On coverings and reduced residues in combinatorial number theory

A dissertation submitted to

Fakultät für Mathematik und Informatik

der Universität Würzburg

for the degree of

Doktor der Naturwissenschaften

presented by

Pascal Stumpf

Referees:

Prof. Dr. Jörn Steuding

Prof. Dr. Jürgen Sander

Würzburg, 2023

For Maryam, Rebecca and Bernd

Acknowledgements

First of all, I would like to express my deep gratitude to my advisor and friend Jörn Steuding for so many things, but most of all for his incredible trust in me from the beginning, and for all the freedom he has given me, to be able to work on the math I enjoy so much. He also introduced me, in very caring way, to our math community, and to expierence it from different perspectives. Here I have met some of the friendliest people I know to date, and who have even shared interest in my work, for which I am very grateful.

Moreover, I would like to thank Richard Greiner and our math department, by whose employment, throughout the years, I had even more time to continue my research. Last but not least, I would like to take this opportunity to thank my family for their everlasting support through ups and downs, and their belief in me no matter what I do, and of course Miriam who has taught me, in the nicest way possible, to never give up (and so much more).

Gerbrunn, February 2022 Pascal Stumpf

Contents

1 Introduction

For a long time understanding additive structures within multiplicatively built ones has been an important task in number theory. One of the oldest examples here are **prime numbers**, namely $2 = p_1, 3 = p_2, 5 = p_3, \ldots$, as they form the multiplicative building blocks of the integers. Every natural number exceeding one can be decomposed uniquely (up to reordering) into a product of primes due to the fundamental theorem of arithmetic. Although we know there are infinitely many primes, first shown by Euclid in ancient times, until today we do not know whether there are infinitely many **twin primes** p such that $p + 2$ is also prime.

Another question concerning additive structures within the primes is how they are distributed among arithmetic progressions. Here we do a bit better, starting from Dirichlet, who could prove in 1837 that every **reduced** residue class

$$a + m\mathbb{Z} = \{a + m \cdot k : k \in \mathbb{Z}\}$$

modulo m, with **relatively prime** positive integers a and m, contains infinitely many primes. Moreover, for a given modulus m, he showed that the primes are in a certain sense (asymptotically) evenly distributed among all reduced residue classes modulo m. Ever since then, based on his foundational work for analytic number theory, there has been a lot of effort in establishing more quantitative estimates of this equidistribution, such as the Siegel-Walfisz theorem and the Bombieri-Vinogradov theorem. In turn, such equidistribution results can often provide the arithmetic input about primes for sieve methods, by which recently Zhang [35] and (independently) Maynard [21] could prove the existence of a constant c such that there exist infinitely many pairs of primes differing by at most c, the current record being $c \leqslant 246$ due to a Polymath project [24].

Let us take one step back in time, even a few decades before the work of Dirichlet. Actually, it is mentioned in [19] that Legendre, in an attempt to prove the quadratic reciprocity law, had already tried to also prove Dirichlet's theorem around 1800. However, his approach was grounded on the erroneous claim that for every $r \geqslant 2$, among any $2p_{r-1}$ consecutive integers at least one of them is not divisible by any of the first r primes $p_1, \ldots, p_r$, or in other words, at least

one of them is relatively prime to their product $P_r = p_1 \cdot \ldots \cdot p_r$. Today, when P_r is replaced with any $m \in \mathbb{N}$, then the smallest number $j(m)$ such that every $j(m)$ consecutive integers contain at least one integer relatively prime to m is known as **Jacobsthal's function**, named after Ernst Jacobsthal, who studied it in a series of three papers (see [16]) in 1960. One hundred years earlier, in 1859, Dupré finally disproved Legendre's assumption $j(P_r) \leqslant 2p_{r-1}$ for $r = 9$, as he found $j(P_9) = 40 > 38 = 2 \cdot 19 = 2p_8$, which one can also verify in [13], where Hagedorn computed exact values of $j(P_r)$ for all $r < 50$.

In a letter to Erdős (see [9]) from 1962, Jacobsthal asked whether

$$j(P_r) \leqslant c \cdot r^2 \quad \text{as well as} \quad j(P_r) \geqslant j(m)$$

for some constant c and for all m which are the products of r distinct primes. Jacobsthal himself checked the last conjecture for all $r \leqslant 10$, and later in 2012 Hajdu and Saradha [14] extended its verification even further up to $r \leqslant 23$, but they also discovered a counterexample at $r = 24$. On the search for large gaps between consecutive primes Rankin [27], building upon work of Erdős [7] and Chang [3], established the lower bound

$$j(P_r) \geqslant c \cdot r \cdot \log r \cdot \frac{\log\log r \cdot \log\log\log\log r}{(\log\log\log r)^2}$$

for any $c < 1/3$. Over the years it then was raised to $c < e^\gamma/2$ by Schönhage [30] (here γ is Euler's constant), to $c < e^\gamma$ by Rankin [28], to $c < 1.31256\,e^\gamma$ by Maier and Pomerance [20], and finally to $c < 2e^\gamma$ by Pintz [25], before in 2014 Ford, Green, Konyagin and Tao [11] and independently Maynard [22] could solve the problem of Erdős to replace c by a function tending to infinity with r. Until today the best known upper bound is

$$j(P_r) \leqslant c \cdot r^2 \cdot (\log r)^2\,,$$

coming from a very careful examination of the error term in the linear sieve by Iwaniec [15]. Unfortunately, the constant c remains unknown, and the currently best known explicit upper bounds are

$$j(P_r) \leqslant 2^r \quad \text{as well as} \quad j(P_r) \leqslant 2 \cdot r^{2+2e\log r}$$

due to Kanold [18] and Stevens [31] by elementary means. In an earlier paper Kanold [17] also demonstrates that an upper bound of the form $j(P_r) \leqslant p_r^{2-\varepsilon}$ (or, equivalently by the prime number theorem, $j(P_r) \leqslant (r \log r)^{2-\varepsilon}$) for some $\varepsilon > 0$ would lead to an elementary proof of Dirichlet's theorem. In addition, it would also imply Linnik's theorem from 1944, which states there exist absolute constants c and L such that the least prime in any reduced residue class modulo m can be found below $c \cdot m^L$. Both of these deep connections suggest it might be quite difficult to improve on Iwaniec's upper bound. A bit later Vaughan [34] extended the result of Iwaniec to all positive integers $m > 1$ in the form

$$j(m) \leqslant c \cdot \omega(m)^2 \cdot \log(2\omega(m))^4 ,$$

where $\omega(m)$ denotes the number of distinct prime factors of m, and mentioned that probably even $j(m) \leqslant c \cdot \omega(m)^{1+\varepsilon}$ and therefore, in particular,

$$j(P_r) \leqslant c \cdot r^{1+\varepsilon}$$

holds for any $\varepsilon > 0$. On the other hand, he also indicates limitations of the linear sieve in this direction, and that a fundamental new idea might be needed here.

From another point of view, $j(m)$ can also be seen as the largest gap between consecutive members in

$$\mathbb{Z} \setminus \bigcup_{p \mid m} p\mathbb{Z} = \bigcup_{u \in \mathcal{R}(m)} u ,$$

where p runs through all prime factors of m and

$$\mathcal{R}(m) := \{a + m\mathbb{Z} : a \text{ is relatively prime to } m\}$$

stands for the family of all reduced residue classes modulo m, which form the multiplicative group of units in $\mathbb{Z}/m\mathbb{Z}$. Once more, this also coincides with the smallest number $n \in \mathbb{N}$ such that

$$\big(\mathcal{R}(m) + 1\big) \cup \big(\mathcal{R}(m) + 2\big) \cup \ldots \cup \big(\mathcal{R}(m) + n\big) = \mathbb{Z}/m\mathbb{Z} ,$$

as these consecutive translates of $\mathcal{R}(m)$ cover each gap stepwise. At first, this insight might not reveal much new about $j(m)$, but it allows us to generalize as

follows. Let us replace the ring $\mathbb{Z}/m\mathbb{Z}$ of residue classes modulo m by a finite additive group $(G,+)$ of order $\mathrm{card}(G)=m$, and instead of $\mathcal{R}(m)$ consider any non-empty subset $\mathcal{A}$ of G. Now, we are interested in sequences of **shifts**

$$s_1, s_2, s_3, \ldots$$

in G such that the induced sequence of **translates**

$$\mathcal{A}+s_1, \mathcal{A}+s_2, \mathcal{A}+s_3, \ldots$$

of $\mathcal{A}$ **covers** G, that is

$$\bigcup_{t=1}^{\infty}(\mathcal{A}+s_t)=\bigcup_{t=1}^{\infty}\{a+s_t : a\in\mathcal{A}\}=G\,.$$

In particular, given a sequence $(s_t)_{t\in\mathbb{N}}$ of shifts, we aim to find an upper bound for the smallest number $n\in\mathbb{N}$ (if it exists) such that

$$\bigcup_{t=1}^{n}(\mathcal{A}+s_t)=\bigcup_{t=1}^{n}\{a+s_t : a\in\mathcal{A}\}=G\,,$$

or, equivalently, each number

$$c_n(u):=\sum_{t=1}^{n}\mathbf{1}_{\mathcal{A}+s_t}(u)\,,$$

counting how often an element $u\in G$ is covered by the first n translates, is positive. Here, $\mathbf{1}_{\mathcal{S}}$ denotes the **characteristic function** of a set $\mathcal{S}$, defined by $\mathbf{1}_{\mathcal{S}}(x)=1$ if $x\in\mathcal{S}$, and $\mathbf{1}_{\mathcal{S}}(x)=0$ otherwise.

But first, in chapter 2, we measure how **uniformly** the elements of G are covered by a sequence of translates of $\mathcal{A}$. For that, we aim to keep track of the difference between the maximum and minimum values of $c_n(u)$ over all $u\in G$ at every (time) $n\in\mathbb{N}$. In particular, we find a way to bound this discrepancy, provided it is known for subsets of $\mathcal{A}$, whose union equals $\mathcal{A}$. Together with the **density** $\mathrm{card}(\mathcal{A})/m$ of $\mathcal{A}$ within G, we then can also deduce an upper bound

for the smallest number n such that the first n translates $\mathcal{A}+s_1,\ldots,\mathcal{A}+s_n$ cover G. As an offspring we recover the upper bound $j(P_r)\leqslant(r+1)\cdot(2^r-1)$ by Jacobsthal [16]. Next, we do not focus on a given sequence of shifts anymore and derive an upper bound for the smallest number of translates of $\mathcal{A}$ one needs to cover G, only depending on their density $\operatorname{card}(\mathcal{A})/m$. At each choice of the next translate we use an **averaging** argument to choose a translate covering at least as many remaining elements as a **randomly** chosen translate would cover. As one application we obtain, for some absolute constant c, that $G=\mathbb{Z}/P_r\mathbb{Z}$ can be covered by $c\cdot r\cdot(\log r)^2$ or less translates of $\mathcal{A}=\mathcal{R}(P_r)$. Actually, this also supports a conjecture of Montgomery [23] that $j(P_r)\leqslant c\cdot r\cdot(\log r)^2$. In order to prove this conjecture, it would be sufficient to show that the sequence of shifts $s_t=t$ $(t\in\mathbb{N})$ is **good** for $\mathcal{A}$, in the sense that for every $n\in\mathbb{N}$, the number of remaining elements in $G\setminus\bigcup_{t=1}^{n}(\mathcal{A}+s_t)$ covered by the next translate $\mathcal{A}+s_{n+1}$ is at least

$$\frac{1}{\operatorname{card}(G)}\cdot\sum_{s\in G}\operatorname{card}\biggl(\Bigl(G\setminus\bigcup_{t=1}^{n}(\mathcal{A}+s_t)\Bigr)\cap(\mathcal{A}+s)\biggr),$$

which represents the arithmetic mean taken over all $\operatorname{card}(G)$ shifts $s\in G$.

Before we investigate this problem further in chapter 3, we look at it in a slightly different setup. By the **Chinese remainder theorem**, $G=\mathbb{Z}/P_r\mathbb{Z}$ can also be identified with the Cartesian product

$$\prod_{i=1}^{r}(\mathbb{Z}/p_i\mathbb{Z})=(\mathbb{Z}/p_1\mathbb{Z})\times\ldots\times(\mathbb{Z}/p_r\mathbb{Z})$$

via the bijection which maps $a+P_r\mathbb{Z}$ to $(a+p_1\mathbb{Z},\ldots,a+p_r\mathbb{Z})$. Similarly, $\mathcal{R}(P_r)\subset\mathbb{Z}/P_r\mathbb{Z}$ can be identified with the **box** $\mathcal{B}(r)=\mathcal{R}(p_1)\times\ldots\times\mathcal{R}(p_r)$, where $\mathcal{R}(p_i)=(\mathbb{Z}/p_i\mathbb{Z})\setminus\{0+p_i\mathbb{Z}\}$, for $i\in\{1,\ldots,r\}$, is missing exactly one residue class modulo p_i. Now, one may remove even more residue classes for some p_i to obtain (smaller) boxes $\mathcal{B}=\prod_{i=1}^{r}\mathcal{B}_i$ with non-empty $\mathcal{B}_i\subset\mathcal{R}(p_i)$. It is easy to see that for some of these boxes, the sequence of shifts

$$\boldsymbol{s}_t=t\cdot(1,\ldots,1)\quad(t\in\mathbb{N}),$$

where $(1,\ldots,1)$ has r entries, is not good. But what happens, if one also considers sequences $\boldsymbol{s}_t = t \cdot \boldsymbol{d}$ $(t \in \mathbb{N})$ forming an **arithmetic progression** with common difference $\boldsymbol{d} \in \mathcal{B}(r)$?

For low dimensions $r \in \{1,2,3\}$, we have been able to check that there indeed does exist a good one for every **simple box** $\mathcal{B} = \prod_{i=1}^{r} \mathcal{B}_i \subset \mathcal{B}(r)$, where the elements of each set $\mathcal{B}_i$ form an arithmetic progression with common difference $1 + p_i\mathbb{Z}$. However, at $r = 4$, we have discovered exactly one counterexample. Fortunately, in the case of $\mathcal{B} = \mathcal{B}(r)$ itself, one and then all (as we will see later) sequences $\boldsymbol{s}_t = t \cdot \boldsymbol{d}$ $(t \in \mathbb{N})$ with $\boldsymbol{d} \in \mathcal{B}(r)$ are good, and we could verify this up to $r \leqslant 8$, with help of a computer.

Furthermore, the box-like structure of $\mathcal{B}(r)$ puts some restrictions on the maximal length l of an arithmetic progression $\big\{\boldsymbol{a} + (k-1) \cdot \boldsymbol{d} : k \in \{1,\ldots,l\}\big\}$, for $\boldsymbol{a}, \boldsymbol{d} \in \prod_{i=1}^{r} (\mathbb{Z}/p_i\mathbb{Z})$, with l distinct members all inside $\mathcal{B}(r)$. It turns out that $l = p_r - 1$, which is corresponding to the maximal length of an arithmetic progression inside $\mathcal{R}(P_r)$. By a slightly modified approach, also upper and lower bounds for the maximal length of an arithmetic progression inside $\mathcal{R}(m)$ can be obtained, again only depending on the largest prime factor of $m \in \mathbb{N}$.

Along the way, we also solve a problem of Recamán (see [12], B40) and prove, for every $l \in \mathbb{N}$ there exists a number $m(l)$ such that for all $m \geqslant m(l)$ the least reduced residue system modulo m, that is $\bigcup_{u \in \mathcal{R}(m)} u \cap \{1,\ldots,m\}$, contains an arithmetic progression of length l or longer (see [32]).

In chapter 3, we first aim to find out more about the structure of **minimal** coverings for $G = \prod_{i=1}^{r} (\mathbb{Z}/p_i\mathbb{Z})$ by as few as possible translates

$$\mathcal{B}(r) + \boldsymbol{s}_1, \mathcal{B}(r) + \boldsymbol{s}_2, \ldots, \mathcal{B}(r) + \boldsymbol{s}_n$$

of $\mathcal{B}(r)$, with shifts $\boldsymbol{s}_t$ in G for $t \in \{1,\ldots,n\}$.

Let $\mathcal{S}_1,\ldots,\mathcal{S}_r$ be r finite sets, and assume that each of them contains at least two elements. For any r-tuple $\boldsymbol{s} = (s_1,\ldots,s_r)$ from $\mathcal{S}_1 \times \ldots \times \mathcal{S}_r$, with entries $\boldsymbol{s}(i) := s_i$ for $i \in \{1,\ldots,r\}$, we put

$$\langle \boldsymbol{s} \rangle = \big\langle (s_1,\ldots,s_r) \big\rangle := \big(\mathcal{S}_1 \setminus \{s_1\}\big) \times \ldots \times \big(\mathcal{S}_r \setminus \{s_r\}\big)\,.$$

In the case $\mathcal{S}_i = \mathbb{Z}/p_i\mathbb{Z}$, for $i \in \{1, \ldots, r\}$, each translate of

$$\mathcal{B}(r) = \big\langle([0]_{p_1}, \ldots, [0]_{p_r})\big\rangle\,,$$

where $[a]_m := a + m\mathbb{Z}$, then can be identified uniquely by an r-tuple

$$\boldsymbol{s} = ([s_1]_{p_1}, \ldots, [s_r]_{p_r}) \in G\,,$$

via $\mathcal{B}(r) + \boldsymbol{s} = \big\langle([s_1]_{p_1}, \ldots, [s_r]_{p_r})\big\rangle$. Looking at the sequence of shifts

$$\boldsymbol{s}_t = t \cdot ([1]_{p_1}, \ldots, [1]_{p_r}) = ([t]_{p_1}, \ldots, [t]_{p_r}) \quad (t \in \mathbb{N})\,,$$

each sequence $\boldsymbol{s}_t(i) = [t]_{p_i}$ $(t \in \mathbb{N})$ is **periodic**, as

$$\boldsymbol{s}_{t\,+\,p_i}(i) = [t + p_i]_{p_i} = [t + 0]_{p_i} = \boldsymbol{s}_t(i)\,.$$

Moreover, each finite sequence $\boldsymbol{s}_1(i), \ldots, \boldsymbol{s}_t(i)$ is **balanced**, in the sense that every element from $\mathbb{Z}/p_i\mathbb{Z}$ appears at most once more than any other element from $\mathbb{Z}/p_i\mathbb{Z}$. Since $p_1, \ldots, p_r$ are pairwise relatively prime, it turns out this kind of balance also prevails among the finite sequences of d-tuples

$$(\boldsymbol{s}_1(i_1), \ldots, \boldsymbol{s}_1(i_d)), \ldots, (\boldsymbol{s}_t(i_1), \ldots, \boldsymbol{s}_t(i_d))$$

for every $t \in \mathbb{N}$, given any $d \leqslant r$ directions $i_1 < \ldots < i_d$ from $\{1, \ldots, r\}$. But how "close" to being balanced are sequences of shifts $\boldsymbol{s}_1, \boldsymbol{s}_2, \ldots, \boldsymbol{s}_n$ of minimal coverings? We analyze this question in the low-dimensional cases $r \in \{1, 2, 3\}$, and study what happens, when one replaces $\prod_{i\,=\,1}^{r}(\mathbb{Z}/p_i\mathbb{Z})$ by $\prod_{i\,=\,1}^{r}(\mathbb{Z}/m_i\mathbb{Z})$ with arbitrary (perhaps not pairwise relatively prime) integers $m_1, \ldots, m_r > 1$.

For example, given any sequence $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n$ of shifts in $G = \prod_{i\,=\,1}^{r}(\mathbb{Z}/m_i\mathbb{Z})$ such that $\boldsymbol{s}_x(i) \neq \boldsymbol{s}_y(i)$ for all pairs of distinct indices $x, y \in \{1, \ldots, n\}$ and in any direction $i \in \{1, \ldots, r\}$, the sequence $\langle\boldsymbol{s}_1\rangle, \ldots, \langle\boldsymbol{s}_n\rangle$ of induced translates always covers the same number of $\mathrm{card}\big(\bigcup_{t\,=\,1}^{n}\langle\boldsymbol{s}_t\rangle\big)$ elements in G. Fixing any (not necessarily balanced) sequence $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n$ of shifts in G, it follows similarly that given any shift $\boldsymbol{s}_{n\,+\,1} \in G$ with $\boldsymbol{s}_{n\,+\,1}(i) \neq \boldsymbol{s}_t(i)$ for all $t \in \{1, \ldots, n\}$ and in any direction $i \in \{1, \ldots, r\}$, the sequence $\langle\boldsymbol{s}_1\rangle, \ldots, \langle\boldsymbol{s}_n\rangle, \langle\boldsymbol{s}_{n\,+\,1}\rangle$ of induced translates always covers the same number of $\mathrm{card}\big(\bigcup_{t\,=\,1}^{n\,+\,1}\langle\boldsymbol{s}_t\rangle\big)$ elements in G.

Additionally, we can prove this number is maximal along all shifts $s_{n+1} \in G$, and, writing $\mathcal{R}$ for $\mathcal{R}(P_r)$, this also leads to a proof of the inequality

$$\operatorname{card}\Big((\mathcal{R}+n+1) \cup \bigcup_{t=1}^{n} (\mathcal{R}+t)\Big) \geqslant \operatorname{card}\Big((\mathcal{R}+s) \cup \bigcup_{t=1}^{n} (\mathcal{R}+t)\Big),$$

or, equivalently,

$$\operatorname{card}\Big((\mathcal{R}+n+1) \cap \bigcup_{t=1}^{n} (\mathcal{R}+t)\Big) \leqslant \operatorname{card}\Big((\mathcal{R}+s) \cap \bigcup_{t=1}^{n} (\mathcal{R}+t)\Big)$$

for every possible shift $s \in \{1, \ldots, P_r\}$, as long as $n \in \{1, \ldots, 5\}$. Hence, we come a step closer to show that the sequence of shifts $s_t = t$ $(t \in \mathbb{N})$ actually might be good for $\mathcal{R}$. In fact, for all $n \in \mathbb{N}$, we can at least prove

$$\sum_{t=1}^{n} \operatorname{card}\big((\mathcal{R}+n+1) \cap (\mathcal{R}+t)\big) \leqslant \sum_{t=1}^{n} \operatorname{card}\big((\mathcal{R}+s) \cap (\mathcal{R}+t)\big)$$

for every possible shift $s \in \{1, \ldots, P_r\}$, which forms our main result.

In the last chapter, for any given set $\mathcal{A} \subset \mathbb{N}_0 = \mathbb{N} \cup \{0\}$, we consider its **sumset** $\mathcal{A}+\mathcal{A} = \{a_1 + a_2 : a_1, a_2 \in \mathcal{A}\}$, which also can be seen as the union $\bigcup_{a \in \mathcal{A}} (\mathcal{A}+a)$ of those translates of $\mathcal{A}$ shifted by the elements a of $\mathcal{A}$ itself. For $n \in \mathbb{N}_0$, let us define

$$\begin{aligned} r_1(\mathcal{A}, n) &= \operatorname{card}\Big(\{(a_1, a_2) \in \mathcal{A} \times \mathcal{A} : a_1 + a_2 = n\}\Big), \\ r_2(\mathcal{A}, n) &= \operatorname{card}\Big(\{(a_1, a_2) \in \mathcal{A} \times \mathcal{A} : a_1 + a_2 = n,\, a_1 \leqslant a_2\}\Big), \\ r_3(\mathcal{A}, n) &= \operatorname{card}\Big(\{(a_1, a_2) \in \mathcal{A} \times \mathcal{A} : a_1 + a_2 = n,\, a_1 < a_2\}\Big), \end{aligned}$$

as the **additive representation functions** r_1, r_2 and r_3 belonging to $\mathcal{A}$, which count all solutions of the equation $a_1 + a_2 = n$ inside of $\mathcal{A}$ with slightly more restrictions as the index of r increases.

Our starting point are the following three results of Erdős, Sárközy and Sós obtained in [10] (and a bit later improved by Balasubramanian [1]), showing the

surprising different **monotonicity** behavior of $r_1(\mathcal{A}, n)$, $r_2(\mathcal{A}, n)$ and $r_3(\mathcal{A}, n)$. Let $\mathcal{A}$ be an **infinite** set of positive integers. Then:

(1) $r_1(\mathcal{A}, n)$ can be monotone increasing from a certain point on, but only if $\mathcal{A}$ contains all integers from a certain point on.

(2) $r_2(\mathcal{A}, n)$ cannot be monotone increasing from a certain point on, when $\lim_{N \to \infty} \operatorname{card}\big(\{1, \ldots, N\} \setminus \mathcal{A}\big) / \log N = \infty$.

(3) $r_3(\mathcal{A}, n)$ can be monotone increasing for all $n \geqslant 1$, while the complement $\mathbb{N} \setminus \mathcal{A}$ is infinite.

First, we calculate $r_1(\mathcal{A}, n)$, $r_2(\mathcal{A}, n)$ and $r_3(\mathcal{A}, n)$ for all $n \in \mathbb{N}_0$ in the special case $\mathcal{A} = \mathbb{N}_0$. For example, one easily finds $r_1(\mathbb{N}_0, n) = n + 1$, which demonstrates that $r_1(\mathcal{A}, n)$ can be **strictly** monotone increasing for all $n \geqslant 0$. In contrast to this, we also present an alternative proof that $r_2(\mathcal{A}, n)$ (as well as $r_3(\mathcal{A}, n)$) cannot be strictly monotone increasing from a certain point on, first proven by Chen and Tang [6].

Answering a question of Sárközy from [29], we then prove that there does exist an infinite set $\mathcal{A}$ such that its upper asymptotic density is less than 1, and $r_1(\mathcal{A}, n)$ is monotone increasing for almost all n. Alongside, we also prove that there does exist an infinite set $\mathcal{A}$ such that its complement $\mathbb{N}_0 \setminus \mathcal{A}$ is infinite, and $r_1(\mathcal{A}, n)$ is strictly monotone increasing for almost all n. Until today it remains uncertain whether or not there does exist an infinite set $\mathcal{A}$ such that $r_2(\mathcal{A}, n)$ is monotone increasing from a certain point on. However, we can show that such a set $\mathcal{A}$ cannot exist, if $r_2(\mathcal{A}, n)$ should be monotone increasing for all $n \geqslant 0$.

2 Coverings, boxes, and arithmetic progressions

In this chapter, we first collect some general properties of coverings for a finite additive group $(G,+)$ by translates of a subset $\mathcal{A} \subset G$. Along the way, we apply our results in the case of $G = \mathbb{Z}/m\mathbb{Z}$ with $\mathcal{A} = \mathcal{R}(m)$, to find out more about $j(m)$. In particular, when m is the product of r distinct primes $q_1, \ldots, q_r$, we then move our setup to $G = \prod_{i=1}^{r} (\mathbb{Z}/q_i\mathbb{Z})$, where $\mathcal{R}(m)$ can be identified by the (simple) box $\mathcal{B} = \mathcal{R}(q_1) \times \ldots \times \mathcal{R}(q_r)$. This change in view turns out to be quite fruitful, as one can also consider sequences of shifts forming an arithmetic progression here. Moreover, the box-like structure of $\mathcal{B}$ (or other simple boxes in G) can also provide some information about arithmetic progressions inside $\mathcal{B}$.

Let us quickly recall the definitions about coverings from the introduction, but this time in a slightly modified form.

For a finite additive group $(G,+)$ of order $\mathrm{card}(G) = m$ and a subset $\mathcal{A} \subset G$, we consider its **translates** $\mathcal{A} + s = \{a + s : a \in \mathcal{A}\}$ by **shifts** $s \in G$. Note that

$$\mathrm{card}(\mathcal{A} + s) = \mathrm{card}(\mathcal{A})$$

for all shifts $s \in G$, since $a_1 + s = a_2 + s$ for $a_1, a_2 \in \mathcal{A}$ always implies $a_1 = a_2$ by adding the inverse element of s on both sides.

Given a sequence $s_1, s_2, s_3, \ldots$ of shifts in G, we say that the induced sequence $\mathcal{A} + s_1, \mathcal{A} + s_2, \mathcal{A} + s_3, \ldots$ of translates of $\mathcal{A}$ **covers** G in **time** n (or less), if

$$\bigcup_{t=1}^{n} (\mathcal{A} + s_t) = \bigcup_{t=1}^{n} \{a + s_t : a \in \mathcal{A}\} = G\,,$$

or, equivalently,

$$c_n(\mathcal{A}, u) := \sum_{t=1}^{n} \mathbf{1}_{\mathcal{A}+s_t}(u) = \sum_{t=1}^{n} \mathbf{1}_{\mathcal{A}}(u - s_t) > 0 \quad \text{for all } u \in G\,.$$

Moreover, we say that the sequence $\mathcal{A} + s_1, \mathcal{A} + s_2, \mathcal{A} + s_3, \ldots$ of translates covers G in time n at least c times, if $c_n(\mathcal{A}, u) \geqslant c$ for all $u \in G$.

2.1 Measuring uniformity of coverings

How **uniformly** does a sequence of translates cover the elements of G?

Let us fix a sequence $s_1, s_2, s_3, \ldots$ of shifts in G throughout this section. For a subset $\mathcal{A} \subset G$, we aim to keep track of the difference

$$\delta_n(\mathcal{A}) := \max\{c_n(\mathcal{A}, u) : u \in G\} - \min\{c_n(\mathcal{A}, u) : u \in G\}$$

at every time $n \in \mathbb{N}$, as well as

$$\Delta(\mathcal{A}) := \sup\{\delta_n(\mathcal{A}) : n \in \mathbb{N}\},$$

called the **discrepancy** of $\mathcal{A}$ (with respect to the given sequence of shifts).

First, note that discrepancy is invariant under complementation.

Lemma 2.1. For any subset $\mathcal{A} \subset G$, we have $\Delta(G \setminus \mathcal{A}) = \Delta(\mathcal{A})$.

