

# ON SETS OF INTEGERS WHICH ARE BOTH SUM-FREE AND PRODUCT-FREE

PÄR KURLBERG, JEFFREY C. LAGARIAS, AND CARL POMERANCE

ABSTRACT. We consider sets of positive integers containing no sum of two elements in the set and also no product of two elements. We show that the upper density of such a set is strictly smaller than  $\frac{1}{2}$  and that this is best possible. Further, we also find the maximal order for the density of such sets that are also periodic modulo some positive integer.

## 1. INTRODUCTION

The sum-product problem in combinatorial number theory asserts that if  $\mathcal{A}$  is a finite set of positive integers, then either  $\mathcal{A} + \mathcal{A}$  or  $\mathcal{A} \cdot \mathcal{A}$  is a much larger set than  $\mathcal{A}$ , where  $\mathcal{A} + \mathcal{B}$  is the set of sums  $a + b$  with  $a \in \mathcal{A}, b \in \mathcal{B}$  and  $\mathcal{A} \cdot \mathcal{B}$  is the set of products  $ab$  with  $a \in \mathcal{A}, b \in \mathcal{B}$ . A famous conjecture by Erdős and Szemerédi [2] asserts that if  $\epsilon > 0$  is arbitrary and  $\mathcal{A}$  is a set of  $N$  positive integers, then for  $N$  sufficiently large depending on the choice of  $\epsilon$ , we have

$$|\mathcal{A} + \mathcal{A}| + |\mathcal{A} \cdot \mathcal{A}| \geq N^{2-\epsilon}.$$

This conjecture is motivated by the cases when either  $|\mathcal{A} + \mathcal{A}|$  or  $|\mathcal{A} \cdot \mathcal{A}|$  is unusually small. For example, if  $\mathcal{A} = \{1, 2, \dots, N\}$ , then  $\mathcal{A} + \mathcal{A}$  is small, namely,  $|\mathcal{A} + \mathcal{A}| < 2N$ . However,  $\mathcal{A} \cdot \mathcal{A}$  is large since there is some  $c > 0$  such that  $|\mathcal{A} \cdot \mathcal{A}| > N^2/(\log N)^c$ . And if  $\mathcal{A} = \{1, 2, 4, \dots, 2^{N-1}\}$ , then  $|\mathcal{A} \cdot \mathcal{A}| < 2N$ , but  $|\mathcal{A} + \mathcal{A}| > N^2/2$ . The best that we currently know towards this conjecture is that it holds with exponent  $4/3$  in the place of 2, a result of Solymosi [9]. (In fact, Solymosi proves this when  $\mathcal{A}$  is a set of positive real numbers.)

In this paper we consider a somewhat different question: how dense can  $\mathcal{A}$  be if both  $\mathcal{A} + \mathcal{A}$  and  $\mathcal{A} \cdot \mathcal{A}$  have no elements in common with  $\mathcal{A}$ ? If  $\mathcal{A} \cap (\mathcal{A} + \mathcal{A}) = \emptyset$  we say that  $\mathcal{A}$  is sum-free and if  $\mathcal{A} \cap (\mathcal{A} \cdot \mathcal{A}) = \emptyset$  we say  $\mathcal{A}$  is product-free. Before stating the main results, we give some background on sets that are either sum-free or product-free.

If  $a \in \mathcal{A}$  and  $\mathcal{A}$  is sum-free, then  $\{a\} + \mathcal{A}$  is disjoint from  $\mathcal{A}$ , and so we immediately have that the upper asymptotic density of  $\mathcal{A}$  is at most  $\frac{1}{2}$ . Density  $\frac{1}{2}$  can be achieved by taking  $\mathcal{A}$  as the set of odd natural numbers. Similarly, if  $\mathcal{A}$  is a set of residues modulo  $n$  and is sum-free, then  $D(\mathcal{A}) := |\mathcal{A}|/n$  is at most  $\frac{1}{2}$ , and this can be achieved when  $n$  is even and  $\mathcal{A}$  consists of the odd residues. The maximal density for  $D(\mathcal{A})$  for  $\mathcal{A}$  a sum-free set in  $\mathbb{Z}/n\mathbb{Z}$  was considered in [1]. In particular, the maximum for  $D(\mathcal{A})$  is  $\frac{1}{3} - \frac{1}{3n}$  if  $n$  is divisible solely by primes that are 1 modulo 3, it is  $\frac{1}{3} + \frac{1}{3p}$  if  $n$  is divisible by some prime that is 2 modulo 3 and  $p$  is the least such, and it is  $\frac{1}{3}$  otherwise. Consequently, we have  $D(\mathcal{A}) \leq \frac{2}{5}$  if  $\mathcal{A}$  is a sum-free set in  $\mathbb{Z}/n\mathbb{Z}$  and  $n$  is odd. It is worth noting that maximal densities of subsets of arbitrary finite abelian groups are determined in [3]. For generalizations to subsets of finite non-abelian groups, see [4].

