leq r$.

The sets $S_{7kw+1+2k} - S_{7kw-2k}$, $1 \leq w \leq r(7k)^{-1}$ are disjoint. Let them contain integers n_w, respectively. The corresponding sets $n_w^{-1}S_k$, $1 \leq w \leq r(7k)^{-1}$ are also disjoint. Their union has density at least $rc_1(7k)^{-1}$.

If $r > 7kc_1^{-1}$, then we obtain a contradiction. Hence Γ is S_t for some t not exceeding $7kc_1^{-1}$.

No attempt has been made to minimize the value of t.

Remark   Let $\bar{S}_j$ denote the set of elements in Γ representable using exactly j of the a_n, counted with multiplicity.

Since $1 = a_n a_n^{-1}$, $\bar{S}_j$ is contained in $\bar{S}_{j+2}$. It is clear that for a non-empty $\bar{S}_j$ to be contained in $\bar{S}_{j+1}$, there must be a representation of 1 by an odd number of the a_n. Granted the existence of such a representation, $\bar{S}_j$ will be a subset of $\bar{S}_{j+m}$ for all $m \geq$ (an odd) y.

Assume, further, the validity of the second part of Proposition (i). Then for $j \geq t + y$,

$$\bar{S}_j \subseteq \Gamma = S_t = \bigcup_{i=1}^{t} \bar{S}_i \subseteq \bigcup_{i=1}^{t} \bar{S}_{i+(j-i)} = \bar{S}_j.$$

Each member of Γ has a product representation employing exactly j terms, from (a_n).

Proof that (i) implies (iii) That the integers belonging to any particular coset of Γ have an asymptotic density follows from Theorem (3.10) of Ruzsa [3]. Moreover, since our group G is finite, at least one density is positive. By the same result every density is positive. Our situation is simpler than that of Ruzsa, and it is pertinent to obtain reasonably explicit values for the various densities rather than just give them bounds. For completion and not to appeal to his somewhat complicated paper we give a proof. Like Ruzsa, we adapt a method of Dirichlet, save that we follow Dirichlet more closely.

Let σ denote the canonical homomorphism $Q^* \to Q^*/\Gamma$.

Let the ω in G for which the sum $\sum p^{-1}$, taken over the primes for which $\sigma(p) = \omega$, diverges generate the subgroup G_1 of G. In particular, $\sum q^{-1}$, taken over the primes q for which $\sigma(q)$ does not lie in G_1, converges.

If a rational is not divisible by a q, then it maps into G_1.

Let Q_1 denote the subgroup of positive rationals not divisible by any q.

Let θ_j, $1 \leq j \leq |G_1|$ denote the characters on G_1, and g_j the composition $\theta_j\sigma$ restricted to Q_1. We extend g_j to Q^* by setting every $g_j(q) = 0$. We obtain in this way a multiplicative arithmetic function with values in the complex unit disc.

Those integers n in Q_1 which σ takes to a particular element μ (of G_1) have an asymptotic density:

$$D(\mu) = \lim_{x \to \infty} \frac{1}{x} \sum_{n \leq x} \frac{1}{|G_1|} \sum_{j=1}^{|G_1|} g_j(n)\overline{\theta_j(\mu)}$$

$$= \frac{1}{|G_1|} \sum_{j=1}^{|G_1|} \overline{\theta_j(\mu)} \lim_{x \to \infty} \frac{1}{x} \sum_{n \leq x} g_j(n).$$

Here we employ a theorem of Wirsing [4], that a multiplicative function which assumes only finitely many values in the complex unit disc possesses an asymptotic mean-value.

According to that same reference, the mean-value of a typical g_j is zero unless the series $\sum p^{-1}\big(1 - \operatorname{Re} g_j(p)\big)$ converges. If δ denotes the minimum of $1 - \operatorname{Re} \rho$ taken over the $|G_1|$-th roots of unity, ρ, then this series cannot converge unless

$$\delta \sum_{\mu,\theta_j(\mu) \neq 1} \sum_{\sigma(p)=\mu,\, p \text{ not } q} \frac{1}{p}$$

also converges. Since $\sum q^{-1}$ converges, we may omit the condition: *p not q*. Then θ_j must be trivial on every ω, and so on G_1.

For the g_j which extends the principal character on G_1 we count those integers not divisible by any q; an application of the sieve of Eratosthenes suffices. We arrive at the value

$$D(\mu) = |G_1|^{-1}\Pi\Big(1 - \frac{1}{q}\Big),$$

which is independent of μ.

Each positive integer has a unique representation $n_1 n_2$, where n_1 is that part of n comprised of powers of the primes q, an empty product interpreted as 1. Corresponding to this decomposition, for any element τ in G,

$$\sum_{\substack{n \leq x \\ \sigma(n)=\tau}} 1 = \sum_{\lambda} \sum_{\substack{n_1 \leq x \\ \sigma(n_1)=\lambda}} \sum_{\substack{n_2 \leq x/n_1 \\ \sigma(n_2)=\tau\lambda^{-1}}} 1,$$

where λ runs over the elements of G. Since n_2 belongs to Q_1, the innersum will be empty unless $\tau\lambda^{-1}$ belongs to G_1; we may then estimate it in terms of $D(\tau\lambda^{-1})$. In this way we see that the integers n with $\sigma(n) = \tau$ have asymptotic density

$$\Delta(\tau) = \sum_{\lambda \in \tau G_1} \sum_{\sigma(n_1)=\lambda} \frac{1}{n_1|G_1|}\Pi\Big(1 - \frac{1}{q}\Big).$$

This density is positive and does not exceed $|G_1|^{-1}$.

We continue with the proof of our theorem. Until now we have employed only the first part of (i). Appealing to the second part, there are only finitely many distinct cosets $\gamma S_t = \gamma\Gamma$, γ rational. For each of these $d(\gamma S_t) = \Delta\big(\gamma(\mathrm{mod}\,\Gamma)\big) > 0$. Proposition (iii) is valid with $w = t$ and c_2 the minimum of $\Delta(\tau)$ taken over the elements τ in G.

The theorem is proved.

Remarks When Γ is generated by the shifted primes, application of Dirichlet's theorem on primes in arithmetic progression together with the sieve of Eratosthenes shows that G_1 coincides with G; *cf.* [1, Lemma 7]. Every coset of Γ then has asymptotic density $|G|^{-1}$.

It is clear that one may replace the lower density in the theorem by any other density that is at least additive on disjoint sets and coincides with the standard asymptotic density when that exists.

We thank the referee for a careful reading of the text.

References

[1]   P. Berrizbeitia and P. D. T. A. Elliott, *On products of shifted primes.* Ramanujan J. **2**(1998), 219–223.
[2]   P. D. T. A. Elliott, *The multiplicative group of rationals generated by the shifted primes, I.* J. Reine Angew. Math. **463**(1995), 169–216.
[3]   I. Z. Ruzsa, *General Multiplicative Functions.* Acta Arith. **32**(1977), 313–347.
[4]   E. Wirsing, *Das asymptotische Verhalten von Summen über multiplikative Funktionen II.* Acta Math. Acad. Sci. Hungar. **18**(1967), 411–467.

Departamento de Matemáticas
Universidad Simón Bolívar
Apartado 8900
Caracas 1080-A
Venezuela

Department of Mathematics
University of Colorado at Boulder
Boulder, Colorado 80309-0395
U.S.A.