Proof. At every time $n \in \mathbb{N}$, we find

$$\begin{aligned} c_n(\mathcal{A}, u) + c_n(G \setminus \mathcal{A}, u) &= \sum_{t=1}^{n} \mathbf{1}_{\mathcal{A}+s_t}(u) + \sum_{t=1}^{n} \mathbf{1}_{(G\setminus\mathcal{A})+s_t}(u) \\ &= \sum_{t=1}^{n} \mathbf{1}_{\mathcal{A}}(u - s_t) + \mathbf{1}_{G\setminus\mathcal{A}}(u - s_t) = \sum_{t=1}^{n} 1 = n \end{aligned}$$

for all $u \in G$. Hence, we can write

$$\begin{aligned} \delta_n(G \setminus \mathcal{A}) &= \max\{n - c_n(\mathcal{A}, u) : u \in G\} - \min\{n - c_n(\mathcal{A}, u) : u \in G\} \\ &= n - \min\{c_n(\mathcal{A}, u) : u \in G\} - n + \max\{c_n(\mathcal{A}, u) : u \in G\} \\ &= \max\{c_n(\mathcal{A}, u) : u \in G\} - \min\{c_n(\mathcal{A}, u) : u \in G\} \\ &= \delta_n(\mathcal{A}), \end{aligned}$$

from which

$$\Delta(G \setminus \mathcal{A}) = \sup\{\delta_n(G \setminus \mathcal{A}) : n \in \mathbb{N}\} = \sup\{\delta_n(\mathcal{A}) : n \in \mathbb{N}\} = \Delta(\mathcal{A})$$

immediately follows. □

If we assume, as usual, that $(G,+)$ is commutative (that is $u+v=v+u$ for all $u,v\in G$), then discrepancy is also invariant under translation.

Lemma 2.2. Let $(G,+)$ be commutative. For any subset $\mathcal{A}\subset G$ and any shift $s\in G$, we have $\Delta(\mathcal{A}+s)=\Delta(\mathcal{A})$.

Proof. At every time $n\in\mathbb{N}$, we find

$$\begin{aligned} c_n(\mathcal{A}+s,u) &= \sum_{t=1}^{n} \mathbf{1}_{\mathcal{A}+s+s_t}(u) \\ &= \sum_{t=1}^{n} \mathbf{1}_{\mathcal{A}+s_t+s}(u) = \sum_{t=1}^{n} \mathbf{1}_{\mathcal{A}+s_t}(u-s) = c_n(\mathcal{A},u-s) \end{aligned}$$

for all $u\in G$. Hence, we can write

$$\begin{aligned} \delta_n(\mathcal{A}+s) &= \max\{c_n(\mathcal{A}+s,u) : u\in G\} - \min\{c_n(\mathcal{A}+s,u) : u\in G\} \\ &= \max\{c_n(\mathcal{A},u-s) : u\in G\} - \min\{c_n(\mathcal{A},u-s) : u\in G\} \\ &= \max\{c_n(\mathcal{A},x) : x\in G-s\} - \min\{c_n(\mathcal{A},x) : x\in G-s\} \\ &= \max\{c_n(\mathcal{A},x) : x\in G\} - \min\{c_n(\mathcal{A},x) : x\in G\} \\ &= \delta_n(\mathcal{A})\,, \end{aligned}$$

from which

$$\Delta(\mathcal{A}+s)=\sup\{\delta_n(\mathcal{A}+s) : n\in\mathbb{N}\}=\sup\{\delta_n(\mathcal{A}) : n\in\mathbb{N}\}=\Delta(\mathcal{A})$$

immediately follows. □

In the important special case, when $\mathcal{A}$ forms a subgroup (respectively coset) of a cyclic group $(G,+)$, we can say a bit more about its discrepancy. For that, given any $g\in G$, define $0\cdot g$ to be the neutral element in G, and then iteratively $k\cdot g=(k-1)\cdot g+g$ as well as $(-k)\cdot g=(1-k)\cdot g-g$ for $k\in\mathbb{N}$. Recall that for a cyclic group $(G,+)$ there exists at least one generating element $g\in G$ such that $\big\{k\cdot g : k\in\{1,\dots,\mathrm{card}(G)\}\big\}=G$.

Lemma 2.3. Let $(G,+)$ be cyclic, $g\in G$ be a generator for G, and $s_t=t\cdot g$ ($t\in\mathbb{N}$). If $\mathcal{A}\subset G$ forms a subgroup or coset in G, then $\Delta(\mathcal{A})\leqslant 1$.

Proof. As subgroup of a cyclic group, $\mathcal{A}$ itself is also cyclic, and we can write

$$\mathcal{A} = \big\{q\,d\cdot g : q \in \{1,\dots,m/d\}\big\} = \{q\,d\cdot g : q\in\mathbb{Z}\}$$

for some divisor d of the group order $\operatorname{card}(G) = m$.

At every time $n\in\mathbb{N}$, for $u = k\cdot g \in G$ ($k\in\mathbb{Z}$), we find

$$\begin{aligned} c_n(\mathcal{A},u) &= \sum_{t=1}^{n} \mathbf{1}_{\mathcal{A}+s_t}(u) = \sum_{t=1}^{n} \mathbf{1}_{\mathcal{A}}(u-s_t) \\ &= \sum_{t=1}^{n} \mathbf{1}_{\mathcal{A}}(k\cdot g - t\cdot g) = \sum_{t=1}^{n} \mathbf{1}_{\mathcal{A}}((k-t)\cdot g)\,. \end{aligned}$$

Here, $\mathbf{1}_{\mathcal{A}}((k-t)\cdot g) = 1$ if and only if $k-t = q\,d$ for some $q\in\mathbb{Z}$.

Let $\lfloor x\rfloor$ denote the largest integer not exeeding $x\in\mathbb{R}$.

Since any d consecutive integers form a complete residue system modulo d, among the n consecutive integers $k-1, k-2, \dots, k-n$ there are (exactly) $\lfloor n/d\rfloor$ or $\lfloor n/d\rfloor + 1$ multiples of d. For all $u\in G$, we thus have

$$\lfloor n/d\rfloor \leqslant c_n(\mathcal{A},u) \leqslant \lfloor n/d\rfloor + 1\,,$$

from which

$$\delta_n(\mathcal{A}) \leqslant (\lfloor n/d\rfloor + 1) - \lfloor n/d\rfloor = 1\,,$$

and so $\Delta(\mathcal{A}) \leqslant 1$ immediately follows.

As cyclic group, $(G,+)$ is commutative, and **Lemma 2.2** yields

$$\Delta(\mathcal{A}+s) = \Delta(\mathcal{A}) \leqslant 1$$

for each coset $\mathcal{A}+s = s+\mathcal{A}$ with $s\in G$.

This completes our proof. □

Next, we establish an upper bound for the discrepancy of a subset $\mathcal{A}\subset G$, provided it is already known for two subsets of $\mathcal{A}$ and their intersection, whose union equals $\mathcal{A}$.

Lemma 2.4. For any two subsets $\mathcal{A}_1, \mathcal{A}_2 \subset G$, we have

$$\Delta(\mathcal{A}_1 \cup \mathcal{A}_2) \leqslant \Delta(\mathcal{A}_1) + \Delta(\mathcal{A}_2) + \Delta(\mathcal{A}_1 \cap \mathcal{A}_2)\,.$$

Proof. At every time $n \in \mathbb{N}$, we find

$$\begin{aligned} c_n(\mathcal{A}_1 \cup \mathcal{A}_2, u) &= \sum_{t=1}^{n} \mathbf{1}_{\mathcal{A}_1 \cup \mathcal{A}_2 + s_t}(u) = \sum_{t=1}^{n} \mathbf{1}_{\mathcal{A}_1 \cup \mathcal{A}_2}(u - s_t) \\ &= \sum_{t=1}^{n} \mathbf{1}_{\mathcal{A}_1}(u - s_t) + \mathbf{1}_{\mathcal{A}_2}(u - s_t) - \mathbf{1}_{\mathcal{A}_1 \cap \mathcal{A}_2}(u - s_t) \\ &= \sum_{t=1}^{n} \mathbf{1}_{\mathcal{A}_1 + s_t}(u) + \mathbf{1}_{\mathcal{A}_2 + s_t}(u) - \mathbf{1}_{\mathcal{A}_1 \cap \mathcal{A}_2 + s_t}(u) \\ &= c_n(\mathcal{A}_1, u) + c_n(\mathcal{A}_2, u) - c_n(\mathcal{A}_1 \cap \mathcal{A}_2, u) \end{aligned}$$

for all $u \in G$. In particular, $c_n(\mathcal{A}_1 \cup \mathcal{A}_2, u)$ is bounded from above by

$$\begin{aligned} &\max\{c_n(\mathcal{A}_1, u) : u \in G\} + \max\{c_n(\mathcal{A}_2, u) : u \in G\} \\ &\quad - \min\{c_n(\mathcal{A}_1 \cap \mathcal{A}_2, u) : u \in G\}\,, \end{aligned}$$

and it is bounded from below by

$$\begin{aligned} &\min\{c_n(\mathcal{A}_1, u) : u \in G\} + \min\{c_n(\mathcal{A}_2, u) : u \in G\} \\ &\quad - \max\{c_n(\mathcal{A}_1 \cap \mathcal{A}_2, u) : u \in G\}\,. \end{aligned}$$

The difference of this upper and lower bound gives us an upper bound for $\delta_n(\mathcal{A}_1 \cup \mathcal{A}_2)$. It is equal to $\delta_n(\mathcal{A}_1) + \delta_n(\mathcal{A}_2) + \delta_n(\mathcal{A}_1 \cap \mathcal{A}_2)$ after simplifying, from which

$$\begin{aligned} \Delta(\mathcal{A}_1 \cup \mathcal{A}_2) &= \sup\{\delta_n(\mathcal{A}_1 \cup \mathcal{A}_2) : n \in \mathbb{N}\} \\ &\leqslant \sup\{\delta_n(\mathcal{A}_1) + \delta_n(\mathcal{A}_2) + \delta_n(\mathcal{A}_1 \cap \mathcal{A}_2) : n \in \mathbb{N}\} \\ &= \Delta(\mathcal{A}_1) + \Delta(\mathcal{A}_2) + \Delta(\mathcal{A}_1 \cap \mathcal{A}_2) \end{aligned}$$

immediately follows. □

We can also expand the inequality from **Lemma 2.4** inductively to any (finite) union of more than two subsets in G, as follows.

Theorem 2.5. For any $n \geqslant 1$ subsets $\mathcal{A}_1, \ldots, \mathcal{A}_n \subset G$, we have

$$\Delta(\mathcal{A}_1 \cup \ldots \cup \mathcal{A}_n) = \Delta\Big(\bigcup_{t \in \{1,\ldots,n\}} \mathcal{A}_t \Big) \leqslant \sum_{\{\} \neq \mathcal{I} \subset \{1,\ldots,n\}} \Delta\Big(\bigcap_{t \in \mathcal{I}} \mathcal{A}_t \Big) .$$

Proof. For $n = 1$, the desired inequality becomes an equality, and everything is fine. Suppose that for some $n \in \mathbb{N}$, we have already established

$$\Delta\Big(\bigcup_{t \in \{1,\ldots,n\}} \mathcal{A}_t \Big) \leqslant \sum_{\{\} \neq \mathcal{I} \subset \{1,\ldots,n\}} \Delta\Big(\bigcap_{t \in \mathcal{I}} \mathcal{A}_t \Big)$$

for any n subsets $\mathcal{A}_1, \ldots, \mathcal{A}_n \subset G$.

Let $\mathcal{A}_{n+1}$ be any subset of G. According to **Lemma 2.4**, the discrepancy

$$\Delta(\mathcal{A}_1 \cup \ldots \cup \mathcal{A}_{n+1}) = \Delta((\mathcal{A}_1 \cup \ldots \cup \mathcal{A}_n) \cup \mathcal{A}_{n+1})$$

is bounded from above by

$$\Delta(\mathcal{A}_1 \cup \ldots \cup \mathcal{A}_n) + \Delta(\mathcal{A}_{n+1}) + \Delta((\mathcal{A}_1 \cup \ldots \cup \mathcal{A}_n) \cap \mathcal{A}_{n+1}) .$$

By induction, the last summand

$$\Delta((\mathcal{A}_1 \cup \cdots \cup \mathcal{A}_n) \cap \mathcal{A}_{n+1}) = \Delta\Big(\bigcup_{t \in \{1,\ldots,n\}} (\mathcal{A}_t \cap \mathcal{A}_{n+1}) \Big)$$

is bounded from above by

$$\sum_{\{\} \neq \mathcal{I} \subset \{1,\ldots,n\}} \Delta\Big(\bigcap_{t \in \mathcal{I}} (\mathcal{A}_t \cap \mathcal{A}_{n+1}) \Big) ,$$

which becomes

$$\sum_{\mathcal{I} \subset \{1,\ldots,n\}} \Delta\Big(\bigcap_{t \in \mathcal{I} \cup \{n+1\}} \mathcal{A}_i \Big)$$

after adding $\Delta(\mathcal{A}_{n+1})$.

Combining all estimates, we arrive at

$$\begin{aligned}\Delta(\mathcal{A}_1 \cup \ldots \cup \mathcal{A}_{n+1}) \\ &\leqslant \sum_{\{\} \neq \mathcal{I} \subset \{1,\ldots,n\}} \Delta\Big(\bigcap_{t \in \mathcal{I}} \mathcal{A}_t\Big) + \sum_{\mathcal{I} \subset \{1,\ldots,n\}} \Delta\Big(\bigcap_{t \in \mathcal{I} \cup \{n+1\}} \mathcal{A}_t\Big) \\ &= \sum_{\{\} \neq \mathcal{I} \subset \{1,\ldots,n,n+1\}} \Delta\Big(\bigcap_{t \in \mathcal{I}} \mathcal{A}_t\Big)\,,\end{aligned}$$

and this completes our proof by induction. □

Now, let us focus on $G = \mathbb{Z}/m\mathbb{Z}$ with the sequence of shifts $s_t = t$ ($t \in \mathbb{N}$), and take $\mathcal{A} = \mathcal{R}(m)$ as the subset of all reduced residue classes modulo m.

For a divisor d of m, $\mathcal{A}(d) := \big\{q\,d + m\mathbb{Z} : q \in \{1,\ldots,m/d\}\big\}$ forms a subgroup of the cyclic group $(\mathbb{Z}/m\mathbb{Z},+)$, and so $\Delta(\mathcal{A}(d)) \leqslant 1$ due to **Lemma 2.3**. Moreover, we can write

$$\mathcal{R}(m) = (\mathbb{Z}/m\mathbb{Z}) \setminus \bigcup_{i \in \{1,\ldots,r\}} \mathcal{A}(q_i)\,,$$

where $q_1,\ldots,q_r$ are the distinct prime factors of m in increasing order.

By **Lemma 2.1** and **Theorem 2.5**, we have

$$\begin{aligned}\Delta(\mathcal{R}(m)) &= \Delta((\mathbb{Z}/m\mathbb{Z}) \setminus \mathcal{R}(m)) \\ &= \Delta\Big(\bigcup_{i \in \{1,\ldots,r\}} \mathcal{A}(q_i)\Big) \leqslant \sum_{\{\} \neq \mathcal{I} \subset \{1,\ldots,r\}} \Delta\Big(\bigcap_{i \in \mathcal{I}} \mathcal{A}(q_i)\Big)\,.\end{aligned}$$

Since $q_1,\ldots,q_r$ are pairwise relatively prime, one finds

$$\bigcap_{i \in \mathcal{I}} q_i\mathbb{Z} = (\prod_{i \in \mathcal{I}} q_i)\mathbb{Z} \quad \text{or, equivalently,} \quad \bigcap_{i \in \mathcal{I}} \mathcal{A}(q_i) = \mathcal{A}(\prod_{i \in \mathcal{I}} q_i)$$

for non-empty $\mathcal{I} \subset \{1,\ldots,r\}$, as $\bigcup_{a \in \mathcal{A}(q_i)} a = q_i\mathbb{Z}$. Hence, we reach

$$\Delta(\mathcal{R}(m)) \leqslant \sum_{\{\} \neq \mathcal{I} \subset \{1,\ldots,r\}} \Delta\Big(\mathcal{A}(\prod_{i \in \mathcal{I}} q_i)\Big) \leqslant \sum_{\{\} \neq \mathcal{I} \subset \{1,\ldots,r\}} 1 = 2^r - 1\,,$$

where r is the number of distinct prime factors of m.

In general, if $\Delta(\mathcal{A}) < \infty$ is known, then we can bound the time in which $\mathcal{A}+s_1, \mathcal{A}+s_2, \ldots$ covers G with help of the density of $\mathcal{A}$ within G.

Lemma 2.6. Let $\mathcal{A} \subset G$ be a non-empty subset with density $\alpha = \operatorname{card}(\mathcal{A})/m$. If $\Delta(\mathcal{A}) < \infty$, then $\mathcal{A}+s_1, \mathcal{A}+s_2, \ldots$ covers G in time $\lfloor \Delta(\mathcal{A})/\alpha \rfloor + 1$.

Proof. At time $n \in \mathbb{N}$ there exists at least one element $u \in G$ which is covered at least $c_n(\mathcal{A}, u) \geqslant n \cdot \alpha$ times, because otherwise we find

$$\sum_{u \in G} c_n(\mathcal{A}, u) < \sum_{u \in G} \alpha \cdot n = m \cdot \alpha \cdot n = \operatorname{card}(\mathcal{A}) \cdot n$$

in contradiction to

$$\begin{aligned} \sum_{u \in G} c_n(\mathcal{A}, u) &= \sum_{u \in G} \Big(\sum_{t=1}^{n} \mathbf{1}_{\mathcal{A}+s_t}(u) \Big) = \sum_{t=1}^{n} \Big(\sum_{u \in G} \mathbf{1}_{\mathcal{A}+s_t}(u) \Big) \\ &= \sum_{t=1}^{n} \operatorname{card}(\mathcal{A}+s_t) = \sum_{t=1}^{n} \operatorname{card}(\mathcal{A}) = n \cdot \operatorname{card}(\mathcal{A}) \,. \end{aligned}$$

In particular, at time $n = \lfloor \Delta(\mathcal{A})/\alpha \rfloor + 1$ there exists an element $u \in G$ with

$$c_n(\mathcal{A}, u) \geqslant (\lfloor \Delta(\mathcal{A})/\alpha \rfloor + 1) \cdot \alpha > (\Delta(\mathcal{A})/\alpha) \cdot \alpha = \Delta(\mathcal{A}) \,.$$

Assume that at the same time there still exists an element $v \in G$ which has not been covered yet, that is $c_n(\mathcal{A}, v) = 0$. But then we find

$$\delta_n(\mathcal{A}) \geqslant c_n(\mathcal{A}, u) - c_n(\mathcal{A}, v) > \Delta(\mathcal{A}) - 0 = \Delta(\mathcal{A})$$

in contradiction to the definition of $\Delta(\mathcal{A})$ as $\sup\{\delta_n(\mathcal{A}) : n \in \mathbb{N}\}$. Therefore, $c_n(\mathcal{A}, v) > 0$ for all $v \in G$, and our statement is proven. □

In the case $\mathcal{A} = \mathcal{R}(m)$, we have

$$\operatorname{card}(\mathcal{R}(m)) = \varphi(m) = m \cdot \prod_{i=1}^{r} \Big(1 - \frac{1}{q_i}\Big) \,,$$

where $\varphi(m)$ denotes **Euler's phi function**, which counts all positive integers

relatively prime and up to m. The reciprocal of the density $\alpha = \varphi(m)/m$ is

$$1/\alpha = 1/\Big(\prod_{i=1}^{r} \frac{q_i - 1}{q_i}\Big) = \prod_{i=1}^{r} \frac{q_i}{q_i - 1} \leqslant \prod_{i=1}^{r} \frac{i+1}{i} = r + 1\,,$$

as $q_i \geqslant i + 1$ implies $q_i \cdot i \leqslant q_i \cdot i + q_i - (i+1) = (i+1) \cdot (q_i - 1)$.

Finally, **Lemma 2.6** can reveal that the sequence of (consecutive) translates $\mathcal{R}(m) + 1, \mathcal{R}(m) + 2, \mathcal{R}(m) + 3, \ldots$ covers $\mathbb{Z}/m\mathbb{Z}$ in time $(2^r - 1) \cdot (r + 1) + 1$. Simultaneously, this also provides an upper bound for the largest gap $j(m)$ between consecutive members in $\bigcup_{u \in \mathcal{R}(m)} u = \mathbb{Z} \setminus \bigcup_{i=1}^{r} q_i\mathbb{Z}$.

Observe that $j(m) = j(q_1 \ldots q_r)$, and so

$$\begin{aligned}
&j(2^{\varepsilon_1}) = j(2) = 2 = (2^1 - 1) \cdot (1 + 1)\,,\\
&j(3^{\varepsilon_1}) = j(3) = 2 = (2^1 - 1) \cdot (1 + 1)\,,\\
&j(2^{\varepsilon_1}3^{\varepsilon_2}) = j(2 \cdot 3) = j(6) = 4 < 9 = (2^2 - 1) \cdot (2 + 1)
\end{aligned}$$

for exponents $\varepsilon_1, \varepsilon_2 \in \mathbb{N}$. In the other case, when m contains a prime factor larger than three, then $q_i \geqslant i + 2 > i + 1$ for at least one index $i \in \{1, \ldots, r\}$. In turn, this results in the strict inequality $1/\alpha < r + 1$, and so

$$\begin{aligned}
j(m) &\leqslant \lfloor (2^r - 1) \cdot 1/\alpha \rfloor + 1\\
&\leqslant (2^r - 1) \cdot (r + 1) - 1 + 1 = (2^r - 1) \cdot (r + 1)
\end{aligned}$$

holds for these m, too. As mentioned in the introduction, this exactly coincides with the upper bound proved by Jacobsthal (see [16]).

Let us return to the discrepancy of $\mathcal{R}(m)$ with respect to the sequence of shifts $s_t = t$ ($t \in \mathbb{N}$), when $m = P_r$ is the product of the first r primes. With help of a computer (see **Algorithm 1** in the appendix), we found the values

$$\begin{aligned}
&\Delta(\mathcal{R}(P_1)) = 1\,, \quad \Delta(\mathcal{R}(P_2)) = 2\,, \quad \Delta(\mathcal{R}(P_3)) = 3\,,\\
&\Delta(\mathcal{R}(P_4)) = 5\,, \quad \Delta(\mathcal{R}(P_5)) = 8\,, \quad \Delta(\mathcal{R}(P_6)) = 13\,.
\end{aligned}$$

Unfortunately, we were not able to compute the next value $\Delta(\mathcal{R}(P_7))$ due to the running time of our algorithm. However, these found values match with the

first **Fibonacci numbers**, which are recursively defined by $f_0 = 0$, $f_1 = 1$ and then $f_{r+1} = f_r + f_{r-1}$ for $r \in \mathbb{N}$. It is known (due to Binet's explicit formula) that the Fibonacci numbers f_r exhibit an exponential growth with r, and thus the discrepancy $\Delta(\mathcal{R}(P_r))$ might also grow exponentially with r.

Moreover, we like to mention that the inequality from **Lemma 2.4** can be tight. For example, if we choose $G = \mathbb{Z}/35\mathbb{Z}$ and the subgroups

$$\mathcal{A}_1 = \big\{5q + 35\mathbb{Z} : q \in \{1, \dots, 7\}\big\},$$
$$\mathcal{A}_2 = \big\{7q + 35\mathbb{Z} : q \in \{1, \dots, 5\}\big\},$$

with $\mathcal{A}_1 \cap \mathcal{A}_2 = 0 + 35\mathbb{Z}$, then by **Lemma 2.3** all three of these subgroups have discrepancy 1 with respect to the sequence of shifts $s_t = t$ ($t \in \mathbb{N}$).

At time $t = 8$, we observe that $c_8(\mathcal{A}_1 \cup \mathcal{A}_2, 21 + 35\mathbb{Z}) = 4$, as there are exactly four multiples of 5 or 7 among the eight consecutive integers from 14 up to 21, and $c_8(\mathcal{A}_1 \cup \mathcal{A}_2, 4 + 35\mathbb{Z}) = 1$, as there is only one multiple of 5 or 7 among the eight consecutive integers from -3 up to 4. Now we can see that

$$\Delta(\mathcal{R}(5 \cdot 7)) = \Delta(\mathcal{A}_1 \cup \mathcal{A}_2) \geqslant 4 - 1 = 3$$

in contrast to $\Delta(\mathcal{R}(P_2)) = \Delta(\mathcal{R}(2 \cdot 3)) = 2$ from above, and that $\Delta(\mathcal{A}_1 \cup \mathcal{A}_2)$ in fact is equal to the sum $\Delta(\mathcal{A}_1) + \Delta(\mathcal{A}_2) + \Delta(\mathcal{A}_1 \cap \mathcal{A}_2) = 1 + 1 + 1 = 3$.

2.2 Bounding minimal covering time via density

Let us not focus on a single fixed sequence of shifts anymore. Instead, for a given non-empty subset $\mathcal{A} \subset G$, we now aim to find an upper bound for the smallest number of translates of $\mathcal{A}$ one needs to cover G.

By an averaging argument, we first prove an auxiliary lemma about how many elements of a non-empty subset $\mathcal{B} \subset G$ a single translate of $\mathcal{A}$ can cover, provided one knows the **density** $\alpha = \operatorname{card}(\mathcal{A})/m$ of $\mathcal{A}$ within G.

Lemma 2.7. Let $(G, +)$ be a finite additive group of order m. For non-empty subsets $\mathcal{A}$ and $\mathcal{B}$ of G with $\alpha = \operatorname{card}(\mathcal{A})/m$ and $B = \operatorname{card}(\mathcal{B})$, we can find:

(1) a translate of $\mathcal{A}$ covering at least αB elements of $\mathcal{B}$.

(2) at least m/B distinct shifts s in G such that each translate $\mathcal{A}+s$ covers at least $\lfloor \alpha B \rfloor$ elements of $\mathcal{B}$.

(3) more than $\alpha m/(2-\alpha)$ distinct shifts s in G such that each translate $\mathcal{A}+s$ covers at least $\alpha B/2$ elements of $\mathcal{B}$.

Proof. First, we compute

$$\begin{aligned}\sum_{s\in G} \operatorname{card}(\mathcal{B}\cap(\mathcal{A}+s)) &= \sum_{s\in G}\Big(\sum_{u\in G} \mathbf{1}_{\mathcal{B}}(u)\cdot \mathbf{1}_{\mathcal{A}+s}(u)\Big)\\ &= \sum_{u\in G}\Big(\sum_{s\in G} \mathbf{1}_{\mathcal{B}}(u)\cdot \mathbf{1}_{\mathcal{A}}(u-s)\Big)\\ &= \sum_{u\in G}\Big(\mathbf{1}_{\mathcal{B}}(u)\cdot \sum_{x\in G} \mathbf{1}_{\mathcal{A}}(x)\Big)\\ &= \sum_{u\in \mathcal{B}} \operatorname{card}(\mathcal{A}) = B\cdot \operatorname{card}(\mathcal{A})\,.\end{aligned}$$

By the pigeonhole principle, at least one of all $\operatorname{card}(G)=m$ summands has to be at least $B\cdot\operatorname{card}(\mathcal{A})/m = B\cdot\alpha$, as necessary for (1).

In the case of statement (2), we may assume $\alpha B \geqslant 1$, because otherwise $\lfloor \alpha B\rfloor = 0$, and (2) would be clear. Let x be the number of shifts $s\in G$ such that $\operatorname{card}(\mathcal{B}\cap(\mathcal{A}+s)) \geqslant \lfloor \alpha B\rfloor$. Each of the $m-x$ other translates of $\mathcal{A}$ covers at most $\lfloor \alpha B\rfloor - 1 \leqslant \alpha B - 1$ elements of $\mathcal{B}$. If $x < m/B$, we then would have

$$\begin{aligned}\sum_{s\in G} \operatorname{card}(\mathcal{B}\cap(\mathcal{A}+s)) &\leqslant x\cdot B + (m-x)\cdot(\alpha B-1)\\ &\leqslant x\cdot B + m\cdot(\alpha B-1)\\ &< m/B\cdot B + B\cdot \alpha m - m\\ &= B\cdot\operatorname{card}(\mathcal{A})\,,\end{aligned}$$

and so only $x\geqslant m/B$ remains, from which (2) follows.

Now, we turn to statement (3). Let x be the number of shifts $s\in G$ such that $\operatorname{card}(\mathcal{B}\cap(\mathcal{A}+s)) \geqslant \alpha B/2$. Each of the $m-x$ other translates of $\mathcal{A}$ covers less

than $\alpha B/2$ elements of $\mathcal{B}$ this time. If $x \leqslant \alpha m/(2-\alpha)$, we then would have

$$\begin{aligned}\sum_{s \in G} \operatorname{card}(\mathcal{B} \cap (\mathcal{A}+s)) &< x \cdot B + (m-x) \cdot \alpha B/2 \\ &= B \cdot (\alpha m/2 + x \cdot (1-\alpha/2)) \\ &\leqslant B \cdot (\alpha m/2 + \alpha m/(2-\alpha) \cdot (2-\alpha)/2) \\ &= B \cdot \operatorname{card}(\mathcal{A})\,,\end{aligned}$$

and so only $x > \alpha m/(2-\alpha)$ remains, from which (3) follows. □

By applying **Lemma 2.7** iteratively, we are now able to bound the minimal (covering) time t_0, for which there exists a sequence $(s_t)_{t \in \mathbb{N}}$ of shifts in G such that the induced sequence $(\mathcal{A}+s_t)_{t \in \mathbb{N}}$ of translates covers G in time t_0.