---

*Date:* Dec. 16, 2011.

*2000 Mathematics Subject Classification.* 11B05, 11B75.

The problem of the maximum density of product-free sets of positive integers, or of subsets of  $\mathbb{Z}/n\mathbb{Z}$ , only recently received attention. For subsets of the positive integers, it was shown in [6] that the upper density of a product-free set must be strictly less than 1. Let  $D(n)$  denote the maximum value of  $D(\mathcal{A})$  as  $\mathcal{A}$  runs over product-free sets in  $\mathbb{Z}/n\mathbb{Z}$ . In [8] it was shown that  $D(n) < \frac{1}{2}$  for the vast majority of integers, namely for every integer not divisible by the square of a product of 6 distinct primes. Moreover, the density of integers which are divisible by the square of a product of 6 distinct primes was shown to be smaller than  $1.56 \times 10^{-8}$ .

Somewhat surprisingly,  $D(n)$  can in fact be arbitrarily close to 1 (see [6]), and thus there are integers  $n$  and sets of residues modulo  $n$  consisting of 99% of all residues, with the set of pairwise products lying in the remaining 1% of the residues. However, it is not easy to find a numerical example that beats 50%. In [6], an example of a number  $n$  with about  $1.61 \times 10^8$  decimal digits was given with  $D(n) > \frac{1}{2}$ ; it is not known if there are any substantially smaller examples, say with fewer than  $10^8$  decimal digits.

In [7] the maximal order of  $D(n)$  was essentially found: There are positive constants  $c, C$  such that for all sufficiently large  $n$ , we have

$$D(n) \leq 1 - \frac{c}{(\log \log n)^{1-\frac{c}{2}} \log^2(\log \log \log n)^{1/2}}$$

and there are infinitely many  $n$  with

$$D(n) \geq 1 - \frac{C}{(\log \log n)^{1-\frac{c}{2}} \log^2(\log \log \log n)^{1/2}}.$$

In this paper we consider two related questions. First, if  $\mathcal{A}$  is a set of integers which is both sum-free and product-free, how large may the upper density of  $\mathcal{A}$  be? Second, set

$$D'(n) := \max\{D(\mathcal{A}) : \mathcal{A} \text{ is a sum-free, product-free subset of } \mathbb{Z}/n\mathbb{Z}\}.$$

What is the maximal order of  $D'(n)$ ? We prove the following results.

**Theorem 1.1.** *If  $\mathcal{A}$  is a set of positive integers that is both product-free and sum-free, then  $\mathcal{A}$  has upper density at most  $\frac{1}{2} \left(1 - \frac{1}{5a_0}\right)$ , where  $a_0$  is the least element of  $\mathcal{A}$ .*

**Theorem 1.2.** *There is a positive constant  $\kappa$  such that for all sufficiently large numbers  $n$ ,*

$$D'(n) \leq \frac{1}{2} - \frac{\kappa}{(\log \log n)^{1-\frac{\kappa}{2}} \log^2(\log \log \log n)^{1/2}}.$$

**Theorem 1.3.** *There is a positive constant  $\kappa'$  and infinitely many integers  $n$  with*

$$D'(n) \geq \frac{1}{2} - \frac{\kappa'}{(\log \log n)^{1-\frac{\kappa'}{2}} \log^2(\log \log \log n)^{1/2}}.$$

Note that  $D'(5) = \frac{2}{5}$  and if  $5|n$ , then  $D'(n) \geq \frac{2}{5}$ . A possibly interesting computational problem is to numerically exhibit some  $n$  with  $D'(n) > \frac{2}{5}$ . Theorem 1.3 assures us that such numbers exist, but the least example might be very large.

One might also ask for the densest possible set  $\mathcal{A}$  for which  $\mathcal{A}$ ,  $\mathcal{A} + \mathcal{A}$ , and  $\mathcal{A} \cdot \mathcal{A}$  are pairwise disjoint. However, Proposition 3.2 below implies immediately that any sum-free, product-free set  $\mathcal{A} \subset \mathbb{Z}/n\mathbb{Z}$  with  $D(\mathcal{A}) > \frac{2}{5}$  also has  $\mathcal{A} + \mathcal{A}$  and  $\mathcal{A} \cdot \mathcal{A}$  disjoint. Thus, from Theorem 1.3, we may have these three sets pairwise disjoint with  $D(\mathcal{A})$  arbitrarily close to  $\frac{1}{2}$ .

