DISCREPANCY IN MODULAR ARITHMETIC PROGRESSIONS

JACOB FOX, MAX WENQIANG XU, AND YUNKUN ZHOU

Abstract. Celebrated theorems of Roth and of Matoušek and Spencer together show that the discrepancy of arithmetic progressions in the first n positive integers is $\Theta(n^{1/4})$. We study the analogous problem in the $\mathbb{Z}_n$ setting. We asymptotically determine the logarithm of the discrepancy of arithmetic progressions in $\mathbb{Z}_n$ for all positive integer n. We further determine up to a constant factor the discrepancy of arithmetic progressions in $\mathbb{Z}_n$ for many n. For example, if $n = p^k$ is a prime power, then the discrepancy of arithmetic progressions in $\mathbb{Z}_n$ is $\Theta(n^{1/3+r_k/(6k)})$, where $r_k \in \{0, 1, 2\}$ is the remainder when k is divided by 3. This solves a problem of Hebbinghaus and Srivastav.

1. Introduction

Given a finite set Ω, a (two-)coloring of Ω is a map $\chi : \Omega \to \{1, -1\}$, and a partial coloring is a map $\chi : \Omega \to \{-1, 0, 1\}$. For $A \subseteq \Omega$, let $\chi(A) = \sum_{x\in A} \chi(x)$. For a family $\mathcal{A}$ of subsets of Ω, the discrepancy of $\mathcal{A}$ is defined to be

$$\operatorname{disc}(\mathcal{A}) := \min_{\chi} \max_{A\in\mathcal{A}} |\chi(A)|,$$

where the minimum is over all colorings of Ω. The discrepancy measures the guaranteed irregularity of colorings with respect to a set system. Discrepancy theory is a rich area of study, see the books [1,3,4,9].

In particular, the study of discrepancy of arithmetic progressions has a long history, including notable results of Weyl from 1916 [13] and Roth from 1964 [11]. Let $[n] := \{1, 2, 3, \dots, n\}$ and $\mathcal{A}$ be the set of arithmetic progressions in $[n]$. Using Fourier analysis, Roth [11] proved that there is an absolute constant $c > 0$ such that

$$\operatorname{disc}(\mathcal{A}) \geq cn^{\frac{1}{4}}.$$

The exponent 1/4 was unexpected, as random colorings suggest that the best exponent might be 1/2. Later, improving on a result of Montgomery and Sárközy (see Problem 10 in [5]), Beck [2] proved that Roth's lower bound is sharp up to a polylogarithmic factor. It was a big challenge to remove the polylogarithmic factor and show that Roth's bound is sharp up to a constant factor, and it was finally done by Matoušek and Spencer [10] via entropy and partial coloring methods.

The modular variant is also a very natural problem to study. For a positive integer n, an arithmetic progression in $\mathbb{Z}_n$ is a set of the form $\{a + kd : 0 \leq k < l\}$ for any $a, d \in \mathbb{Z}_n$ and $l \geq 0$. To avoid repeated elements in the set, we may assume that $l \leq \frac{n}{\gcd(n,d)}$. Let $\mathcal{A}_n$ be the set of all arithmetic progressions in $\mathbb{Z}_n$. The quantity we are interested in is

$$\operatorname{disc}(\mathcal{A}_n) := \min_{\chi:\mathbb{Z}_n\to\{1,-1\}} \max_{A\in\mathcal{A}_n} |\chi(A)|.$$

Fox is supported by a Packard Fellowship and by NSF award DMS-1855635.
Xu is supported by the Cuthbert C. Hurd Graduate Fellowship in the Mathematical Sciences, Stanford.
Zhou is supported by NSF GRFP Grant DGE-1656518.

In the case where $n = p$ is a prime, the following lower and upper bounds are proved by Hebbinghaus and Srivastav [7] and Alon and Spencer (Theorem 13.1.1 in [1]) respectively. There exist positive constants c_1, c_2 such that

$$c_1\sqrt{p} \le \operatorname{disc}(\mathcal{A}_p) \le c_2\sqrt{p\log p}.$$

Hebbinghaus and Srivastav [7] wrote that it seemed to be a difficult open problem to close the $O(\sqrt{\log p})$ multiplicative gap between the upper and lower bounds. As part of our results, we remove the $\sqrt{\log p}$ factor in the upper bound and resolve the problem of determining $\operatorname{disc}(\mathcal{A}_p)$ up to a constant factor.

The problem for general $\mathbb{Z}_n$ is more challenging and interesting. Note that any arithmetic progression in $[n]$ is also an arithmetic progression in $\mathbb{Z}_n$, so Roth's lower bound from the integer case also applies. As the number of sets in $\mathcal{A}_n$ is polynomial in n, considering a random coloring gives the following upper bound (see Theorem 13.1.1 in [1]). So there are $c_1, c_2 > 0$ such that

$$c_1 n^{\frac{1}{4}} \le \operatorname{disc}(\mathcal{A}_n) \le c_2 n^{\frac{1}{2}} (\log n)^{\frac{1}{2}}.$$

Our main theorem asymptotically determines the logarithm of $\operatorname{disc}(\mathcal{A}_n)$. It shows that $\operatorname{disc}(\mathcal{A}_n)$ depends heavily on the arithmetic structure of n, and neither of the above bounds are sharp.

Let $\omega(n)$ be the number of distinct prime factors of n and $d(n)$ be the number of divisors of n.

Theorem 1.1. *There exists an absolute constant $c > 0$ such that for any positive integer n,*

$$\frac{1}{8\sqrt{d(n)}} \cdot \min_{r|n}\left(\frac{n}{r} + \sqrt{r}\right) \le \operatorname{disc}(\mathcal{A}_n) \le \min_{r|n}\left(\frac{n}{r} + c\sqrt{r}\cdot 2^{\omega(r)}\right).$$

Note that we have $2^{\omega(r)} \le 2^{\omega(n)} \le d(n) = n^{o(1)}$ (see [6]). This implies that

$$\operatorname{disc}(\mathcal{A}_n) = n^{\frac{1}{3}+x+o(1)},$$

where $x \ge 0$ is the largest real number such that there is no factor of n in the range $(n^{\frac{2}{3}-x}, n^{\frac{2}{3}+2x})$. Thus, our results determine the correct exponent of n for $\operatorname{disc}(\mathcal{A}_n)$ up to $o(1)$.

Notice that when n has a bounded number of factors, Theorem 1.1 determines $\operatorname{disc}(\mathcal{A}_n)$ up to a constant factor. In particular, when n is prime, we have $\operatorname{disc}(\mathcal{A}_n) = \Theta(n^{1/2})$, and this solves the problem of Hebbinghaus and Srivastav [7] discussed earlier.

We actually prove slightly stronger bounds, but we choose the formulation in Theorem 1.1 for simplicity. These stronger bounds give the following sharp bound for $\operatorname{disc}(\mathcal{A}_n)$ when n is a prime power.

Theorem 1.2. *If $n = p^k$ for prime p and positive integer k, then*

$$\operatorname{disc}(\mathcal{A}_n) = \Theta\left(p^{\frac{k-\lfloor k/3\rfloor}{2}}\right) = \Theta\left(n^{\frac{1}{3}+\frac{r_k}{6k}}\right),$$

where $r_k \in \{0,1,2\}$ is the remainder when k is divided by 3.

Remark 1.3. It is also natural to study the discrepancy problem in the case where the coloring function χ is allowed to take any value in the unit circle in the complex plane $\{z \in \mathbb{C} : |z| = 1\}$. For example, this choice of coloring functions is studied in Tao's [12] remarkable solution to the Erdős discrepancy problem. By comparing the definitions of the coloring functions, we know that the discrepancy under the more general choice of χ is at most as large as the discrepancy under the choice $\chi : \mathbb{Z}_n \to \{1, -1\}$. We remark that our proof is robust enough to give the same lower bound on discrepancy when χ is under the above choice. See Remark 4.8 for details on how to extend the proof of the lower bound to the more general setting.

Notations. Throughout the paper, all logarithms are base e unless otherwise specified.

We use symbols c, c_0, c_1, c_2, etc. to denote absolute constants. To avoid using too many symbols in different parts of the paper, we reuse these symbols to denote different constants. We make no attempt to optimize constant factors in our results.

We treat elements in $\mathbb{Z}_n$ as if they are in $\mathbb{Z}$ in the following ways. For an element $r \in \mathbb{Z}_n$ and integers $a, b \in \mathbb{Z}$, we say $a \le r \le b$ if there exists an element $r' \in \mathbb{Z}$ such that $a \le r' \le b$ and $r' \equiv r \pmod{n}$. The notation is similar if either $\le$ is replaced with $<$. We typically use it when $0 \le a \le b < n$, so this notation should not cause any confusion. For any $a \in \mathbb{Z}_n$, we may also define $\gcd(a, n) = \gcd(a', n)$ for any $a' \in \mathbb{Z}$ with $a' \equiv a \pmod{n}$. For two nonnegative integers a and b, we write $a|b$ if a divides b. For any factor r of n and $a \in \mathbb{Z}_n$, we say that $r|a$ if $r|\gcd(a, n)$.

Organization. In Section 2, we derive our first upper bound on $\operatorname{disc}(\mathcal{A}_n)$ (see Corollary 2.3). The upper bounds in Theorems 1.1 and 1.2 are proved in Section 3 (see Theorem 3.1). In Section 4, we prove the lower bounds in Theorem 1.1 (Corollary 4.9) and Theorem 1.2 (Corollary 4.10). We end with some concluding remarks and open problems in Section 5.

2. The First Step towards the Upper Bounds

We use the following version of a lemma of Matoušek and Spencer [10] to show there is a partial coloring that colors a constant fraction of the elements of a set system with low discrepancy. The proof of this lemma uses the entropy method.

Lemma 2.1 (Section 4.6 in [9])**.** *Let (V, C) be a set system on n elements, and let a number $\Delta_S \ge 2\sqrt{|S|}$ be given for each set $S \in C$. If*

$$\sum_{S \in C : S \neq \emptyset} \exp\left(-\frac{\Delta_S^2}{4|S|}\right) \le \frac{n}{50}, \tag{2.1}$$

then there is a partial coloring χ that assigns ± 1 to at least $n/10$ variables (and 0 to the rest) satisfying $|\chi(S)| \le \Delta_S$ for each $S \in C$.

The following lemma shows that there is a partial coloring of a constant fraction of any subset X of $\mathbb{Z}_n$ such that modular arithmetic progressions have low discrepancy. The proof utilizes the previous lemma applied to a special family of intersections of X with modular arithmetic progressions. Each set in this special family has size a power of 2. We show that any set which is an intersection of X with a modular arithmetic progression can be written as the union of two sets, and each of them is a set difference of two sets that each has a canonical decomposition into sets of different sizes from this special family. We obtain the lemma by putting these together and using the triangle inequality.