Theorem 2.8. Let $(G,+)$ be a finite additive group of order m. For any non-empty subset $\mathcal{A} \subset G$ with density $\alpha = \operatorname{card}(\mathcal{A})/m$, there exists a sequence $s_1, s_2, \ldots$ of shifts in G such that the induced sequence $\mathcal{A}+s_1, \mathcal{A}+s_2, \ldots$ of translates covers G in time $\lfloor (\log m)/\alpha \rfloor + 1$.

Proof. We claim that there exists a sequence $(s_t)_{t \in \mathbb{N}}$ of shifts in G such that $G'_n := G \setminus \bigcup_{t=1}^{n} (\mathcal{A}+s_t)$ contains at most $(1-\alpha)^n \cdot m$ elements, which have not been covered by the corresponding first n translates of $\mathcal{A}$ yet.

For $\mathcal{A}+s_1$ we can take any translate of $\mathcal{A}$, since each of them covers exactly $\operatorname{card}(\mathcal{A}) = \alpha \cdot m$ elements in G, and thus leaves $m - \alpha \cdot m = (1-\alpha) \cdot m$ many elements in $G'_1 = G \setminus (\mathcal{A}+s_1)$. Suppose that we have already found the first n translates such that $\operatorname{card}(G'_n) \leqslant (1-\alpha)^n \cdot m$. Choosing $\mathcal{B} = G'_n$ in **Lemma 2.7**, one can also find a translate $\mathcal{A}+s_{n+1}$ covering at least $\alpha \cdot \operatorname{card}(G'_n)$ elements in G'_n. This leaves at most

$$\operatorname{card}(G'_n) - \alpha \cdot \operatorname{card}(G'_n) = (1-\alpha) \cdot \operatorname{card}(G'_n) \leqslant (1-\alpha)^{n+1} \cdot m$$

elements in $G'_{n+1} = G'_n \setminus (\mathcal{A}+s_{n+1})$, and our claim follows by induction.

As soon as $\operatorname{card}(G'_n) \leqslant (1-\alpha)^n \cdot m < 1$ $(*)$, we get $\bigcup_{t=1}^{n} (\mathcal{A}+s_t) = G$. In the special case $\alpha = 1$, which means that $\mathcal{A} = G$, the inequality $(*)$ is satisfied at time $n = 1$, and thus we may assume $\alpha < 1$ from now on.

After multiplying the inequality $(*)$ with the reciprocal of $(1-\alpha)^n > 0$, and taking the (monotone increasing) natural logarithm on both sides, we can see that it holds true for all natural numbers n larger than

$$\log m \Big/ \log\Big(\frac{1}{1-\alpha}\Big)\,.$$

In particular, there is one of them not exceeding

$$\Big\lfloor \log m \Big/ \log\Big(\frac{1}{1-\alpha}\Big)\Big\rfloor + 1\,,$$

where the denominator is bounded from below by

$$\Big(\frac{1}{1-\alpha} - 1\Big)\Big/\Big(\frac{1}{1-\alpha}\Big) = \Big(\frac{\alpha}{1-\alpha}\Big)\Big/\Big(\frac{1}{1-\alpha}\Big) = \alpha$$

due to the well-known inequality $\log x \geqslant (x-1)/x$ being valid for all $x \geqslant 1$. This completes our proof. □

As our main application, let us return to the case of $G = \mathbb{Z}/m\mathbb{Z}$ with $\mathcal{A} = \mathcal{R}(m)$, where m is the product P_r of the first r primes. Here, we know that the density of $\mathcal{R}(P_r)$ within $\mathbb{Z}/P_r\mathbb{Z}$ is given by

$$\alpha = \varphi(m)/m = \prod_{i=1}^{r}\Big(1-\frac{1}{p_i}\Big) = \prod_{p\leqslant p_r}\Big(1-\frac{1}{p}\Big) \geqslant \frac{c_1}{\log p_r}\,,$$

for some absolute positive constant c_1, due to Mertens' asymptotic formula

$$\lim_{x\to\infty}(\log x)\cdot\prod_{p\leqslant x}\Big(1-\frac{1}{p}\Big) = 1/e^{\gamma}\,,$$

where γ is Euler's constant. Moreover, for absolute constants c_2 and c_3, we get

$$m = P_r = \prod_{i=1}^{r} p_i = \prod_{p\leqslant p_r} p \leqslant c_2\, e^{p_r} \quad \text{and} \quad p_r \leqslant c_3\, r\log r\,,$$

via the **prime number theorem** in the forms

$$\lim_{x\to\infty}\Big(\prod_{p\leqslant x} p\Big)/e^{x} = 1 \quad \text{and} \quad \lim_{r\to\infty} p_r/(r\log r) = 1\,.$$

Finally, **Theorem 2.8** implies that $G = \mathbb{Z}/P_r\mathbb{Z}$ can be covered by

$$\begin{aligned}\lfloor(\log m)/\alpha\rfloor + 1 &\leqslant (\log P_r)/(c_1/\log p_r) + 1\\ &\leqslant (1/c_1)\log(c_2\, e^{p_r})\,(\log p_r) + 1\\ &= (1/c_1)\,((\log c_2) + p_r)\,(\log p_r) + 1\\ &\leqslant c_4 \cdot p_r(\log p_r)\\ &\leqslant c_4 \cdot (c_3\, r\log r)\log(c_3\, r\log r)\\ &= c_4 \cdot (c_3\, r\log r)\,(\log r + \log\log r + \log c_3)\\ &\leqslant c_4 \cdot (c_3\, r\log r)\,(c_5\log r)\\ &= c_3\, c_4\, c_5 \cdot r\,(\log r)^2\end{aligned}$$

many translates of $\mathcal{A} = \mathcal{R}(P_r)$, where c_4 and c_5 are absolute constants.

Actually, in his book [23] from 1994, Montgomery conjectures that

$$j(P_r) \leqslant c \cdot r\,(\log r)^2$$

for some absolute constant c. Recall that $j(m)$ coincides with the minimal (covering) time, in which $(\mathcal{R}(m) + t)_{t\in\mathbb{N}}$ covers $\mathbb{Z}/m\mathbb{Z}$. In view of the proof for **Theorem 2.8**, the conjecture of Montgomery would then follow, if one can choose $(t)_{t\in\mathbb{N}}$ as the sequence $(s_t)_{t\in\mathbb{N}}$ of shifts, which we built up stepwise via **Lemma 2.7**, to ensure that $\operatorname{card}(G'_{n-1} \cap (\mathcal{A} + s_n)) \geqslant \alpha \cdot \operatorname{card}(G'_{n-1})$ holds at every time $n \in \mathbb{N}$. This leads to the following definition.

Given a subset $\mathcal{A} \subset G$ and a sequence $(s_t)_{t\in\mathbb{N}}$ of shifts in G, let us again write $G'_n := G \setminus \bigcup_{t=1}^{n}(\mathcal{A} + s_t)$ for each $n \in \mathbb{N}$, and set $G'_0 := G$.

A sequence $(s_t)_{t\in\mathbb{N}}$ of shifts is called **good** for $\mathcal{A}$ at time n, if

$$\begin{aligned}\operatorname{card}(G'_{n-1} \cap (\mathcal{A} + s_n)) &\geqslant \alpha \cdot \operatorname{card}(G'_{n-1})\\ &= (1/m) \cdot \sum_{s\in G} \operatorname{card}(G'_{n-1} \cap (\mathcal{A} + s))\,,\end{aligned}$$

where the sum equals $\operatorname{card}(G'_{n-1}) \cdot \operatorname{card}(\mathcal{A})$, as in the proof of property (1) from **Lemma 2.7** (with $\mathcal{B} = G'_{n-1}$). Moreover, if a sequence $(s_t)_{t\in\mathbb{N}}$ of shifts is good for $\mathcal{A}$ at every time $n \in \mathbb{N}$, then we simply say $(s_t)_{t\in\mathbb{N}}$ is good for $\mathcal{A}$.

Since $\mathrm{card}(G'_{n-1}) = \mathrm{card}(G) - \mathrm{card}\big(\bigcup_{t=1}^{n-1}(\mathcal{A}+s_t)\big)$ and

$$\mathrm{card}(G'_{n-1} \cap (\mathcal{A}+s_n)) = \mathrm{card}\Big(\bigcup_{t=1}^{n}(\mathcal{A}+s_t)\Big) - \mathrm{card}\Big(\bigcup_{t=1}^{n-1}(\mathcal{A}+s_t)\Big)\,,$$

note that if a sequence $(s_t)_{t\in\mathbb{N}}$ of shifts is good for $\mathcal{A}$ (at time n), then it is also good for any translate of $\mathcal{A}$ (at time n), whenever $(G,+)$ is commutative, as the following identity holds in this case.

Lemma 2.9. Let $(G,+)$ be commutative and $(s_t)_{t\in\mathbb{N}}$ be a sequence of shifts in G. For any given subset $\mathcal{A}\subset G$ and any shift $s\in G$, we have

$$\mathrm{card}\Big(\bigcup_{t=1}^{n}((\mathcal{A}+s)+s_t)\Big) = \mathrm{card}\Big(\bigcup_{t=1}^{n}(\mathcal{A}+s_t)\Big)$$

at every time $n\in\mathbb{N}$.

Proof. At every time $n\in\mathbb{N}$, we find $c_n(\mathcal{A}+s,u) = c_n(\mathcal{A},u-s)$ for every $u\in G$, as seen in the proof of **Lemma 2.2**. In particular, $c_n(\mathcal{A}+s,u)>0$ if and only if $c_n(\mathcal{A},u-s)>0$. In turn, this equivalence can be restated as

$$u\in\bigcup_{t=1}^{n}((\mathcal{A}+s)+s_t) \quad\text{if and only if}\quad u-s\in\bigcup_{t=1}^{n}(\mathcal{A}+s_t)\,.$$

Since the map $u\mapsto u-s$ forms a bijection on G, our claim follows. □

Later, we also make use of the following simple fact.

Lemma 2.10. Let $(s_t)_{t\in\mathbb{N}}$ be good for $\mathcal{A}\subset G$ at time n. If

$$\mathrm{card}(G'_{n}\cap(\mathcal{A}+s_{n+1})) \geqslant \mathrm{card}(G'_{n-1}\cap(\mathcal{A}+s_n))\,,$$

then $(s_t)_{t\in\mathbb{N}}$ is also good for $\mathcal{A}$ at time $n+1$.

Proof. By definition, we have

$$\mathrm{card}(G'_{n-1}\cap(\mathcal{A}+s_n)) \geqslant \alpha\cdot\mathrm{card}(G'_{n-1})$$

at time n, and therefore also

$$\begin{aligned}\operatorname{card}(G'_n \cap (\mathcal{A} + s_{n+1})) &\geqslant \operatorname{card}(G'_{n-1} \cap (\mathcal{A} + s_n)) \\ &\geqslant \alpha \cdot \operatorname{card}(G'_{n-1}) \\ &\geqslant \alpha \cdot \operatorname{card}(G'_n)\end{aligned}$$

at time $n+1$, as $G'_n = G'_{n-1} \setminus (\mathcal{A} + s_n) \subset G'_{n-1}$. □

Recall that $j(P_r) \leqslant c \cdot r\,(\log r)^2$ would follow, if one can show that the sequence $(s_t)_{t\in\mathbb{N}}$ of shifts $s_t = t$ (or $s_t = t-1$), which forms an **arithmetic progression**, is good for $\mathcal{R}(P_r)$. In the next section, we therefore proceed by studying the existence of good arithmetic progressions in more detail.

2.3 Good arithmetic progressions for simple boxes

Again, let m be the product of r distinct primes $q_1, \ldots, q_r$.

By the Chinese remainder theorem, $\mathbb{Z}/m\mathbb{Z}$ can then also be identified with the Cartesian product $\prod_{i=1}^{r}(\mathbb{Z}/q_i\mathbb{Z})$ via the bijection which maps $[a]_m = a + m\mathbb{Z}$ to $([a]_{q_1}, \ldots, [a]_{q_r})$ in $G = \prod_{i=1}^{r}(\mathbb{Z}/q_i\mathbb{Z})$. For example, $\mathcal{R}(m)$ then becomes $\mathcal{R}(q_1) \times \ldots \times \mathcal{R}(q_r)$, where $\mathcal{R}(q_i) = \{[1]_{q_i}, \ldots, [q_i - 1]_{q_i}\} = (\mathbb{Z}/q_i\mathbb{Z}) \setminus \{[0]_{q_i}\}$ is only missing the additive neutral element of $\mathbb{Z}/q_i\mathbb{Z}$, for each $i \in \{1, \ldots, r\}$. In general, a **box** $\mathcal{B} = \prod_{i=1}^{r} \mathcal{B}_i \subset G$ with non-empty sets $\mathcal{B}_i \subset \mathbb{Z}/q_i\mathbb{Z}$ is called **simple**, if each $\mathcal{B}_i$ forms an arithmetic progression with common difference $[1]_{q_i}$. For $b_i \in \{1, \ldots, q_i\}$, let us put $\mathcal{B}_{q_1,\ldots,q_r}(b_1, \ldots, b_r) := \prod_{i=1}^{r}\{[1]_{q_i}, \ldots, [b_i]_{q_i}\}$.

Given any simple box $\mathcal{B} \subset G$, does there always exist a good sequence $(\boldsymbol{s}_t)_{t\in\mathbb{N}}$ of shifts (in G) for $\mathcal{B}$, whose members $\boldsymbol{s}_t = t \cdot \boldsymbol{d}$ (or $(t-1) \cdot \boldsymbol{d}$) form an arithmetic progression for some $\boldsymbol{d} \in G$? Actually, every simple box $\mathcal{B} \subset G$ forms a translate of some simple box in the shape $\mathcal{B}_{q_1,\ldots,q_r}(b_1, \ldots, b_r)$, and so (due to **Lemma 2.9**) it is enough to consider only these ones.

In the case $r = 1$, given any simple box $\mathcal{B}_q(b) = \{[1]_q, \ldots, [b]_q\}$ for a prime q and $b \in \{1, \ldots, q\}$, the sequence of shifts $\boldsymbol{s}_t = (t-1) \cdot [b]_q$ $(t \in \mathbb{N})$ turns out to be good for $\mathcal{B}_q(b)$. Of course, as the first translate, $\mathcal{B}_q(b)$ is covering exactly $b = b/q \cdot q$ elements of $\mathbb{Z}/q\mathbb{Z}$ (where b/q is the density of $\mathcal{B}_q(b)$ within $\mathbb{Z}/q\mathbb{Z}$).

As long as $t \leqslant \lceil q/b \rceil - 1 < q/b$, where $\lceil x \rceil$ denotes the smallest integer larger than or equal to $x \in \mathbb{R}$, each next translate

$$\mathcal{B}_q(b) + \boldsymbol{s}_t = \{[(t-1)\cdot b + 1]_q, \ldots, [(t-1)\cdot b + b]_q\}$$

covers exactly b not yet covered elements again, and **Lemma 2.10** ensures that $(\boldsymbol{s}_t)_{t\in\mathbb{N}}$ stays good for $\mathcal{B}_q(b)$ here. Finally, at time $t = \lceil q/b \rceil$, we have

$$\mathcal{B}_q(b) + \boldsymbol{s}_{\lceil q/b \rceil} = \{[(\lceil q/b \rceil - 1)\cdot b + 1]_q, \ldots, [(\lceil q/b \rceil - 1)\cdot b + b]_q\}\,,$$

where $(\lceil q/b \rceil - 1)\cdot b + b \geqslant (q/b - 1)\cdot b + b = q$. Hence, the members of the translate $\mathcal{B}_q(b) + \boldsymbol{s}_{\lceil q/b \rceil}$ cover perhaps fewer (than b) but all remaining elements in $\mathbb{Z}/q\mathbb{Z}$, and everything is fine.

In particular, the arithmetic progression $((t-1)\cdot [q-1]_q)_{t\in\mathbb{N}}$ is good for

$$\mathcal{B}_q(q-1) = \{[1]_q, \ldots, [q-1]_q\} = \mathcal{R}(q)\,,$$

and one easily checks that $((t-1)\cdot d)_{t\in\mathbb{N}}$ is good for all $d \in \mathcal{R}(q)$, as we only need to ensure that the missing element $[q]_q = [0]_q$ is covered at time $t = 2$.

Actually, in higher dimensions r it also turns out that either all or none of the arithmetic progressions $(t\cdot \boldsymbol{d})_{t\in\mathbb{N}}$ with $\boldsymbol{d} \in \mathcal{R}(q_1)\times\ldots\times\mathcal{R}(q_r)$ are good for $\mathcal{B}_{q_1,\ldots,q_r}(q_1-1,\ldots,q_r-1)$.

Proposition 2.11. Let $(s_t)_{t\in\mathbb{N}}$ be a sequence of integers, and let m be a product of r distinct primes $q_1,\ldots,q_r$. If $d \in \mathbb{N}$ is relatively prime to m, then

$$\operatorname{card}\Big(\bigcup_{t=1}^{n} (\mathcal{R}(m) + d\cdot s_t)\Big) = \operatorname{card}\Big(\bigcup_{t=1}^{n} (\mathcal{R}(m) + s_t)\Big)$$

holds at every time $n \in \mathbb{N}$.

Proof. For an element $[a]_m \in \mathbb{Z}/m\mathbb{Z}$ and $n \in \mathbb{N}$, let us compare the number

$$c_n(\mathcal{R}(m), [a]_m) = \sum_{t=1}^{n} \mathbf{1}_{\mathcal{R}(m)+s_t}([a]_m) = \sum_{t=1}^{n} \mathbf{1}_{\mathcal{R}(m)}([a-s_t]_m)$$

with the value of the sum

$$\sum_{t=1}^{n} \mathbf{1}_{\mathcal{R}(m)+d\cdot s_t}([d\cdot a]_m) = \sum_{t=1}^{n} \mathbf{1}_{\mathcal{R}(m)}([d\cdot(a-s_t)]_m)\,,$$

which counts how many times the element $[d\cdot a]_m$ is covered by one of the translates $\mathcal{R}(m)+d\cdot s_1,\dots,\mathcal{R}(m)+d\cdot s_n$. In fact, both of them are equal, because we have the identity

$$\mathbf{1}_{\mathcal{R}(m)}([a-s_t]_m) = \mathbf{1}_{\mathcal{R}(m)}([d\cdot(a-s_t)]_m) \quad \text{for all } t\in\{1,\dots,n\}$$

due to the equivalence $[a-s_t]_m\in\mathcal{R}(m) \Leftrightarrow [d\cdot(a-s_t)]_m\in\mathcal{R}(m)$, as d is relatively prime to m. In particular, the element $[a]_m$ is covered by at least one of the translates $\mathcal{R}(m)+s_1,\dots,\mathcal{R}(m)+s_n$ if and only if the element $[d\cdot a]_m$ is covered by at least one of the translates $\mathcal{R}(m)+d\cdot s_1,\dots,\mathcal{R}(m)+d\cdot s_n$.

Since the map $[a]_m\mapsto[d\cdot a]_m=[d]_m\cdot[a]_m$ forms a bijection on $\mathbb{Z}/m\mathbb{Z}$ (together with the inverse map $[a]_m\mapsto[d]_m^{-1}\cdot[a]_m$, where $[d]_m^{-1}$ from $\mathcal{R}(m)$ is the multiplicative inverse element of $[d]_m$ in $\mathcal{R}(m)$), our claim follows. □

As a direct consequence, we can restate **Proposition 2.11**, in the special case $s_t=t$ ($t\in\mathbb{N}$), in the following form.

Corollary 2.12. Let $q_1,\dots,q_r$ be r distinct primes.
If $\boldsymbol{d}\in\mathcal{R}(q_1)\times\ldots\times\mathcal{R}(q_r)=\mathcal{B}_{q_1,\dots,q_r}(q_1-1,\dots,q_r-1)=:\mathcal{B}$, then

$$\operatorname{card}\Big(\bigcup_{t=1}^{n}(\mathcal{B}+t\cdot\boldsymbol{d})\Big) = \operatorname{card}\Big(\bigcup_{t=1}^{n}(\mathcal{B}+t\cdot([1]_{q_1},\dots,[1]_{q_r})\Big)$$

holds at every time $n\in\mathbb{N}$.

From now on, we sometimes simply say that $\boldsymbol{d}\in\prod_{i=1}^{r}(\mathbb{Z}/q_i\mathbb{Z})=G$ is good for a simple box $\mathcal{B}\subset G$, if the arithmetic progression $((t-1)\cdot\boldsymbol{d})_{t\in\mathbb{N}}$ (or, equivalently, $(t\cdot\boldsymbol{d})_{t\in\mathbb{N}}$) is good for $\mathcal{B}$.

In the case $r=2$, let us first consider the simple box $\mathcal{B}(2)=\mathcal{B}_{2,3}(1,2)$, where $\mathcal{B}(r)=\mathcal{B}_{p_1,\dots,p_r}(p_1-1,\dots,p_r-1)$ from the introduction. Here one can easily check that $([1]_2,[1]_3)$ is good for $\mathcal{B}(2)$ (see **Figure 1**).

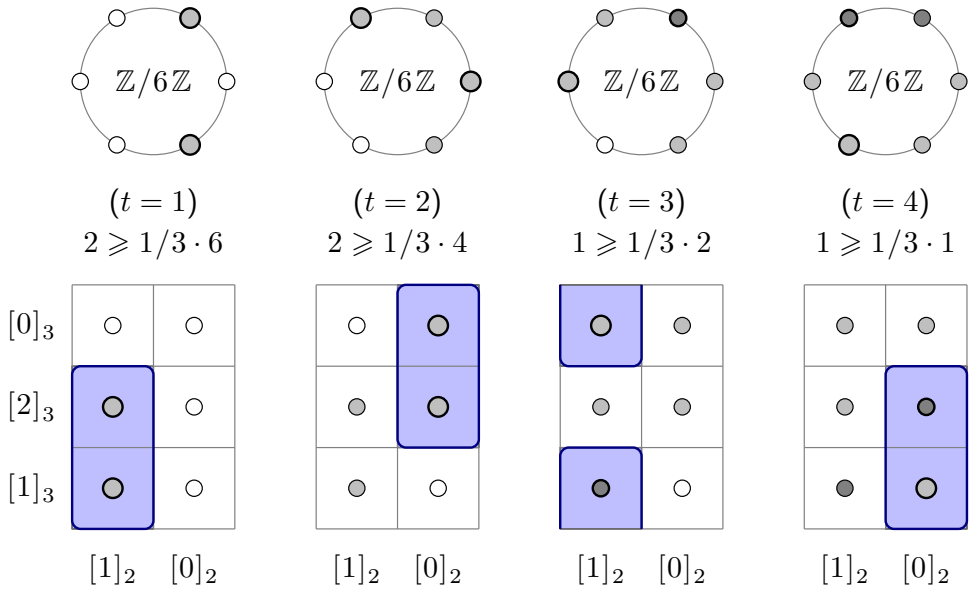


Figure 1: A good covering of $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ by translates of $\mathcal{B}(2) = \mathcal{B}_{2,3}(1,2)$, and the corresponding covering of $\mathbb{Z}/6\mathbb{Z}$ by translates of $\mathcal{R}(6)$.

Similarly, $([1]_3, [1]_5)$ turns out to be good for $\mathcal{B}_{3,5}(2,4)$ (see **Figure 2**).

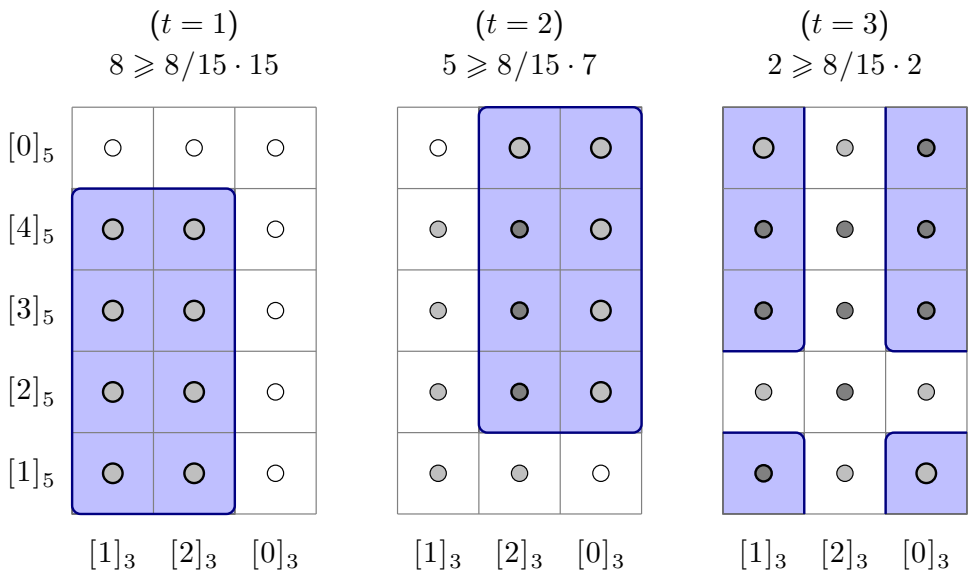


Figure 2: A good covering of $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$ by translates of $\mathcal{B}_{3,5}(2,4)$.

Note that in our modular setup one only needs three translates of $\mathcal{B}_{3,5}(2,4)$ in order to cover $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$, as opposed to $2^2 = 4$ translates arranged in a lattice-like pattern (where each translate covers only one of the four "corners").

Both examples might lead to the idea that in order to construct a good $\boldsymbol{d} \in \mathcal{R}(q_1) \times \mathcal{R}(q_2)$ for $\mathcal{B}_{q_1,q_2}(b_1,b_2)$, one can choose a good $d_1 \in \mathcal{R}(q_1)$ for $\mathcal{B}_{q_1}(b_1)$ and a good $d_2 \in \mathcal{R}(q_2)$ for $\mathcal{B}_{q_2}(b_2)$, and then combine both of them to $\boldsymbol{d} = (d_1, d_2)$. Unfortunately, this is not true in general. For example, if we look at $\mathcal{B}_{3,5}(1,2)$, then $d_1 = [1]_3$ is good for $\mathcal{B}_3(1)$ and $d_2 = [2]_5$ is good for $\mathcal{B}_5(2)$, but $\boldsymbol{d} = ([1]_3, [2]_5)$ is not good for $\mathcal{B}_{3,5}(1,2)$ at time $t = 4$ (see **Figure 3**).

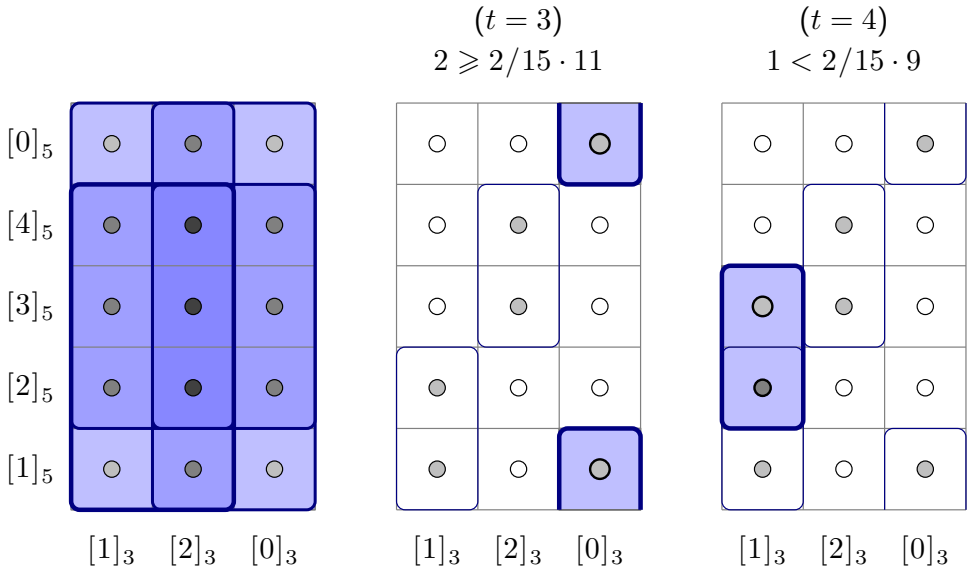


Figure 3: A covering of $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$ by four translates of $\mathcal{B}_{3,5}(2,4)$ arranged in a lattice-like pattern, and a demonstration that $((t-1) \cdot \boldsymbol{d})_{t \in \mathbb{N}}$ with $\boldsymbol{d} = ([1]_3, [2]_5)$ is not good for $\mathcal{B}_{3,5}(1,2)$ at time $t = 4$.

However, in the special cases $b_1 = 1$ or $b_2 = 1$, we can successfully modify the idea from above in the following (even more generally applicable) way.

Proposition 2.13. Let $q_1, \ldots, q_r$ and p be distinct primes. For $i \in \{1, \ldots, r\}$, let $[p]_{q_i}^{-1}$ be the multiplicative inverse element of $[p]_{q_i}$ in $\mathbb{Z}/q_i\mathbb{Z}$. If the sequence $(\boldsymbol{s}_t)_{t \in \mathbb{N}}$ of shifts $\boldsymbol{s}_t = (t-1) \cdot \boldsymbol{d}$ with $\boldsymbol{d} \in \prod_{i=1}^{r} (\mathbb{Z}/q_i\mathbb{Z}) = G$ is good for the

simple box $\mathcal{B}_{q_1,\dots,q_r}(b_1,\dots,b_r) =: \mathcal{B}$, then the sequence $(\overline{\boldsymbol{s}}_t)_{t\in\mathbb{N}}$ of shifts

$$\overline{\boldsymbol{s}}_t = (t-1)\cdot(\boldsymbol{d}(1)\cdot[p]_{q_1}^{-1},\dots,\boldsymbol{d}(r)\cdot[p]_{q_r}^{-1},[1]_p)$$

in $G\times(\mathbb{Z}/p\mathbb{Z})$ is good for the simple box $\mathcal{B}_{q_1,\dots,q_r,p}(b_1,\dots,b_r,1) =: \mathcal{B}_p$.