## 2. THE UPPER DENSITY

Here we prove Theorem 1.1. We begin with some notation that we use in this section: For a set of positive integers  $\mathcal{A}$ , we write  $\mathcal{A}(x)$  for  $\mathcal{A} \cap [1, x]$ . If  $a$  is an integer, we write  $a + \mathcal{A}$  for  $\{a\} + \mathcal{A}$ .

**Lemma 2.1.** *Suppose that  $\mathcal{A}$  is a sum-free set of positive integers and that  $I$  is an interval of length  $y$  in the positive reals. Then*

$$|\mathcal{A} \cap I| \leq \frac{y}{2} + O_{\mathcal{A}}(1).$$

*Proof.* Let  $N = |\mathcal{A} \cap I|$ . For any positive integer  $m$  we have  $|(m + \mathcal{A}) \cap I| \geq |\mathcal{A} \cap I| - m$ . Let  $a_0$  be the least element of  $\mathcal{A}$ . Thus  $|(a_0 + \mathcal{A}) \cap I| \geq N - a_0$ . But  $a_0 + \mathcal{A}$  is disjoint from  $\mathcal{A}$ , so

$$2N - a_0 \leq |\mathcal{A} \cap I| + |(a_0 + \mathcal{A}) \cap I| \leq |I \cap \mathbb{Z}| = y + O(1).$$

Solving this inequality for  $N$  proves the result.  $\square$

For a set  $\mathcal{A}$  of positive integers and a real number  $x > 0$ , let

$$\delta_x := 1 - 2 \frac{|\mathcal{A}(x)|}{x}, \quad \text{so that} \quad |\mathcal{A}(x)| = \frac{1}{2}(1 - \delta_x)x.$$

Note that  $\delta_x \geq 0$  for  $|\mathcal{A}(x)| \leq \frac{1}{2}$ .

**Lemma 2.2.** *Suppose that  $\mathcal{A}$  is a sum-free set of positive integers and that  $a_1, a_2 \in \mathcal{A}$ . Then for all  $x > 0$ ,*

$$|(a_1 + \mathcal{A}(x - a_1)) \cap (a_2 + \mathcal{A}(x - a_2))| \geq \frac{1}{2}(1 - 3\delta_x) - (a_1 + a_2).$$

*Proof.* We have the sets  $\mathcal{A}(x)$ ,  $a_1 + \mathcal{A}(x - a_1)$ ,  $a_2 + \mathcal{A}(x - a_2)$  all lying in  $[1, x]$  and the latter two sets are disjoint from the first set (since  $\mathcal{A}$  is sum-free). Thus,

$$\begin{aligned} & |(a_1 + \mathcal{A}(x - a_1)) \cap (a_2 + \mathcal{A}(x - a_2))| \\ &= |a_1 + \mathcal{A}(x - a_1)| + |a_2 + \mathcal{A}(x - a_2)| - |(a_1 + \mathcal{A}(x - a_1)) \cup (a_2 + \mathcal{A}(x - a_2))| \\ &\geq |a_1 + \mathcal{A}(x - a_1)| + |a_2 + \mathcal{A}(x - a_2)| - (x - |\mathcal{A}(x)|) \\ &\geq (|\mathcal{A}(x)| - a_1) + (|\mathcal{A}(x)| - a_2) + (|\mathcal{A}(x)| - x) = 3|\mathcal{A}(x)| - x - (a_1 + a_2). \end{aligned}$$

But  $3|\mathcal{A}(x)| - x = \frac{1}{2}(1 - 3\delta_x)x$ , so this completes the proof.  $\square$

For a set  $\mathcal{A}$  of positive integers, define the *difference set*

$$\Delta\mathcal{A} := \{a_1 - a_2 : a_1, a_2 \in \mathcal{A}\}.$$

Further, for an integer  $g$ , let

$$\mathcal{A}_g := \mathcal{A} \cap (-g + \mathcal{A}) = \{a \in \mathcal{A} : a + g \in \mathcal{A}\}.$$

**Corollary 2.3.** *If  $\mathcal{A}$  is a sum-free set of positive integers and  $g \in \Delta\mathcal{A}$  then, for any  $x > 0$ ,*

$$|\mathcal{A}_g(x)| \geq \frac{1}{2}(1 - 3\delta_x)x + O(1),$$

*in which the implied constant depends on both  $g$  and  $\mathcal{A}$ .*

*Proof.* Suppose that  $g \in \Delta\mathcal{A}$ , so that there exist  $a_1, a_2 \in \mathcal{A}$  such that  $a_1 - a_2 = g$ . If  $a \in \mathcal{A}(x - a_1)$  and  $a + a_1 \in a_2 + \mathcal{A}(x - a_2)$ , then  $a + g = a + a_1 - a_2 \in \mathcal{A}$ , so that  $a \in \mathcal{A}_g$ . That is,  $\mathcal{A}_g(x - a_1)$  contains  $-a_1 + (a_1 + \mathcal{A}(x - a_1)) \cap (a_2 + \mathcal{A}(x - a_2))$ . Thus, by Lemma 2.2,