Lemma 2.2. *Let $X \subseteq \mathbb{Z}_n$ be a set of size $m > 0$. There exists a partial coloring $\chi : X \to \{-1, 0, 1\}$ that assigns ± 1 to at least $m/10$ elements in X such that*

$$\max_{A \in \mathcal{A}_n} |\chi(A \cap X)| \le 200 m^{\frac{1}{2}} \left(\log \frac{en}{m}\right)^{\frac{1}{2}}.$$

Proof. Let $\mathrm{AP}_n(a, d, i, j) := \{a + kd : i \le k \le j\}$ where $a, d \in \mathbb{Z}_n$ and $i, j \in \mathbb{Z}$. By definition,

$$\mathcal{A}_n = \left\{ \mathrm{AP}_n(a, d, 0, l-1) : a, d \in \mathbb{Z}_n, 0 \le l \le \frac{n}{\gcd(n, d)} \right\}.$$

Consider the following decomposition of sets in $\mathcal{A}_n$. Let

$$C_1 = \left\{ \mathrm{AP}_n(a,d,i,j) : 1 \le d < n, 0 \le a < \gcd(n,d), 0 \le i \le j < \frac{n}{\gcd(n,d)} \right\}.$$

Now we show that any set $A \in \mathcal{A}_n$ can be written as the disjoint union of at most two sets in C_1. For any set $A = \mathrm{AP}_n(a,d,0,l-1)$ with $a,d \in \mathbb{Z}_n$ and $0 \le l \le \frac{n}{\gcd(n,d)}$, we may assume that $l > 0$, or otherwise it is an empty set. If $d = 0$, then the set is the singleton $\{a\}$, which is also $\mathrm{AP}_n(0,1,a,a) \in C_1$ by choosing i,j to be the integer representative of a in the range $[0,n)$. Now we may assume $1 \le d < n$. Note that $\{kd : 0 \le k < \frac{n}{\gcd(n,d)}\}$ splits $\mathbb{Z}_n$ into $\frac{n}{\gcd(n,d)}$ equal-sized intervals, so there is some $0 \le k < \frac{n}{\gcd(n,d)}$ such that $0 \le a - kd < \gcd(n,d)$. Define $a' = a - kd$, and we have

$$\mathrm{AP}_n(a,d,0,l-1) = \mathrm{AP}_n(a',d,k,k+l-1).$$

Moreover we have $k < \frac{n}{\gcd(n,d)}$ and $l - 1 < \frac{n}{\gcd(n,d)}$, so $0 \le k + l - 1 < 2\frac{n}{\gcd(n,d)}$. If $k + l - 1 < \frac{n}{\gcd(n,d)}$, then $\mathrm{AP}_n(a',d,k,k+l-1) \in C_1$. If $k + l - 1 \ge \frac{n}{\gcd(n,d)}$, then we may write

$$\mathrm{AP}_n(a',d,k,k+l-1) = \mathrm{AP}_n\left(a',d,k,\frac{n}{\gcd(n,d)} - 1\right) \cup \mathrm{AP}_n\left(a',d,0,k+l-1-\frac{n}{\gcd(n,d)}\right).$$

Hence we know that for any partial coloring $\chi : \mathbb{Z}_n \to \{-1,0,1\}$, we always have

$$\max_{A \in \mathcal{A}_n} |\chi(A \cap X)| \le 2 \max_{A \in C_1} |\chi(A \cap X)|. \tag{2.2}$$

Now we study the sets in $C_X := \{A \cap X : A \in C_1\}$. By definition we have

$$\max_{A \in C_1} |\chi(A \cap X)| = \max_{B \in C_X} |\chi(B)|. \tag{2.3}$$

For each $1 \le d < n$ and $0 \le a < \gcd(n,d)$, we define $A_{d,a} = \left\{ a + kd : 0 \le k < \frac{n}{\gcd(d,n)} \right\}$, and define $X_{d,a} = A_{d,a} \cap X$. Since each element x in $X_{d,a}$ is associated to an integer $0 \le k < \frac{n}{\gcd(d,n)}$ via the relation $x = a + kd$, we may order elements in $X_{d,a}$ in ascending order of k. We write $X_{d,a} = \left\{ x_{d,a}^{(1)}, \ldots, x_{d,a}^{(l_{d,a})} \right\}$, where $l_{d,a} = |X_{d,a}|$. For integers i and j, we define $X_{d,a}(i,j) = \left\{ x_{d,a}^{(t)} : i \le t \le j \right\}$.

For each $d \in \mathbb{Z}_n$, because each element of $\mathbb{Z}_n$ is in exactly one $A_{d,a}$ for $0 \le a < \gcd(d,n)$, we have

$$\sum_{a=0}^{\gcd(d,n)-1} l_{d,a} = \sum_{a=0}^{\gcd(d,n)-1} |X \cap A_{d,a}| = |X| = m. \tag{2.4}$$

For $A = \mathrm{AP}_n(a,d,i,j)$, if we take i' to be the smallest index such that $x_{d,a}^{(i')} = a + k_1 d$ with $k_1 \ge i$ (or $l_{d,a} + 1$ if no such index with $0 \le k_1 < \frac{n}{\gcd(d,n)}$ exists), and j' to be the largest index such that $x_{d,a}^{(j')} = a + k_2 d$ with $k_2 \le j$ (or 0 if no such index with $0 \le k_2 < \frac{n}{\gcd(d,n)}$ exists), then we have $A \cap X = X_{d,a}(i',j')$. Hence each nonempty set in C_X is of the form $X_{d,a}(i,j)$ with $1 \le i \le j \le l_{d,a}$. Therefore we may write

$$C_X = \{X_{d,a}(i,j) : 1 \le d < n, 0 \le a < \gcd(n,d), 1 \le i \le j \le l_{d,a}\} \cup \{\emptyset\}.$$

Now we further decompose sets in C_X into canonical sets. Formally,

$$C_2 := \left\{ X_{d,a}(1 + (t-1)2^i, t2^i) : 1 \le d < n, 0 \le a < \gcd(n,d), 0 \le i, 1 \le t \le \left\lfloor \frac{l_{d,a}}{2^i} \right\rfloor \right\}. \tag{2.5}$$

Notice that each set $S \in C_X$ can be written as $U \setminus V$ with $V \subseteq U$ where both U and V can be written as the disjoint union of sets in C_2 of different sizes. This is trivially true for the empty set. For $S = X_{d,a}(i,j)$, we may take $U = X_{d,a}(1,j)$ and $V = X_{d,a}(1,i-1)$. If we write j in binary form $2^{b_1} + 2^{b_2} + \cdots + 2^{b_s}$ for $b_1 > b_2 > \cdots > b_s$, then U is the disjoint union of sets of the form $X_{d,a}(1 + \sum_{k=1}^{t-1} 2^{b_k}, \sum_{k=1}^{t} 2^{b_k})$ for $t = 1, \ldots, s$. We can decompose V similarly.

Note that sets in C_2 are all of size 2^i for $2^i \le m$. If $\chi : X \to \{-1, 0, 1\}$ is such that for all $0 \le i \le \log_2 m$ we have $\chi(S) \le \Delta_i$ for any set $S \in C_2$ of size 2^i, then by using the decomposition property above we have

$$\max_{B \in C_X} |\chi(B)| \le 2 \sum_{0 \le i \le \log_2 m} \Delta_i. \tag{2.6}$$

For each i, we upper bound the number of sets in C_2 of size 2^i as following. For each $1 \le d < n$ and $0 \le a < \gcd(d,n)$, the number of choices of t in (2.5) is $\lfloor l_{d,a}/2^i \rfloor$. By (2.4) the number of such sets is at most

$$\sum_{d=1}^{n-1} \sum_{a=0}^{\gcd(d,n)-1} \left\lfloor \frac{l_{d,a}}{2^i} \right\rfloor \le \sum_{d=1}^{n-1} \sum_{a=0}^{\gcd(d,n)-1} \frac{l_{d,a}}{2^i} = \frac{(n-1)m}{2^i}. \tag{2.7}$$

Now we define $b(0) = 0$ and for $0 < s \le n$,

$$b(s) = 5\sqrt{s} \left(\log \frac{en}{s} \right)^{1/2}. \tag{2.8}$$

From the definition, we know that $b(s) \ge 2\sqrt{s}$ for all $s \in \mathbb{N}$. We want to show that there exists a partial coloring χ that colors at least $m/10$ elements in X, and for any $S \in C_2$,

$$|\chi(S)| \le b(|S|). \tag{2.9}$$

In order to apply Lemma 2.1 to X and $C = C_2$, it remains to check that

$$\sum_{S \in C_2} \exp\left(-\frac{b(|S|)^2}{4|S|} \right) \le m/50. \tag{2.10}$$

From the definition of $b(\cdot)$ in (2.8), we know that

$$\sum_{S \in C_2} \exp\left(-\frac{b(|S|)^2}{4|S|} \right) = \sum_{S \in C_2} e^{-\frac{25}{4}} \cdot \left(\frac{|S|}{n} \right)^{\frac{25}{4}} \le e^{-6} \cdot \sum_{S \in C_2} \left(\frac{|S|}{n} \right)^2. \tag{2.11}$$

Using the bound in (2.7), we have

$$\sum_{S \in C_2} \left(\frac{|S|}{n} \right)^2 \le \sum_{0 \le i \le \log_2 m} \frac{(n-1)m}{2^i} \left(\frac{2^i}{n} \right)^2 \le 2m.$$

Put this into (2.11). We get

$$\sum_{S \in C_2} \exp\left(-\frac{b(|S|)^2}{4|S|} \right) \le e^{-6} \cdot 2m \le m/50.$$

This shows that (2.10) holds. By Lemma 2.1, we conclude that there exists a partial coloring $\chi : X \to \{-1, 0, 1\}$ that assigns ± 1 to at least $m/10$ elements, and (2.9) holds for any $S \in C_2$. Thus in (2.6) we may take $\Delta_i = b(2^i)$ for $0 \le i \le \log_2 m$.

It remains to show that χ satisfies the desired property. By (2.2), (2.3), and (2.6),

$$\max_{A\in\mathcal{A}_n}|\chi(A\cap X)| \le 4\sum_{0\le i\le \log_2 m} b(2^i) = 20\sum_{i=0}^{\lfloor \log_2 m\rfloor} 2^{i/2}\left(\log\frac{en}{2^i}\right)^{\frac{1}{2}} \le 200\cdot\sqrt{m}\left(\log\frac{en}{m}\right)^{\frac{1}{2}}.$$

To obtain the last inequality, observe that the sum is roughly a geometric series with ratio $2^{1/2}$ (although there is an extra logarithmic factor that slightly complicates this) and can be bounded by a constant factor times the largest term. A careful analysis gives the claimed bound.

Hence the partial coloring χ satisfies the desired inequality. □

Corollary 2.3. *Let $X\subseteq\mathbb{Z}_n$ be a set of size $m>0$. There exists an absolute constant c such that there is a coloring $\chi: X\to\{-1,1\}$ satisfying*

$$\max_{A\in\mathcal{A}_n}|\chi(A\cap X)| \le cm^{\frac{1}{2}}\left(\log\frac{en}{m}\right)^{\frac{1}{2}}.$$

In particular, for $X=\mathbb{Z}_n$, we have

$$\operatorname{disc}(\mathcal{A}_n) = O(\sqrt{n}).$$

Proof. The main idea is to iteratively apply Lemma 2.2 to the set of uncolored elements of X until all elements of X are colored.

Start with $X_0=X$. For each $i\ge 0$, we apply Lemma 2.2 to X_i to get a partial coloring $\chi_i: X_i\to\{-1,0,1\}$, and we let $X_{i+1}=\chi_i^{-1}(0)\subseteq X_i$ to be the set of uncolored elements in i-th iteration. We continue this process until the k-th iteration where all elements are colored (i.e. $X_{k+1}=\emptyset$). Let χ be the final coloring given by $\chi(x_i)=\chi_i(x_i)$ if $x_i\in X_i\setminus X_{i+1}$ for $0\le i\le k$. We know that $|X_i|\le 0.9|X_{i-1}|$ for all $1\le i\le k$, so $|X_i|\le (0.9)^i|X_0| = (0.9)^i m$. Moreover, we know that for any $A\in\mathcal{A}_n$, noting that $x^{1/2}\cdot\left(\log\frac{en}{x}\right)^{\frac{1}{2}}$ is monotonically increasing for real number $x\in(0,n]$,

$$\begin{aligned}|\chi(A\cap X)| &= \left|\sum_{i=0}^{k}\chi_i(X_i\cap A)\right| \le \sum_{i=0}^{k}|\chi_i(X_i\cap A)| < \sum_{i=0}^{k}200\cdot|X_i|^{\frac{1}{2}}\left(\log\frac{n}{e|X_i|}\right)^{\frac{1}{2}}\\ &\le 200m^{\frac{1}{2}}\cdot\sum_{i=0}^{k}(0.9)^{\frac{i}{2}}\left(\log\frac{en}{(0.9)^i m}\right)^{\frac{1}{2}} < cm^{\frac{1}{2}}\left(\log\frac{en}{m}\right)^{\frac{1}{2}}\end{aligned}$$

for some appropriate choice of the absolute constant c. □

3. Upper Bounds

By Corollary 2.3, we have $\operatorname{disc}(\mathcal{A}_n)=O(\sqrt{n})$. In this section, we prove the following upper bound on the same quantity, which shows that the previous bound is not always tight, and that $\operatorname{disc}(\mathcal{A}_n)$ depends on the factorization of n. Recall that $\omega(r)$ denotes the number of distinct prime factors of r.