Proof. Let $\varepsilon_n := \operatorname{card}(G'_{n-1}\cap(\mathcal{B}+\boldsymbol{s}_n)) = \operatorname{card}\big((\mathcal{B}+\boldsymbol{s}_n)\setminus\bigcup_{t=1}^{n-1}(\mathcal{B}+\boldsymbol{s}_t)\big)$ and $\overline{\varepsilon}_n := \operatorname{card}\big((\mathcal{B}_p+\overline{\boldsymbol{s}}_n)\setminus\bigcup_{t=1}^{n-1}(\mathcal{B}_p+\overline{\boldsymbol{s}}_t)\big)$.

By the assumption that $(\boldsymbol{s}_t)_{t\in\mathbb{N}}$ is good for $\mathcal{B}$, we have

$$\varepsilon_n \geqslant \alpha\cdot\operatorname{card}(G'_{n-1}) = \alpha\cdot\Big(\operatorname{card}(G)-\sum_{t=1}^{n-1}\varepsilon_t\Big)\,,$$

where $\alpha = (b_1\dots b_r)/(q_1\dots q_r)$ is the density of $\mathcal{B}$ within G, and we need to show that

$$\overline{\varepsilon}_n \geqslant \alpha/p\cdot\Big(\operatorname{card}(G)\cdot p-\sum_{t=1}^{n-1}\overline{\varepsilon}_t\Big) = \alpha\cdot\operatorname{card}(G)-\alpha/p\cdot\sum_{t=1}^{n-1}\overline{\varepsilon}_t\,,$$

where $\alpha\cdot 1/p$ is the density of $\mathcal{B}_p$ within $G\times(\mathbb{Z}/p\mathbb{Z})$.

Observe that $\bigcup_{a=1}^{p}(G\times\{[a]_p\})$ forms a partition of $G\times(\mathbb{Z}/p\mathbb{Z})$.

Moreover, $\mathcal{B}_p = \mathcal{B}_{q_1,\dots,q_r,p}(b_1,\dots,b_r,1) = \mathcal{B}\times\{[1]_p\}\subset G\times\{[1]_p\}$, and so

$$\mathcal{B}_p+\overline{\boldsymbol{s}}_t = \mathcal{B}_p+(t-1)\cdot(\overline{\boldsymbol{s}}_t(1),\dots,\overline{\boldsymbol{s}}_t(r),[1]_p)\subset G\times\{[t]_p\}\,.$$

In particular, $(\mathcal{B}_p+\overline{\boldsymbol{s}}_t)\cap(G\times\{[a]_p\})$ is empty for all $[a]_p\in(\mathbb{Z}/p\mathbb{Z})\setminus\{[t]_p\}$. At time $n = u\cdot p+v$, with (unique) $u\in\mathbb{N}_0$ and $v\in\{1,\dots,p\}$, this means

$$(G\times\{[v]_p\})\cap\bigcup_{t=1}^{u\cdot p+v}(\mathcal{B}_p+\overline{\boldsymbol{s}}_t) = \bigcup_{k=0}^{u}(\mathcal{B}_p+\overline{\boldsymbol{s}}_{k\cdot p+v})\,,$$

where $\overline{\boldsymbol{s}}_{k\cdot p+v} = \overline{\boldsymbol{s}}_{k\cdot p+1}+\overline{\boldsymbol{s}}_v$ and

$$\overline{\boldsymbol{s}}_{k\cdot p+1} = (k\cdot p)\cdot(\boldsymbol{d}(1)\cdot[p]_{q_1}^{-1},\dots,\boldsymbol{d}(r)\cdot[p]_{q_r}^{-1},[1]_p)\,.$$

For $i \in \{1, \ldots, r\}$, the i-th component of $\overline{\boldsymbol{s}}_{k \cdot p+1}$ turns out to be

$$(k \cdot p) \cdot \boldsymbol{d}(i) \cdot [p]_{q_i}^{-1} = k \cdot \boldsymbol{d}(i) \cdot [p]_{q_i} \cdot [p]_{q_i}^{-1} = k \cdot \boldsymbol{d}(i)\,,$$

while its last component is $(k \cdot p) \cdot [1]_p = [k \cdot p]_p = [0]_p$. By the so found link,

$$\begin{aligned}\mathcal{B}_p + \overline{\boldsymbol{s}}_{k \cdot p+1} &= \mathcal{B} \times \{[1]_p\} + (k \cdot \boldsymbol{d}(1), \ldots, k \cdot \boldsymbol{d}(r), [0]_p) \\ &= \mathcal{B} \times \{[1]_p\} + (\boldsymbol{s}_{k+1}(1), \ldots, \boldsymbol{s}_{k+1}(r), [0]_p) \subset G \times \{[1]_p\}\,,\end{aligned}$$

the cardinality $\overline{\varepsilon}_{u \cdot p+1}$ of

$$\begin{aligned}&\Big(\bigcup_{t=1}^{u \cdot p+1} (\mathcal{B}_p + \overline{\boldsymbol{s}}_t)\Big) \setminus \Big(\bigcup_{t=1}^{u \cdot p} (\mathcal{B}_p + \overline{\boldsymbol{s}}_t)\Big) \\ &\quad = \Big(\bigcup_{k=0}^{u} (\mathcal{B}_p + \overline{\boldsymbol{s}}_{k \cdot p+1})\Big) \setminus \Big(\bigcup_{k=0}^{u-1} (\mathcal{B}_p + \overline{\boldsymbol{s}}_{k \cdot p+1})\Big)\end{aligned}$$

now can be seen to agree with

$$\operatorname{card}\Big(\bigcup_{k=0}^{u} (\mathcal{B} + \boldsymbol{s}_{k+1})\Big) - \operatorname{card}\Big(\bigcup_{k=0}^{u-1} (\mathcal{B} + \boldsymbol{s}_{k+1})\Big) = \varepsilon_{u+1}\,.$$

For any chosen $v \in \{2, \ldots, p\}$, the cardinality $\overline{\varepsilon}_{u \cdot p+v}$ of

$$\begin{aligned}&\Big(\bigcup_{t=1}^{u \cdot p+v} (\mathcal{B}_p + \overline{\boldsymbol{s}}_t)\Big) \setminus \Big(\bigcup_{t=1}^{u \cdot p+v-1} (\mathcal{B}_p + \overline{\boldsymbol{s}}_t)\Big) \\ &\quad = \Big(\bigcup_{k=0}^{u} (\mathcal{B}_p + \overline{\boldsymbol{s}}_{k \cdot p+v})\Big) \setminus \Big(\bigcup_{k=0}^{u-1} (\mathcal{B}_p + \overline{\boldsymbol{s}}_{k \cdot p+v})\Big) \\ &\quad = \Big(\bigcup_{k=0}^{u} ((\mathcal{B}_p + \overline{\boldsymbol{s}}_v) + \overline{\boldsymbol{s}}_{k \cdot p+1})\Big) \setminus \Big(\bigcup_{k=0}^{u-1} ((\mathcal{B}_p + \overline{\boldsymbol{s}}_v) + \overline{\boldsymbol{s}}_{k \cdot p+1})\Big)\end{aligned}$$

in turn agrees with $\overline{\varepsilon}_{u \cdot p+1}$, by help of **Lemma 2.9** (with $s_t = \overline{\boldsymbol{s}}_{t \cdot p+1}$ ($t \in \mathbb{N}$), $\mathcal{A} = \mathcal{B}_p$ and $s = \overline{\boldsymbol{s}}_v$), since $\overline{\boldsymbol{s}}_v = (v-1) \cdot (\boldsymbol{d}(1) \cdot [p]_{q_1}^{-1}, \ldots, \boldsymbol{d}(r) \cdot [p]_{q_r}^{-1}, [1]_p)$ is independent of k.

Hence $\overline{\varepsilon}_{u\cdot p+1} = \ldots = \overline{\varepsilon}_{u\cdot p+p} = \varepsilon_{u+1}$ for all $u \in \mathbb{N}_0$, and by **Lemma 2.10** we only need to check, whether $(\overline{\boldsymbol{s}}_t)_{t\in\mathbb{N}}$ is good for $\mathcal{B}_p$ at times $n = u\cdot p+1$. For this, we first calculate the cardinality of $\bigcup_{t=1}^{u\cdot p}(\mathcal{B}_p + \overline{\boldsymbol{s}}_t)$ as

$$\sum_{t=1}^{u\cdot p}\overline{\varepsilon}_t = \sum_{t=0}^{u-1}\Big(\sum_{v=1}^{p}\overline{\varepsilon}_{t\cdot p+v}\Big) = \sum_{t=0}^{u-1}\Big(\sum_{v=1}^{p}\varepsilon_{t+1}\Big) = p\cdot\sum_{t=1}^{u}\varepsilon_t\,.$$

By the assumption that $(\boldsymbol{s}_t)_{t\in\mathbb{N}}$ is good for $\mathcal{B}$, we thus obtain

$$\begin{aligned}\overline{\varepsilon}_{u\cdot p+1} = \varepsilon_{u+1} &\geqslant \alpha\cdot\Big(\operatorname{card}(G) - \sum_{t=1}^{(u+1)-1}\varepsilon_t\Big)\\ &= \alpha\cdot\operatorname{card}(G) - \alpha/p\cdot p\cdot\sum_{t=1}^{u}\varepsilon_t = \alpha\cdot\operatorname{card}(G) - \alpha/p\cdot\sum_{t=1}^{u\cdot p}\overline{\varepsilon}_t\,,\end{aligned}$$

and this completes our proof. □

Since we have already shown (in the case $r=1$) that $((t-1)\cdot[b]_q)_{t\in\mathbb{N}}$ is good for $\mathcal{B}_q(b)$, **Proposition 2.13** can ensure us that $\boldsymbol{d} = ([b]_q\cdot[p]_q^{-1}, [1]_p)$ is good for $\mathcal{B}_{q,p}(b,1)$, where q and p are two distinct primes.

In general, the existence of some good $\boldsymbol{d}\in\mathcal{R}(q_1)\times\mathcal{R}(q_2)$ for a simple box $\mathcal{B}_{q_1,q_2}(b_1,b_2)$ remains open, and we pose this as a problem.

Problem 2.14. Let q_1 and q_2 be two distinct primes. Given any (simple) box $\mathcal{B}\subset(\mathbb{Z}/q_1\mathbb{Z})\times(\mathbb{Z}/q_2\mathbb{Z})$, does there always exist some $\boldsymbol{d}\in\mathcal{R}(q_1)\times\mathcal{R}(q_2)$ such that the arithmetic progression $((t-1)\cdot\boldsymbol{d})_{t\in\mathbb{N}}$ is good for $\mathcal{B}$?

In the case $r=3$, let us first consider the simple box

$$\mathcal{B}(3) = \mathcal{B}_{2,3,5}(1,2,4) = \{[1]_2\}\times\mathcal{B}_{3,5}(2,4)\,.$$

Recall that $([1]_3,[1]_5)$ is good for $\mathcal{B}_{3,5}(2,4)$, and thus **Proposition 2.13** can produce a good $\boldsymbol{d}\in\mathcal{R}(2)\times\mathcal{R}(3)\times\mathcal{R}(5)$ for $\mathcal{B}(3)$. By **Corollary 2.12**, one can then particularly choose $\boldsymbol{d} = ([1]_2,[1]_3,[1]_5)$. Actually, with help of a computer (see **Algorithm 2** in the appendix), we could find at least one good $\boldsymbol{d}$ for each of the possible $2\cdot3\cdot5 = 30$ simple boxes of the form $\mathcal{B}_{2,3,5}(b_1,b_2,b_3)$.

On the other hand, when we checked all possible $3 \cdot 5 \cdot 7 = 105$ simple boxes $\mathcal{B} \subset (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/7\mathbb{Z})$, we have discovered that there does **not** exist a good $\boldsymbol{d} \in \mathcal{R}(3) \times \mathcal{R}(5) \times \mathcal{R}(7)$ for $\mathcal{B} = \mathcal{B}_{3,5,7}(2,4,2)$.

However, there exists a good $\boldsymbol{d} \in \mathcal{R}(3) \times \mathcal{R}(5) \times \mathcal{R}(7)$ for $\mathcal{B}_{3,5,7}(2,4,6)$, and **Proposition 2.13** also ensures a good $\boldsymbol{d} \in \mathcal{R}(2) \times \mathcal{R}(3) \times \mathcal{R}(5) \times \mathcal{R}(7)$ for $\mathcal{B}_{2,3,5,7}(1,2,4,6) = \mathcal{B}(4)$. Again, with help of **Corollary 2.12**, one can choose $\boldsymbol{d} = ([1]_2, [1]_3, [1]_5, [1]_7)$, and **Algorithm 2** (from the appendix) has allowed us to check that $\boldsymbol{d} = ([1]_{p_1}, \ldots, [1]_{p_r})$ is good for $\mathcal{B}(r)$ up to $r \leqslant 8$, at least.

2.4 Arithmetic progressions inside simple boxes

It turns out that the box-like structure of $\mathcal{B} = \mathcal{B}_{q_1,\ldots,q_r}(b_1, \ldots, b_r)$ puts some restrictions on the maximal length of an arithmetic progression inside $\mathcal{B}$, when one assumes that $b_i < q_i$ for all $i \in \{1, \ldots, r\}$.

For $\boldsymbol{a}, \boldsymbol{d} \in \prod_{i=1}^{r} (\mathbb{Z}/q_i\mathbb{Z})$, let $\big\{\boldsymbol{a} + (k-1) \cdot \boldsymbol{d} : k \in \{1, \ldots, l\}\big\}$ be an arithmetic progression whose l members are distinct and all inside $\mathcal{B}$. Note that for each (direction) $i \in \{1, \ldots, r\}$, all not necessarily distinct l members of the (projected) arithmetic progression $\big\{\boldsymbol{a}(i) + (k-1) \cdot \boldsymbol{d}(i) : k \in \{1, \ldots, l\}\big\}$ have to be inside $\mathcal{B}_{q_i}(b_i) = \{[1]_{q_i}, \ldots, [b_i]_{q_i}\}$.

If $l > b_i$ for some i, then $\boldsymbol{d}(i) = [0]_{q_i}$. Otherwise, for $\boldsymbol{d}(i) \in \mathcal{R}(q_i)$, we have

$$\begin{aligned}&\big\{\boldsymbol{a}(i) + (k-1) \cdot \boldsymbol{d}(i) : k \in \{1, \ldots, q_i\}\big\} \\ &\quad = \boldsymbol{a}(i) + \big\{(k-1) \cdot \boldsymbol{d}(i) : k \in \{1, \ldots, q_i\}\big\} = \boldsymbol{a}(i) + \mathbb{Z}/q_i\mathbb{Z} = \mathbb{Z}/q_i\mathbb{Z}\,,\end{aligned}$$

and so at least one of the $b_i + 1$ distinct members of

$$\big\{\boldsymbol{a}(i) + (k-1) \cdot \boldsymbol{d}(i) : k \in \{1, \ldots, b_i, b_i + 1\} \subset \{1, \ldots, l\}\big\}$$

would not be inside $\mathcal{B}_{q_i}(b_i) = \{[1]_{q_i}, \ldots, [b_i]_{q_i}\}$.

Especially, if $l > \max\{b_1, \ldots, b_r\}$, then $\boldsymbol{d}(i) = [0]_{q_i}$ for all $i \in \{1, \ldots, r\}$, and $\boldsymbol{a} + (k-1) \cdot \boldsymbol{d} = \boldsymbol{a} + (k-1) \cdot ([0]_{q_1}, \ldots, [0]_{q_r}) = \boldsymbol{a}$ would be the only member of our chosen arithmetic progression.

Hence, for $l > 1$, only $l \leqslant \max\{b_1, \ldots, b_r\}$ remains.

In the case of the simple box $\mathcal{B} = \mathcal{R}(q_1) \times \ldots \times \mathcal{R}(q_r)$, that is $b_i = q_i - 1$, this means $l \leqslant q_r - 1$. Indeed, we can reach $l = q_r - 1$ by choosing

$$\boldsymbol{a} = ([1]_{q_1}, \ldots, [1]_{q_{r-1}}, [1]_{q_r}) \quad \text{and} \quad \boldsymbol{d} = ([0]_{q_1}, \ldots, [0]_{q_{r-1}}, [1]_{q_r})\,.$$

By the Chinese remainder theorem, this simultaneously also corresponds to the maximal length of an arithmetic progression inside $\mathcal{R}(q_1 \ldots q_r)$.

Unfortunately, in the general case, when m might not be squarefree anymore, our method cannot be used directly. For example, when $m = 4 = 2 \cdot 2$, then the map $[a]_4 \mapsto ([a]_2, [a]_2)$ from $\mathbb{Z}/4\mathbb{Z}$ to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ is not bijective, as $[1]_4$ and $[3]_4$ are both mapped onto the same element $([1]_2, [1]_2)$. Furthermore, $\mathcal{R}(4) = \{[1]_4, [3]_4\}$ does not form a simple box in $\mathbb{Z}/4\mathbb{Z}$, as both of its residue classes form an arithmetic progression of common difference $[2]_4$.

However, by a slightly different approach in [32], we were able to establish lower and upper bounds for the maximal possible length $l(m)$ of an arithmetic progression $a, a+d, a+2d, \ldots$ $(a, d \in \mathbb{N})$ inside the set

$$\mathcal{R}_m := \Big(\bigcup_{u \,\in\, \mathcal{R}(m)} u \Big) \cap \{1, \ldots, m\} = \Big(\mathbb{Z} \setminus \bigcup_{i=1}^{r} q_i \mathbb{Z} \Big) \cap \{1, \ldots, m\}$$

of all positive integers relatively prime and up to m. In other words, $\mathcal{R}_m$ forms the least positive reduced residue system modulo m.

Before we present those bounds for $l(m)$, we make a small preparation and include a proof of the following simple fact about arithmetic progressions.

Lemma 2.15. For $a \in \mathbb{Z}$ and $d \in \mathbb{N}$, let $(a_k)_{k \in \mathbb{N}}$ with $a_k = a + (k-1) \cdot d$ be an arithmetic progression. If q is a positive integer relatively prime to d, then any q consecutive members of $(a_k)_{k \in \mathbb{N}}$ form a complete residue system modulo q.

Proof. Assume that the consecutive members $a_{i+1}, \ldots, a_{i+q}$ do not form a complete residue system modulo q for some $i \in \mathbb{N}_0$, that is

$$a_{i+x} \equiv a_{i+y} \pmod{q}$$

for some integers x and y with $1 \leqslant x < y \leqslant q$ $(*)$.

In this case, we find

$$\begin{aligned} 0 \equiv a_{i+y} - a_{i+x} &= (a + (i+y-1)\cdot d) - (a + (i+x-1)\cdot d) \\ &= (y-x)\cdot d \pmod{q}\,. \end{aligned}$$

Since d is relatively prime to q, only $y - x \equiv 0 \pmod{q}$ remains, that is $x \equiv y \pmod{q}$ in contradiction to condition $(*)$. □

Now we are going to prove a lower bound for $l(m)$.

Proposition 2.16. For any integer $m > 1$, we have

$$l(m) \geqslant \max\{(q-1)/2, m/Q\}\,,$$

where q is the largest prime factor of m, and Q denotes the squarefree product of all prime factors of m.

Proof. Let $q_1^{\varepsilon_1} \cdot \ldots \cdot q_r^{\varepsilon_r}$ be the unique prime factorization of m into primes $q_1 < \ldots < q_r = q$ with exponents $\varepsilon_1, \ldots, \varepsilon_r \in \mathbb{N}$.

If m is squarefree, that is $\varepsilon_1 = \ldots = \varepsilon_r = 1$, let us consider the q numbers

$$a_k = 1 + (k-1)\cdot m/q = 1 + (k-1)\cdot q_1 \ldots q_{r-1}$$

for $k \in \{1, \ldots, q\}$, which build up an arithmetic progression inside $\{1, \ldots, m\}$ (with common difference m/q) of length q. By construction, none of them is divisible by any of the $r-1$ primes $q_1, \ldots, q_{r-1}$ (if there are any), but we cannot deduce non-divisibility by $q_r = q$ yet. However, m/q and q are relatively prime, and thus by **Lemma 2.15**, the consecutive members $a_1, \ldots, a_q$ form a complete residue system modulo q.

In particular, exactly one member among $a_1, \ldots, a_q$ is divisible by q, say a_m, while all others are not. By the pigeonhole principle, we find that

$$a_1, \ldots, a_{m-1} \quad \text{or} \quad a_{m+1}, \ldots, a_q$$

is an arithmetic progression (with common difference m/q) of length at least $(q-1)/2$, which is contained inside $\mathcal{R}_m$. This implies $l(m) \geqslant (q-1)/2$, and so $l(m) \geqslant \max\{(q-1)/2, m/Q\}$, as $m/Q = m/(q_1 \ldots q_r) = 1$.

If m is not squarefree, that is $\varepsilon_1 + \ldots + \varepsilon_r > r$, then m at least still has the same prime factors as $Q = q_1 \ldots q_r$. We find that $\mathcal{R}_Q$ forms a subset of

$$\big\{a + (k-1) \cdot Q : a \in \mathcal{R}_Q, k \in \{1, \ldots, m/Q\}\big\} = \mathcal{R}_m \,,$$

by noting that an integer a is relatively prime to m if and only if a is relatively prime to Q. In particular, we have $l(m) \geqslant l(Q)$, and $l(Q) \geqslant (q-1)/2$ from the squarefree case above.

On the other hand, let us consider the numbers

$$a_k = 1 + (k-1) \cdot Q \quad \text{for } k \in \{1, \ldots, m/Q\} \,.$$

They form an arithmetic progression (with common difference Q) of length m/Q, whose members are all contained inside $\mathcal{R}_m$, as $1 + (k-1) \cdot Q$ is not divisible by any of the r prime factors $q_1, \ldots, q_r$. Both observations lead to $l(m) \geqslant \max\{(q-1)/2, m/Q\}$ again, and our proof is complete. □

Note that the inequality from **Proposition 2.16** can be tight. For example, when we choose $m = 10 = 2 \cdot 5$, then $\mathcal{R}_{10} = \{1, 3, 7, 9\}$, and one easily checks that $l(10) = 2 = (5-1)/2$ (while $\mathcal{R}(10) = \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\}$ contains the arithmetic progression $[7]_{10}, [9]_{10}, [11]_{10} = [1]_{10}, [13]_{10} = [3]_{10}$ of length $4 = 5 - 1$). Next, we establish an upper bound for $l(m)$.

Proposition 2.17. For any integer $m > 1$, we have

$$l(m) \leqslant \max\{q - 1, m/Q\} \,,$$

where q is the largest prime factor of m, and Q denotes the squarefree product of all prime factors of m.

Proof. Suppose that $a_1, a_2, \ldots, a_l$ is an arithmetic progression of length l with common difference $d > 0$ contained inside $\mathcal{R}_m$. Let us focus on d.

If $d \geqslant Q$, we must have $l \leqslant m/Q$, because otherwise $l > m/Q$ implies

$$a_l = a_1 + (l-1) \cdot d \geqslant 1 + ((m/Q + 1) - 1) \cdot Q = m + 1 \,,$$

and the last member a_l would not be inside $\mathcal{R}_m$ anymore.

In the other case, $d < Q$, we know that d is missing at least one prime factor p of the (squarefree) number Q. In particular, d and p are relatively prime, and thus, whenever $l \geqslant p$, the first p members $a_1, a_2, \ldots, a_p$ represent a complete residue system modulo p due to **Lemma 2.15**. But then one of them has to be a multiple of p, and would not be inside $\mathcal{R}_m$. This forces $l \leqslant p-1 \leqslant q-1$.

Combining both cases we reach $l(m) \leqslant \max\{m/Q, q-1\}$, as desired. □

Our main result in [32] was a solution to a problem of Recamán who asked in a letter to Guy from 1995 (see Chapter B40 of [12]), if $l(m)$ tends to infinity with m. Let us conclude this section by revisiting our proof thereof.

Theorem 2.18. For every $l \in \mathbb{N}$, there exists a constant m_l such that the least positive reduced residue system modulo m contains an arithmetic progression of length l for all $m \geqslant m_l$.

Proof. Let $P(x) = \prod_{p \leqslant x} p$ denote the product of all primes p not exceeding $x \geqslant 2$, and put $m_l = l \cdot P(2l) \geqslant 1 \cdot 2 > 1$. Moreover, let us fix some $m \geqslant m_l$, and (as in **Proposition 2.16**) denote its largest prime factor by q.

If $q \geqslant 2l+1$, we immediately arrive at

$$(q-1)/2 \geqslant ((2l+1)-1)/2 = l\,.$$

In the other case $q < 2l+1$, we note that all prime factors of m do not exceed $2l$, which implies their (squarefree) product Q divides $P(2l)$, and so we find

$$m/q \geqslant m_l/q = l \cdot P(2l)/q \geqslant l \cdot 1\,.$$

Combining both cases and **Proposition 2.16**, we get

$$l(m) \geqslant \max\{(q-1)/2, m/Q\} \geqslant l\,,$$

and our claim follows. □

As a last note, we like to mention that (building on our work) Pongsriiam managed to find the exact value of $l(m)$ for every $m > 1$ in [26]. Moreover, he gave some estimates for the partial sums of $l(m)$, which have been improved further by Chen and Lei in [4], where they gave an asymptotic formula.

3 Minimal coverings and reduced residues

In this chapter, we first study minimal coverings of $G = \prod_{i=1}^{r}(\mathbb{Z}/m_i\mathbb{Z})$, for positive integers $m_1, \ldots, m_r$ with $2 \leqslant m_1 \leqslant \ldots \leqslant m_r$, by as few translates of $\mathcal{A} = \prod_{i=1}^{r}\left((\mathbb{Z}/m_i\mathbb{Z}) \setminus \{[0]_{m_i}\}\right)$ as possible. In particular, if any one translate is removed from a minimal covering, then the remaining translates would not cover G anymore. In other words, each translate of a minimal covering contains at least one element from G, which is not contained in any other translate of the minimal covering. Actually, we have not been able to prove or disprove this property for the sequence of translates $\mathcal{R}(P_r)+1, \ldots, \mathcal{R}(P_r)+j(P_r)$, which forms a covering of $\mathbb{Z}/P_r\mathbb{Z}$, and pose it as a problem.

Problem 3.1. For any $r \in \mathbb{N}$ and any $k \in \{1, \ldots, j(P_r)\}$, does the family of translates $\mathcal{R}(P_r)+t$ with $t \in \{1, \ldots, j(P_r)\} \setminus \{k\}$ not cover $\mathbb{Z}/P_r\mathbb{Z}$ anymore?

However, we revisit this problem in section 3.2, where we obtain some optimal result about sums over the cardinalities of pairwise intersections of translates of $\mathcal{R}(P_r)$, which also indicates that $(t)_{t\in\mathbb{N}}$ might indeed be good for $\mathcal{R}(P_r)$.

As described in the introduction, in our setup, where only one residue class (namely $[0]_{m_i}$) is removed from each ring $\mathbb{Z}/m_i\mathbb{Z}$, it turns out useful to identify a translate $\mathcal{A}+\boldsymbol{s}$ by the shift $\boldsymbol{s} \in G$ itself. Recall that for $\boldsymbol{s} \in G$, we write

$$\langle \boldsymbol{s} \rangle = \big\langle (\boldsymbol{s}(1), \ldots, \boldsymbol{s}(r)) \big\rangle := \prod_{i=1}^{r} \left((\mathbb{Z}/m_i\mathbb{Z}) \setminus \{\boldsymbol{s}(i)\}\right),$$

that is $\mathcal{A}+\boldsymbol{s} = \langle \boldsymbol{s} \rangle$, and $\operatorname{card}(\langle \boldsymbol{s} \rangle) = \prod_{i=1}^{r}(m_i - 1)$. Instead of a sequence $\mathcal{A}+\boldsymbol{s}_1, \ldots, \mathcal{A}+\boldsymbol{s}_n$ of translates itself, we now analyse the sequence $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n$ of underlying shifts in G more carefully.

Let $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n$ be a sequence of r-tuples from G. For any non-empty subset $\mathcal{D} \subset \{1, \ldots, r\}$ of directions and any (test) r-tuple $\boldsymbol{a}$ from G, we put

$$\begin{aligned} &C_{\mathcal{D}}(\boldsymbol{a}; \boldsymbol{s}_1, \ldots, \boldsymbol{s}_n) \\ &\quad := \operatorname{card}\Big(\big\{t \in \{1, \ldots, n\} : \boldsymbol{s}_t(i) = \boldsymbol{a}(i) \text{ for all } i \in \mathcal{D}\big\}\Big). \end{aligned}$$

It might seem technical at first, but this notation now allows us to define, when a finite sequence of r-tuples is **balanced**, as mentioned in the introduction. If

$$\left|C_{\mathcal{D}}(\boldsymbol{a};\boldsymbol{s}_1,\ldots,\boldsymbol{s}_n)-C_{\mathcal{D}}(\boldsymbol{b};\boldsymbol{s}_1,\ldots,\boldsymbol{s}_n)\right|\leqslant 1 \quad \text{for all } \boldsymbol{a},\boldsymbol{b}\in G\,,$$

we say that $\boldsymbol{s}_1,\ldots,\boldsymbol{s}_n$ is balanced on $\mathcal{D}$. Moreover, if $\boldsymbol{s}_1,\ldots,\boldsymbol{s}_n$ is balanced on every non-empty subset $\mathcal{D}\subset\{1,\ldots,r\}$, we say that $\boldsymbol{s}_1,\ldots,\boldsymbol{s}_n$ is balanced.