$$|\mathcal{A}_g(x - a_1)| \geq |(a_1 + \mathcal{A}(x - a_1)) \cap (a_2 + \mathcal{A}(x - a_2))| \geq \frac{1}{2}(1 - 3\delta_x) - (a_1 + a_2),$$

from which the corollary follows.  $\square$

**Corollary 2.4.** *If  $\mathcal{A}$  is a sum-free set of positive integers with upper density greater than  $\frac{2}{5}$ , then  $\Delta\mathcal{A}$  is a subgroup of  $\mathbb{Z}$ .*

*Proof.* Since  $\Delta\mathcal{A}$  is closed under multiplication by  $-1$ , it suffices to show that if  $g_1, g_2 \in \Delta\mathcal{A}$ , then  $g_1 + g_2 \in \Delta\mathcal{A}$ . If  $g_1 + \mathcal{A}_{g_1}$  contains a member  $a$  of  $\mathcal{A}_{g_2}$ , then  $a - g_1 \in \mathcal{A}$  and  $a + g_2 \in \mathcal{A}$ , so that  $g_1 + g_2 \in \Delta\mathcal{A}$ . Note that  $g_1 + \mathcal{A}_{g_1}$  and  $\mathcal{A}_{g_2}$  are both subsets of  $\mathcal{A}$ . Now by Corollary 2.3, if  $g_1 + \mathcal{A}_{g_1}$  and  $\mathcal{A}_{g_2}$  were disjoint, we would have for each positive real number  $x$ ,

$$(1 - 3\delta_x)x + O(1) \leq \frac{1}{2}(1 - \delta_x)x,$$

so that  $\delta_x \geq \frac{1}{5} + O(\frac{1}{x})$ . Hence  $\liminf \delta_x \geq \frac{1}{5}$ , contradicting the assumption that  $\mathcal{A}$  has upper density greater than  $\frac{2}{5}$ . Thus,  $g_1 + \mathcal{A}_{g_1}$  and  $\mathcal{A}_{g_2}$  are not disjoint, which as we have seen, implies that  $g_1 + g_2 \in \Delta\mathcal{A}$ . This completes the proof.  $\square$

**Remark 2.5.** Corollary 2.4 is best possible, as can be seen by taking  $\mathcal{A}$  as the set of positive integers that are either 2 or 3 modulo 5.

We now prove the following result which immediately implies Theorem 1.1.

**Proposition 2.6.** *Suppose that  $\mathcal{A}$  is a sum-free set of positive integers with least member  $a_0$ . Suppose in addition that  $\{a_0\} \cdot \mathcal{A}$  is disjoint from  $\mathcal{A}$ . Then the upper density of  $\mathcal{A}$  is at most  $\frac{1}{2} \left(1 - \frac{1}{5a_0}\right)$ .*

*Proof.* If the upper density of  $\mathcal{A}$  is at most  $\frac{2}{5}$ , the result holds trivially, so we may assume the upper density exceeds  $\frac{2}{5}$ . It follows from Corollary 2.4 that  $\Delta\mathcal{A}$  is the set of multiples of some positive number  $g$ , which is necessarily either 1 or 2. (If  $g \geq 3$ , then the upper density of  $\mathcal{A}$  would be at most  $\frac{1}{3}$ .)

Suppose that  $g = 2$  so that  $\Delta\mathcal{A}$  consists of all even numbers. Then either  $\mathcal{A}$  consists of all even numbers or all odd numbers. In the former case, the set  $\{\frac{1}{2}\} \cdot \mathcal{A}$  is a sum-free set of positive integers, and so has upper density at most  $\frac{1}{2}$ . It follows that  $\mathcal{A}$  has upper density at most  $\frac{1}{4}$ , a contradiction.

Now suppose that  $\mathcal{A}$  consists solely of odd numbers. For any real number  $x \geq a_0$ , both  $\{a_0\} \cdot \mathcal{A}(x/a_0)$  and  $\mathcal{A}(x)$  consist only of odd numbers, they are disjoint, and they lie in  $[1, x]$ . Thus, by Lemma 2.1,

$$|\mathcal{A}(x)| \leq \frac{1}{2}x - \left| \mathcal{A}\left(\frac{x}{a_0}\right) \right| + O(1) \quad \text{and} \quad |\mathcal{A}(x)| \leq \frac{1}{2}\left(x - \frac{x}{a_0}\right) + \left| \mathcal{A}\left(\frac{x}{a_0}\right) \right| + O(1).$$

Adding these two inequalities and dividing by 2 gives that  $|\mathcal{A}(x)| \leq \left(\frac{1}{2} - \frac{1}{2a_0}\right)x + O(1)$ , so that  $\mathcal{A}$  has upper density at most  $\frac{1}{2} - \frac{1}{2a_0}$ , giving the result in this case.