Theorem 3.1. *There exists an absolute constant $c>0$ such that for any positive integer n, we have*

$$\operatorname{disc}(\mathcal{A}_n) \le \min_{r|n}\left(\frac{n}{r}+c\sqrt{r}\cdot 2^{\omega(r)}\right).$$

The proof of Theorem 3.1 consists of two steps. The first key step is to establish an upper bound on $\operatorname{disc}(\mathcal{A}_n)$ using a coloring of $\mathbb{Z}_r$ where r divides n that simultaneously has low discrepancy with respect to two particular families of arithmetic progressions in $\mathbb{Z}_r$. This is achieved by Lemma 3.2. To accomplish this, we need to introduce a special type of arithmetic progression in $\mathbb{Z}_n$. Recall that $\mathcal{A}_n$

is the set of all arithmetic progressions in $\mathbb{Z}_n$. We define $\mathcal{A}_n^0$ to be the set of all congruence classes of $\mathbb{Z}_n$. Formally, for any $r, i \in \mathbb{Z}_n$, let

$$C(r,i) := \{x \in \mathbb{Z}_n : x \equiv i \pmod r\}$$

and

$$\mathcal{A}_n^0 := \{C(r,i) : r, i \in \mathbb{Z}_n\}.$$

In particular we know that $\mathcal{A}_n^0 \subseteq \mathcal{A}_n$. In Lemma 3.2 we obtain an upper bound on $\operatorname{disc}(\mathcal{A}_n)$ if there is an r that divides n and a coloring χ of $\mathbb{Z}_r$ that has low discrepancy over both $\mathcal{A}_r$ and $\mathcal{A}_r^0$.

The second step is to find a coloring of $\mathbb{Z}_r$ which has nearly optimal discrepancy over $\mathcal{A}_r$ and $\mathcal{A}_r^0$ simultaneously. Finally we will complete the proof by applying Lemma 3.2 with this coloring of $\mathbb{Z}_r$.

Lemma 3.2. *Let n be a positive integer and r be a positive factor of n. For any $\chi : \mathbb{Z}_r \to \{1,-1\}$,*

$$\operatorname{disc}(\mathcal{A}_n) \le \max_{A\in\mathcal{A}_r} |\chi(A)| + \frac{n}{r} \cdot \max_{A_0\in\mathcal{A}_r^0} |\chi(A_0)|.$$

Proof. Let $m = n/r$. For the subgroup $(m) \subseteq \mathbb{Z}_n$, we have a quotient map $\tau : \mathbb{Z}_n \to \mathbb{Z}_n/(m) = \mathbb{Z}_r$ given by $\tau(x) = \overline{x} = x + (m)$. Suppose we are given an arbitrary $\chi : \mathbb{Z}_r \to \{1,-1\}$. Now we define $\chi' = \chi \circ \tau : \mathbb{Z}_n \to \{1,-1\}$. It suffices to show

$$\max_{A'\in\mathcal{A}_n} |\chi'(A')| \le \max_{A\in\mathcal{A}_r} |\chi(A)| + m \cdot \max_{A_0\in\mathcal{A}_r^0} |\chi(A_0)|. \tag{3.1}$$

Let $A' = \{a + kd : 0 \le k < L\}$ for some $a, d \in \mathbb{Z}_n$ be an arithmetic progression in $\mathbb{Z}_n$ of length L. We may assume that $L \le n/\gcd(d,n)$ so that there is no repeated element in A'.

Let $L_0 = r/\gcd(r,\overline{d})$ where $\overline{d} = \tau(d)$. For any integer $t > 0$, we know that $\{\overline{a} + k\overline{d} : t \le k < t + L_0\}$ is a set of size L_0 in $\mathcal{A}_n^0$, as it covers each element in the congruence class exactly once. For any $0 \le l < L_0$, as the set $\{\overline{a} + k\overline{d} : t \le k < t + l\}$ has no repeated element, it is a set of size l in $\mathcal{A}_n$.

Now we may write $L = qL_0 + r$ for some integers q and $0 \le r < L_0$. We know that

$$q \le \frac{L}{L_0} \le \frac{n/\gcd(d,n)}{r/\gcd(r,\overline{d})} = m \cdot \frac{\gcd(r,d)}{\gcd(n,d)} \le m.$$

Applying the triangle inequality, we get

$$\begin{aligned}
|\chi'(A')| &= \left|\sum_{k=0}^{L-1} \chi'(a+kd)\right| = \left|\sum_{k=0}^{L-1} \chi(\overline{a}+k\overline{d})\right| = \left|\sum_{t=0}^{q-1}\sum_{k=tL_0}^{(t+1)L_0-1} \chi(\overline{a}+k\overline{d}) + \sum_{k=qL_0}^{qL_0+r-1} \chi(\overline{a}+k\overline{d})\right| \\
&\le \sum_{t=0}^{q-1}\left|\sum_{k=tL_0}^{(t+1)L_0-1} \chi(\overline{a}+k\overline{d})\right| + \left|\sum_{k=qL_0}^{qL_0+r-1} \chi(\overline{a}+k\overline{d})\right| \\
&\le q \cdot \max_{A_0\in\mathcal{A}_r^0} |\chi(A_0)| + \max_{A\in\mathcal{A}_r} |\chi(A)| \le m \cdot \max_{A_0\in\mathcal{A}_r^0} |\chi(A_0)| + \max_{A\in\mathcal{A}_r} |\chi(A)|.
\end{aligned}$$

Since the bound is uniform for all $A' \in \mathcal{A}_n$, we conclude that (3.1) holds. □

After the above deduction, the second step is to find a coloring $\chi : \mathbb{Z}_n \to \{1,-1\}$ that has nearly optimal discrepancy over $\mathcal{A}_n$ and $\mathcal{A}_n^0$ simultaneously. Formally we have the following statement.

Lemma 3.3. *There exists an absolute constant $c > 0$ such that the following holds. Suppose that n is a positive integer with k distinct prime factors. Then there exists $\chi : \mathbb{Z}_n \to \{1,-1\}$ such that*

$$\max_{A_0\in\mathcal{A}_n^0} |\chi(A_0)| \le 1 \quad \text{and} \quad \max_{A\in\mathcal{A}_n} |\chi(A)| \le c\sqrt{n} \cdot 2^k.$$

We can now deduce Theorem 3.1 from the above two steps.

Proof of Theorem 3.1 assuming Lemma 3.3. For any positive factor r of n, by Lemma 3.3, there is a coloring χ of $\mathbb{Z}_r$ such that

$$\max_{A_0\in\mathcal{A}_r^0}|\chi(A_0)|\le 1 \quad \text{and} \quad \max_{A\in\mathcal{A}_r}|\chi(A)|\le c\sqrt{r}\cdot 2^{\omega(r)},$$

where c is an absolute constant. Then applying Lemma 3.2, we conclude that

$$\operatorname{disc}(\mathcal{A}_n)\le \frac{n}{r}+c\sqrt{r}\cdot 2^{\omega(r)}.$$

As this holds for all positive factors r of n, the desired result follows. □

It remains to prove Lemma 3.3. We first present a proof of the case that n is a prime power. The proof of this case is simpler and illustrates the main ideas in the proof of Lemma 3.3.

Lemma 3.4. *There exists absolute constant $c>0$ such that the following holds. Let $n=p^\alpha$ for some prime p and positive integer α. Then there exists $\chi:\mathbb{Z}_n\to\{1,-1\}$ such that*

$$\max_{A_0\in\mathcal{A}_n^0}|\chi(A_0)|\le 1 \quad \text{and} \quad \max_{A\in\mathcal{A}_n}|\chi(A)|\le c\sqrt{n}.$$

To find a coloring with low discrepancy over $\mathcal{A}_n^0$, the main idea is to color simultaneously two disjoint subsets S_1 and S_2 of $\mathbb{Z}_n$ that are translations of each other, and we hope that $\chi(S_1\cap A_0)$ and $\chi(S_2\cap A_0)$ cancel out for many $A_0\in\mathcal{A}_n^0$. The $c\sqrt{n}$ upper bound on the discrepancy over $\mathcal{A}_n$ in Lemma 3.4 is achieved via Corollary 2.3. We first derive the following lemma that gives a desired coloring for a subset X of $\mathbb{Z}_n$, provided that X is an initial interval of some special length.

Lemma 3.5. *There exists absolute constant $c>0$ such that the following holds. Let $n=p^\alpha$ for some prime p and positive integer α. Suppose that $X=\{0,\dots,m-1\}\subseteq\mathbb{Z}_n$ for some $m\le n$ satisfies that $m=sp^\beta$ with s even and β being a nonnegative integer. Then there exists $\chi:X\to\{1,-1\}$ such that*

$$\max_{A\in\mathcal{A}_n}|\chi(A\cap X)|\le c\sqrt{m}\left(\log\frac{en}{m}\right)^{\frac12},$$

and for any $w\in\mathbb{Z}_n$ and $r=p^\gamma$ with $0\le\gamma\le\beta$,

$$\chi(C(r,w)\cap X)=0.$$

Proof. Let $S=\{0,\dots,m/2-1\}$. By Corollary 2.3, there is $\chi_0:X\to\{1,-1\}$ such that

$$|\chi_0(A\cap S)|\le c_0\sqrt{\frac{m}{2}}\left(\log\frac{2en}{m}\right)^{\frac12},$$

holds for any $A\in\mathcal{A}_n$, where c_0 is an absolute constant. We know that X is the disjoint union of S and $S+\frac{m}{2}$, i.e. each element $x\in X$ is of the form $x=s+v\frac{m}{2}$ for some $s\in S$ and $v\in\{0,1\}$. We define $\chi:X\to\{1,-1\}$ given by $\chi(s+v\frac{m}{2})=(-1)^v\cdot\chi_0(s)$ for any $s\in S$ and $v\in\{0,1\}$.
For any $A\in\mathcal{A}_n$, noting that $A-\frac{m}{2}$ is also an arithmetic progression,

$$\begin{aligned}|\chi(A\cap X)|&=|\chi(A\cap S)+\chi(A\cap(S+m/2))|=|\chi_0(A\cap S)+(-1)\cdot\chi_0((A-m/2)\cap S)|\\&\le|\chi_0(A\cap S)|+|\chi_0((A-m/2)\cap S)|\le 2\cdot c_0\sqrt{\frac{m}{2}}\left(\log\frac{2en}{m}\right)^{\frac12}\le c\sqrt{m}\left(\log\frac{en}{m}\right)^{\frac12},\end{aligned}$$

where c is an absolute constant. Next we verify that for any $r = p^\gamma$ with $\gamma \le \beta$ and any $w \in \mathbb{Z}_n$, $\chi(C(r,w) \cap X) = 0$. Note that $m/2$ is a multiple of r, so $C(r,w) - m/2 = C(r,w)$. Hence we have

$$\chi(C(r,w)\cap X) = \chi_0(C(r,w)\cap S)+(-1)\cdot\chi_0((C(r,w)-m/2)\cap S) = \chi_0(C(r,w)\cap S)-\chi_0(C(r,w)\cap S) = 0.$$

We have thus shown the existence of such a coloring χ with the desired properties. □

In the case $n = p^\alpha$, we partition $\mathbb{Z}_n$ into a few sets, each being an interval of $\mathbb{Z}_n$ of length an even number times a power of p as in Lemma 3.5.