Later, in section 3.2, it will also play a crucial role in obtaining our main result.

3.1 Balance in minimal coverings

Let us find out more about minimal coverings in the low dimensional cases $r\in\{1,2,3\}$, and particularly if there exist balanced minimal coverings, in the sense that the underlying sequence of shifts is balanced. Along the way, we prove two lemmas which are also applicable in higher dimensions $r\geqslant 4$.

In the case $r=1$, any translate of $\langle[0]_{m_1}\rangle$ is missing exactly one residue class from $\mathbb{Z}/m_1\mathbb{Z}$, and thus any two distinct shifts $s_1,s_2\in\mathbb{Z}/m_1\mathbb{Z}$ induce a minimal covering $\langle s_1\rangle,\langle s_2\rangle$ of $\mathbb{Z}/m_1\mathbb{Z}$, which is balanced.

In the case $r=2$, a minimal covering might not be balanced anymore.

For example, when $m_1=2$ and $m_2=3$, then

$$\big\langle([0]_2,[0]_3)\big\rangle,\big\langle([0]_2,[1]_3)\big\rangle,\big\langle([1]_2,[0]_3)\big\rangle,\big\langle([1]_2,[1]_3)\big\rangle$$

forms a minimal covering of $(\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/3\mathbb{Z})$. For this, we note that any translate of $\big\langle([0]_2,[0]_3)\big\rangle=\{[1]_2\}\times\{[1]_3,[2]_3\}$ is forming a subset of either $\{[0]_2\}\times(\mathbb{Z}/3\mathbb{Z})$ or $\{[1]_2\}\times(\mathbb{Z}/3\mathbb{Z})$. Now, in order to cover one of these two sets, we need two translates whose underlying shifts are differing in the second component (and coinciding in the first). On the other hand, the sequence

$$([0]_2,[0]_3),([0]_2,[1]_3),([1]_2,[0]_3),([1]_2,[1]_3)$$

of shifts is not balanced on $\mathcal{D}=\{2\}$, as $[0]_3$ and $[1]_3$ each appear twice in the second component, while $[2]_3$ does not appear at all there.

However, there always exists a minimal covering which is balanced.

If $m_1 = 2$, we can choose

$$\big\langle([0]_2, [0]_{m_2})\big\rangle, \big\langle([0]_2, [1]_{m_2})\big\rangle, \big\langle([1]_2, [2]_{m_2})\big\rangle, \big\langle([1]_2, [3]_{m_2})\big\rangle$$

as a balanced minimal covering of $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$, which becomes

$$\big\langle([0]_2, [0]_3)\big\rangle, \big\langle([0]_2, [1]_3)\big\rangle, \big\langle([1]_2, [2]_3)\big\rangle, \big\langle([1]_2, [0]_3)\big\rangle$$

when $m_2 = 3$, and

$$\big\langle([0]_2, [0]_2)\big\rangle, \big\langle([0]_2, [1]_2)\big\rangle, \big\langle([1]_2, [0]_2)\big\rangle, \big\langle([1]_2, [1]_2)\big\rangle$$

when $m_2 = 2$.

If $m_1 \geqslant 3$, we can even choose

$$\big\langle([0]_{m_1}, [0]_{m_2})\big\rangle, \big\langle([1]_{m_1}, [1]_{m_2})\big\rangle, \big\langle([2]_{m_1}, [2]_{m_2})\big\rangle$$

as a balanced minimal covering of $(\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})$.

In fact, this holds true in the following more general form.

Lemma 3.2. If $m_1, \ldots, m_r$ are integers exceeding r, then

$$\big\langle([0]_{m_1}, \ldots, [0]_{m_r})\big\rangle, \big\langle([1]_{m_1}, \ldots, [1]_{m_r})\big\rangle, \ldots, \big\langle([r]_{m_1}, \ldots, [r]_{m_r})\big\rangle$$

forms a balanced minimal covering of $G = \prod_{i=1}^{r} (\mathbb{Z}/m_i\mathbb{Z})$.

Proof. Let $\boldsymbol{a}$ be any r-tuple from G, and write

$$\boldsymbol{s}_t = (t-1) \cdot ([1]_{m_1}, \ldots, [1]_{m_r}) \quad \text{for } t \in \{1, \ldots, r+1\}\,.$$

In each direction $i \in \{1, \ldots, r\}$, we have $C_{\{i\}}(\boldsymbol{a}; \boldsymbol{s}_1, \ldots, \boldsymbol{s}_{r+1}) \leqslant 1$, because the $r+1$ entries $\boldsymbol{s}_1(i) = [0]_{m_i}, \ldots, \boldsymbol{s}_{r+1}(i) = [r]_{m_i}$ are all distinct, as $r < m_i$. By the pigeonhole principle, among the $r+1$ shifts $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_{r+1}$ there has to be at least one, say $\boldsymbol{s}_t$, such that $\boldsymbol{a}(i) \neq \boldsymbol{s}_t(i)$ for all $i \in \{1, \ldots, r\}$. In turn, this means that $\boldsymbol{a}$ is covered by $\langle \boldsymbol{s}_t \rangle$, and thus $\langle \boldsymbol{s}_1 \rangle, \ldots, \langle \boldsymbol{s}_{r+1} \rangle$ covers G.

Assume that $\langle \boldsymbol{s}_1 \rangle, \ldots, \langle \boldsymbol{s}_{r+1} \rangle$ is not a minimal covering of G, and so there exist only r shifts $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r$ in G such that $\langle \boldsymbol{u}_1 \rangle, \ldots, \langle \boldsymbol{u}_r \rangle$ covers G. Let us consider the r-tuple $\boldsymbol{a}$ from G, whose components are defined as $\boldsymbol{a}(i) = \boldsymbol{u}_i(i)$ for $i \in \{1, \ldots, r\}$. By construction, each of the r shifts $\boldsymbol{u}_i$ agrees in (at least) one component with $\boldsymbol{a}$. In turn, this means that $\boldsymbol{a}$ is not covered by any of the r translates $\langle \boldsymbol{u}_i \rangle$, and we have found a contradiction to our assumption.

Finally, we check that $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_{r+1}$ is balanced. Again, let $\boldsymbol{a}$ be any r-tuple from G. For any non-empty subset $\mathcal{D} \subset \{1, \ldots, r\}$ and any $i \in \mathcal{D}$, we have

$$C_{\mathcal{D}}(\boldsymbol{a}; \boldsymbol{s}_1, \ldots, \boldsymbol{s}_{r+1}) \leqslant C_{\{i\}}(\boldsymbol{a}; \boldsymbol{s}_1, \ldots, \boldsymbol{s}_{r+1}) \,,$$

which follows easily from the definition of $C_{\mathcal{D}}$. Since we have already seen $C_{\{i\}}(\boldsymbol{a}; \boldsymbol{s}_1, \ldots, \boldsymbol{s}_{r+1}) \leqslant 1$, we have $C_{\mathcal{D}}(\boldsymbol{a}; \boldsymbol{s}_1, \ldots, \boldsymbol{s}_{r+1}) \leqslant 1$. In particular, $C_{\mathcal{D}}(\boldsymbol{a}; \boldsymbol{s}_1, \ldots, \boldsymbol{s}_{r+1})$ and $C_{\mathcal{D}}(\boldsymbol{b}; \boldsymbol{s}_1, \ldots, \boldsymbol{s}_{r+1})$ differ by at most 1, for all $\boldsymbol{a}, \boldsymbol{b} \in G$. Hence, $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_{r+1}$ is balanced, and our proof is complete. □

In the case $r = 3$, **Lemma 3.2** immediately guarantees the existence of a balanced minimal covering of $(\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z}) \times (\mathbb{Z}/m_3\mathbb{Z})$, when $m_1 > 3$. Let us consider the special case of $m_1 = m_2 = m_3 = 3$, that is $G = (\mathbb{Z}/3\mathbb{Z})^3$. We have already seen (in the case $r = 2$) that the sequence

$$\big\langle ([0]_3, [0]_3) \big\rangle, \big\langle ([1]_3, [1]_3) \big\rangle, \big\langle ([2]_3, [2]_3) \big\rangle$$

is a (minimal) covering of $(\mathbb{Z}/3\mathbb{Z})^2$, and so, for any $u \in \mathbb{Z}/3\mathbb{Z}$, the sequence

$$\big\langle ([0]_3, [0]_3, u) \big\rangle, \big\langle ([1]_3, [1]_3, u) \big\rangle, \big\langle ([2]_3, [2]_3, u) \big\rangle$$

covers all elements in $(\mathbb{Z}/3\mathbb{Z})^2 \times \big((\mathbb{Z}/3\mathbb{Z}) \setminus \{u\}\big)$. Hence, the sequence

$$\begin{aligned} &\big\langle ([0]_3, [0]_3, [0]_3) \big\rangle, \big\langle ([1]_3, [1]_3, [0]_3) \big\rangle, \big\langle ([2]_3, [2]_3, [0]_3) \big\rangle, \\ &\big\langle ([0]_3, [0]_3, [1]_3) \big\rangle, \big\langle ([1]_3, [1]_3, [1]_3) \big\rangle, \big\langle ([2]_3, [2]_3, [1]_3) \big\rangle \end{aligned}$$

is forming a covering of $(\mathbb{Z}/3\mathbb{Z})^2 \times \big(\{[1]_3, [2]_3\} \cup \{[2]_3, [0]_3\}\big) = (\mathbb{Z}/3\mathbb{Z})^3$. In fact, this covering by $3 \cdot 2 = 6$ translates is already quite close to a minimal covering, as the following lemma demonstrates.

Lemma 3.3. Let $m_1, \dots, m_r$ and m be any integers exceeding 1. If n is the minimal number of translates of $\big\langle([0]_{m_1}, \dots, [0]_{m_r})\big\rangle$, which one needs to cover $G = \prod_{i=1}^{r}(\mathbb{Z}/m_i\mathbb{Z})$, then any minimal covering of $G \times (\mathbb{Z}/m\mathbb{Z})$ must consist of at least $\lceil n \cdot m/(m-1)\rceil$ translates of $\big\langle([0]_{m_1}, \dots, [0]_{m_r}, [0]_m)\big\rangle$.

Proof. Let $\boldsymbol{s}_1, \dots, \boldsymbol{s}_N$ be a sequence of N shifts in $G \times (\mathbb{Z}/m\mathbb{Z})$ such that $\langle \boldsymbol{s}_1\rangle, \dots, \langle \boldsymbol{s}_N\rangle$ is a minimal covering of $G \times (\mathbb{Z}/m\mathbb{Z})$. For each of the m residue classes $u \in \mathbb{Z}/m\mathbb{Z}$, let $\mathcal{I}(u) \subset \{1, \dots, N\}$ denote the subset of those indices j such that $\boldsymbol{s}_j(r+1) = u$. Here, $\langle \boldsymbol{s}_j\rangle$ does not cover any element of $G \times \{u\}$. Therefore, the indexed family of the $N - \operatorname{card}(\mathcal{I}(u))$ other translates $\langle \boldsymbol{s}_t\rangle$, with $t \in \{1, \dots, N\} \setminus \mathcal{I}(u)$, has to cover all elements of $G \times \{u\}$. Equivalently, the indexed family of the corresponding translates $\big\langle(\boldsymbol{s}_t(1), \dots, \boldsymbol{s}_t(r))\big\rangle \subset G$, with $t \in \{1, \dots, N\} \setminus \mathcal{I}(u)$, has to cover all elements of G.

By assumption, each of those indexed families has at least n members, that is $N - \operatorname{card}(\mathcal{I}(u)) \geqslant n$ for each $u \in \mathbb{Z}/m\mathbb{Z}$. In particular, we find

$$\begin{aligned} m \cdot n = \sum_{u \in \mathbb{Z}/m\mathbb{Z}} n &\leqslant \sum_{u \in \mathbb{Z}/m\mathbb{Z}} N - \operatorname{card}(\mathcal{I}(u)) \\ &= m \cdot N - \sum_{u \in \mathbb{Z}/m\mathbb{Z}} \operatorname{card}(\mathcal{I}(u))\,, \end{aligned}$$

where the value of the last sum equals N, since $\bigcup_{u \in \mathbb{Z}/m\mathbb{Z}} \mathcal{I}(u)$ forms a partition of $\{1, \dots, N\}$. Therefore, we reach $m \cdot n \leqslant (m-1) \cdot N$, and so $N \geqslant n \cdot m/(m-1)$, as desired. □

In our case, **Lemma 3.3** yields that a minimal covering of $G = (\mathbb{Z}/3\mathbb{Z})^3$ must consist of at least $\lceil 3 \cdot 3/2\rceil = \lceil 4.5\rceil = 5$ translates of

$$\big\langle([0]_3, [0]_3, [0]_3)\big\rangle = \{[1]_3, [2]_3\}^3\,.$$

In fact, we find that the sequence

$$\begin{aligned} &\big\langle([0]_3, [0]_3, [0]_3)\big\rangle, \big\langle([1]_3, [1]_3, [0]_3)\big\rangle, \big\langle([2]_3, [2]_3, [2]_3)\big\rangle, \\ &\big\langle([1]_3, [0]_3, [1]_3)\big\rangle, \big\langle([0]_3, [1]_3, [1]_3)\big\rangle \end{aligned}$$

forms a balanced minimal covering of $(\mathbb{Z}/3\mathbb{Z})^3$ (see **Figure 4**).

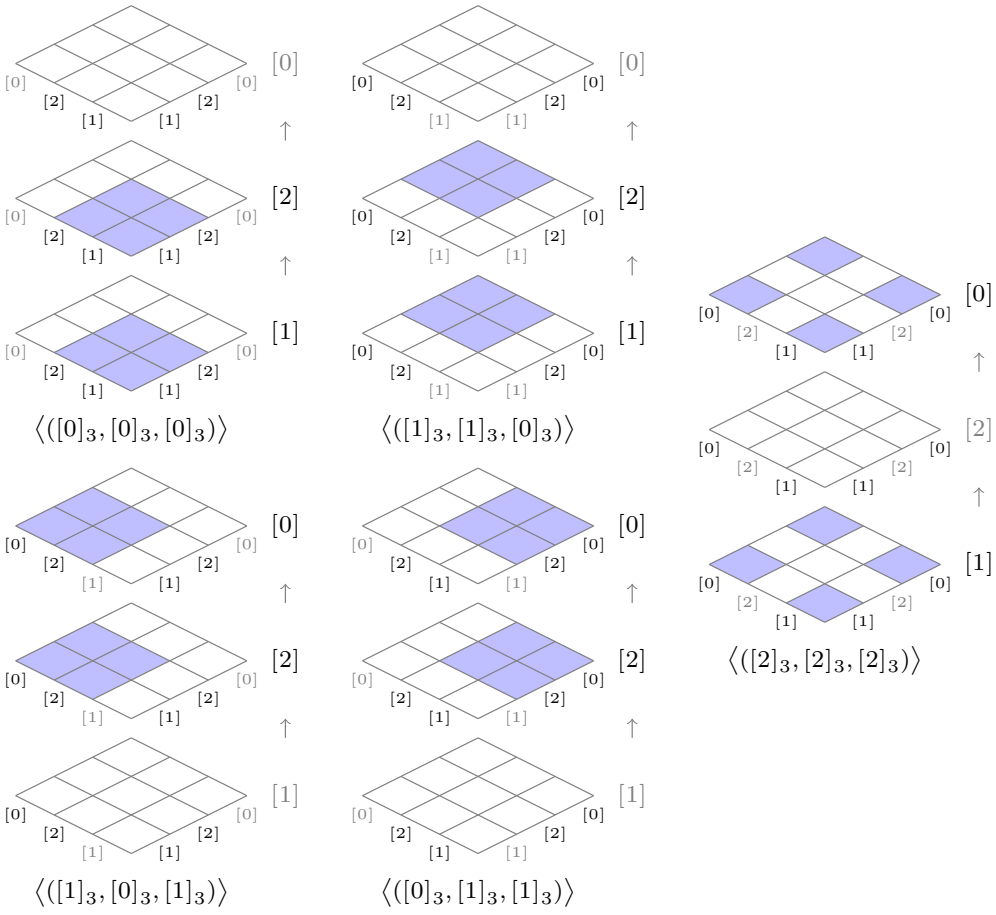


Figure 4: A (balanced) minimal covering of $(\mathbb{Z}/3\mathbb{Z})^3 = \{[1]_3, [2]_3, [0]_3\}^3$ by five translates of $\langle([0]_3, [0]_3, [0]_3)\rangle = \{[1]_3, [2]_3\}^3$. For better readability, we have also written $[a]$ instead of $[a]_3$.

In the more general case of $G = (\mathbb{Z}/3\mathbb{Z})^r$, let n_r stand for the number of translates of $\{[1]_3, [2]_3\}^r$ in a minimal covering of G. Starting with $n_1 = 2$, and then applying **Lemma 3.3** iteratively, we reach $n_r \geqslant 2 \cdot (3/2)^{r-1} > (3/2)^r$ for all $r \in \mathbb{N}$. On the other hand, we can also use **Theorem 2.8** with $G = (\mathbb{Z}/3\mathbb{Z})^r$ and the subset $\mathcal{A} = \{[1]_3, [2]_3\}^r$, whose density is $\alpha = 2^r/3^r$, to get

$$n_r \leqslant \lfloor \log(3^r)/(2^r/3^r) \rfloor + 1 \leqslant r\,(\log 3) \cdot (3/2)^r + 1 \leqslant c \cdot r \cdot (3/2)^r$$

for some absolute (positive) constant c.

Note that the geometric mean of the ratios $n_2/n_1, \ldots, n_{r+1}/n_r$ is given by

$$\Big(\prod_{i=1}^{r}(n_{i+1}/n_i)\Big)^{1/r} = (n_{r+1}/n_1)^{1/r} = (n_{r+1}/2)^{1/r}\,.$$

Both inequalities for n_r can now yield

$$(n_{r+1}/2)^{1/r} > ((3/2)^{r+1}/2)^{1/r} = 3/2 \cdot (3/4)^{1/r}\,,$$

as well as

$$\begin{aligned}(n_{r+1}/2)^{1/r} &\leqslant (c\cdot(r+1)\cdot(3/2)^{r+1}/2)^{1/r}\\ &\leqslant 3/2\cdot(3/4)^{1/r}\cdot c^{1/r}\cdot(2r)^{1/r} = 3/2\cdot(3c/2)^{1/r}\cdot r^{1/r}\,.\end{aligned}$$

Since $\lim_{r\to\infty}(r^{1/r}) = 1$ and $\lim_{r\to\infty}(x^{1/r}) = 1$ for any $x > 0$, we get

$$\lim_{r\to\infty}\Big(\prod_{i=1}^{r}(n_{i+1}/n_i)\Big)^{1/r} = 3/2\,.$$

Instead of studying the global structure of minimal coverings further, from now on we are going to work more locally again, with respect to our main goal to find out more about how "close" the sequence of shifts $\boldsymbol{s}_t = ([t]_{p_1}, \ldots, [t]_{p_r})$ ($t \in \mathbb{N}$) is to being good for $\mathcal{B}(r) = \big\langle([0]_{p_1}, \ldots, [0]_{p_r})\big\rangle$. In general, given some shifts $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n$ from $G = \prod_{i=1}^{r}(\mathbb{Z}/m_i\mathbb{Z})$, with their corresponding translates $\langle\boldsymbol{s}_1\rangle, \ldots, \langle\boldsymbol{s}_n\rangle$, we are interested in how the choice of the next shift $\boldsymbol{s}_{n+1} \in G$ effects the cardinality of the union $\langle\boldsymbol{s}_{n+1}\rangle \cup \bigcup_{t=1}^{n}\langle\boldsymbol{s}_t\rangle$.

3.2 An optimal result for reduced residues

Let $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n$ be a finite sequence of shifts in $G = \prod_{i=1}^{r}(\mathbb{Z}/m_i\mathbb{Z})$, where the integers $m_1, \ldots, m_r > 1$ do not have to be in increasing order anymore.

By the inclusion-exclusion principle, we have

$$\operatorname{card}\Big(\bigcup_{t=1}^{n}\langle\boldsymbol{s}_t\rangle\Big) = \sum_{\{\}\neq\mathcal{I}\subset\{1,\ldots,n\}}(-1)^{\operatorname{card}(\mathcal{I})+1}\cdot\operatorname{card}\Big(\bigcap_{t\in\mathcal{I}}\langle\boldsymbol{s}_t\rangle\Big)\,,$$

where the cardinality of each intersection satisfies

$$\begin{aligned}\operatorname{card}\Big(\bigcap_{t\in\mathcal{I}}\langle \boldsymbol{s}_t\rangle\Big) &= \operatorname{card}\Big(\prod_{i=1}^{r}\big((\mathbb{Z}/m_i\mathbb{Z})\setminus\bigcup_{t\in\mathcal{I}}\{\boldsymbol{s}_t(i)\}\big)\Big)\\ &= \prod_{i=1}^{r}\operatorname{card}\Big((\mathbb{Z}/m_i\mathbb{Z})\setminus\bigcup_{t\in\mathcal{I}}\{\boldsymbol{s}_t(i)\}\Big)\,.\end{aligned}$$

If now $\boldsymbol{s}_x(i)\neq\boldsymbol{s}_y(i)$ for all $1\leqslant x<y\leqslant n$ and in any direction $i\in\{1,\ldots,r\}$, then we have $\operatorname{card}\big(\bigcup_{t\in\mathcal{I}}\{\boldsymbol{s}_t(i)\}\big)=\operatorname{card}(\mathcal{I})$, and therefore

$$\operatorname{card}\Big(\bigcap_{t\in\mathcal{I}}\langle \boldsymbol{s}_t\rangle\Big)=\prod_{i=1}^{r}\big(m_i-\operatorname{card}(\mathcal{I})\big)\,,$$

independent of the particular choice of the shifts $\boldsymbol{s}_t$. In turn, the cardinality of the union $\bigcup_{t=1}^{n}\langle \boldsymbol{s}_t\rangle$ is also independent of the particular choice of the shifts $\boldsymbol{s}_t$, as long as any two r-tuples from $\boldsymbol{s}_1,\ldots,\boldsymbol{s}_n$ do not share any component.

In a similar way, we could also verify that given any sequence $\boldsymbol{s}_1,\ldots,\boldsymbol{s}_n$ of r-tuples from G, if $\boldsymbol{a}$ and $\boldsymbol{b}$ are two r-tuples from G such that $\boldsymbol{a}(i)\neq\boldsymbol{s}_t(i)$ and $\boldsymbol{b}(i)\neq\boldsymbol{s}_t(i)$ for all $t\in\{1,\ldots,n\}$ and in any direction $i\in\{1,\ldots,r\}$, then both unions $\langle \boldsymbol{a}\rangle\cup\bigcup_{t=1}^{n}\langle \boldsymbol{s}_t\rangle$ and $\langle \boldsymbol{b}\rangle\cup\bigcup_{t=1}^{n}\langle \boldsymbol{s}_t\rangle$ have the same cardinality.

However, by the following alternative approach, which does not depend on the inclusion-exclusion principle, we are able to show a bit more in **Proposition 3.5**. But first, we concentrate on a certain special case, which builds the core piece for the proof of **Proposition 3.5**.

Lemma 3.4. Let $m_1,\ldots,m_r>1$ be integers, and let $\boldsymbol{s}_1,\ldots,\boldsymbol{s}_n$ be a finite sequence of r-tuples from $G=\prod_{i=1}^{r}(\mathbb{Z}/m_i\mathbb{Z})$. Suppose that $\boldsymbol{a}$ is an r-tuple from G, for which there exists at least one direction $i\in\{1,\ldots,r\}$ such that $\boldsymbol{a}(i)\neq\boldsymbol{s}_t(i)$ for all $t\in\{1,\ldots,n\}$. If $\boldsymbol{a}_u$ is the r-tuple which one obtains from $\boldsymbol{a}$ by replacing $\boldsymbol{a}(i)$ with another residue class $u\in\mathbb{Z}/m_i\mathbb{Z}$, then we have

$$\operatorname{card}\Big(\langle \boldsymbol{a}\rangle\cup\bigcup_{t=1}^{n}\langle \boldsymbol{s}_t\rangle\Big)\geqslant\operatorname{card}\Big(\langle \boldsymbol{a}_u\rangle\cup\bigcup_{t=1}^{n}\langle \boldsymbol{s}_t\rangle\Big)\,.$$

Proof. First, we note that after exchanging m_i with m_1 in $m_1, \ldots, m_r$, and then reordering the indices, we may assume that $i = 1$ without loss of generality. Now we are going to prove that

$$\operatorname{card}\Big(\langle \boldsymbol{a}\rangle \cup \bigcup_{t=1}^{n} \langle \boldsymbol{s}_t\rangle\Big) \geqslant \operatorname{card}\Big(\big\langle (u, \boldsymbol{a}(2), \ldots, \boldsymbol{a}(r))\big\rangle \cup \bigcup_{t=1}^{n} \langle \boldsymbol{s}_t\rangle\Big)$$

for any r-tuple $(u, \boldsymbol{a}(2), \ldots, \boldsymbol{a}(r)) = \boldsymbol{a}_u$, where the first component $\boldsymbol{a}(1)$ of $\boldsymbol{a}$ has been replaced by another residue class $u \in \mathbb{Z}/m_1\mathbb{Z}$.

For this, we construct a bijective map $f_u : \langle \boldsymbol{a}_u\rangle \to \langle \boldsymbol{a}\rangle$ with the property that whenever an r-tuple $\boldsymbol{x}$ from

$$\langle \boldsymbol{a}_u\rangle = \big((\mathbb{Z}/m_1\mathbb{Z}) \setminus \{u\}\big) \times \prod_{i=2}^{r} \big((\mathbb{Z}/m_i\mathbb{Z}) \setminus \{\boldsymbol{a}(i)\}\big)$$

is not covered by $\langle \boldsymbol{s}_1\rangle, \ldots, \langle \boldsymbol{s}_n\rangle$, then the corresponding r-tuple $f_u(\boldsymbol{x})$ from

$$\langle \boldsymbol{a}\rangle = \big((\mathbb{Z}/m_1\mathbb{Z}) \setminus \{\boldsymbol{a}(1)\}\big) \times \prod_{i=2}^{r} \big((\mathbb{Z}/m_i\mathbb{Z}) \setminus \{\boldsymbol{a}(i)\}\big)$$

is not covered by $\langle \boldsymbol{s}_1\rangle, \ldots, \langle \boldsymbol{s}_n\rangle$, too.

Let us choose $f_u(\boldsymbol{x}) = \boldsymbol{x}$ if $\boldsymbol{x} \in \langle \boldsymbol{a}_u\rangle$ is also contained in $\langle \boldsymbol{a}\rangle$, that is if

$$\boldsymbol{x} \in \langle \boldsymbol{a}_u\rangle \cap \langle \boldsymbol{a}\rangle = \big((\mathbb{Z}/m_1\mathbb{Z}) \setminus \{u, \boldsymbol{a}(1)\}\big) \times \prod_{i=2}^{r} \big((\mathbb{Z}/m_i\mathbb{Z}) \setminus \{\boldsymbol{a}(i)\}\big)\,,$$

and $f_u(\boldsymbol{x}) = (u, \boldsymbol{x}(2), \ldots, \boldsymbol{x}(r))$ otherwise, that is if

$$\boldsymbol{x} \in \langle \boldsymbol{a}_u\rangle \setminus \langle \boldsymbol{a}\rangle = \{\boldsymbol{a}(1)\} \times \prod_{i=2}^{r} \big((\mathbb{Z}/m_i\mathbb{Z}) \setminus \{\boldsymbol{a}(i)\}\big)\,.$$

Of course, in the case $\boldsymbol{x} \in \langle \boldsymbol{a}_u\rangle \cap \langle \boldsymbol{a}\rangle$, if $\boldsymbol{x}$ is not covered by $\langle \boldsymbol{s}_1\rangle, \ldots, \langle \boldsymbol{s}_n\rangle$, then also $f_u(\boldsymbol{x}) = \boldsymbol{x}$ is not covered by $\langle \boldsymbol{s}_1\rangle, \ldots, \langle \boldsymbol{s}_n\rangle$.

In the other case, $\boldsymbol{x} \in \langle \boldsymbol{a}_u\rangle \setminus \langle \boldsymbol{a}\rangle$ is of the form $(\boldsymbol{a}(1), \boldsymbol{x}(2), \ldots, \boldsymbol{x}(r))$, where the $(r-1)$-tuple $(\boldsymbol{x}(2), \ldots, \boldsymbol{x}(r))$ is from $\prod_{i=2}^{r} \big((\mathbb{Z}/m_i\mathbb{Z}) \setminus \{\boldsymbol{a}(i)\}\big)$.

If $(\boldsymbol{x}(2),\dots,\boldsymbol{x}(r))$ is not covered by one of the translates $\big\langle(\boldsymbol{s}_t(2),\dots,\boldsymbol{s}_t(r))\big\rangle$ of $\big\langle([0]_{m_2},\dots,[0]_{m_r})\big\rangle$ for any $t\in\{1,\dots,n\}$, then $\boldsymbol{x}=(\boldsymbol{x}(1),\boldsymbol{x}(2),\dots,\boldsymbol{x}(r))$ and $f_u(\boldsymbol{x})=(u,\boldsymbol{x}(2),\dots,\boldsymbol{x}(r))$ are both not covered by $\langle\boldsymbol{s}_1\rangle,\dots,\langle\boldsymbol{s}_n\rangle$.