It remains to consider the case that  $g = 1$ , that is,  $\Delta\mathcal{A} = \mathbb{Z}$ . Let  $x \geq a_0$  be any real number and consider the two sets  $a_0 + \mathcal{A}(x - a_0)$  and  $\{a_0\} \cdot \mathcal{A}_{-1}(x/a_0)$ . They both lie in

$[1, x]$  and by hypothesis are both disjoint from  $\mathcal{A}(x)$ . If these two sets share an element in common then there would be some  $a \in \mathcal{A}_{-1}(x/a_0)$  with  $a_0a - a_0 \in \mathcal{A}(x - a_0)$ . In this case  $a_0(a - 1) \in \mathcal{A}$  and also  $a_0 \in \mathcal{A}$  and  $a - 1 \in \mathcal{A}$ , which contradicts our hypothesis. We conclude that the three sets  $a_0 + \mathcal{A}(x - a_0)$ ,  $\{a_0\} \cdot \mathcal{A}_{-1}(x/a_0)$ , and  $\mathcal{A}(x)$  must be pairwise disjoint. Thus,

$$\left| \mathcal{A}_{-1} \left( \frac{x}{a_0} \right) \right| = \left| \{a_0\} \cdot \mathcal{A}_{-1} \left( \frac{x}{a_0} \right) \right| \leq x - |\mathcal{A}(x)| - |a_0 + \mathcal{A}(x - a_0)| = \delta_x x + O(1).$$

On the other hand, using Lemma 2.1 and Corollary 2.3,

$$\begin{aligned} \left| \mathcal{A}_{-1} \left( \frac{x}{a_0} \right) \right| &\geq |\mathcal{A}_{-1}(x)| - \frac{1}{2} \left( 1 - \frac{1}{a_0} \right) x + O(1) \\ &\geq \frac{1}{2}(1 - 3\delta_x)x - \frac{1}{2} \left( 1 - \frac{1}{a_0} \right) x + O(1) = \left( \frac{1}{2a_0} - \frac{3}{2}\delta_x \right) x + O(1). \end{aligned}$$

Putting these two inequalities together and dividing by  $x$ , we obtain

$$\delta_x \geq \frac{1}{2a_0} - \frac{3}{2}\delta_x + O\left(\frac{1}{x}\right).$$

Hence  $\delta_x \geq \frac{1}{5a_0} + O\left(\frac{1}{x}\right)$ , implying that  $\liminf \delta_x \geq \frac{1}{5a_0}$ , whence

$$\bar{d}(\mathcal{A}) = \limsup_{x \rightarrow \infty} \frac{1}{x} |\mathcal{A}(x)| = \limsup_{x \rightarrow \infty} \frac{1}{2}(1 - \delta_x) = \frac{1}{2} - \liminf_{x \rightarrow \infty} \frac{1}{2}\delta_x \geq \frac{1}{2} \left( 1 - \frac{1}{5a_0} \right),$$

which proves the proposition.  $\square$

### 3. AN UPPER BOUND FOR THE DENSITY IN $\mathbb{Z}/n\mathbb{Z}$

In this section we prove Theorem 1.2. We use the following theorem of Kneser [5]; see also [10, Theorem 5.5].

**Theorem 3.1** (Kneser). *Suppose in an abelian group  $G$  (written additively) we have finite nonempty sets  $\mathcal{A}, \mathcal{B}, \mathcal{C}$  where  $\mathcal{A} + \mathcal{B} = \mathcal{C}$ . Let  $H$  be the stabilizer of  $\mathcal{C}$  in  $G$ , that is,  $H$  is the subgroup of elements  $g \in G$  with  $g + \mathcal{C} = \mathcal{C}$ . Then*

$$|\mathcal{C}| \geq |\mathcal{A} + H| + |\mathcal{B} + H| - |H| \geq |\mathcal{A}| + |\mathcal{B}| - |H|.$$

We next deduce restrictions on the structure of sum-free sets having density greater than  $\frac{2}{5}$ .