Proof of Lemma 3.4. Note that for any $C(r,w) \in \mathcal{A}_n^0$, we have $C(r,w) = C(\gcd(r,n),w)$. Hence it suffices to check $|\chi(C(r,w))| \le 1$ where r divides $n = p^\alpha$, i.e., $r = p^\gamma$ for some nonnegative $\gamma \le \alpha$.

Let c_0 be the constant in Lemma 3.5.

If $p = 2$, we can take $m = n = 2 \cdot 2^{\alpha-1}$ in Lemma 3.5. Thus, there exists $\chi : \mathbb{Z}_n \to \{1,-1\}$ such that

$$\max_{A\in\mathcal{A}_n} |\chi(A)| \le c_0\sqrt{n},$$

and that for any $w \in \mathbb{Z}_n$ and any $r = 2^\gamma$ with $\gamma \le \alpha - 1$, $\chi(C(r,w)) = 0$. This means that, for any $r = 2^\gamma$, if $\gamma \le \alpha - 1$, then $\chi(C(r,w)) = 0$; if $\gamma = \alpha$, then $C(r,w)$ contains a single element w, so $|\chi(C(r,w))| = 1$ in this case. We conclude that

$$\max_{A_0\in\mathcal{A}_n^0} |\chi(A_0)| \le 1.$$

If $p > 2$ is an odd prime, then we partition $\mathbb{Z}_n$ into a few intervals: $X_0 = \{0\}, X_i = \{x : p^{i-1} \le x < p^i\}$ for $1 \le i \le \alpha$. Note that for each $i \ge 1$, X_i is an interval of length $(p-1)\cdot p^{i-1}$. We would like to apply Lemma 3.5 to each X_i for $i \ge 1$. It is applicable because the property is maintained by translation. Therefore for each $1 \le i \le \alpha$ there is a coloring $\chi_i : X_i \to \{1,-1\}$ such that

$$\max_{A\in\mathcal{A}_n} |\chi_i(A\cap X_i)| \le c_0\sqrt{(p-1)\cdot p^{i-1}}\left(1+\log\frac{p^\alpha}{(p-1)\cdot p^{i-1}}\right)^{\frac{1}{2}},$$

and for each $w \in \mathbb{Z}_n$ and $r = p^\gamma$ with $\gamma \le i-1$, we have $\chi_i(C(r,w)\cap X_i) = 0$.

For X_0 we may take any arbitrary $\chi_0 : X_0 \to \{1,-1\}$. Note that $X_0 = \{0\}$ contains only one element, so $|\chi_0(A\cap X_0)| \le 1$ for all $A \subseteq \mathbb{Z}_n$.

Since $X = \coprod_{i=0}^\alpha X_i$, we define $\chi : X \to \{1,-1\}$ such that $\chi(x_i) = \chi_i(x_i)$ for all $0 \le i \le \alpha$ and $x_i \in X_i$. Consequently, we know that for each $A \in \mathcal{A}_n$,

$$|\chi(A)| = \sum_{i=0}^{\alpha}|\chi_i(A\cap X_i)| \le 1+\sum_{i=1}^{\alpha} c_0\sqrt{(p-1)\cdot p^{i-1}}\left(1+\log\frac{p^\alpha}{(p-1)\cdot p^{i-1}}\right)^{\frac{1}{2}} \le c\sqrt{n}$$

for some appropriate constant c. Moreover, for each $C(r,w) \in \mathcal{A}_n^0$, we may assume that $r = p^\gamma$ for some $0 \le \gamma \le \alpha$ and it gives that

$$\chi(C(r,w)) = \chi\left(C(r,w)\cap\left(\bigcup_{i=0}^{\gamma} X_i\right)\right) + \sum_{i=\gamma+1}^{\alpha}\chi_i(C(r,w)\cap X_i).$$

Now, for each $i \ge \gamma+1$, i.e. $\gamma \le i-1$, we have $\chi_i(C(r,w)\cap X_i) = 0$. Also note that $\bigcup_{i=0}^{\gamma} X_i$ is $\{x : 0 \le x < p^\gamma\}$, so there is exactly one element of $C(r,w)$ in it. Hence

$$|\chi(C(r,w))| = \left|\chi\left(C(r,w)\cap\left(\bigcup_{i=0}^{\gamma} X_i\right)\right)\right| = 1.$$

Thus we may conclude that

$$\max_{A_0 \in \mathcal{A}_n^0} |\chi(A_0)| \le 1.$$

Hence for both $p = 2$ and p is odd, we can always find such a coloring χ. □

Finally we extend the argument above to arbitrary n using Chinese remainder theorem.

Notations. Suppose that number n has prime factorization $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. By Chinese remainder theorem, we have an isomorphism

$$\psi_n : \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}} \to \mathbb{Z}_n.$$

Again, we first show the following analogue of Lemma 3.5. This shows that if $X \subseteq \mathbb{Z}_n$ has some special structure, then we have a coloring of X with low discrepancy with respect to both $\mathcal{A}_n$ and $\mathcal{A}_n^0$.

Lemma 3.6. *Let n be a positive integer with prime factorization $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. For each $1 \le i \le k$, let $T_i \le p_i^{\alpha_i}$ be a positive integer. Let $X = \{\psi_n(t_1, \dots, t_k) : 0 \le t_i < T_i \text{ for all } 1 \le i \le k\}$. Then $X \subseteq \mathbb{Z}_n$ is a set of $m = \prod_{i=1}^k T_i$ elements. Suppose that $I \subseteq [k]$ is a subset of indices and $(\beta_i)_{i \in I}$ is a sequence of nonnegative integers, such that for each $i \in I$, $T_i = s_i p_i^{\beta_i}$ for some even number s_i. Then there exists a coloring $\chi : X \to \{-1, 1\}$ such that the following holds. Its discrepancy over $\mathcal{A}_n$ satisfies that*

$$\max_{A \in \mathcal{A}_n} |\chi(A \cap X)| \le c 2^{\frac{|I|}{2}} \cdot \sqrt{m} \left(|I| + 1 + \log \frac{n}{m}\right)^{\frac{1}{2}}, \tag{3.2}$$

and for any $w \in \mathbb{Z}_n$ and any $i \in I$,

$$\chi(C(n/p_i^{\alpha_i - \beta_i}, w) \cap X) = 0. \tag{3.3}$$

Proof. Let $L = |I|$. Let $S_i = T_i/2$ if $i \in I$, and $S_i = T_i$ otherwise. For each $i \in I$, from the condition that $T_i/p_i^{\beta_i}$ is even, we know that S_i is a multiple of $p_i^{\beta_i}$. We define

$$X_0 = \{\psi_n(t_1, \dots, t_k) : 0 \le t_i < S_i \text{ for all } 1 \le i \le k\}.$$

We know that $X_0 \subseteq \mathbb{Z}_n$ is a set of size $m/2^L$. Next we apply Corollary 2.3 to get the constant $c_0 > 0$ and a partial coloring of $\chi_0 : X_0 \to \{-1, 1\}$ such that

$$\max_{A \in \mathcal{A}_n} |\chi_0(X_0 \cap A)| \le c_0 \sqrt{\frac{m}{2^L}} \left(1 + \log \frac{2^L n}{m}\right)^{\frac{1}{2}} \le c \sqrt{\frac{m}{2^L}} \left(L + 1 + \log \frac{n}{m}\right)^{\frac{1}{2}},$$

where c is another absolute constant.

For each $v = (v_i)_{i \in I} \in \{0,1\}^I$ (binary tuples of length L indexed by I), we define $\mathrm{sgn}(v) = (-1)^{\sum_{i \in I} v_i}$, and let $u_v \in \mathbb{Z}_n$ be the unique element, by the Chinese remainder theorem, such that

$$u_v \equiv v_i S_i \pmod{p_i^{\alpha_i}} \text{ for all } i \in I \quad \text{and} \quad u_v \equiv 0 \pmod{p_j^{\alpha_j}} \text{ for all } j \notin I.$$

Thus we have the decomposition of X into disjoint copies of translations of X_0:

$$X = \coprod_{v \in \{0,1\}^I} X_v, \quad \text{where} \quad X_v := u_v + X_0.$$

This implies that each $x \in X$ can be written in the form $x = u_v + x_0$ for some $v \in \{0,1\}^I$ and $x_0 \in X_0$. Now we define $\chi : X \to \{1, -1\}$ by $\chi(u_v + x_0) = \mathrm{sgn}(v) \cdot \chi(x_0)$ for all $v \in \{0,1\}^I, x_0 \in X_0$. For any

$A \in \mathcal{A}_n$, noting that $A - u_v$ is also in $\mathcal{A}_n$, so

$$\begin{aligned}|\chi(X \cap A)| &= \left|\sum_{v\in\{0,1\}^I} \chi(X_v \cap A)\right| = \left|\sum_{v\in\{0,1\}^I} \operatorname{sgn}(v)\cdot\chi_0(X_v \cap A - u_v)\right| \\ &\le \sum_{v\in\{0,1\}^I} |\chi_0(X_0 \cap (A-u_v))| \le 2^L \max_{A\in\mathcal{A}_n} |\chi_0(X_0\cap A)| \\ &\le 2^L \cdot c\sqrt{\frac{m}{2^L}}\left(L+1+\log\frac{n}{m}\right)^{\frac{1}{2}} = c2^{\frac{L}{2}}\cdot\sqrt{m}\left(L+1+\log\frac{n}{m}\right)^{\frac{1}{2}}.\end{aligned}$$

This shows that the coloring χ satisfies the condition (3.2) on the discrepancy over $\mathcal{A}_n$.

It remains to show (3.3). For each $i \in I$, let $r_i = n/p_i^{\alpha_i-\beta_i} = p_1^{\alpha_1}\cdots p_i^{\beta_i}\cdots p_k^{\alpha_k}$. For any $i \in I$ and any $w \in \mathbb{Z}_n$, we know that $C(r_i, w)$ contains $p^{\alpha_i-\beta_i}$ elements. If $C(r_i, w) \cap X = \emptyset$, then (3.3) trivially holds. It suffices to check $\chi(C(r_i, w) \cap X) = 0$ for $w = \psi_n(t_1, \ldots, t_k) \in X_v$ for some $v \in \{0, 1\}^I$. Since $p_j^{\alpha_j}$ divides r_i, each element in $C(r_i, w)$ is congruent to t_j mod $p_j^{\alpha_j}$ for $j \neq i$. This implies that $C(r_i, w)$ only has nonempty intersection with X_v and $X_{v'}$ where $v, v' \in \{0, 1\}^I$ differ only at the entry indexed by i. Moreover by the definition of u, $u_v - u_{v'}$ is congruent to 0 mod $p_j^{\alpha_j}$ for all $j \neq i$, and is congruent to $\pm\frac{s_i}{2}p_i^{\beta_i}$ mod $p_i^{\alpha_i}$. Thus $u_v - u_{v'}$ is a multiple of r_i, which implies $C(r_i, w) = C(r_i, w) + (u_v - u_{v'})$, or equivalently $C(r_i, w) - u_v = C(r_i, w) - u_{v'}$. Therefore we have

$$\begin{aligned}\chi(C(r_i, w) \cap X) &= \chi(C(r_i, w) \cap X_v) + \chi(C(r_i, w) \cap X_{v'}) \\ &= \operatorname{sgn}(v)\cdot\chi_0((C(r_i, w) - u_v) \cap X_0) + \operatorname{sgn}(v')\cdot\chi_0((C(r_i, w) - u_{v'}) \cap X_0) = 0.\end{aligned}$$

This is true for all $i \in I$ and $w \in \mathbb{Z}_n$, and thus we conclude that χ satisfies (3.3) as well. □

We are now ready to prove Lemma 3.3. The idea is that, we partition $\mathbb{Z}_n$ into a few subsets, one for each factor r of n, and for each of them we use Lemma 3.6 to get a coloring of this subset with low discrepancy over $\mathcal{A}_n$ and nearly optimal discrepancy over $\mathcal{A}_n^0$. Finally we show that the full coloring we get from combining these subset colorings satisfies the properties.