On the other hand, in the remaining case, if $(\boldsymbol{x}(2),\dots,\boldsymbol{x}(r))$ is covered by a translate $\big\langle(\boldsymbol{s}_t(2),\dots,\boldsymbol{s}_t(r))\big\rangle$ for some $t\in\{1,\dots,n\}$, then $\boldsymbol{x}$ is covered by $\langle\boldsymbol{s}_t\rangle$ due to $\boldsymbol{x}(1)\neq\boldsymbol{s}_t(1)$, and we do not have to worry about $f_u(\boldsymbol{x})$ here.

This completes our proof. □

Now everything is ready, and we can apply **Lemma 3.4** iteratively.

Proposition 3.5. Let $m_1,\dots,m_r>1$ be integers, and let $\boldsymbol{s}_1,\dots,\boldsymbol{s}_n$ be a finite sequence of r-tuples from $G=\prod_{i=1}^{r}(\mathbb{Z}/m_i\mathbb{Z})$. If $\boldsymbol{a}$ is an r-tuple from G such that $\boldsymbol{a}(i)\neq\boldsymbol{s}_t(i)$ for all $t\in\{1,\dots,n\}$ and in any direction $i\in\{1,\dots,r\}$, then, for any r-tuple $\boldsymbol{b}$ from G, we have

$$\operatorname{card}\Big(\langle\boldsymbol{a}\rangle\cup\bigcup_{t=1}^{n}\langle\boldsymbol{s}_t\rangle\Big)\geqslant\operatorname{card}\Big(\langle\boldsymbol{b}\rangle\cup\bigcup_{t=1}^{n}\langle\boldsymbol{s}_t\rangle\Big)\,.$$

Proof. Let us write $\mathcal{S}_n$ for the union $\bigcup_{t=1}^{n}\langle\boldsymbol{s}_t\rangle$. By iteratively replacing the i-th component $\boldsymbol{a}(i)$ of $\boldsymbol{a}$ with the i-th component $\boldsymbol{b}(i)$ of $\boldsymbol{b}$ for $i\in\{1,\dots,r\}$, **Lemma 3.4** can produce a chain of inequalities, starting with

$$\operatorname{card}\big(\langle\boldsymbol{a}\rangle\cup\mathcal{S}_n\big)\geqslant\operatorname{card}\Big(\big\langle(\boldsymbol{b}(1),\boldsymbol{a}(2),\dots,\boldsymbol{a}(r))\big\rangle\cup\mathcal{S}_n\Big)\,,$$

and then, for $i\in\{2,\dots,r-1\}$, we inductively obtain

$$\begin{aligned}&\operatorname{card}\Big(\big\langle(\boldsymbol{b}(1),\dots,\boldsymbol{b}(i-1),\boldsymbol{a}(i),\boldsymbol{a}(i+1),\dots,\boldsymbol{a}(r))\big\rangle\cup\mathcal{S}_n\Big)\\&\quad\geqslant\operatorname{card}\Big(\big\langle(\boldsymbol{b}(1),\dots,\boldsymbol{b}(i-1),\boldsymbol{b}(i),\boldsymbol{a}(i+1),\dots,\boldsymbol{a}(r))\big\rangle\cup\mathcal{S}_n\Big)\,,\end{aligned}$$

until we reach

$$\begin{aligned}\operatorname{card}\big(\langle\boldsymbol{a}\rangle\cup\mathcal{S}_n\big)&\geqslant\ldots\geqslant\operatorname{card}\Big(\big\langle(\boldsymbol{b}(1),\dots,\boldsymbol{b}(r-1),\boldsymbol{a}(r))\big\rangle\cup\mathcal{S}_n\Big)\\&\geqslant\operatorname{card}\Big(\big\langle(\boldsymbol{b}(1),\dots,\boldsymbol{b}(r-1),\boldsymbol{b}(r))\big\rangle\cup\mathcal{S}_n\Big)\,,\end{aligned}$$

as needed for our statement. □

Before we apply **Proposition 3.5** in the case of $G = \prod_{i=1}^{r}(\mathbb{Z}/p_i\mathbb{Z})$, we need one more lemma which builds a connection between unions of translates of $\mathcal{R}(P_r/2) \subset \mathbb{Z}/(P_r/2)\mathbb{Z}$ and unions of translates of $\mathcal{R}(P_r) \subset \mathbb{Z}/P_r\mathbb{Z}$.

Lemma 3.6. Let $(s_t)_{t\in\mathbb{N}}$ be a sequence of integers. If m is a (squarefree) product of distinct odd primes, then

$$\operatorname{card}\Big(\bigcup_{t=1}^{n}(\mathcal{R}(m)+s_t)\Big) = \operatorname{card}\Big(\bigcup_{t=1}^{n}(\mathcal{R}(2m)+2s_t)\Big)$$

holds at every time $n \in \mathbb{N}$.

Proof. By **Proposition 2.11** (with $d = 2$), we can write

$$\operatorname{card}\Big(\bigcup_{t=1}^{n}(\mathcal{R}(m)+s_t)\Big) = \operatorname{card}\Big(\bigcup_{t=1}^{n}(\mathcal{R}(m)+2s_t)\Big).$$

Moreover, note that $\mathcal{R}(2m) \subset \big\{2a+1+2m\mathbb{Z} : a \in \{0,\dots,m-1\}\big\} =: \mathcal{O}$, and that the map $f : \mathcal{O} \to \mathbb{Z}/m\mathbb{Z}, [2a+1]_{2m} \mapsto [2a+1]_m$ forms a bijection together with the inverse map

$$f^{-1} : \mathbb{Z}/m\mathbb{Z} \to \mathcal{O}, [a]_m \mapsto \begin{cases} [a]_{2m} & \text{if } a \text{ is odd}, \\ [a+m]_{2m} & \text{if } a \text{ is even}. \end{cases}$$

If $[2a+1]_{2m}$ from $\mathcal{O}$ is covered by a translate $\mathcal{R}(2m)+2s_t$ for at least one $t \in \{1,\dots,n\}$, then we have $[2a+1-2s_t]_{2m} \in \mathcal{R}(2m)$, which means that $2(a-s_t)+1$ is relatively prime to $2m$. In particular, $2(a-s_t)+1$ is relatively prime to m, which in turn leads to $[2a+1-2s_t]_m \in \mathcal{R}(m)$, and thus we find that $f([2a+1]_{2m}) = [2a+1]_m$ is covered by the translate $\mathcal{R}(m)+2t$.

On the other hand, if $[a]_m$ from $\mathbb{Z}/m\mathbb{Z}$ is covered by a translate $\mathcal{R}(m)+2s_t$ for at least one $t \in \{1,\dots,n\}$, then we have $[a-2s_t]_m \in \mathcal{R}(m)$, which means that $a-2t$ is relatively prime to m.

If a is odd, then $a-2s_t$ is also odd and relatively prime to $2m$, which in turn leads to $[a-2s_t]_{2m} \in \mathcal{R}(2m)$, and thus we find that $f^{-1}([a]_m) = [a]_{2m}$ is covered by the translate $\mathcal{R}(2m)+2s_t$.

In the other case, if a is even, then $a - 2\,s_t + m$ is odd and relatively prime to $2m$, which in turn leads to $[a + m - 2\,s_t]_{2m} \in \mathcal{R}(2m)$, and thus we find that $f^{-1}([a]_m) = [a + m]_{2m}$ is covered by the translate $\mathcal{R}(2m) + 2\,s_t$.

This completes our proof. □

Finally, we are ready to prove that the sequence of shifts $s_t = t$ ($t \in \mathbb{N}$) is good for $\mathcal{R}(P_r)$ up to time 6, at least. In fact, we are going to show that after the first $n - 1$ consecutive translates $\mathcal{R}(P_r) + 1, \ldots, \mathcal{R}(P_r) + n - 1$, the next translate $\mathcal{R}(P_r) + n$ covers at least as many not yet covered elements as any other translate of $\mathcal{R}(P_r)$ would cover, as long as $n \leqslant 6$.

Theorem 3.7. For $r \in \mathbb{N}$ and $n \in \{1, \ldots, 6\}$, the inequality

$$\operatorname{card}\Big(\bigcup_{t=1}^{n} (\mathcal{R}(P_r) + t)\Big) \geqslant \operatorname{card}\Big((\mathcal{R}(P_r) + s) \cup \bigcup_{t=1}^{n-1} (\mathcal{R}(P_r) + t)\Big)$$

holds for any shift $s \in \{1, \ldots, P_r\}$.

Proof. In the special case $r = 1$, that is $P_r = P_1 = p_1 = 2$, we find

$$\operatorname{card}(\mathcal{R}(2) + 1) = \operatorname{card}(\{[0]_2\}) = 1 = \operatorname{card}(\{[1]_2\}) = \operatorname{card}(\mathcal{R}(2) + 2)$$

and $(\mathcal{R}(2) + 1) \cup (\mathcal{R}(2) + 2) = \mathbb{Z}/2\mathbb{Z}$, which gives $\bigcup_{t=1}^{n} (\mathcal{R}(2) + t) = \mathbb{Z}/2\mathbb{Z}$ for all $n \geqslant 2$, and everything is fine.

In the case $r \geqslant 2$, we can choose $G = \prod_{i=1}^{r-1} (\mathbb{Z}/p_{i+1}\mathbb{Z})$ and the sequence of $(r-1)$-tuples $\boldsymbol{s}_t = ([t]_{p_2}, \ldots, [t]_{p_r})$ in **Proposition 3.5**, to obtain

$$\operatorname{card}\Big(\langle \boldsymbol{s}_k \rangle \cup \bigcup_{t=1}^{k-1} \langle \boldsymbol{s}_t \rangle\Big) \geqslant \operatorname{card}\Big(\langle \boldsymbol{b} \rangle \cup \bigcup_{t=1}^{k-1} \langle \boldsymbol{s}_t \rangle\Big)$$

for any $\boldsymbol{b} \in G$, as long as $k \in \{1, 2, 3\}$, since the $(r-1)$-tuples $\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{s}_3$ do not share any component due to $p_{i+1} \geqslant 3$ for $i \geqslant 1$. Equivalently, we can write

$$\operatorname{card}\Big(\bigcup_{t=1}^{k} (\mathcal{R}(P_r/2) + t)\Big) \geqslant \operatorname{card}\Big((\mathcal{R}(P_r/2) + b) \cup \bigcup_{t=1}^{k-1} (\mathcal{R}(P_r/2) + t)\Big)$$

for any $b \in \{1, \dots, P_r/2\}$, as long as $k \in \{1, 2, 3\}$. Once more, by **Lemma 3.6** (with $m = P_r/2$), we can rewrite this inequality as

$$\operatorname{card}\Big(\bigcup_{t=1}^{k} (\mathcal{R}(P_r) + 2t)\Big) \geqslant \operatorname{card}\Big((\mathcal{R}(P_r) + 2b) \cup \bigcup_{t=1}^{k-1} (\mathcal{R}(P_r) + 2t)\Big) .$$

Let us denote the last inequality by $(*)$, and abbreviate $\mathcal{R}(P_r)$ with $\mathcal{R}$.

Now we distinguish two cases for n, according to its parity.

Case 1: $n = 2k - 1$ is odd.

If $s = 2b - 1$ is odd, then (with help of **Lemma 2.9**) we have

$$\begin{aligned}
&\operatorname{card}\Big((\mathcal{R} + 2b - 1) \cup \bigcup_{t=1}^{k-1} (\mathcal{R} + 2t - 1)\Big) \\
&\quad = \operatorname{card}\Big((\mathcal{R} + 2b) \cup \bigcup_{t=1}^{k-1} (\mathcal{R} + 2t)\Big) \\
&\quad \leqslant \operatorname{card}\Big(\bigcup_{t=1}^{k} (\mathcal{R} + 2t)\Big) = \operatorname{card}\Big(\bigcup_{t=1}^{k} (\mathcal{R} + 2t - 1)\Big)
\end{aligned}$$

due to inequality $(*)$, and therefore indeed

$$\begin{aligned}
&\operatorname{card}\Big((\mathcal{R} + s) \cup \bigcup_{t=1}^{n-1} (\mathcal{R} + t)\Big) = \operatorname{card}\Big((\mathcal{R} + s) \cup \bigcup_{t=1}^{2k-2} (\mathcal{R} + t)\Big) \\
&\quad = \operatorname{card}\Big((\mathcal{R} + 2b - 1) \cup \bigcup_{t=1}^{k-1} (\mathcal{R} + 2t - 1)\Big) + \operatorname{card}\Big(\bigcup_{t=1}^{k-1} (\mathcal{R} + 2t)\Big) \\
&\quad \leqslant \operatorname{card}\Big(\bigcup_{t=1}^{k} (\mathcal{R} + 2t - 1)\Big) + \operatorname{card}\Big(\bigcup_{t=1}^{k-1} (\mathcal{R} + 2t)\Big) \\
&\quad = \operatorname{card}\Big(\bigcup_{t=1}^{2k-1} (\mathcal{R} + t)\Big) = \operatorname{card}\Big(\bigcup_{t=1}^{n} (\mathcal{R} + t)\Big)
\end{aligned}$$

as long as $k \in \{1, 2, 3\}$.

If $s = 2b$ is even, then we also have

$$\begin{aligned}
&\operatorname{card}\Big((\mathcal{R}+s) \cup \bigcup_{t=1}^{n-1} (\mathcal{R}+t)\Big) \\
&\quad = \operatorname{card}\Big(\bigcup_{t=1}^{k-1} (\mathcal{R}+2t-1)\Big) + \operatorname{card}\Big((\mathcal{R}+2b) \cup \bigcup_{t=1}^{k-1} (\mathcal{R}+2t)\Big) \\
&\quad \leqslant \operatorname{card}\Big(\bigcup_{t=1}^{k-1} (\mathcal{R}+2t-1)\Big) + \operatorname{card}\Big(\bigcup_{t=1}^{k} (\mathcal{R}+2t)\Big) \\
&\quad = \operatorname{card}\Big(\bigcup_{t=1}^{k-1} (\mathcal{R}+2t)\Big) + \operatorname{card}\Big(\bigcup_{t=1}^{k} (\mathcal{R}+2t-1)\Big) \\
&\quad = \operatorname{card}\Big(\bigcup_{t=1}^{n} (\mathcal{R}+t)\Big)\,.
\end{aligned}$$

due to inequality $(*)$, as long as $k \in \{1,2,3\}$.

Combining both subcases, we have verified **Proposition 3.7** for $n \in \{1,3,5\}$.

Case 2: $n = 2k$ is even.

If $s = 2b-1$ is odd, then we have

$$\begin{aligned}
&\operatorname{card}\Big((\mathcal{R}+s) \cup \bigcup_{t=1}^{k} (\mathcal{R}+2t-1)\Big) - \operatorname{card}\Big(\bigcup_{t=1}^{k} (\mathcal{R}+2t-1)\Big) \\
&\quad \leqslant \operatorname{card}\Big((\mathcal{R}+s) \cup \bigcup_{t=1}^{k-1} (\mathcal{R}+2t-1)\Big) - \operatorname{card}\Big(\bigcup_{t=1}^{k-1} (\mathcal{R}+2t-1)\Big) \\
&\quad = \operatorname{card}\Big((\mathcal{R}+2b) \cup \bigcup_{t=1}^{k-1} (\mathcal{R}+2t)\Big) - \operatorname{card}\Big(\bigcup_{t=1}^{k-1} (\mathcal{R}+2t)\Big) \\
&\quad \leqslant \operatorname{card}\Big(\bigcup_{t=1}^{k} (\mathcal{R}+2t)\Big) - \operatorname{card}\Big(\bigcup_{t=1}^{k-1} (\mathcal{R}+2t)\Big)\,,
\end{aligned}$$

where the last inequality is due to $(*)$, as long as $k \in \{1,2,3\}$, and the first

inequality follows from

$$\begin{aligned}\operatorname{card}(\mathcal{A}\cup\mathcal{B})-\operatorname{card}(\mathcal{B})&=\operatorname{card}(\mathcal{A})-\operatorname{card}(\mathcal{A}\cap\mathcal{B})\\&\leqslant\operatorname{card}(\mathcal{A})-\operatorname{card}(\mathcal{A}\cap\mathcal{B}')=\operatorname{card}(\mathcal{A}\cup\mathcal{B}')-\operatorname{card}(\mathcal{B}')\end{aligned}$$

for any finite sets $\mathcal{A},\mathcal{B},\mathcal{B}'$ with $\mathcal{B}'\subset\mathcal{B}$. After reordering, we again reach

$$\begin{aligned}&\operatorname{card}\Big((\mathcal{R}+s)\cup\bigcup_{t=1}^{n-1}(\mathcal{R}+t)\Big)=\operatorname{card}\Big((\mathcal{R}+s)\cup\bigcup_{t=1}^{2k-1}(\mathcal{R}+t)\Big)\\&=\operatorname{card}\Big((\mathcal{R}+s)\cup\bigcup_{t=1}^{k}(\mathcal{R}+2t-1)\Big)+\operatorname{card}\Big(\bigcup_{t=1}^{k-1}(\mathcal{R}+2t)\Big)\\&\leqslant\operatorname{card}\Big(\bigcup_{t=1}^{k}(\mathcal{R}+2t)\Big)+\operatorname{card}\Big(\bigcup_{t=1}^{k}(\mathcal{R}+2t-1)\Big)\\&=\operatorname{card}\Big(\bigcup_{t=1}^{2k}(\mathcal{R}+t)\Big)=\operatorname{card}\Big(\bigcup_{t=1}^{n}(\mathcal{R}+t)\Big).\end{aligned}$$

If $s=2b$ is even, then we also have

$$\begin{aligned}&\operatorname{card}\Big((\mathcal{R}+s)\cup\bigcup_{t=1}^{n-1}(\mathcal{R}+t)\Big)\\&=\operatorname{card}\Big(\bigcup_{t=1}^{k}(\mathcal{R}+2t-1)\Big)+\operatorname{card}\Big((\mathcal{R}+2b)\cup\bigcup_{t=1}^{k-1}(\mathcal{R}+2t)\Big)\\&\leqslant\operatorname{card}\Big(\bigcup_{t=1}^{k}(\mathcal{R}+2t-1)\Big)+\operatorname{card}\Big(\bigcup_{t=1}^{k}(\mathcal{R}+2t)\Big)\\&=\operatorname{card}\Big((\mathcal{R}+n)\cup\bigcup_{t=1}^{n-1}(\mathcal{R}+t)\Big)\end{aligned}$$

due to inequality $(*)$, as long as $k\in\{1,2,3\}$.

Combining both subcases, we have verified **Proposition 3.7** for $n\in\{2,4,6\}$.

This completes our proof. □

Let us restate the inequality of **Theorem 3.7** in the form

$$\begin{aligned}&\operatorname{card}\big(\{u \in \mathcal{R}(P_r)+n : c_{n-1}(u)=0\}\big)\\ &\quad \geqslant \operatorname{card}\big(\{u \in \mathcal{R}(P_r)+s : c_{n-1}(u)=0\}\big),\end{aligned}$$

where $c_n(u)=\sum_{t=1}^{n} \mathbf{1}_{\mathcal{R}(P_r)+t}(u)$ counts how often u has been covered by one of the first n consecutive translates $\mathcal{R}(P_r)+1,\ldots,\mathcal{R}(P_r)+n$. Although we have not been able to verify this inequality beyond $n=6$, we actually can prove (as our main result) that at every time $n \in \mathbb{N}$, the inequality

$$\sum_{u \in \mathcal{R}(P_r)+n+1} c_n(u) \leqslant \sum_{u \in \mathcal{R}(P_r)+s} c_n(u)$$

holds for any shift $s \in \{1,\ldots,P_r\}$. Note that

$$\begin{aligned}\sum_{u \in \mathcal{R}(P_r)+s} c_n(u) &= \sum_{u \in \mathcal{R}(P_r)+s} \Big(\sum_{t=1}^{n} \mathbf{1}_{\mathcal{R}(P_r)+t}(u)\Big)\\ &= \sum_{t=1}^{n} \Big(\sum_{u \in \mathcal{R}(P_r)+s} \mathbf{1}_{\mathcal{R}(P_r)+t}(u)\Big)\\ &= \sum_{t=1}^{n} \operatorname{card}\big((\mathcal{R}(P_r)+s)\cap(\mathcal{R}(P_r)+t)\big),\end{aligned}$$

and therefore the desired inequality is equivalent to

$$\sum_{t=1}^{n} \operatorname{card}\big(\langle \boldsymbol{s}_{n+1}\rangle \cap \langle \boldsymbol{s}_t\rangle\big) \leqslant \sum_{t=1}^{n} \operatorname{card}\big(\langle \boldsymbol{s}\rangle \cap \langle \boldsymbol{s}_t\rangle\big)$$

in the familiar setup, where $G=\prod_{i=1}^{r}(\mathbb{Z}/p_i\mathbb{Z})$ with the sequence of r-tuples $\boldsymbol{s}_t=([t]_{p_1},\ldots,[t]_{p_r})$ $(t \in \mathbb{N})$ and any r-tuple $\boldsymbol{s}$ from G.

If one zooms out even further to $G=\prod_{i=1}^{r}(\mathbb{Z}/m_i\mathbb{Z})$ with any r integers $m_1,\ldots,m_r>1$, we have discovered the following condition, which allows us to compare sums of the interested form $\sum_{t=1}^{n} \operatorname{card}\big(\langle \boldsymbol{s}\rangle \cap \langle \boldsymbol{s}_t\rangle\big)$ between different shifts $\boldsymbol{s} \in G$ for any given finite sequence $\boldsymbol{s}_1,\ldots,\boldsymbol{s}_n$ of shifts in G.

Proposition 3.8. Let $m_1, \dots, m_r > 1$ be integers. Suppose that $\boldsymbol{x}_1, \dots, \boldsymbol{x}_A$ and $\boldsymbol{y}_1, \dots, \boldsymbol{y}_B$ are two finite sequences of r-tuples from $G = \prod_{i=1}^{r} (\mathbb{Z}/m_i\mathbb{Z})$, with $A \leqslant B$. If $\boldsymbol{a}$ and $\boldsymbol{b}$ are two r-tuples from G such that

$$C_{\mathcal{D}}(\boldsymbol{a}; \boldsymbol{x}_1, \dots, \boldsymbol{x}_A) \leqslant C_{\mathcal{D}}(\boldsymbol{b}; \boldsymbol{y}_1, \dots, \boldsymbol{y}_B)$$

for all non-empty subsets $\mathcal{D} \subset \{1, \dots, r\}$, then we have

$$\sum_{t=1}^{A} \operatorname{card}\big(\langle \boldsymbol{a} \rangle \cap \langle \boldsymbol{x}_t \rangle\big) \leqslant \sum_{t=1}^{B} \operatorname{card}\big(\langle \boldsymbol{b} \rangle \cap \langle \boldsymbol{y}_t \rangle\big)\,.$$

Proof. We use induction on the dimension $r \in \mathbb{N}$.

For an intersection of two translates of $\big\langle ([0]_{m_1}, \dots, [0]_{m_r}) \big\rangle$, we can write

$$\begin{aligned} \operatorname{card}\big(\langle \boldsymbol{a} \rangle \cap \langle \boldsymbol{x}_t \rangle\big) &= \operatorname{card}\Big(\prod_{i=1}^{r} \big((\mathbb{Z}/m_i\mathbb{Z}) \setminus \{\boldsymbol{a}(i), \boldsymbol{x}_t(i)\}\big)\Big) \\ &= \prod_{i=1}^{r} (m_i - 2 + \alpha_{i,t})\,, \end{aligned}$$

where $\alpha_{i,t} = 1$ if $\boldsymbol{a}(i) = \boldsymbol{x}_t(i)$, and $\alpha_{i,t} = 0$ otherwise. Similarly, let us write

$$\operatorname{card}\big(\langle \boldsymbol{b} \rangle \cap \langle \boldsymbol{y}_t \rangle\big) = \prod_{i=1}^{r} (m_i - 2 + \beta_{i,t})\,,$$

where $\beta_{i,t} = 1$ if $\boldsymbol{b}(i) = \boldsymbol{y}_t(i)$, and $\beta_{i,t} = 0$ otherwise.

In the special case $r = 1$, we have

$$\sum_{t=1}^{A} \operatorname{card}\big(\langle \boldsymbol{a} \rangle \cap \langle \boldsymbol{x}_t \rangle\big) = \sum_{t=1}^{A} (m_1 - 2 + \alpha_{1,t}) = A \cdot (m_1 - 2) + \sum_{t=1}^{A} \alpha_{1,t}\,,$$

and the last sum satisfies

$$\sum_{t=1}^{A} \alpha_{1,t} = C_{\{1\}}(\boldsymbol{a}; \boldsymbol{x}_1, \dots, \boldsymbol{x}_A) \leqslant C_{\{1\}}(\boldsymbol{b}; \boldsymbol{y}_1, \dots, \boldsymbol{y}_B) = \sum_{t=1}^{B} \beta_{1,t}\,.$$

Together with $A \leqslant B$, we reach

$$\sum_{t=1}^{A} \operatorname{card}\big(\langle \boldsymbol{a}\rangle \cap \langle \boldsymbol{x}_t\rangle\big) \leqslant B\cdot(m_1-2) + \sum_{t=1}^{B} \beta_{1,t} = \sum_{t=1}^{B} \operatorname{card}\big(\langle \boldsymbol{b}\rangle \cap \langle \boldsymbol{y}_t\rangle\big)\,,$$

and everything is fine.

Suppose that we have already established **Proposition 3.8** in some dimension $r \in \mathbb{N}$. Now, let $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_A$ and $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_B$ be two sequences of $(r+1)$-tuples from $G \times (\mathbb{Z}/m_{r+1}\mathbb{Z})$, with $A \leqslant B$, and let us assume that $\boldsymbol{a}$ and $\boldsymbol{b}$ are two $(r+1)$-tuples from $G \times (\mathbb{Z}/m_{r+1}\mathbb{Z})$ such that

$$C_{\mathcal{D}}(\boldsymbol{a}; \boldsymbol{x}_1, \ldots, \boldsymbol{x}_A) \leqslant C_{\mathcal{D}}(\boldsymbol{b}; \boldsymbol{y}_1, \ldots, \boldsymbol{y}_B)$$

for all non-empty subsets $\mathcal{D} \subset \{1, \ldots, r, r+1\}$. We have

$$\begin{aligned}
\sum_{t=1}^{A} \operatorname{card}\big(\langle \boldsymbol{a}\rangle \cap \langle \boldsymbol{x}_t\rangle\big) &= \sum_{t=1}^{A} \Big(\prod_{i=1}^{r+1} (m_i - 2 + \alpha_{i,t}) \Big) \\
&= \sum_{t=1}^{A} \Big((m_{r+1} - 2 + \alpha_{r+1,t}) \cdot \prod_{i=1}^{r} (m_i - 2 + \alpha_{i,t}) \Big) \\
&= (m_{r+1}-2) \cdot \sum_{t=1}^{A} \Big(\prod_{i=1}^{r} (m_i - 2 + \alpha_{i,t}) \Big) \\
&\quad + \sum_{t=1}^{A} \Big(\alpha_{r+1,t} \cdot \prod_{i=1}^{r} (m_i - 2 + \alpha_{i,t}) \Big) \qquad =: (m_{r+1}-2)\cdot S_1 + S_2\,,
\end{aligned}$$

and next we estimate both sums S_1 and S_2 seperately.