**Proposition 3.2.** *Suppose that  $n$  is a positive integer and  $\mathcal{A} \subset \mathbb{Z}/n\mathbb{Z}$  is sum-free. If  $D(\mathcal{A}) > \frac{2}{5}$ , then  $n$  is even and  $\mathcal{A}$  is a subset of the odd residues in  $\mathbb{Z}/n\mathbb{Z}$ .*

*Proof.* It follows from [1] that  $D(\mathcal{A}) > \frac{2}{5}$  implies  $n$  must be even (see the comments in Section 1). The result holds for  $n = 2$  since a sum-free set cannot contain 0. It also holds for  $n = 4$  since the double of an odd residue is 2, so the only option for  $\mathcal{A}$  is  $\{1, 3\}$ . We now suppose  $n \geq 6$  is even and proceed by induction assuming that the proposition holds for all even numbers smaller than  $n$ . Let  $\mathcal{C}$  denote the set of residues mod  $n$  of the form  $a + b$ , where  $a, b \in \mathcal{A}$ . Since  $|\mathcal{A}| > \frac{2}{5}n$  and  $\mathcal{A}$  is sum-free, we have  $|\mathcal{C}| < \frac{3}{5}n$ , so that  $|\mathcal{C}| < 2|\mathcal{A}| - 1$  (using  $n \geq 6$ ). We apply Kneser's theorem in the group  $G = \mathbb{Z}/n\mathbb{Z}$  to conclude that the stabilizer  $H$  of  $\mathcal{C}$  must be nontrivial. Thus  $H = \langle h \rangle$ , where  $h|n$  and  $h < n$ .

Next note that if  $\psi$  denotes the projection map of  $\mathbb{Z}/n\mathbb{Z}$  to  $\mathbb{Z}/h\mathbb{Z}$ , then  $\psi(\mathcal{A})$  is still sum-free. To show this, suppose not, whence there are  $a_1, a_2, a_3 \in \mathcal{A}$  and  $\psi(a_1) + \psi(a_2) = \psi(a_3)$ .

Now  $a_3 \equiv a_1 + a_2 \pmod{h}$ , so that there is some  $c \in \mathcal{C}$  (namely  $c = a_1 + a_2$ ) with  $a_3 \in H + c$ . But  $H + c \subset H + \mathcal{C} = \mathcal{C}$ , so  $a_3 = a'_1 + a'_2$  for some  $a'_1, a'_2 \in \mathcal{A}$ , contradicting the assumption that  $\mathcal{A}$  is sum-free.

The projection map  $\psi$  is  $n/h$  to 1, so  $|\psi(\mathcal{A})| \geq |\mathcal{A}|/(n/h) > \frac{2}{5}h$ , and this implies that  $h$  must be even. By the induction hypothesis  $\psi(\mathcal{A})$  cannot contain any even residues modulo  $h$ . But even residues in  $\mathcal{A}$  reduce to even residues modulo  $h$ , so  $\mathcal{A}$  cannot contain any even residues modulo  $n$ . This completes the proof.  $\square$

We now prove Theorem 1.2. For those  $n$  with  $D'(n) \leq \frac{2}{5}$ , the result holds for any number  $\kappa$ , so assume that  $D'(n) > \frac{2}{5}$ . Let  $\mathcal{A} \subset \mathbb{Z}/n\mathbb{Z}$  be a product-free, sum-free set with  $D(\mathcal{A}) = D'(n)$ . By Proposition 3.2, we have that  $n$  is even and that  $\mathcal{A}$  is a subset of the odd residues modulo  $n$ . Suppose that  $k$  is an integer with  $n \leq 2^k < 2n$ . Let  $N = 2^{2k}n$  and let  $\mathcal{B}$  be the set of positive integers of the form  $2^j b$  where  $j \leq k$  and  $b \leq N/2^j = 2^{2k-j}n$ , such there is some  $a \in \mathcal{A}$  with  $b \equiv a \pmod{n}$ . Then the members of  $\mathcal{B}$  are in  $[1, N]$  and

$$|\mathcal{B}| = \sum_{j=0}^k 2^{2k-j} |\mathcal{A}| = 2^k (2^{k+1} - 1) |\mathcal{A}| > \left(1 - \frac{1}{n}\right) 2^{2k+1} |\mathcal{A}|. \quad (3.1)$$

We note that  $\mathcal{B}$  is product-free as a set of residues modulo  $N$ . Indeed, suppose  $2^{j_i} b_i \in \mathcal{B}$ , for  $i = 1, 2, 3$  and

$$2^{j_1} b_1 2^{j_2} b_2 \equiv 2^{j_3} b_3 \pmod{N}.$$

Let  $a_i \in \mathcal{A}$  be such that  $b_i \equiv a_i \pmod{n}$  for  $i = 1, 2, 3$ . We have that  $a_1, a_2, a_3$  are odd, and since  $n$  is even, this implies that  $b_1, b_2, b_3$  are odd. Using  $j_1 + j_2 \leq 2k, j_3 \leq k$  and  $2^{2k}|N$ , we have  $j_1 + j_2 = j_3$ . Hence  $a_1 a_2 \equiv a_3 \pmod{n}$ , a violation of the assumption that  $\mathcal{A}$  is product-free modulo  $n$ . We conclude that  $\mathcal{B}$  is product-free modulo  $N$ .