Proof of Lemma 3.3. Suppose that n has prime factorization $n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$. For each $1 \le i \le k$, we partition $\mathbb{Z}_{p_i^{\alpha_i}}$ into $\alpha_i + 1$ intervals $\left(S_i^{(t)}\right)_{t=0}^{\alpha_i}$ in the following way. If $p_i = 2$, then we set $S_i^{(\alpha_i)} = \mathbb{Z}_{p_i^{\alpha_i}}$ and $S_i^{(t)} = \emptyset$ for all $0 \le t < \alpha_i$. If $p_i > 2$, then we set $S_i^{(0)} = \{0\} \subseteq \mathbb{Z}_{p_i^{\alpha_i}}$ and $S_i^{(t)} = \{x : p_i^{t-1} \le x < p_i^t\}$ for $1 \le t \le \alpha_i$. In particular we have $|S_i^{(t)}| \le p_i^t$ for all i and t. Moreover, for each i and $t > 0$, $S_i^{(t)}$ is always an interval of length $s_i p_i^{t-1}$ in $\mathbb{Z}_{p_i^{\alpha_i}}$ for some even s_i.

For each factor $r = p_1^{\delta_1}\cdots p_k^{\delta_k}$ of n, we define $Y_r = S_1^{(\delta_1)} \times \cdots \times S_k^{(\delta_k)} \subseteq \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}$ and $X_r = \psi_n(Y_r) \subseteq \mathbb{Z}_n$. Since each $\mathbb{Z}_{p_i^{\alpha_i}}$ is partitioned into $S_i^{(t)}$ for $0 \le t \le \alpha_i$, their product is partitioned into Y_r for r divides n, so $\mathbb{Z}_n$ is partitioned into X_r for r divides n. Because $|S_i^{(t)}| \le p_i^t$ for all i and t,

$$|X_r| = |Y_r| = \prod_{i=1}^k |S_i^{(\delta_i)}| \le \prod_{i=1}^k p_i^{\delta_i} = r. \tag{3.4}$$

For each nonempty X_r with $r = p_1^{\delta_1}\cdots p_k^{\delta_k}$, we would like to apply Lemma 3.6 to get a coloring of X_r with bounded discrepancy. Note that we can translate Y_r so that all intervals $S_j^{(\delta_j)}$ for $1 \le j \le k$ start at 0, and notice those properties from Lemma 3.6 are invariant under translation, so it is applicable to X_r. Let $I_r = \{i \in [k] : \delta_i > 0\} \subseteq [k]$. We have that for each $i \in I_r$, $S_i^{(\delta_i)}$ is an interval of length $s_i p_i^{\beta_i}$

for some even s_i and $\beta_i = \delta_i - 1$. This implies that we can find a partial coloring $\chi_r : X_r \to \{-1, 1\}$ such that

$$\max_{A\in\mathcal{A}_n} |\chi_r(A \cap X_r)| \le c_0 2^{\frac{|I_r|}{2}} \sqrt{|X_r|} \left(|I_r| + 1 + \log \frac{n}{|X_r|}\right)^{\frac{1}{2}}, \tag{3.5}$$

and for any $i \in I_r$ and any $w \in \mathbb{Z}_n$,

$$\chi_r(C(n/p_i^{\alpha_i-\beta_i}, w) \cap X_r) = \chi_r(C(n/p_i^{\alpha_i-\delta_i+1}, w) \cap X_r) = 0. \tag{3.6}$$

Having defined χ_r as above for each nonempty X_r, we now construct χ by setting $\chi(x_r) = \chi_r(x_r)$ for each $x_r \in X_r$ for all r that divides n. We first show that χ has low discrepancy over $\mathcal{A}_n$. By (3.4) we have $|X_r| \le r$. By definition we have $|I_r| \le k$. Also note that $x^{1/2} \cdot \left(k + 1 + \log \frac{n}{x}\right)^{\frac{1}{2}}$ is increasing for $x \in (0, n]$. Combining these together, we know that for any nonempty X_r,

$$2^{\frac{|I_r|}{2}} \sqrt{|X_r|} \left(|I_r| + 1 + \log \frac{n}{|X_r|}\right)^{\frac{1}{2}} \le 2^{\frac{k}{2}} \sqrt{r} \left(k + 1 + \log \frac{n}{r}\right)^{\frac{1}{2}} \le 2^{\frac{k}{2}} (k+1)^{\frac{1}{2}} \sqrt{r} \left(\log \frac{en}{r}\right)^{\frac{1}{2}}. \tag{3.7}$$

Combining (3.5) and (3.7), there exists an absolute constant c_1 such that for each nonempty X_r,

$$\max_{A\in\mathcal{A}_n} |\chi_r(A \cap X_r)| \le c_0 2^{\frac{k}{2}} (k+1)^{\frac{1}{2}} \cdot \sqrt{r} \left(\log \frac{en}{r}\right)^{\frac{1}{2}} \le c_1 2^{\frac{3}{4}k} \cdot \sqrt{r} \left(1 + \log \frac{n}{r}\right)^{\frac{1}{2}}. \tag{3.8}$$

This is also true for $X_r = \emptyset$. Moreover we know that for any $r = p_1^{\delta_1} \cdots p_k^{\delta_k}$,

$$\sqrt{r} \left(1 + \log \frac{n}{r}\right)^{\frac{1}{2}} \le \prod_{i=1}^{k} p_i^{\delta_i/2} \left(1 + \log \frac{p_i^{\alpha_i}}{p_i^{\delta_i}}\right)^{\frac{1}{2}} = \sqrt{n} \prod_{i=1}^{k} p_i^{-(\alpha_i-\delta_i)/2} \left(1 + (\alpha_i - \delta_i) \log p_i\right)^{\frac{1}{2}}.$$

Summing this over all factors $r = p_1^{\delta_1} \cdots p_k^{\delta_k}$ for $0 \le \delta_i \le \alpha_i$, we have that if we set $t_i = \alpha_i - \delta_i$,

$$\begin{aligned}\sum_{r|n} \sqrt{r} \left(1 + \log \frac{n}{r}\right)^{\frac{1}{2}} &\le \sqrt{n} \cdot \sum_{\delta_1=0}^{\alpha_1} \cdots \sum_{\delta_k=0}^{\alpha_k} \prod_{i=1}^{k} p_i^{-(\alpha_i-\delta_i)/2} \left(1 + (\alpha_i - \delta_i) \log p_i\right)^{\frac{1}{2}} \\ &= \sqrt{n} \prod_{i=1}^{k} \left(\sum_{t_i=0}^{\alpha_i} p_i^{-t_i/2} (1 + t_i \log p_i)^{\frac{1}{2}}\right) \le \sqrt{n} \prod_{i=1}^{k} \left(\sum_{t_i=0}^{\infty} p_i^{-t_i/2} (1 + t_i \log p_i)^{\frac{1}{2}}\right).\end{aligned}$$

Note that for $p \ge 2$,

$$f(p) := \sum_{t=0}^{\infty} p^{-t/2} (1 + t \log p)^{\frac{1}{2}}$$

is well-defined and tends to 1 as $p \to \infty$. Thus there exists an absolute constant $P > 0$ such that if $p \ge P$, then $f(p) < 2^{\frac{1}{4}}$. Since there are only finitely many prime numbers less than P, we conclude that there exists an absolute constant c_2 such that

$$\prod_{i=1}^{k} \left(\sum_{t_i=0}^{\infty} p_i^{-t_i/2} (1 + t_i \log p_i)^{\frac{1}{2}}\right) = \prod_{i=1}^{k} f(p_i) \le c_2 \cdot 2^{\frac{k}{4}}.$$

Thus we have

$$\sum_{r|n} \sqrt{r} \left(1 + \log \frac{n}{r}\right)^{\frac{1}{2}} \le \sqrt{n} \prod_{i=1}^{k} \left(\sum_{t_i=0}^{\infty} p_i^{-t_i/2} (1 + t_i \log p_i)^{\frac{1}{2}}\right) \le c_2 2^{\frac{k}{4}} \sqrt{n}. \tag{3.9}$$

Thus for any $A \in \mathcal{A}_n$, by (3.8) and (3.9),

$$|\chi(A)| = \left|\sum_{r|n} \chi_r(A \cap X_r)\right| \leq \sum_{r|n} c_1 2^{\frac{3}{4}k} \cdot \sqrt{r} \left(1 + \log \frac{n}{r}\right)^{\frac{1}{2}} \leq c_1 c_2 2^k \sqrt{n}.$$

Here we set $c = c_1 c_2$ to get the desired bound on the discrepancy over $\mathcal{A}_n$.

Now we study the discrepancy of χ over $\mathcal{A}_n^0$. Note that $C(r', w) = C(\gcd(r', n), w)$. We may only consider the set of $C(r', w) \in \mathcal{A}_n^0$ for which $r' = p_1^{\gamma_1} \cdots p_k^{\gamma_k}$ is a factor of n. By definition of χ, we have the relation that

$$\chi(C(r', w)) = \sum_{r|n} \chi_r(C(r', w) \cap X_r). \tag{3.10}$$

If r' is not a multiple of $r = p_1^{\delta_1} \cdots p_k^{\delta_k}$, then we know that there exists some $1 \leq i \leq k$ for which $\gamma_i \leq \delta_i - 1$. It follows that $\delta_i > 0$, and $i \in I_r$. Since r' is a factor of n and $\gamma_i \leq \delta_i - 1$, it is a factor of $n/p_i^{\alpha_i - \delta_i + 1}$. Consequently, the congruence class $C(r', w)$ can be partitioned into congruence classes of the form $C(n/p_i^{\alpha_i - \delta_i + 1}, w')$. Noting that (3.6) holds for any $w' \in \mathbb{Z}_n$, we know that if r is not a factor of r', then $\chi_r(C(r', w) \cap X_r) = 0$. Thus we can remove all summands on the right hand side of (3.10) except those r that divides r'. We get

$$\chi(C(r', w)) = \sum_{r|r'} \chi_r(C(r', w) \cap X_r) = \chi\left(C(r', w) \cap \left(\bigcup_{r|r'} X_r\right)\right).$$

Note that we are taking union over all $r = p_1^{\delta_1} \cdots p_k^{\delta_k}$ for which $0 \leq \delta_i \leq \gamma_i$ for all $1 \leq i \leq k$. We have

$$\begin{aligned}
\bigcup_{r|r'} X_r &= \psi_n\left(\bigcup_{r|r'} Y_r\right) \\
&= \psi_n\left(\bigcup_{\delta_1=0}^{\gamma_1} \cdots \bigcup_{\delta_k=0}^{\gamma_k} S_1^{(\delta_1)} \times \cdots \times S_k^{(\delta_k)}\right) \\
&= \psi_n\left(\prod_{i=1}^{n} \left(\bigcup_{\delta_i=0}^{\gamma_i} S_i^{(\delta_i)}\right)\right).
\end{aligned}$$

From our construction, we know that $\bigcup_{\delta_i=0}^{\gamma_i} S_i^{(\delta_i)} = \emptyset$ if $p_i = 2$ and $\gamma_i < \alpha_i$, and otherwise

$$\bigcup_{\delta_i=0}^{\gamma_i} S_i^{(\delta_i)} = \{x : 0 \leq x < p_i^{\gamma_i}\} \subseteq \mathbb{Z}_{p_i^{\alpha_i}}.$$