For every non-empty subset $\mathcal{D} \subset \{1, \ldots, r\}$, we have

$$\begin{aligned}
&C_{\mathcal{D}}\Big((\boldsymbol{a}(1), \ldots, \boldsymbol{a}(r)); \big((\boldsymbol{x}_t(1), \ldots, \boldsymbol{x}_t(r))\big)_{t\in\{1,\ldots,A\}} \Big) \\
&\quad = C_{\mathcal{D}}(\boldsymbol{a}; \boldsymbol{x}_1, \ldots, \boldsymbol{x}_A) \\
&\quad \leqslant C_{\mathcal{D}}(\boldsymbol{b}; \boldsymbol{y}_1, \ldots, \boldsymbol{y}_B) \\
&\quad = C_{\mathcal{D}}\Big((\boldsymbol{b}(1), \ldots, \boldsymbol{b}(r)); \big((\boldsymbol{y}_t(1), \ldots, \boldsymbol{y}_t(r))\big)_{t\in\{1,\ldots,B\}} \Big)
\end{aligned}$$

by assumption, and so we inductively reach

$$\begin{aligned}
S_1 &= \sum_{t=1}^{A} \Big(\prod_{i=1}^{r} (m_i - 2 + \alpha_{i,t}) \Big) \\
&= \sum_{t=1}^{A} \operatorname{card}\Big(\big\langle (\boldsymbol{a}(1), \ldots, \boldsymbol{a}(r)) \big\rangle \cap \big\langle (\boldsymbol{x}_t(1), \ldots, \boldsymbol{x}_t(r)) \big\rangle \Big) \\
&\leqslant \sum_{t=1}^{B} \operatorname{card}\Big(\big\langle (\boldsymbol{b}(1), \ldots, \boldsymbol{b}(r)) \big\rangle \cap \big\langle (\boldsymbol{y}_t(1), \ldots, \boldsymbol{y}_t(r)) \big\rangle \Big) \\
&= \sum_{t=1}^{B} \Big(\prod_{i=1}^{r} (m_i - 2 + \beta_{i,t}) \Big) .
\end{aligned}$$

In the case of S_2, let $\mathcal{A} \subset \{1, \ldots, n\}$ be the set of those indices t, where $\boldsymbol{x}_t(r+1) = \boldsymbol{a}(r+1)$, and let $\mathcal{B} \subset \{1, \ldots, n\}$ be the set of those indices t, where $\boldsymbol{y}_t(r+1) = \boldsymbol{b}(r+1)$. Note that we can now write

$$\begin{aligned}
S_2 &= \sum_{t=1}^{A} \Big(\alpha_{r+1,t} \cdot \prod_{i=1}^{r} (m_i - 2 + \alpha_{i,t}) \Big) = \sum_{t \in \mathcal{A}} \Big(\prod_{i=1}^{r} (m_i - 2 + \alpha_{i,t}) \Big) \\
&= \sum_{t \in \mathcal{A}} \operatorname{card}\Big(\big\langle (\boldsymbol{a}(1), \ldots, \boldsymbol{a}(r)) \big\rangle \cap \big\langle (\boldsymbol{x}_t(1), \ldots, \boldsymbol{x}_t(r)) \big\rangle \Big) .
\end{aligned}$$

For every non-empty subset $\mathcal{D} \subset \{1, \ldots, r\}$, we have

$$\begin{aligned}
&C_{\mathcal{D}}\Big((\boldsymbol{a}(1), \ldots, \boldsymbol{a}(r)); \big((\boldsymbol{x}_t(1), \ldots, \boldsymbol{x}_t(r)) \big)_{t \in \mathcal{A}} \Big) \\
&\quad = C_{\mathcal{D} \cup \{r+1\}}(\boldsymbol{a}; (\boldsymbol{x}_t)_{t \in \mathcal{A}}) = C_{\mathcal{D} \cup \{r+1\}}(\boldsymbol{a}; \boldsymbol{x}_1, \ldots, \boldsymbol{x}_A) ,
\end{aligned}$$

and by assumption $C_{\mathcal{D} \cup \{r+1\}}(\boldsymbol{a}; \boldsymbol{x}_1, \ldots, \boldsymbol{x}_A) \leqslant C_{\mathcal{D} \cup \{r+1\}}(\boldsymbol{b}; \boldsymbol{y}_1, \ldots, \boldsymbol{y}_B)$, which leads into

$$\begin{aligned}
&C_{\mathcal{D}}\Big((\boldsymbol{a}(1), \ldots, \boldsymbol{a}(r)); \big((\boldsymbol{x}_t(1), \ldots, \boldsymbol{x}_t(r)) \big)_{t \in \mathcal{A}} \Big) \\
&\quad \leqslant C_{\mathcal{D} \cup \{r+1\}}(\boldsymbol{b}; \boldsymbol{y}_1, \ldots, \boldsymbol{y}_B) = C_{\mathcal{D} \cup \{r+1\}}(\boldsymbol{b}; (\boldsymbol{y}_t)_{t \in \mathcal{B}}) \\
&\quad = C_{\mathcal{D}}\Big((\boldsymbol{b}(1), \ldots, \boldsymbol{b}(r)); \big((\boldsymbol{y}_t(1), \ldots, \boldsymbol{y}_t(r)) \big)_{t \in \mathcal{B}} \Big) .
\end{aligned}$$

Together with the inequality

$$\operatorname{card}(\mathcal{A}) = C_{\{r+1\}}(\boldsymbol{a}; \boldsymbol{x}_1, \ldots, \boldsymbol{x}_A) \leqslant C_{\{r+1\}}(\boldsymbol{b}; \boldsymbol{y}_1, \ldots, \boldsymbol{y}_B) = \operatorname{card}(\mathcal{B}),$$

we inductively reach

$$\begin{aligned} S_2 &= \sum_{t \in \mathcal{A}} \operatorname{card}\Big(\big\langle (\boldsymbol{a}(1), \ldots, \boldsymbol{a}(r)) \big\rangle \cap \big\langle (\boldsymbol{x}_t(1), \ldots, \boldsymbol{x}_t(r)) \big\rangle \Big) \\ &\leqslant \sum_{t \in \mathcal{B}} \operatorname{card}\Big(\big\langle (\boldsymbol{b}(1), \ldots, \boldsymbol{b}(r)) \big\rangle \cap \big\langle (\boldsymbol{y}_t(1), \ldots, \boldsymbol{y}_t(r)) \big\rangle \Big) \\ &= \sum_{t \in \mathcal{B}} \Big(\prod_{i=1}^{r} (m_i - 2 + \beta_{i,t}) \Big) = \sum_{t=1}^{B} \Big(\beta_{r+1,t} \cdot \prod_{i=1}^{r} (m_i - 2 + \beta_{i,t}) \Big). \end{aligned}$$

Combining the estimates for both sums S_1 and S_2, we obtain

$$\begin{aligned} \sum_{t=1}^{A} \operatorname{card}\big(\langle \boldsymbol{a} \rangle \cap \langle \boldsymbol{x}_t \rangle \big) &\leqslant (m_{r+1} - 2) \cdot S_1 + S_2 \\ &\leqslant (m_{r+1} - 2) \cdot \sum_{t=1}^{B} \Big(\prod_{i=1}^{r} (m_i - 2 + \beta_{i,t}) \Big) \\ &\quad + \sum_{t=1}^{B} \Big(\beta_{r+1,t} \cdot \prod_{i=1}^{r} (m_i - 2 + \beta_{i,t}) \Big) \\ &= \sum_{t=1}^{B} \Big((m_{r+1} - 2 + \beta_{r+1,t}) \cdot \prod_{i=1}^{r} (m_i - 2 + \beta_{i,t}) \Big) \\ &= \sum_{t=1}^{B} \Big(\prod_{i=1}^{r+1} (m_i - 2 + \beta_{i,t}) \Big) = \sum_{t=1}^{B} \operatorname{card}\big(\langle \boldsymbol{b} \rangle \cap \langle \boldsymbol{y}_t \rangle \big), \end{aligned}$$

and this completes our proof by induction. □

In the special case, when $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_A$ and $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_B$ form the same sequence (up to reordering of their members) of length $A = B$, the condition $C_{\mathcal{D}}(\boldsymbol{a}; \boldsymbol{x}_1, \ldots, \boldsymbol{x}_A) \leqslant C_{\mathcal{D}}(\boldsymbol{b}; \boldsymbol{y}_1, \ldots, \boldsymbol{y}_B)$ for all non-empty $\mathcal{D} \subset \{1, \ldots, r\}$ encodes that after adjoining $\boldsymbol{a}$, the sequence $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_A, \boldsymbol{a}$ is balanced on at

least as many subsets $\mathcal{D} \subset \{1, \ldots, r\}$ as the sequence $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_B, \boldsymbol{b}$, where we have adjoined $\boldsymbol{b}$. With this in mind, we turn to our main result.

Theorem 3.9. For a given $r \in \mathbb{N}$, let $\mathcal{R}$ denote the set $\mathcal{R}(P_r)$ of reduced residue classes modulo P_r. At every time $n \in \mathbb{N}$, the inequality

$$\sum_{t=1}^{n} \operatorname{card}\big((\mathcal{R}+n+1) \cap (\mathcal{R}+t)\big) \leqslant \sum_{t=1}^{n} \operatorname{card}\big((\mathcal{R}+s) \cap (\mathcal{R}+t)\big)$$

holds for any shift $s \in \{1, \ldots, P_r\}$.

Proof. We are going to use **Proposition 3.8** in the case $G = \prod_{i=1}^{r} (\mathbb{Z}/p_i\mathbb{Z})$, when both finite sequences $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_A$ and $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_B$ of r-tuples from G are given by the same sequence $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_n$ of shifts $\boldsymbol{s}_t = ([t]_{p_1}, \ldots, [t]_{p_r})$.

For $\boldsymbol{a} = \boldsymbol{s}_{n+1}$, we now check that $C_{\mathcal{D}}(\boldsymbol{a}; \boldsymbol{s}_1, \ldots, \boldsymbol{s}_n) \leqslant C_{\mathcal{D}}(\boldsymbol{b}; \boldsymbol{s}_1, \ldots, \boldsymbol{s}_n)$ holds for any shift $\boldsymbol{b} = \boldsymbol{s} \in G$ and any given non-empty subset $\mathcal{D} \subset \{1, \ldots, r\}$. Of course, for $q = \prod_{i \in \mathcal{D}} p_i$ and any integer a, we have $\bigcup_{t=a+1}^{a+q} [t]_q = \mathbb{Z}/q\mathbb{Z}$. Since $p_1, \ldots, p_r$ are pairwise relatively prime, this also transfers into

$$\bigcup_{t=a+1}^{a+q} ([t]_{p_i})_{i \in \mathcal{D}} = \prod_{i \in \mathcal{D}} (\mathbb{Z}/p_i\mathbb{Z}) \,,$$

by the Chinese remainder theorem (where i runs through $\mathcal{D}$ in increasing order). In other words, we have $C_{\mathcal{D}}(\boldsymbol{s}; \boldsymbol{s}_{a+1}, \ldots, \boldsymbol{s}_{a+q}) = 1$ for all $\boldsymbol{s} \in G$, as well as $C_{\mathcal{D}}(\boldsymbol{s}_{a+q}; \boldsymbol{s}_{a+1}, \ldots, \boldsymbol{s}_{a+q-1}) = C_{\mathcal{D}}(\boldsymbol{s}_a; \boldsymbol{s}_{a+1}, \ldots, \boldsymbol{s}_{a+q-1}) = 0$. If we write $n = u \cdot q + v$, with (unique) $u \in \mathbb{N}_0$ and $v \in \{1, \ldots, q\}$, the value of

$$\begin{aligned} C_{\mathcal{D}}(\boldsymbol{s}; \boldsymbol{s}_1, \ldots, \boldsymbol{s}_n) &= \sum_{k=0}^{u-1} C_{\mathcal{D}}(\boldsymbol{s}; \boldsymbol{s}_{k \cdot q+1}, \ldots, \boldsymbol{s}_{k \cdot q+q}) \\ &\quad + C_{\mathcal{D}}(\boldsymbol{s}; \boldsymbol{s}_{u \cdot q+1}, \ldots, \boldsymbol{s}_{u \cdot q+v}) \\ &= u \cdot 1 + C_{\mathcal{D}}(\boldsymbol{s}; \boldsymbol{s}_{u \cdot q+1}, \ldots, \boldsymbol{s}_{u \cdot q+v}) \end{aligned}$$

can be seen to equal $\lfloor n/q \rfloor$ or $\lceil n/q \rceil$, while $C_{\mathcal{D}}(\boldsymbol{s}_{n+1}; \boldsymbol{s}_1, \ldots, \boldsymbol{s}_n) = \lfloor n/q \rfloor$ due to $C_{\mathcal{D}}(\boldsymbol{s}_{u \cdot q+v+1}; \boldsymbol{s}_{u \cdot q+1}, \ldots, \boldsymbol{s}_{u \cdot q+v}) = 0$ for $v \in \{1, \ldots, q-1\}$.

Hence, $C_{\mathcal{D}}(\boldsymbol{s}_{n+1};\boldsymbol{s}_1,\ldots,\boldsymbol{s}_n)\leqslant C_{\mathcal{D}}(\boldsymbol{s};\boldsymbol{s}_1,\ldots,\boldsymbol{s}_n)$ is indeed true for all $\boldsymbol{s}\in G$, and **Proposition 3.8** can ensure that at every time $n\in\mathbb{N}$, the inequality

$$\sum_{t=1}^{n}\operatorname{card}\big(\langle\boldsymbol{s}_{n+1}\rangle\cap\langle\boldsymbol{s}_t\rangle\big)\leqslant\sum_{t=1}^{n}\operatorname{card}\big(\langle\boldsymbol{s}\rangle\cap\langle\boldsymbol{s}_t\rangle\big)$$

holds for any shift $\boldsymbol{s}\in G$, exactly as needed to complete our proof. □

After having established our main result, we can also make a little progress towards **Problem 3.1**, which is a good point to round out this section.

Corollary 3.10. For $r\in\mathbb{N}$ and any given $k\in\{1,\ldots,j(P_r)\}$, the value of

$$\sum_{t\,\in\,\{1,\ldots,j(P_r)\}\,\setminus\,\{k\}}\operatorname{card}\big((\mathcal{R}(P_r)+s)\cap(\mathcal{R}(P_r)+t)\big)$$

is minimized for the shift $s=k$, along all shifts $s\in\{1,\ldots,P_r\}$.

Proof. Let us abbreviate $\mathcal{R}(P_r)$ with $\mathcal{R}$ and $j(P_r)$ with j. We can split the sum at hand into two parts, as

$$\sum_{t=1}^{k-1}\operatorname{card}\big((\mathcal{R}+s)\cap(\mathcal{R}+t)\big)+\sum_{t=k+1}^{j}\operatorname{card}\big((\mathcal{R}+s)\cap(\mathcal{R}+t)\big)\,.$$

By **Theorem 3.9** (with $n=k-1$), the first sum is indeed minimized at $s=k$. On the other hand, the second sum can be transformed into

$$\sum_{t=1}^{j-k}\operatorname{card}\big((\mathcal{R}+s-k)\cap(\mathcal{R}+t)\big)\,,$$

and thus **Theorem 3.9** (with $n=j-k$) can ensure that it is minimized when $s-k=j-k+1$, that is at $s=j+1$. Since we have the identity

$$\sum_{t=k+1}^{j}\operatorname{card}\big((\mathcal{R}+j+1)\cap(\mathcal{R}+t)\big)=\sum_{t=k+1}^{j}\operatorname{card}\big((\mathcal{R}+k)\cap(\mathcal{R}+t)\big)\,,$$

it is also minimized at $s=k$ again, and this completes our proof. □

4 Additive representation functions

In this last chapter, for a set $\mathcal{A} \subset \mathbb{N}_0$, we take a closer look at its **sumset** $\mathcal{A}+\mathcal{A} = \{a_1 + a_2 : a_1, a_2 \in \mathcal{A}\}$, by considering its **additive representation functions** r_1, r_2 and r_3 defined as

$$r_1(\mathcal{A}, n) = \operatorname{card}\Big(\{(a_1, a_2) \in \mathcal{A} \times \mathcal{A} : a_1 + a_2 = n\}\Big),$$
$$r_2(\mathcal{A}, n) = \operatorname{card}\Big(\{(a_1, a_2) \in \mathcal{A} \times \mathcal{A} : a_1 + a_2 = n,\, a_1 \leqslant a_2\}\Big),$$
$$r_3(\mathcal{A}, n) = \operatorname{card}\Big(\{(a_1, a_2) \in \mathcal{A} \times \mathcal{A} : a_1 + a_2 = n,\, a_1 < a_2\}\Big),$$

for all $n \in \mathbb{N}_0$. In particular, $r_2(\mathcal{A}, n)$ also stands for the number of how many times n is covered by those translates of $\mathcal{A}$ shifted by the elements of $\mathcal{A}$ itself.

In 1941, Erdős and Turán [8] proved that if $\mathcal{A}$ is infinite, then $r_1(\mathcal{A}, n)$ cannot be constant for all $n \geqslant n_0$ from a certain point n_0 onwards. Moreover, they conjectured that if $r_1(\mathcal{A}, n) > 0$ for all $n \geqslant n_0$, then $r_1(\mathcal{A}, n)$ has to be unbounded. This is also known as the Erdős-Turán conjecture on additive bases and it remains wide open, although Borwein, Choi and Chu [2] proved that if $r_1(\mathcal{A}, n) > 0$ for all $n \geqslant n_0$, then $r_1(\mathcal{A}, n) \geqslant 8$ for some n. Another direction has been opened by Erdős, Sárközy and Sós in [10], where they demonstrated how differently r_1, r_2 and r_3 can behave with respect to **monotonicity**:

Theorem 4.1 ([10])**.** Let $\mathcal{A}$ be an infinite set of positive integers.

(1) $r_1(\mathcal{A}, n)$ can be monotone increasing from a certain point on, but only if $\mathcal{A}$ contains all integers from a certain point on.

(2) $r_2(\mathcal{A}, n)$ cannot be monotone increasing from a certain point on, when $\lim_{N\to\infty} \operatorname{card}\big(\{1, \dots, N\} \setminus \mathcal{A}\big)/\log N = \infty$.

(3) There exists a set $\mathcal{A}$ such that $\mathbb{N} \setminus \mathcal{A}$ is infinite and $r_3(\mathcal{A}, n)$ is monotone increasing for all $n \geqslant 1$.

Our main purpose of this chapter is to investigate these monotonicity properties further. Alongside, we solve one open problem and another one partially ([33]).

4.1 A special case and strict monotonicity

In order to become a bit more familiar with all three additive representation functions, let us first collect the following three helpful formulas for $r_1(\mathcal{A},n)$, $r_2(\mathcal{A},n)$ and $r_3(\mathcal{A},n)$ in the special case $\mathcal{A}=\mathbb{N}_0$.

Lemma 4.2. For $n\in\mathbb{N}_0$, we have

(1) $r_1(\mathbb{N}_0,n)=n+1$,

(2) $r_2(\mathbb{N}_0,n)=\lfloor n/2\rfloor+1$,

(3) $r_3(\mathbb{N}_0,n)=\lfloor (n-1)/2\rfloor+1$,

where $\lfloor x\rfloor$ denotes the largest integer not exceeding $x\in\mathbb{R}$.

Proof. By definition, we have

$$r_1(\mathbb{N}_0,n)=\operatorname{card}\Big(\{(a,n-a):a\in\{0,1,\dots,n\}\}\Big)=n+1\,.$$

If $n=2k$ ($k\in\mathbb{N}_0$) is even, we find

$$r_2(\mathbb{N}_0,n)=\operatorname{card}\Big(\{(a,n-a):a\in\mathbb{N}_0,\,a\leqslant n/2=k\}\Big)=k+1\,,$$
$$r_3(\mathbb{N}_0,n)=\operatorname{card}\Big(\{(a,n-a):a\in\mathbb{N}_0,\,a<n/2=k\}\Big)=k\,.$$

In the other case, when $n=2k+1$ is odd, then

$$r_2(\mathbb{N}_0,n)=\operatorname{card}\Big(\{(a,n-a):a\in\mathbb{N}_0,\,a\leqslant n/2=k+1/2\}\Big)=k+1\,,$$
$$r_3(\mathbb{N}_0,n)=\operatorname{card}\Big(\{(a,n-a):a\in\mathbb{N}_0,\,a<n/2=k+1/2\}\Big)=k+1\,.$$

Both cases together also lead us to formula (2) and (3). □

Note that formula (1) of **Lemma 4.2** implies that $r_1(\mathcal{A},n)$ is **strictly** monotone increasing for all $n\geqslant 0$ in the case $\mathcal{A}=\mathbb{N}_0$. However, formula (2) and (3) cannot immediately reveal something about strict monotonicity of $r_2(\mathcal{A},n)$ or $r_3(\mathcal{A},n)$. In fact, $r_2(\mathcal{A},n)$ as well as $r_3(\mathcal{A},n)$ cannot be strictly monotone increasing for all $n\geqslant n_0$, as shown by Chen and Tang [6].

In what follows, we like to present an alternative proof of their result, where one does not need property (1) of **Theorem 4.1** for $r_1(\mathcal{A}, n)$ anymore.

Theorem 4.3 ([6]). If $\mathcal{A} \subset \mathbb{N}_0$, then $r_2(\mathcal{A}, n)$ (and $r_3(\mathcal{A}, n)$, respectively) cannot be strictly monotone increasing from a certain point on.

Proof. Suppose that there exists an integer n_0 such that $r_2(\mathcal{A}, n)$ is strictly monotone increasing for all $n \geqslant n_0$. But then from this point onwards $r_2(\mathcal{A}, n)$ grows by at least 1 whenever n increases by 1. Thus, at $n = 2n_0 + 3$, we find

$$\begin{aligned} r_2(\mathcal{A}, 2n_0 + 3) &\geqslant r_2(\mathcal{A}, 2n_0 + 2) + 1 \geqslant \ldots \\ &\geqslant r_2(\mathcal{A}, n_0) + 1 \cdot (n_0 + 3) \geqslant n_0 + 3 \end{aligned}$$

in contradiction to

$$r_2(\mathcal{A}, 2n_0 + 3) \leqslant r_2(\mathbb{N}_0, 2n_0 + 3) = \lfloor (2n_0 + 3)/2 \rfloor + 1 \leqslant n_0 + 5/2$$

by **Lemma 4.2**. Therefore, all that remains is that $r_2(\mathcal{A}, n)$ cannot be strictly monotone increasing from a certain point on.

Similarly, also $r_3(\mathcal{A}, n)$ cannot be strictly monotone increasing from a certain point on. For this, note that one can simply replace r_2 with r_3 in the first chain of inequalities, and that one has $r_3(\mathcal{A}, 2n_0 + 3) \leqslant r_2(\mathcal{A}, 2n_0 + 3)$ in the last chain of inequalities, as $r_3(\mathcal{A}, n)$ never exceeds $r_2(\mathcal{A}, n)$. □

4.2 Monotonicity properties of r_1 and r_2

In his collection of unsolved problems [29], Sárközy has asked with respect to property (1) of **Theorem 4.1**, whether or not there exists an infinite set $\mathcal{A} \subset \mathbb{N}_0$ such that its upper asymptotic density is less than 1, and $r_1(\mathcal{A}, n)$ is monotone increasing for almost all n. We can answer this positively and show a bit more.

Theorem 4.4. There exists an infinite set $\mathcal{A} \subset \mathbb{N}_0$ such that its natural density is 0, and $r_1(\mathcal{A}, n)$ is monotone increasing almost everywhere, that is

$$r_1(\mathcal{A}, n) \leqslant r_1(\mathcal{A}, n + 1) \quad \text{for almost all } n \in \mathbb{N}\,.$$

In addition, there exists a set $\mathcal{A} \subset \mathbb{N}_0$ such that its complement $\mathbb{N}_0 \setminus \mathcal{A}$ is infinite, and $r_1(\mathcal{A}, n)$ is strictly monotone increasing almost everywhere.

Proof. First, let us choose the set $\mathcal{A} = \{2^i : i \in \mathbb{N}\}$ whose natural density

$$\lim_{N \to \infty} \frac{\operatorname{card}(\mathcal{A} \cap \{1, \ldots, N\})}{N} = \lim_{N \to \infty} \frac{\lfloor \log_2 N \rfloor}{N} \leqslant \lim_{N \to \infty} \frac{\log_2 N}{N} = 0$$

does exist and equals 0. Out of the $\lfloor \log_2 N \rfloor$ members of $\mathcal{A}$ up to $N \geqslant 1$ we can build no more than $(\log_2 N)^2$ pairwise sums. In other words, there exist at least $N - (\log_2 N)^2$ positive integers $n \leqslant N$ such that

$$r_1(\mathcal{A}, n) = 0 \leqslant r_1(\mathcal{A}, n+1)\,.$$

Hence, the probability that a positive integer n chosen at random satisfies $r_1(\mathcal{A}, n) \leqslant r_1(\mathcal{A}, n+1)$ is at least

$$\lim_{N \to \infty} \frac{N - (\log_2 N)^2}{N} = 1 - \lim_{N \to \infty} \frac{(\log_2 N)^2}{N} = 1 - 0 = 1\,,$$

as desired.

Now, let us choose $\mathcal{A} = \mathbb{N}_0 \setminus \{2^i : i \in \mathbb{N}\}$ whose natural density is $1 - 0 = 1$, and define the family of sets $\mathcal{A}_j = \mathbb{N}_0 \setminus \{2^i : i \in \mathbb{N}, i \leqslant j\}$, where for $j \in \mathbb{N}$ we only have removed the first j powers of 2.

If $n \in \{2^j + 1, 2^j + 2, \ldots, 2^{j+1}\}$, we have (with help of **Lemma 4.2**)

$$r_1(\mathcal{A}_{j-1}, n) = r_1(\mathbb{N}_0, n) - 2 \cdot (j-1) = n + 1 - 2 \cdot (j-1)\,,$$

since $a + b \leqslant 2^{j-1} + 2^{j-1} = 2^j < n$ for any a and b in $\{2^i : i \in \mathbb{N}, i \leqslant j-1\}$. Additionally, if n is also not of the form $2^j + 2^i$ with $i \in \mathbb{N}$ $(i \leqslant j)$, we even get

$$r_1(\mathcal{A}, n) = r_1(\mathcal{A}_j, n) = r_1(\mathcal{A}_{j-1}, n) - 2 = n + 1 - 2 \cdot j$$

(while $r_1(\mathcal{A}, n) = n + 1 - 2 \cdot (j-1)$ for $n = 2^j + 2^i$). Moreover, we have

$$\begin{aligned} r_1(\mathcal{A}, n+1) &= r_1(\mathcal{A}_j, n+1) \\ &\geqslant r_1(\mathbb{N}_0, n+1) - 2 \cdot j = (n+1) + 1 - 2 \cdot j > r_1(\mathcal{A}, n) \end{aligned}$$

as long as $n+1 < 2^{j+1}$. Since there are no more than j numbers of the form $2^j + 2^i$ from 2^j+1 up to $2^{j+1}-2$, we have found at least $2^j - 2 - j$ numbers n in $\{2^j+1, 2^j+2, \ldots, 2^{j+1}\}$ such that $r_1(\mathcal{A}, n) < r_1(\mathcal{A}, n+1)$.

In view of the partition

$$\mathbb{N} = \{1,2\} \cup \bigcup_{j=1}^{\infty} \{2^j+1, 2^j+2, \ldots, 2^{j+1}\}\,,$$

up to an integer $N \geqslant 1$ we then find at most

$$\begin{aligned} &2 + \sum_{j=1}^{\lfloor \log_2 N \rfloor + 1} (2+j) \\ &\quad \leqslant 2 + (\lfloor \log_2 N \rfloor + 1) \cdot (2 + \lfloor \log_2 N \rfloor + 1) \leqslant 2 + (\log_2 N + 3)^2 \end{aligned}$$

positive integers n such that $r_1(\mathcal{A}, n) \geqslant r_1(\mathcal{A}, n+1)$. Hence, the probability that a positive integer n chosen at random satisfies $r_1(\mathcal{A}, n) < r_1(\mathcal{A}, n+1)$ is again at least

$$\begin{aligned} &\lim_{N\to\infty} \frac{N - (2 + (\log_2 N + 3)^2)}{N} \\ &\quad = 1 - \lim_{N\to\infty} \left(\frac{(\log_2 N)^2}{N} + \frac{6 \log_2 N}{N} + \frac{11}{N} \right) = 1 - (0+0+0) = 1\,, \end{aligned}$$

as desired. □

Until today the existence of a set $\mathcal{A} \subset \mathbb{N}_0$ such that its complement $\mathbb{N}_0 \setminus \mathcal{A}$ is infinite, and $r_2(\mathcal{A}, n)$ is monotone increasing from a certain point on, remains uncertain. After property (2) of **Theorem 4.1**, even more conditions have been collected (see [5] or [6]), under which $r_2(\mathcal{A}, n)$ cannot be monotone increasing. On the other hand, in their original paper [10], Erdős, Sárközy and Sós suggest that perhaps a similar construction of a set $\mathcal{A}$ as the one they did for property (3) in **Theorem 4.1** is also possible for $r_2(\mathcal{A}, n)$.

However, in what follows, we can show that this is not possible, if $r_2(\mathcal{A}, n)$ should be monotone increasing for all $n \geqslant 0$.

Theorem 4.5. If $\mathcal{A} \subset \mathbb{N}_0$ is non-empty and the complement $\mathbb{N}_0 \setminus \mathcal{A}$ is infinite, then $r_2(\mathcal{A}, n)$ cannot be monotone increasing for all $n \geqslant 0$.

In the appendix we provide some diagrams illustrating our proof.

Proof. Let $c_1, c_2, c_3, \ldots$ denote the elements of $\mathbb{N}_0 \setminus \mathcal{A}$ in increasing order.

If $c_1 = 2k+1$ $(k \in \mathbb{N}_0)$ is odd, then (with help of **Lemma 4.2**)

$$\begin{aligned} r_2(\mathcal{A}, c_1 - 1) &= r_2(\mathcal{A} \cap \{0, 1, \ldots, c_1 - 1\}, c_1 - 1) \\ &= r_2(\{0, 1, \ldots, c_1 - 1\}, c_1 - 1) \\ &= r_2(\mathbb{N}_0, c_1 - 1) = \lfloor (2k+1-1)/2 \rfloor + 1 = k + 1\,, \end{aligned}$$

while on the other side

$$\begin{aligned} r_2(\mathcal{A}, c_1) &= r_2(\mathcal{A} \cap \{0, 1, \ldots, c_1 - 1, c_1\}, c_1) \\ &= r_2(\{0, 1, \ldots, c_1 - 1\}, c_1) = r_2(\mathbb{N}_0 \setminus \{c_1\}, c_1) \\ &= r_2(\mathbb{N}_0, c_1) - 1 = \lfloor (2k+1)/2 \rfloor + 1 - 1 = k\,. \end{aligned}$$

Hence, there would be a decrease $r_2(\mathcal{A}, c_1 - 1) > r_2(\mathcal{A}, c_1)$, which means c_1 has to be even. At this point, we distinguish two cases for c_1.

Case 1: $c_1 = 2x$ for $x > 0$.

If the next number $c_2 = 2k+1$ $(k \geqslant x)$ missing from $\mathcal{A}$ is odd, then

$$\begin{aligned} r_2(\mathcal{A}, c_2 - 1) &= r_2(\mathbb{N}_0 \setminus \{c_1\}, c_2 - 1) \\ &= r_2(\mathbb{N}_0, c_2 - 1) - 1 = \lfloor (2k+1-1)/2 \rfloor + 1 - 1 = k\,, \end{aligned}$$

while due to $c_1 + c_2 \neq c_2$ $(c_1 > 0)$ we get

$$\begin{aligned} r_2(\mathcal{A}, c_2) &= r_2(\mathbb{N}_0 \setminus \{c_1, c_2\}, c_2) \\ &= r_2(\mathbb{N}_0, c_2) - 2 = \lfloor (2k+1)/2 \rfloor + 1 - 2 = k - 1\,. \end{aligned}$$

Hence, again there would be a decrease $r_2(\mathcal{A}, c_2 - 1) > r_2(\mathcal{A}, c_2)$, which means that c_2 has to be even, and we write $c_2 = 2y$ $(y > x)$.