It now follows from Theorem 1.1 in [7] that for  $n$  sufficiently large,

$$|\mathcal{B}| \leq N \left(1 - \frac{c}{(\log \log N)^{1-\frac{\epsilon}{2}} \log^2 (\log \log \log N)^{1/2}}\right).$$

Further, since  $N$  is of order of magnitude  $n^3$ , we have that  $\log \log N = \log \log n + O(1)$ , and so for any fixed choice of  $c_0 < c$  we have for  $n$  sufficiently large that

$$|\mathcal{B}| \leq N \left(1 - \frac{c_0}{(\log \log n)^{1-\frac{\epsilon}{2}} \log^2 (\log \log \log n)^{1/2}}\right).$$

Thus, from our lower bound for  $|\mathcal{B}|$  in (3.1) we have

$$|\mathcal{A}| < \frac{N}{2^{2k+1}} \left(1 - \frac{1}{n}\right)^{-1} \left(1 - \frac{c_0}{(\log \log n)^{1-\frac{\epsilon}{2}} \log^2 (\log \log \log n)^{1/2}}\right).$$

Since  $N/2^{2k+1} = n/2$ , it follows that for any fixed  $c_1 < c_0$  and  $n$  sufficiently large, we have

$$|\mathcal{A}| < \frac{n}{2} \left(1 - \frac{c_1}{(\log \log n)^{1-\frac{\epsilon}{2}} \log^2 (\log \log \log n)^{1/2}}\right).$$

We thus may choose  $\kappa$  as any number smaller than  $c/2$ . This concludes the proof of Theorem 1.2.

## 4. EXAMPLES WITH LARGE DENSITY

In this section we prove Theorem 1.3. We follow the argument in [6] with a supplementary estimate from [7]. Let  $x$  be a large number, let  $\ell_x$  be the least common multiple of the integers in  $[1, x]$  and let  $n_x = \ell_x^2$ . Then  $n_x = e^{(2+o(1))x}$  as  $x \rightarrow \infty$  so that  $\log \log n_x = \log x + O(1)$ . For a positive integer  $m$ , let  $\Omega(m)$  denote the number of prime factors of  $m$  counted with multiplicity. Let  $k = k(x) = \lfloor \frac{x}{4} \log \log n_x \rfloor$ , let

$$\mathcal{D}'_x = \{d|\ell_x : d \text{ odd}, k < \Omega(d) < 2k\},$$

and let  $\mathcal{A}$  be the set of residues  $a$  modulo  $n_x$  with  $\gcd(a, n_x) \in \mathcal{D}'_x$ . Then  $\mathcal{A}$  is product-free (cf. Lemma 2.3 in [6]), and since  $n_x$  is even and every residue in  $\mathcal{A}$  is odd, we have that  $\mathcal{A}$  is sum-free as well. We shall now establish a sufficiently large lower bound on  $D(\mathcal{A})$  to show that  $D'(n_x)$  satisfies the inequality in the theorem with  $n = n_x$ .

For  $d \in \mathcal{D}'_x$ , the number of  $a \pmod{n_x}$  with  $\gcd(a, n_x) = d$  is  $\varphi(n_x)/d$ , so that

$$D(\mathcal{A}) = \frac{\varphi(n_x)}{n_x} \sum_{d \in \mathcal{D}'_x} \frac{1}{d} = \frac{\varphi(n_x)}{n_x} \left( \sum_{\substack{d|\ell_x \\ d \text{ odd}}} \frac{1}{d} - \sum_{\substack{d|\ell_x \\ d \text{ odd} \\ d \notin \mathcal{D}'_x}} \frac{1}{d} \right) \geq \frac{\varphi(n_x)}{n_x} \left( \sum_{\substack{d|\ell_x \\ d \text{ odd}}} \frac{1}{d} - \sum_{\substack{d|\ell_x \\ d \notin \mathcal{D}'_x}} \frac{1}{d} \right). \quad (4.1)$$

We have

$$\sum_{\substack{d|\ell_x \\ d \text{ odd}}} \frac{1}{d} = \prod_{2 < p \leq x} \frac{p}{p-1} \cdot \prod_{\substack{2 < p \leq x \\ p^a \parallel \ell_x}} \left(1 - \frac{1}{p^{a+1}}\right) \geq \prod_{2 < p \leq x} \frac{p}{p-1} \cdot \left(1 - \frac{1}{x}\right)^{\pi(x)}$$

and, since  $\varphi(n_x)/n_x = 2^{-1} \cdot \prod_{p|n_x, p > 2} (1 - 1/p)$ , we find that

$$\frac{\varphi(n_x)}{n_x} \sum_{\substack{d|\ell_x \\ d \text{ odd}}} \frac{1}{d} \geq \frac{1}{2} \left(1 - \frac{1}{x}\right)^{\pi(x)} \geq \frac{1}{2} - \frac{\pi(x)}{x}. \quad (4.2)$$