Thus we may conclude that

$$\bigcup_{r|r'} X_r \subseteq \{\psi_n(t_1, \cdots, t_k) : 0 \leq t_i < p_i^{\gamma_i} \text{ for all } 1 \leq i \leq k\}. \tag{3.11}$$

Let $Z_{r'}$ be the set on the right hand side of (3.11). Any two distinct elements of $Z_{r'}$ differ on some t_i for $1 \leq i \leq k$, i.e., they have different remainders when divided by $p_i^{\gamma_i}$ for some i. Therefore their difference is not divisible by r'. Hence there is at most one element of $C(r', w)$ in $\bigcup_{r|r'} X_r \subseteq Z_{r'}$ for

any $w \in \mathbb{Z}_n$. We conclude that for any r' that divides n and any $w \in \mathbb{Z}_n$,

$$|\chi(C(r', w))| = \left|\chi\left(C(r', w) \cap \left(\bigcup_{r|r'} X_r\right)\right)\right| \leq 1.$$

This finishes our proof. □

Remark 3.7. By being a little more careful with bounds in the above proof, we may improve the latter inequality in Lemma 3.3 to

$$\max_{A \in \mathcal{A}_n} |\chi(A)| \leq \sqrt{n} \cdot 2^{\left(\frac{1}{2}+o(1)\right)k},$$

where the $o(1)$ term tends to 0 as $k \to \infty$. This in turn improves the bound on $\mathrm{disc}(\mathcal{A}_n)$ to $\min_{r|n}\left(\frac{n}{r} + \sqrt{r} \cdot 2^{\left(\frac{1}{2}+o(1)\right)\omega(r)}\right)$ in Theorem 3.1, where the $o(1)$ term goes to 0 as $\omega(r) \to \infty$.

4. Lower Bounds

In this section, we prove the lower bounds in Theorems 1.1 and 1.2. These proofs use Fourier analysis. We first set up helpful notations and prove a consequence of the Plancherel theorem in Lemma 4.1.

Notations. Let $f : \mathbb{Z}_n \to \mathbb{C}$. Any coloring $\chi : \mathbb{Z}_n \to \{1, -1\}$ is a special case. In this section, all summations are over $\mathbb{Z}_n$ unless otherwise specified.

We define the Fourier transform $\widehat{f} : \mathbb{Z}_n \to \mathbb{C}$ by $\widehat{f}(r) = \sum_{x \in \mathbb{Z}_n} f(x) e^{-\frac{2\pi i}{n} xr}$.

For two functions $f_1, f_2 : \mathbb{Z}_n \to \mathbb{C}$, their convolution $f_1 * f_2 : \mathbb{Z}_n \to \mathbb{C}$ is given by $f_1 * f_2(a) = \sum_x f_1(x) f_2(a - x)$. We have the convolution identity $\widehat{f_1 * f_2} = \widehat{f_1} \cdot \widehat{f_2}$.

For any $r \in \mathbb{N}$ that divides n, we say that $x \equiv y \pmod r$ for $x, y \in \mathbb{Z}_n$ if $x = y + kr$ for some $k \in \mathbb{Z}_n$. We define, for any $r \in \mathbb{N}$ that divides n and $a \in \mathbb{Z}_n$,

$$g_f(a, r) := \sum_{x \in \mathbb{Z}_n : x \equiv a \,(\mathrm{mod}\ r)} f(x) \quad \text{and} \quad G_f(r) := \sum_{a=0}^{r-1} |g(a, r)|^2.$$

We see that $g_f(a, r) = g_f(a + kr, r)$, so $g_f(\cdot, r)$ can be treated as a function on $\mathbb{Z}_r$.

Let M be a set or a multiset of elements in $\mathbb{Z}_n$. For $a, r \in \mathbb{Z}_n$, we define rM to be the multiset $\{rx : x \in M\}$, and $a + M$ to be the multiset $\{a + x : x \in M\}$. We define m_M to be the multiplicity function, i.e. $m_M(x)$ is the multiplicity of x in M. In particular, when M is a set, $m_M = 1_M$ is the indicator function. We also define

$$f(M) = \sum_{x \in M} f(x).$$

Lemma 4.1. *For any $f : \mathbb{Z}_n \to \mathbb{C}$, let $\widehat{f}$ be its Fourier transform. Let $r \in \mathbb{N}$ be a factor of n. Then*

$$\sum_{k=0}^{r-1} \left|\widehat{f}\left(k \cdot \frac{n}{r}\right)\right|^2 = r G_f(r).$$

Proof. Let $t = n/r$. For each $0 \leq k \leq r - 1$, we know that by definition

$$\widehat{f}(kt) = \sum_{x=0}^{n-1} f(x) e^{-\frac{2\pi i}{n} x \cdot kt} = \sum_{x=0}^{tr-1} f(x) e^{-\frac{2\pi i}{r} xk} = \sum_{a=0}^{r-1} g_f(a, r) e^{-\frac{2\pi i}{r} ak}.$$

Hence for $g : \mathbb{Z}_r \to \mathbb{C}$ defined by $g(a) := g_f(a, r)$, its Fourier transform is $\widehat{g}(k) = \widehat{f}(kt)$. By the Plancherel theorem we have

$$\sum_{k=0}^{r-1} \left|\widehat{f}\left(k \cdot \frac{n}{r}\right)\right|^2 = \sum_{k=0}^{r-1} |\widehat{g}(k)|^2 = r \sum_{a=0}^{r-1} |g(a)|^2 = rG_f(r).$$

□

In Lemmas 4.2 and 4.3, we prove lower and upper bounds on the same quantity respectively. Combining them we get Corollary 4.4. This corollary lower bounds the discrepancy of a function f over arithmetic progressions in $\mathbb{Z}_n$ by the Fourier coefficients of f.

The next lemma lower bounds the quantity by a weighted L^2 sum of Fourier coefficients $\widehat{f}$. The weights depend on the arithmetic structure of n.

Lemma 4.2. *Let $f : \mathbb{Z}_n \to \mathbb{C}$, $1 \le m \le n$ be an integer, and $M := \{0, 1 \ldots, m-1\} \subseteq \mathbb{Z}_n$. Then*

$$\sum_{a \in \mathbb{Z}_n} \sum_{b \in \mathbb{Z}_n} |f(a + bM)|^2 \ge \sum_{r \in \mathbb{Z}_n} |\widehat{f}(r)|^2 \cdot \max\left(\frac{m^2 \cdot \gcd(r, n)}{n}, m\right). \tag{4.1}$$

Proof. We show some properties about the multiplicity function. For the set M, we have

$$f(a + bM) = \sum_{x \in M} f(a + bx) = \sum_x f(x) m_{a+bM}(x) = \sum_x f(x) m_{-bM}(a - x) = f * m_{-bM}(a). \tag{4.2}$$

For any $u, v \in \mathbb{Z}_n$, we have

$$\widehat{m_{-uM}}(v) = \sum_x m_{-uM}(x) e^{-\frac{2\pi i}{n} vx} = \sum_{x \in -uM} e^{-\frac{2\pi i}{n} vx} = \sum_{y \in -M} e^{-\frac{2\pi i}{n} vuy} = \widehat{m_{-M}}(uv). \tag{4.3}$$

Applying (4.3) twice we have $\widehat{m_{-uM}}(v) = \widehat{m_{-vM}}(u)$. We have

$$\begin{aligned}
\sum_a \sum_b |f(a + bM)|^2 &= \sum_b \sum_a |f * m_{-bM}(a)|^2 = \sum_b \frac{1}{n} \sum_r \left|\widehat{f * m_{-bM}}(r)\right|^2 \\
&= \frac{1}{n} \sum_b \sum_r |\widehat{f}(r)|^2 \cdot \left|\widehat{m_{-bM}}(r)\right|^2 = \frac{1}{n} \sum_b \sum_r |\widehat{f}(r)|^2 \left|\widehat{m_{-rM}}(b)\right|^2 \\
&= \sum_r |\widehat{f}(r)|^2 \cdot \left(\frac{1}{n} \sum_b \left|\widehat{m_{-rM}}(b)\right|^2\right) = \sum_r |\widehat{f}(r)|^2 \cdot \sum_s |m_{-rM}(s)|^2,
\end{aligned} \tag{4.4}$$

where the first equality uses (4.2), the second uses the Planchrel theorem, the third uses the Fourier identity of convolution, the fourth uses (4.3) twice, and the last uses the Plancherel theorem. Now we evaluate $\sum_s |m_{-rM}(s)|^2$. Let $k = \gcd(r, n)$. When $km \le n$, we know that rM contains m elements with multiplicity 1. Thus in this case we have

$$\sum_s |m_{-rM}(s)|^2 = m.$$

Otherwise when $km > n$, we know that rM contains elements that are multiples of k. There are $\frac{n}{k}$ such elements in $\mathbb{Z}_n$. Therefore, by the Cauchy-Schwarz inequality, we have

$$\sum_s |m_{-rM}(s)|^2 = \sum_{t=0}^{\frac{n}{k}-1} |m_{-rM}(tk)|^2 \ge \frac{\left(\sum_{t=0}^{\frac{n}{k}-1} |m_{-rM}(tk)|\right)^2}{n/k} = \frac{m^2 k}{n}.$$

Hence we may conclude that for any $r \in \mathbb{Z}_n$,

$$\sum_s |m_{-rM}(s)|^2 \geq \max\left(\frac{m^2 \cdot \gcd(r,n)}{n}, m\right). \tag{4.5}$$

Combining this with (4.4), we obtain (4.1). □

The next lemma gives an upper bound on the quantity above. The upper bound involves the discrepancy of f over $\mathcal{A}_n$ and some arithmetic sums of f. Let $\phi(\cdot)$ be Euler's totient function.

Lemma 4.3. *Let $f : \mathbb{Z}_n \to \mathbb{C}$. Suppose that*

$$T_f := \max_{A \in \mathcal{A}_n} |f(A)|.$$

Let $m \leq n$ be a positive integer, and $M := \{0, 1, \ldots, m-1\} \subseteq \mathbb{Z}_n$. Then we have

$$\sum_{a \in \mathbb{Z}_n} \sum_{b \in \mathbb{Z}_n} |f(a+bM)|^2 \leq n^2 T_f^2 + \sum_{0 \leq k < m : k | N} m^2 \frac{\phi(k)}{k} G_f(n/k). \tag{4.6}$$

Proof. For each fixed $b \in \mathbb{Z}_n$, we analyze the summation $\sum_a |f(a+bM)|^2$. Let $r = \gcd(b,n)$ and $k = n/r$. There are two possibilities: $rm \leq n$ or $rm > n$.

If $rm \leq n$, then each element in bM has multiplicity 1. Therefore $a + bM$ is a set for all $a \in \mathbb{Z}_n$. Moreover from our definition of $M = \{0, 1, \ldots, m-1\}$, we know that $a + bM \in \mathcal{A}_n$ is an arithmetic progression in $\mathbb{Z}_n$. In this case, for any a, $|f(a+bM)| \leq T_f$, so

$$\sum_a |f(a+bM)|^2 \leq \sum_a T_f^2 = nT_f^2. \tag{4.7}$$

If $rm > n$, i.e., $m > k$, then some elements in bM have multiplicity greater than 1. The bound in (4.7) no longer applies. Let $K = \{0, 1, \ldots, k-1\}$ and it follows that each element in bK has multiplicity 1. Moreover, it covers each multiple of r in $\mathbb{Z}_n$ exactly once. Hence

$$f(a+bK) = \sum_{t=0}^{k-1} f(a+bt) = g_f(a,r).$$

Suppose that $m = qk + s$ for integers q and $0 \leq s < k$. Then we may write $m_M = m_S + \sum_{j=0}^{q-1} m_{s+jk+K}$ where $S = \{0, 1, \ldots, s-1\}$. Thus, for any $a \in \mathbb{Z}_n$, we have

$$\begin{aligned} f(a+bM) &= f(a+bS) + \sum_{j=0}^{q-1} f(a + b \cdot (s+jk) + bK) \\ &= f(a+bS) + \sum_{j=0}^{q-1} g_f(a + b \cdot (s+jk), r) = f(a+bS) + q \cdot g_f(a,r). \end{aligned} \tag{4.8}$$

In the last step, we use the fact that $b \cdot (s+jk)$ is a multiple of r.