Assume for a moment that c_3 is larger than $c_1 + c_2 + 1$, then

$$\begin{aligned} r_2(\mathcal{A}, c_1 + c_2) &= r_2(\mathbb{N}_0 \setminus \{c_1, c_2\}, c_1 + c_2) \\ &= r_2(\mathbb{N}_0, c_1 + c_2) - 1 \\ &= \lfloor (2\,x + 2\,y)/2 \rfloor + 1 - 1 \\ &= x + y\,, \end{aligned}$$

while due to $c_1 + c_2 \neq c_1 + c_2 + 1$ we get

$$\begin{aligned} r_2(\mathcal{A}, c_1 + c_2 + 1) &= r_2(\mathbb{N}_0 \setminus \{c_1, c_2\}, c_1 + c_2 + 1) \\ &= r_2(\mathbb{N}_0, c_1 + c_2 + 1) - 2 \\ &= \lfloor (2\,x + 2\,y + 1)/2 \rfloor + 1 - 2 \\ &= x + y - 1\,. \end{aligned}$$

The found decrease $r_2(\mathcal{A}, c_1 + c_2) > r_2(\mathcal{A}, c_1 + c_2 + 1)$ even remains as long as $c_3 > c_2 + 1$, because here

$$(c_1 + c_2) - c_i < (c_1 + c_2 + 1) - c_i \leqslant (c_1 + c_2 + 1) - c_3 < c_1$$

for $i \geqslant 3$, which means $(c_1 + c_2) - c_i$ and $(c_1 + c_2 + 1) - c_i$ are not in $\mathbb{N}_0 \setminus \mathcal{A}$.

If now c_j is the largest number less than $c_1 + c_2 + 2$ missing from $\mathcal{A}$, then

$$\begin{aligned} r_2(\mathcal{A}, c_1 + c_2) &= r_2(\mathbb{N}_0 \setminus \{c_1, c_2, \ldots, c_j\}, c_1 + c_2) \\ &\geqslant r_2(\mathbb{N}_0, c_1 + c_2) - 1 - (j - 2) \\ &= \lfloor (2\,x + 2\,y)/2 \rfloor + 1 - 1 - (j - 2) \\ &= x + y - j + 2\,, \end{aligned}$$

while due to $c_1 + c_2 \neq c_1 + c_2 + 1$ we get

$$\begin{aligned} r_2(\mathcal{A}, c_1 + c_2 + 1) &= r_2(\mathbb{N}_0 \setminus \{c_1, c_2, \ldots, c_j\}, c_1 + c_2 + 1) \\ &= r_2(\mathbb{N}_0, c_1 + c_2 + 1) - 2 - (j - 2) \\ &= \lfloor (2\,x + 2\,y + 1)/2 \rfloor + 1 - 2 - (j - 2) \\ &= x + y - j + 1\,. \end{aligned}$$

In order to avoid this decrease all that remains is the choice $c_3 = c_2 + 1$. But then we discover an unavoidable decrease from $r_2(\mathcal{A}, c_2)$ to $r_2(\mathcal{A}, c_2 + 1)$, since

$$\begin{aligned} r_2(\mathcal{A}, c_2) &= r_2(\mathbb{N}_0 \setminus \{c_1, c_2\}, c_2) \\ &= r_2(\mathbb{N}_0, c_2) - 2 \\ &= \lfloor 2y/2 \rfloor + 1 - 2 = y - 1 \end{aligned}$$

due to $c_1 + c_2 \geqslant 2 + c_2 > c_2$, and

$$\begin{aligned} r_2(\mathcal{A}, c_2 + 1) &= r_2(\mathbb{N}_0 \setminus \{c_1, c_2, c_3\}, c_2 + 1) \\ &= r_2(\mathbb{N}_0, c_2 + 1) - 3 \\ &= \lfloor (2y + 1)/2 \rfloor + 1 - 3 = y - 2 \end{aligned}$$

due to $c_2 + c_3 > c_1 + c_3 > c_1 + c_2 \geqslant 2 + c_2 > c_2 + 1$.

Case 2: $c_1 = 0$.

In this case, when $m > 0$ denotes the minimum of $\mathcal{A}$, we can write

$$\begin{aligned} r_2(\mathcal{A}, 2m + n) &= r_2(\mathcal{A} \cap \{m + 0, m + 1, \ldots, m + n\}, 2m + n) \\ &= r_2((\mathcal{A} - m) \cap \{0, 1, \ldots, n\}, n) \\ &= r_2(\mathcal{A} - m, n) \end{aligned}$$

for all $n \geqslant 0$. Here, for the set $\mathcal{A} - m = \{a - m : a \in \mathcal{A}\}$ (in place of $\mathcal{A}$), we have already shown in the first case that one can find some n such that

$$r_2(\mathcal{A} - m, n) > r_2(\mathcal{A} - m, n + 1)\,.$$

By the just found link, this in turn also leads to

$$r_2(\mathcal{A}, 2m + n) > r_2(\mathcal{A}, 2m + n + 1)\,,$$

and so we have found a decrease in any case, completing our proof. □

Appendix: Algorithms and Diagrams

In this appendix, we first present all algorithms written in PYTHON, which we used for several computations throughout this work. At the end we also provide some diagrams illustrating our proof of **Theorem 4.5**.

Algorithm 1: Computing the discrepancy $\Delta(\mathcal{A})$ in the case $\mathcal{A} = \mathcal{R}(q_1 \dots q_r) \subset \mathbb{Z}/(q_1 \dots q_r)\mathbb{Z} = G$ for distinct primes $q_1, \dots, q_r$ with respect to the sequence of shifts $s_t = t$ $(t \in \mathbb{N})$.

```
import math

""" Delta(q)
" input:
"   q is an array (of length r),
"     whose entries represent distinct primes q_1 , ... , q_r.
" output:
"   Delta(q) returns the discrepancy
"   of the set of all reduced residue classes modulo the product (m) of
"   primes in q with respect to the sequence 1 , 2 , 3 , ... of shifts.
"""

def Delta(q):
  r = len(q);
  m = 1;
  for i in range(0, r):
    m = m * q[i];
  # build the array R_set of length m such that
  # R_set[u] = 1 if u is relatively prime to m, and
  # R_set[u] = 0 otherwise:
  R_set = [Null] * m;
  # set all values in R_set to 1:
  for u in range(0, m):
    R_set[u] = 1;
  for i in range(0, r):
    # reset the value of R_set[u] to 0, if u is divisble by q[i]:
    for k in range(0, m // q[i]):
      R_set[k * q[i]] = 0;
  # initialize the array c_set of length m, where c_set[u] counts
  # how many times u has been covered by a translate so far:
  c_set = [0] * m;
  c_min = 0; # minimum value in c_set
  c_max = 0; # maximum value in c_set
  delta = c_max - c_min;
```

```
  # loop over all shifts s:
  for s in range(1, m + 1):
    # update the values in c_set
    # after adding the next translate of r_set:
    for u in range(0, m):
      c_set[u] = c_set[u] + R_set[(u - s) % m];
    # search for new minimum and maximum value in c_set
    # (note that c_min grows by at most one each time):
    c_min = c_min + 1;
    for u in range(0, m):
      if c_set[u] > c_max:
        c_max = c_set[u];
      if c_set[u] < c_min:
        c_min = c_set[u];
    # update the value of delta:
    if c_max - c_min > delta:
      delta = c_max - c_min;
  return delta;
```

Algorithm 2: A collection of methods to check which arithmetic progressions $(t \cdot \boldsymbol{d})_{t \in \mathbb{N}}$ with common difference $\boldsymbol{d} \in \mathcal{R}(q_1) \times \ldots \times \mathcal{R}(q_r)$ are good for simple boxes $\mathcal{B}_{q_1,\ldots,q_r}(b_1, \ldots, b_r)$ (as mentioned in section 2.3). One may also remove the "`#`"-symbols around both "`print`"-commands, to obtain more information while the corresponding methods are running.

```
import math

""" B_set(q, b)
" input:
"   q is an array (of length r),
"     whose entries represent q_1 , ... , q_r;
"   b is an array (of length r),
"     whose entries represent b_1 , ... , b_r;
" output:
"   B_set(q, b) returns an array B (of length m = q_1 * ... * q_r)
"   such that
"     B[n] = 1,
"       if n + q_i Z is among 1 + q_i Z , ... , b_i + q_i Z
"       for each i from {1 , ... , r};
"     B[n] = 0,
"       otherwise;
"""
```

```
def B_set(q, b):
  r = len(q);
  m = 1;
  for i in range(0, r):
    m = m * q[i];
  B = [1] * m;
  for i in range(0, r):
    for k in range(0, m // q[i]):
      for n in range(b[i], q[i]):
        B[n + k * q[i]] = 0;
  return B;

""" R_set(q)
" input:
"   q is an array (of length r)
"     whose entries represent q_1 , ... , q_r;
" output:
"   R_set(q) returns an array given by B_set(q, b),
"   where b is an array (of length r),
"     whose entries represent q_1 - 1 , ... , q_r - 1;
"""

def R_set(q):
  r = len(q);
  b = [];
  for i in range(0, r):
    b.append(q[i] - 1);
  return B_set(q, b);

""" is_good_AP(B, d)
" input:
"   B is an array (of length m),
"     which represents a subset A of residue classes modulo m,
"     where
"       B[u] = 1, if u + m Z is a member of A,
"     and
"       B[u] = 0, otherwise;
"   d is an integer,
"     which represents the arithmetic progression 1 d , 2 d , 3 d , ...;
" output:
"   is_good_AP(B, d) returns
"   True,
"     if 1 d , 2 d , 3 d , ... is good for the set A (represented by B);
"   False,
"     otherwise;
"""
```

```
def is_good_AP(B, d):
  m = len(B);
  a = 0; # number of elements in A
  for u in range(0, m):
    a = a + B[u];
  # initialize the array c_set of length m, where c_set[u] counts
  # how many times u has been covered by a translate of A so far:
  c_set = [0] * m;
  is_good = True;
  count = 0; # number of elements which have been covered so far
  t = 1;
  while is_good and count < m and t <= m:
    # reset local_count to 0, which counts
    # how many not yet covered elements are covered this time:
    local_count = 0;
    # loop over all elements u:
    for u in range(0, m):
      # check if u is covered at time t:
      if B[(u - t * d) % m] > 0:
        c_set[u] = c_set[u] + 1;
        # check if u is covered for the first time:
        if c_set[u] - 1 == 0:
          local_count = local_count + 1;
    # check if d is good at this time:
    if local_count * m < (m - count) * a or a == 0:
      is_good = False;
#   print(
#     str(t) + " : " +
#     str(local_count) + " / " + str(m - count) + " = " +
#     str(local_count / (m - count))
#   );
    count = count + local_count;
    t = t + 1;
  return is_good;

""" all_good_APs(q, b)
" input:
"   q is an array (of length r),
"     whose entries represent p_1 , ... , p_r.
"   b is an array (of length r),
"     whose entries represent b_1 , ... , b_r.
" output:
"   all_good_APs(q, b) returns an array,
"   which contains every good arithmetic progression
"   (represented by its common difference d)
"   for the simple box defined by the input;
"""
```

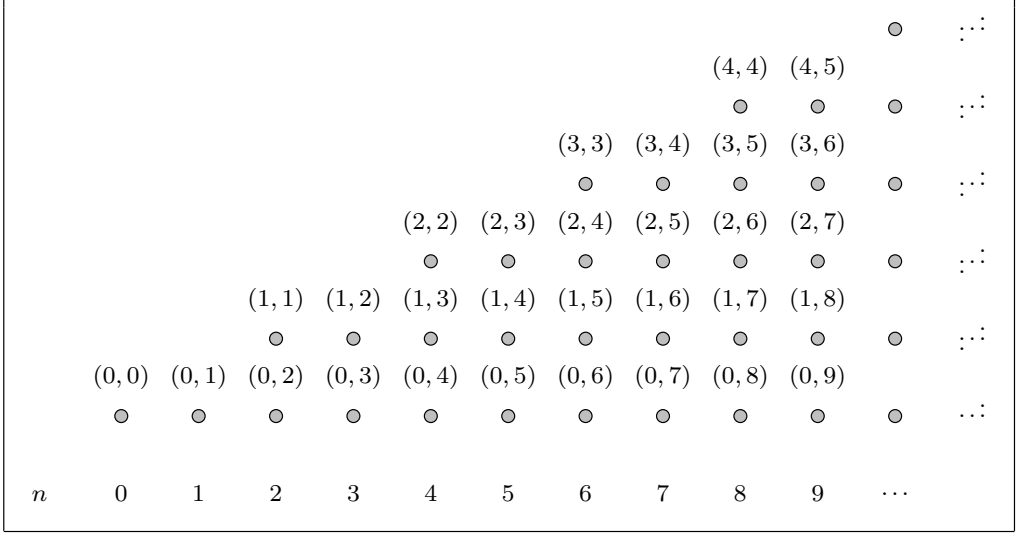
```
def all_good_APs(q, b):
  r = len(q);
  B = B_set(q, b);
  m = len(B);
  good_APs = [];
  # loop over all possible common differences d:
  for d in range(0, m):
    # check if d is good for the simple box defined by the input:
    if is_good_AP(B, d):
      D = [];
      for i in range(0, r):
        D.append(d % q[i]);
      good_APs.append(D);
  return good_APs;

""" check_simple_boxes_for_good_APs(q)
" input:
"   q is an array (of length r),
"     whose entries represent q_1 , ... , q_r;
" output:
"   check_simple_boxes_for_good_APs(q) returns an array,
"   which contains all simple boxes inside (Z / q_1 Z) x ... x (Z / q_r Z),
"   for which there does not exist a good arithmetic progression of shifts;
"""

def check_simple_boxes_for_good_APs(q):
  r = len(q);
  m = 1;
  for i in range(0, r):
    m = m * q[i];
  poor_simple_boxes = [];
  # loop over all possible simple boxes in (Z / q_1 Z) x ... x (Z / q_r Z):
  for u in range(0, m):
    b = [];
    for i in range(0, r):
      if u % q[i] != 0: # check if the simple box is empty
        b.append(u % q[i]);
    if len(b) == r:
      # check if there exist good arithmetic progressions:
      good_APs = all_good_APs(q, b);
      if len(good_APs) == 0:
        poor_simple_boxes.append(b);
#     else:
#       print(
#         str(b) + " : " + str(good_APs) + "\n\r"
#       );
  return poor_simple_boxes;
```

```
def main():
  check_simple_boxes_for_good_APs([2, 3, 5]);
  # returns [];
  check_simple_boxes_for_good_APs([3, 5, 7]);
  # returns [[2, 4, 2]];
  is_good_AP(R_set([2, 3, 5, 7, 11]), 1);
  # returns True;
  is_good_AP(R_set([2, 3, 5, 7, 11, 13]), 1);
  # returns True;
  is_good_AP(R_set([2, 3, 5, 7, 11, 13, 17]), 1);
  # returns True;
  is_good_AP(R_set([2, 3, 5, 7, 11, 13, 17, 19]), 1);
  # returns True;
```

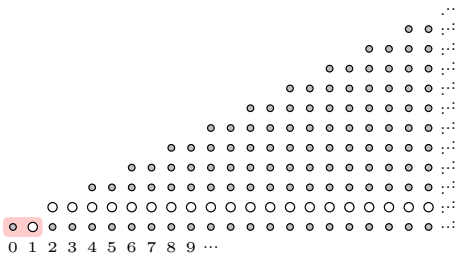
Finally, with respect to chapter 4, we like to mention that illustrating the pairs (a_1, a_2) from $\mathbb{N}_0 \times \mathbb{N}_0$ as points $(a_1 + a_2, a_1)$ in the plane, such that the corresponding points of all pairs with the same sum $a_1 + a_2 = n$ are lying on one vertical line, has been helpful in finding our proofs. Here, we are providing some diagrams for **Theorem 4.5**, where for an integer $c \in \mathbb{N}_0 \setminus \mathcal{A}$, we then remove all points (c, x) and (x, c) with $x \in \mathbb{N}_0$ lying on two certain lines.

Diagrams.

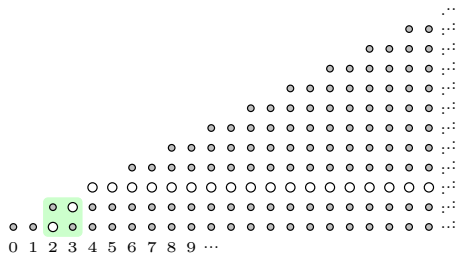
$\mathcal{A} = \mathbb{N}_0$:



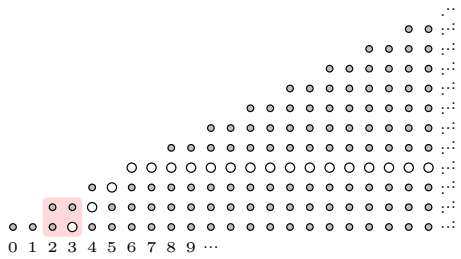
$\mathcal{A} = \mathbb{N}_0 \setminus \{c_1 = 1\}$:



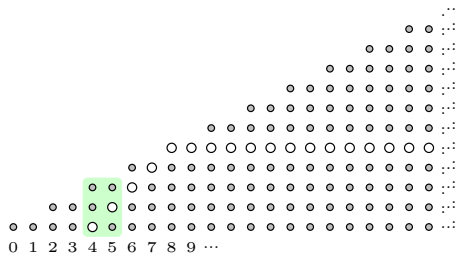
$\mathcal{A} = \mathbb{N}_0 \setminus \{c_1 = 2\}$:



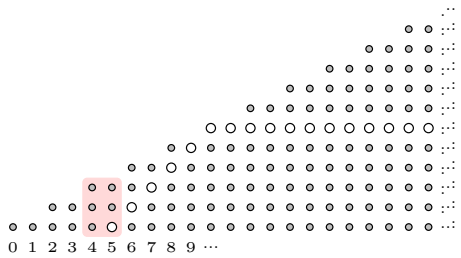
$\mathcal{A} = \mathbb{N}_0 \setminus \{c_1 = 3\}$:



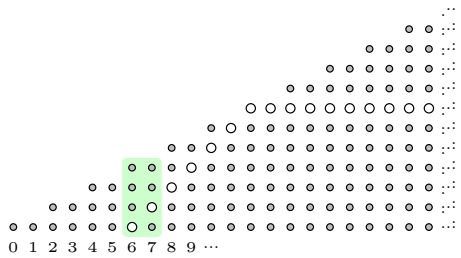
$\mathcal{A} = \mathbb{N}_0 \setminus \{c_1 = 4\}$:



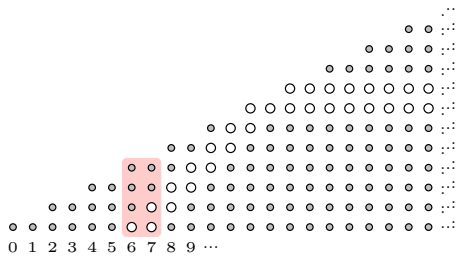
$\mathcal{A} = \mathbb{N}_0 \setminus \{c_1 = 5\}$:



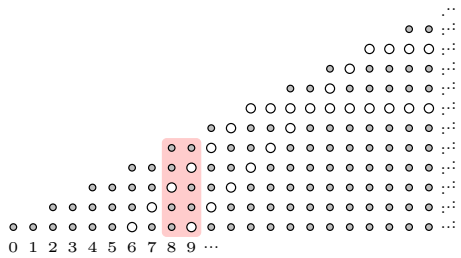
$\mathcal{A} = \mathbb{N}_0 \setminus \{c_1 = 6\}$:



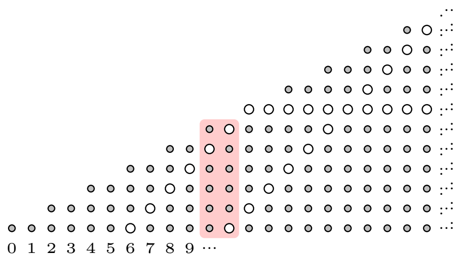
$\mathcal{A} = \mathbb{N}_0 \setminus \{c_1 = 6, c_2 = 7\}$:



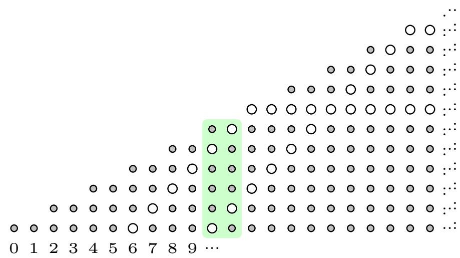
$\mathcal{A} = \mathbb{N}_0 \setminus \{c_1 = 6, c_2 = 9\}$:



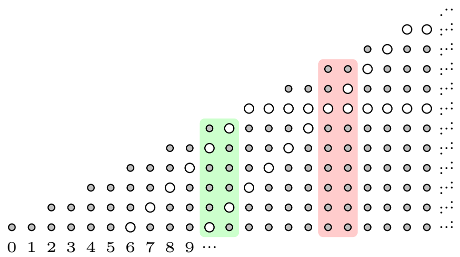
$\mathcal{A} = \mathbb{N}_0 \setminus \{c_1 = 6, c_2 = 11\}$:



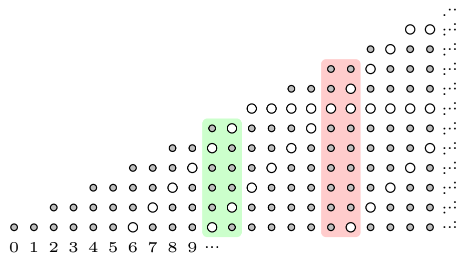
$\mathcal{A} = \mathbb{N}_0 \setminus \{c_1 = 6, c_2 = 10\}$:



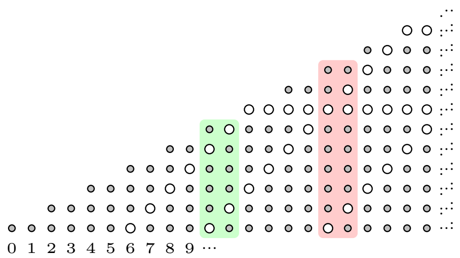
$\mathcal{A} = \mathbb{N}_0 \setminus \{c_1 = 6, c_2 = 10\}$:



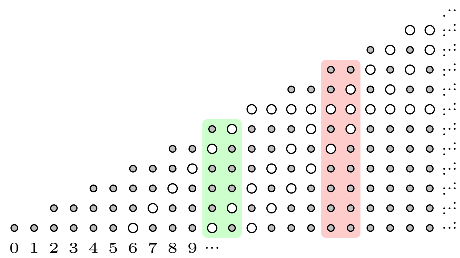
$\mathcal{A} = \mathbb{N}_0 \setminus \{c_1 = 6, c_2 = 10, c_3 = 17\}$:



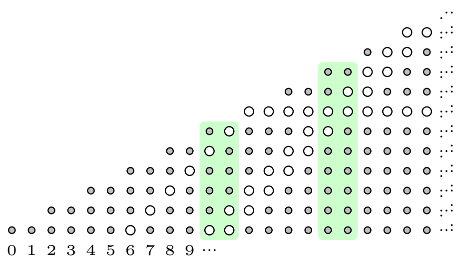
$\mathcal{A} = \mathbb{N}_0 \setminus \{c_1 = 6, c_2 = 10, c_3 = 16\}$:



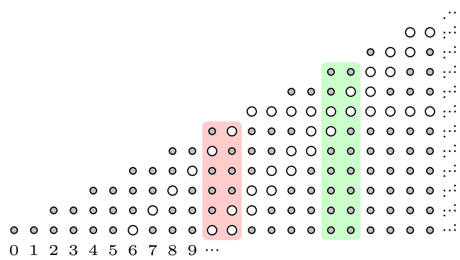
$\mathcal{A} = \mathbb{N}_0 \setminus \{c_1 = 6, c_2 = 10, c_3 = 12\}$:



$\mathcal{A} = \mathbb{N}_0 \setminus \{c_1 = 6, c_2 = 10, c_3 = 11\}$:



$\mathcal{A} = \mathbb{N}_0 \setminus \{c_1 = 6, c_2 = 10, c_3 = 11\}$:



Bibliography

[1] R. Balasubramanian:
A note on a result of Erdős, Sárközy and Sós.
Acta Arith. **49** (1987), 45 – 53.

[2] P. Borwein, S. Choi, and F. Chu:
An old conjecture of Erdős-Turán on additive bases.
Math. Comp. **75** (2006), no. 253, 475 – 484.

[3] T.-H. Chang:
Über aufeinanderfolgende Zahlen, von denen jede mindestens einer von n linearen Kongruenzen genügt, deren Moduln die ersten n Primzahlen sind.
Schr. Math. Semin. u. Inst. Angew. Math. Univ. Berlin **4** (1938), 35 – 55.

[4] Y.-G. Chen and C.-H. Lei:
Arithmetic progressions in the least positive reduced residue systems.
J. Number Theory **190** (2018), 303 – 310.

[5] Y.-G. Chen, A. Sárközy, V. T. Sós, and M. Tang:
On the monotonicity properties of additive representation functions.
Bull. Austral. Math. Soc. **72** (2005), no. 1, 129 – 138.

[6] Y.-G. Chen and M. Tang:
On the monotonicity properties of additive representation functions, II.
Discrete Math. **309** (2009), 1368 – 1373.

[7] P. Erdős:
On the difference of consecutive primes.
Quart. Journ. of Math. **6** (1935), 124 – 128.

[8] P. Erdős, P. Turán:
On a problem of Sidon in additive number theory, and on some related problems.
J. London Math. Soc. **16** (1941), 212 – 215.

[9] P. Erdős:
On the integers relatively prime to n and on a number-theoretic function considered by Jacobsthal. Math. Scand. **10** (1962), 163 – 170.

[10] P. Erdős, A. Sárközy, and V. T. Sós:
Problems and results on additive properties of general sequences, IV.
Lecture Notes in Math. **1122**, Springer (1986), 85 – 104.

[11] K. Ford, B. Green, S. Konyagin, and T. Tao:
Large gaps between consecutive prime numbers.
Ann. of Math. (2) **183** (2016), no. 3, 935 – 974.

[12] R. K. Guy:
Unsolved problems in number theory. (3rd edition)
Problem Books in Mathematics, Springer (2004).

[13] T. R. Hagedorn:
Computation of Jacobsthal's function $h(n)$ for $n < 50$.
Math. Comp. **78** (2009), no. 266, 1073 – 1087.

[14] L. Hajdu and N. Saradha:
Disproof of a conjecture of Jacobsthal.
Math. Comp. **81** (2012), no. 280, 2461 – 2471.

[15] H. Iwaniec:
On the error term in the linear sieve.
Acta Arith. **19** (1971), 1 – 30.

[16] E. Jacobsthal:
Über Sequenzen ganzer Zahlen, von denen keine zu n teilerfremd ist, I-III.
Norske Vid. Selsk. Forhdl. **33** (1960), 117 – 124, 125 – 131, 132 – 139.

[17] H.-J. Kanold:
Über Primzahlen in arithmetischen Folgen, II.
Math. Ann. **157** (1965), 358 – 362.

[18] H.-J. Kanold:
Über eine zahlentheoretische Funktion von Jacobsthal.
Math. Ann. **170** (1967), 314 – 326.

[19] F. Lemmermeyer:
Reciprocity laws: From Euler to Eisenstein.
Springer Monographs in Mathematics, Springer (2000).

[20] H. Maier, C. Pomerance:
Unusually large gaps between consecutive primes.
Trans. Amer. Math. Soc. **322** (1990), no. 1, 201 – 237.

[21] J. Maynard:
Small gaps between primes.
Ann. of Math. (2) **181** (2015), no. 1, 383 – 413.

[22] J. Maynard:
Large gaps between primes.
Ann. of Math. (2) **183** (2016), no. 3, 915 – 933.

[23] H. L. Montgomery:
Ten lectures on the interface between analytic number theory and harmonic analysis. CBMS Regional Conference Series in Mathematics 84, AMS (1994).

[24] D. H. J. Polymath:
Variants of the Selberg sieve, and bounded intervals containing many primes.
Res. Math. Sci. **1** (2014), Art. 12, 83pp.

[25] J. Pintz:
Very large gaps between consecutive primes.
J. Number Theory **63** (1997), no. 2, 286 – 301.

[26] P. Pongsriiam:
Longest arithmetic progressions in reduced residue systems.
J. Number Theory **183** (2018), 309 – 325.

[27] R. A. Rankin:
The difference between consecutive prime numbers.
J. London Math. Soc. **11** (1938), no. 4, 242 – 245.

[28] R. A. Rankin:
The difference between consecutive prime numbers, V.
Proc. Edinburgh Math. Soc. (2) **13** (1962/63), 331 – 332.

[29] A. Sárközy:
Unsolved problems in number theory.
Period. Math. Hungar. **42** (2001), 17 – 35.

[30] A. Schönhage:
Eine Bemerkung zur Konstruktion großer Primzahllücken.
Arch. Math. (Basel) **14** (1963), 29 – 30.

[31] H. Stevens:
On Jacobsthal's $g(n)$-function.
Math. Ann. **226** (1977), no. 1, 95 – 97.

[32] P. Stumpf:
A short note on reduced residues.
Integers **17** (2017), no. A4, 4 pp.

[33] P. Stumpf:
On the monotonicity of additive representation functions.
Integers **20** (2020), no. A104, 7 pp.

[34] R. C. Vaughan:
On the order of magnitude of Jacobsthal's function.
Proc. Edinburgh Math. Soc. (2) **20** (1976/77), no. 4, 329 – 331.

[35] Y. Zhang:
Bounded gaps between primes.
Ann. of Math. (2) **179** (2014), no. 3, 1121 – 1174.