We now use (6.2) in [7] which is the assertion that

$$\sum_{\substack{P(d) \leq x \\ \Omega(d) \notin (k, 2k)}} \frac{1}{d} \ll \frac{(\log x)^{\frac{x}{2} \log 2}}{(\log \log x)^{1/2}}.$$

Here,  $P(d)$  denotes the largest prime factor of  $d$ . Since this sum includes every integer  $d|\ell_x$  that is not in  $\mathcal{D}'_x$ , we have

$$\frac{\varphi(n_x)}{n_x} \sum_{\substack{d|\ell_x \\ d \notin \mathcal{D}'_x}} \frac{1}{d} \ll \frac{\varphi(n_x)}{n_x} \cdot \frac{(\log x)^{\frac{x}{2} \log 2}}{(\log \log x)^{1/2}} \ll \frac{1}{(\log x)^{1 - \frac{x}{2} \log 2} (\log \log x)^{1/2}},$$

where we use Mertens' theorem in the form  $\varphi(n_x)/n_x = \prod_{p \leq x} (1 - 1/p) \ll 1/\log x$  for the last step. Putting this estimate and (4.2) into (4.1), we get

$$D(\mathcal{A}) \geq \frac{1}{2} - \frac{\pi(x)}{x} - \frac{c'}{(\log x)^{1 - \frac{x}{2} \log 2} (\log \log x)^{1/2}}$$

for some positive constant  $c'$ . Using  $\pi(x)/x \ll 1/\log x$  and  $\log x = \log \log n_x + O(1)$ , we have

$$D(\mathcal{A}) \geq \frac{1}{2} - \frac{\kappa'}{(\log \log n_x)^{1-\frac{\epsilon}{2}} \log^2(\log \log n_x)^{1/2}}$$

for any fixed constant  $\kappa' > c'$  and  $x$  sufficiently large. Thus,  $D'(n_x)$  satisfies the condition of Theorem 1.3 for  $x$  sufficiently large, completing the proof.

#### ACKNOWLEDGMENTS

We thank Albert Bush, Chris Pryby, and Joseph Vandehey for raising the question of sets which are both sum-free and product-free. PK was supported in part by grants from the Göran Gustafsson Foundation, and the Swedish Research Council. JCL was supported in part by NSF grant DMS-1101373. CP was supported in part by NSF grant DMS-1001180.

#### REFERENCES

- [1] P. H. Diananda and H. P. Yap, Maximal sum-free sets of elements of finite groups, *Proc. Japan Acad.* **45** (1969), No. 1, 1–5.
- [2] P. Erdős and E. Szemerédi, On sums and products of integers, in: *Studies in pure mathematics*, Birkhäuser, Basel, 1983, pp. 213–218.
- [3] B. Green and I. Z. Ruzsa, Sum-free sets in abelian groups, *Israel J. Math.* **147** (2005), 157–188.
- [4] K. S. Kedlaya, Product-free subsets of groups, then and now, *Communicating mathematics*, Contemp. Math., **479**, (2009). 169–177. Amer. Math. Soc., Providence, RI.
- [5] M. Kneser, Abschätzung der asymptotischen Dichte von Summenmengen, *Math. Z.* **58**, (1953). 459–484.
- [6] P. Kurlberg, J. C. Lagarias and C. Pomerance, Product-free sets with high density, *Acta Arith.*, to appear.
- [7] P. Kurlberg, J. C. Lagarias and C. Pomerance, The maximal density of product-free sets in  $\mathbb{Z}/n\mathbb{Z}$ , preprint, 2011.
- [8] C. Pomerance and A. Schinzel, Multiplicative properties of sets of residues, *Moscow J. Combinatorics and Number Theory* **1** (2011), 52–66.
- [9] J. Solymosi, Bounding multiplicative energy by the sumset, *Adv. Math.* **222** (2009), 402–408.
- [10] T. Tao and V. Vu, *Additive combinatorics*, Cambridge U. Press, 2006.

DEPARTMENT OF MATHEMATICS, KTH, SE-10044, STOCKHOLM, SWEDEN  
*E-mail address:* kurlberg@math.kth.se

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MICHIGAN, ANN ARBOR, MI 48109, USA  
*E-mail address:* lagarias@umich.edu

MATHEMATICS DEPARTMENT, DARTMOUTH COLLEGE, HANOVER, NH 03755, USA  
*E-mail address:* carl.pomerance@dartmouth.edu