Since $s < k$, each element in bS has multiplicity at most 1, and further $a + bS \in \mathcal{A}_n$ for all a. Thus

$$|f(a+bS)| \leq T_f. \tag{4.9}$$

We now partition $a \in \mathbb{Z}_n$ into congruence classes mod r. In particular, we have

$$\sum_a |f(a+bM)|^2 = \sum_{i=0}^{r-1} \sum_{a \equiv i \,(\mathrm{mod}\ r)} |f(a+bM)|^2. \tag{4.10}$$

For each $a' \equiv i \pmod r$, there are exactly s choices of $a \equiv i \pmod r$ such that $a' \in a + bS$. Thus,

$$\sum_{j=0}^{k-1} f(i + jr + bS) = \sum_{a \equiv i \,(\mathrm{mod}\ r)} f(a + bS) = s \cdot g_f(i, r). \tag{4.11}$$

Consequently, we have

$$\begin{aligned}
\sum_{a \equiv i \,(\mathrm{mod}\ r)} |f(a + bM)|^2 &= \sum_{j=0}^{k-1} |f(i + jr + bM)|^2 \\
[\text{by (4.8)}] \quad &= \sum_{j=0}^{k-1} |f(i + jr + bS) + q \cdot g_f(i, r)|^2 \\
&= \sum_{j=0}^{k-1} \left(|f(i + jr + bS)|^2 + 2 \,\mathrm{Re}\left(q \cdot f(i + jr + bS) \overline{g_f(i, r)} \right) + q^2 |g_f(i, r)|^2 \right) \\
[\text{by (4.9)}] \quad &\le kT_f^2 + kq^2 |g_f(i, r)|^2 + 2q \,\mathrm{Re}\left(\overline{g_f(i, r)} \sum_{j=0}^{k-1} f(i + jr + bS) \right) \\
[\text{by (4.11)}] \quad &= kT_f^2 + kq^2 |g_f(i, r)|^2 + 2qs |g_f(i, r)|^2 \\
&\le kT_f^2 + |g_f(i, r)|^2 \cdot \frac{k^2 q^2 + 2kqs + s^2}{k} \\
[\text{by } m = kq + s] \quad &= kT_f^2 + \frac{m^2}{k} |g_f(i, r)|^2.
\end{aligned}$$

Put this into (4.10). We know that in the second case where $rm > n$, i.e., $k < m$,

$$\sum_a |f(a + bM)|^2 = \sum_{i=0}^{r-1} \sum_{a \equiv i \,(\mathrm{mod}\ r)} |f(a + bM)|^2 \le nT_f^2 + \frac{m^2}{k} G_f(r) = nT_f^2 + \frac{m^2}{k} G_f(n/k). \tag{4.12}$$

The second case happens exactly when $\gcd(b, n) = n/k$ for some $k < m$ which divides n. The number of such choices of b is exactly $\phi(k)$ for any fixed k. Hence combining (4.7) and (4.12), we get (4.6). □

Combining Lemma 4.2 and Lemma 4.3, we deduce the following general lower bounds.

Corollary 4.4. *Let $f : \mathbb{Z}_n \to \mathbb{C}$ and $\widehat{f}$ be its Fourier transform. Suppose that*

$$T_f := \max_{A \in \mathcal{A}_n} |f(A)|.$$

For any positive integer $m \le n$, we have

$$n^2 T_f^2 + \sum_{1 \le k < m : k | n} \frac{m^2 \phi(k)}{k} G_f(n/k) \ge \sum_{r \in \mathbb{Z}_n} |\widehat{f}(r)|^2 \cdot \max\left(\frac{m^2 \cdot \gcd(r, n)}{n}, m \right). \tag{4.13}$$

In Corollary 4.4, the inequality involves G_f and $\widehat{f}$ besides T_f. We aim to get a lower bound on $\mathrm{disc}(\mathcal{A}_n)$ that only depends on arithmetic structure of n (Proposition 4.7). To achieve that, we need two lemmas (Lemma 4.5 and Lemma 4.6) to remove the dependency on $\widehat{f}$ and G_f.

Lemma 4.5. *Let $f : \mathbb{Z}_n \to \mathbb{C}$ and $\widehat{f}$ be its Fourier transform and $m \le n$ be a positive integer. Then*

$$\sum_{1 \le k \le n : k | n} \frac{m^2 \phi(k)}{k} G_f(n/k) = \sum_{r \in \mathbb{Z}_n} |\widehat{f}(r)|^2 \cdot \frac{m^2 \cdot \gcd(r, n)}{n}.$$

Proof. By Lemma 4.1, we know that

$$\frac{n}{k}G_f(n/k) = \sum_{r\in\mathbb{Z}_n:k|r} |\widehat{f}(r)|^2.$$

Thus we have (noticing that $\sum_{k|l}\phi(k) = l$ for any positive integer l)

$$\begin{aligned}\sum_{1\le k\le n:k|n} \frac{m^2\phi(k)}{k}G_f(n/k) &= \sum_{1\le k\le n:k|n} \frac{m^2\phi(k)}{n}\sum_{r\in\mathbb{Z}_n:k|r}|\widehat{f}(r)|^2 = \sum_{r\in\mathbb{Z}_n}|\widehat{f}(r)|^2\cdot\frac{m^2}{n}\sum_{1\le k\le n:k|n,k|r}\phi(k)\\ &= \sum_{r\in\mathbb{Z}_n}|\widehat{f}(r)|^2\cdot\frac{m^2}{n}\sum_{1\le k\le n:k|\gcd(n,r)}\phi(k) = \sum_{r\in\mathbb{Z}_n}|\widehat{f}(r)|^2\cdot\frac{m^2}{n}\gcd(r,n).\end{aligned}$$

Hence we have the desired equality. □

Lemma 4.6. *Let $f:\mathbb{Z}_n\to\mathbb{C}$ and $\widehat{f}$ be its Fourier transform. Let $m,l\le n$ be positive integers. Then*

$$\sum_{r\in\mathbb{Z}_n}|\widehat{f}(r)|^2\cdot\min\left(\frac{m^2\cdot\gcd(r,n)}{n},m\right) \le \sum_{1\le k\le l:k|n}\frac{m^2\phi(k)}{k}G_f(n/k) + \sum_{l<k\le n:k|n}\frac{mn}{k}G_f(n/k). \quad (4.14)$$

Proof. It suffices to compare the coefficient of each $|\widehat{f}(r)|^2$ on both sides after expanding all terms of G_f on the right hand side (4.14) using Lemma 4.1. By Lemma 4.1, for any k that divides n,

$$\frac{n}{k}G_f(n/k) = \sum_{r\in\mathbb{Z}_n:k|r}|\widehat{f}(r)|^2.$$

For each $r\in\mathbb{Z}_n$, the coefficient t_r of $|\widehat{f}(r)|^2$ on the right hand side of (4.14) is given by

$$t_r = \sum_{1\le k\le l:k|\gcd(r,n)}\frac{m^2\phi(k)}{n} + \sum_{l<k\le n:k|\gcd(r,n)} m = \frac{m^2}{n}\sum_{1\le k\le l:k|\gcd(r,n)}\phi(k) + m\sum_{l<k\le n:k|\gcd(r,n)}1.$$

If $\gcd(r,n)\le l$, then we know that the first summation sums over all factors of $\gcd(r,n)$, and the second summation is zero. Hence we know that in this case,

$$t_r = \frac{m^2}{n}\gcd(r,n).$$

If $\gcd(r,n) > l$, then in particular the second summation contains at least one term $k=\gcd(r,n)$, and the first summation is nonnegative. Hence in this case,

$$t_r > m.$$

We may conclude that $t_r \ge \min\left(\frac{m^2\cdot\gcd(r,n)}{n},m\right)$ for all $r\in\mathbb{Z}_n$. This yields (4.14). □

Using the lemmas above, we prove a lower bound on $\mathrm{disc}(\mathcal{A}_n)$ which depends only on the arithmetic structure of n.

Proposition 4.7. *For any positive integers n and $l\le n$,*

$$\frac{1}{(\mathrm{disc}(\mathcal{A}_n))^2} \le \frac{8}{n}\sum_{1\le k\le l:k|n}\phi(k) + 2\sum_{l<k\le n:k|n}\frac{1}{k^2}.$$

Proof. For simplicity let us denote

$$S_1 := \sum_{1\le k\le l:k|n} \phi(k) \quad \text{and} \quad S_2 := \sum_{l<k\le n:k|n} \frac{1}{k^2}.$$

We aim to show

$$\operatorname{disc}(\mathcal{A}_n)^2 \ge \frac{1}{\frac{8}{n}S_1 + 2S_2}. \tag{4.15}$$

Because we always have $\operatorname{disc}(\mathcal{A}_n) \ge 1$, we may assume that $S_1 < \frac{n}{8}$.

Let $\chi : \mathbb{Z}_n \to \{1,-1\}$ be any coloring of $\mathbb{Z}_n$, and let $T_\chi := \max_{A\in\mathcal{A}_n} |\chi(A)|$. Let $m \le n$ be a positive integer to be determined later. By Corollary 4.4, we know that

$$n^2 T_\chi^2 + \sum_{1\le k<m:k|n} \frac{m^2\phi(k)}{k} G_\chi(n/k) \ge \sum_{r\in\mathbb{Z}_n} |\widehat{\chi}(r)|^2 \cdot \max\left(\frac{m^2\cdot\gcd(r,n)}{n}, m\right). \tag{4.16}$$

By Lemma 4.5, we know that

$$\sum_{1\le k\le n:k|n} \frac{m^2\phi(k)}{k} G_\chi(n/k) = \sum_{r\in\mathbb{Z}_n} |\widehat{\chi}(r)|^2 \cdot \frac{m^2\cdot\gcd(r,n)}{n}.$$

Subtract both sides from (4.16). We get

$$n^2 T_\chi^2 + \sum_{r\in\mathbb{Z}_n} |\widehat{\chi}(r)|^2 \cdot \min\left(\frac{m^2\cdot\gcd(r,n)}{n}, m\right) \ge \sum_{r\in\mathbb{Z}_n} |\widehat{\chi}(r)|^2 \cdot m + \sum_{m\le k\le n:k|n} \frac{m^2\phi(k)}{k} G_\chi(n/k). \tag{4.17}$$

Since χ takes value in $\{-1,1\}$, we know that

$$\sum_{r\in\mathbb{Z}_n} |\widehat{\chi}(r)|^2 = nG_\chi(n) = n^2. \tag{4.18}$$

Note that each $G_\chi(\cdot)$ is nonnegative. By (4.18), the right hand side of (4.17) is lower bounded by

$$\sum_{r\in\mathbb{Z}_n} |\widehat{\chi}(r)|^2 \cdot m + \sum_{m\le k\le n:k|n} \frac{m^2\phi(k)}{k} G_\chi(n/k) \ge n^2 m. \tag{4.19}$$

For the left hand side of (4.17), we apply Lemma 4.6 for m and l and get

$$\sum_{r\in\mathbb{Z}_n} |\widehat{\chi}(r)|^2 \cdot \min\left(\frac{m^2\cdot\gcd(r,n)}{n}, m\right) \le \sum_{1\le k\le l:k|n} \frac{m^2\phi(k)}{k} G_\chi(n/k) + \sum_{l<k\le n:k|n} \frac{mn}{k} G_\chi(n/k). \tag{4.20}$$

Note that by definition, each single $g_\chi(a, n/k)$ is the sum of k values of χ. Because χ takes value in $\{-1,1\}$, we have

$$G_\chi(n/k) \le \frac{n}{k}\cdot k^2 = nk. \tag{4.21}$$

Moreover, each $g_\chi(a,n/k)$ is $\chi(A)$ for some $A\in\mathcal{A}_n$, so $|g_\chi(a,n/k)| \le T_\chi$. This means that for all k,

$$G_\chi(n/k) \le \frac{n}{k}\cdot T_\chi^2. \tag{4.22}$$

We bound the first term on the right hand side of (4.20) using (4.21) and get

$$\sum_{1\le k\le l:k|n} \frac{m^2\phi(k)}{k} G_\chi(n/k) \le m^2 n \sum_{1\le k\le l:k|n} \phi(k) = nm^2\cdot S_1. \tag{4.23}$$

On the other hand, we bound the second term on the right hand side of (4.20) using (4.22) and get

$$\sum_{l<k\le n:k|n} \frac{mn}{k} G_\chi(n/k) \le \sum_{l<k\le n:k|n} \frac{mn^2}{k^2} T_\chi^2 = n^2 m T_\chi^2 \cdot S_2. \tag{4.24}$$

Put (4.23) and (4.24) into (4.20). We get

$$\sum_{r\in\mathbb{Z}_n} |\widehat{\chi}(r)|^2 \cdot \min\left(\frac{m^2\cdot \gcd(r,n)}{n}, m\right) \le nm^2 \cdot S_1 + T_\chi^2 n^2 m S_2. \tag{4.25}$$

Finally we put (4.19) and (4.25) into (4.17). We get

$$\left(n^2 + n^2 m S_2\right) T_\chi^2 \ge n^2 m - nm^2 S_1.$$

Dividing both sides by $n^2 m$, we get

$$\left(\frac{1}{m} + S_2\right) T_\chi^2 \ge 1 - \frac{m}{n} S_1. \tag{4.26}$$

Now we pick $m = \lfloor n/(2S_1)\rfloor$. Note that $S_1 < n/8$ from our assumption, so $m \ge \frac{n}{4S_1}$. Therefore,

$$\frac{1}{m} \le \frac{4}{n} S_1 \quad \text{and} \quad 1 - \frac{m}{n} S_1 \ge \frac{1}{2}.$$

Put them into (4.26). We conclude that

$$T_\chi^2 \ge \frac{1 - \frac{m}{n} S_1}{\frac{1}{m} + S_2} \ge \frac{1/2}{\frac{4}{n} S_1 + S_2} = \frac{1}{\frac{8}{n} S_1 + 2S_2}.$$

Since this bound applies to all T_χ^2, it also applies to $(\mathrm{disc}(\mathcal{A}_n))^2 = \min_\chi T_\chi^2$. Hence we have (4.15). □

Remark 4.8. As mentioned earlier in Remark 1.3, the proof above also applies to the case where χ takes value in the unit circle on the complex plane $\{z \in \mathbb{C} : |z| = 1\}$ (instead of $\{1, -1\}$). Just note that (4.18) and (4.21) hold in this more general case as well, and all other steps are identical.

Now we prove two corollaries. The first shows that the upper bound in Theorem 3.1 is tight up to an $n^{o(1)}$ factor.

Corollary 4.9 (Lower bound in Theorem 1.1)**.** *There exists an absolute constant $c > 0$ such that, for any positive integer n,*

$$\mathrm{disc}(\mathcal{A}_n) \ge \frac{1}{8\sqrt{d(n)}} \cdot \min_{r|n}\left(\frac{n}{r} + \sqrt{r}\right),$$

where $d(n)$ is the number of factors of n.

Proof. Let t_1 be the minimum factor of n that is at least $n^{\frac{2}{3}}$, and let t_2 be the maximum factor of n less than $n^{\frac{2}{3}}$. As

$$2 \cdot \min\left(\sqrt{t_1}, \frac{n}{t_2}\right) \ge \min\left(\sqrt{t_1} + \frac{n}{t_1}, \sqrt{t_2} + \frac{n}{t_2}\right) = \min_{r|n}\left(\frac{n}{r} + \sqrt{r}\right),$$

it suffices to show that

$$\mathrm{disc}(\mathcal{A}_n) \ge \frac{1}{4\sqrt{d(n)}} \cdot \min\left(\sqrt{t_1}, \frac{n}{t_2}\right). \tag{4.27}$$

Now we apply Proposition 4.7 to n and $l = \frac{n}{t_1}$. We bound the two summations as follows. We have

$$\sum_{1\le k\le \frac{n}{t_1}:k|n} \phi(k) \le \sum_{1\le k\le \frac{n}{t_1}:k|n} k \le \frac{n}{t_1}\cdot d(n). \tag{4.28}$$

Note that t_2 is the largest factor of n less than t_1, so the minimum k in $\{\frac{n}{t_1} < k \le n : k|n\}$ is n/t_2. Thus we have

$$\sum_{\frac{n}{t_1}<k\le n:k|n} \frac{1}{k^2} \le \sum_{\frac{n}{t_2}\le k\le n:k|n} \frac{1}{k^2} \le \frac{t_2^2}{n^2}\cdot d(n). \tag{4.29}$$

Using above two bounds, we get

$$(\mathrm{disc}(\mathcal{A}_n))^2 \ge \frac{1}{\frac{8}{t_1}d(n) + 2\frac{t_2^2}{n^2}d(n)} \ge \frac{1}{16d(n)}\min\left(t_1, \frac{n^2}{t_2^2}\right).$$

This is equivalent to (4.27), so we have the expected inequality. □

The second corollary proves the lower bound in Theorem 1.2. The main observation is that the factor $d(n)$ can be removed in (4.28) and (4.29) when n is a prime power.

Corollary 4.10 (Lower bound in Theorem 1.2)**.** *Let p be a prime number, and k be a positive integer. Then for $n = p^k$,*

$$\mathrm{disc}(\mathcal{A}_n) \ge \frac{1}{4}p^{\frac{k-\lfloor k/3\rfloor}{2}}. \tag{4.30}$$

Proof. In Proposition 4.7, we pick $l = p^t$ for some $1 \le t < n$ to be determined later. Note that the factors of n between 1 and l are given by $s = p^i$ for $0 \le i \le t$, which are all factors of l. Hence we have

$$\sum_{1\le s\le l:s|n} \phi(s) = l = p^t.$$

All factors of n larger than l are given by $s = p^i$ for $t+1 \le i \le k$. Thus

$$\sum_{l<s\le l:s|n} \frac{1}{s^2} = \sum_{i=t+1}^{k} p^{-2i} \le p^{-2t-2}\cdot\left(1 + \frac{1}{p^2} + \frac{1}{p^4} + \cdots\right) \le 2p^{-2t-2}.$$

Therefore, by Proposition 4.7 we get

$$\mathrm{disc}(\mathcal{A}_n) \ge \sqrt{\frac{1}{8p^{t-k} + 4p^{-2t-2}}} \ge \frac{1}{4}\cdot\min\left(p^{\frac{k-t}{2}}, p^{t+1}\right) = \frac{1}{4}\cdot p^{\min(\frac{k-t}{2}, t+1)}.$$

We pick $t = \lfloor k/3\rfloor$ to get (4.30).

□

5. Concluding Remarks

In Theorem 1.1, the upper and lower bounds are off by a factor of $O(d(n)^{3/2})$. We were not able to close this gap, and it seems that major improvement of either bound would require new observations.

Problem 5.1. *Determine* $\mathrm{disc}(\mathcal{A}_n)$ *up to a constant factor for all n.*

There are other notions of discrepancy besides the one studied in this paper. Among them there is the *hereditary discrepancy*, defined for a system $(\Omega, \mathcal{A})$ as

$$\operatorname{herdisc}(\mathcal{A}) := \max_{X \subseteq \Omega} \operatorname{disc}(\mathcal{A}|_X)$$

where $\mathcal{A}|_X = \{A \cap X : A \in \mathcal{A}\}$. Clearly $\operatorname{disc}(\mathcal{A}) \leq \operatorname{herdisc}(\mathcal{A})$. For the set $\mathcal{A}$ of arithmetic progressions in $[n]$, Matoušek and Spencer [10] proved a stronger statement that $\operatorname{herdisc}(\mathcal{A}) = O(n^{\frac{1}{4}})$. This is because their partial coloring method works not just for $\mathcal{A}$, but also for $\mathcal{A}|_X$ for any $X \subseteq [n]$.

In contrast, our construction of the coloring in Section 3 is only valid for coloring the whole set $\mathbb{Z}_n$. While it can be adapted so that the same upper bound (possibly with a larger constant factor) applies to some special subsets of $\mathbb{Z}_n$, it does not work for all subsets $X \subseteq \mathbb{Z}_n$.

Problem 5.2. *Estimate the hereditary discrepancy of $\mathcal{A}_n$.*

By Corollary 2.3 we have $\operatorname{herdisc}(\mathcal{A}_n) = O(n^{\frac{1}{2}})$. The method used in Section 2 can be adapted to give the following slightly stronger statement. Let $\phi(\cdot)$ be Euler's totient function.

Theorem 5.1. *There exists a constant c such that for all positive integers n, we have*

$$\operatorname{herdisc}(\mathcal{A}_n) \leq c\phi(n)^{\frac{1}{2}} \left(\log \frac{en}{\phi(n)}\right)^{\frac{3}{2}}.$$

We leave the proof of this theorem to the Appendix. It shows that the upper bound $O(n^{\frac{1}{2}})$ is not always tight. It would be interesting to determine if there is a matching lower bound of the form $n^{\frac{1}{2}-o(1)}$.

References

[1] N. Alon and J. H. Spencer, *The probabilistic method*, 4th ed. Wiley, Hoboken, NJ, 2016.

[2] J. Beck, Roth's estimate of the discrepancy of integer sequences is nearly sharp, *Combinatorica* **1** (1981), 319-325.

[3] J. Beck and W. W. L Chen, *Irregularities of distribution*, Cambridge Tracts in Mathematics, 89. Cambridge University Press, Cambridge, 1987.

[4] B. Chazelle, (2000). *The Discrepancy Method: Randomness and Complexity*, Cambridge University Press, New York, 2000.

[5] P. Erdős, and A. Sárközy, Some solved and unsolved problems in combinatorial number theory, *Math. Slovaca* **28** (1978), 407-421.

[6] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 6th ed. Oxford University Press, Oxford, 2008.

[7] N. Hebbinghaus and A. Srivastav, Discrepancy of (centered) arithmetic progressions in $\mathbb{Z}_p$, *European J. Combin.* **35** (2014), 324-334.

[8] E. Landau, Ueber die zahlentheoretische Funktion $\phi(n)$ und ihre Beziehung zum Goldbachschen Satz, *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse* **1900** (1900), 177–186.

[9] J. Matoušek, *Geometric Discrepancy: An Illustrated Guide*, Algorithms Combin. **18**, Springer, Berlin, 1999.

[10] J. Matoušek and J. Spencer, Discrepancy in arithmetic progressions, *J. Amer. Math. Soc.* **9** (1996), 195-204.

[11] K. F. Roth, Remark concerning integer sequences, *Acta Arith.* **9** (1964), 257-260.

[12] T. Tao, The Erdős discrepancy problem, *Discrete Anal.* **1** (2016), 27pp.

[13] H. Weyl, Über die Gleichverteilung von Zahlen mod. Eins. (German) *Math. Ann.* **77** (1916), 313–352.

Appendix A. Improved bound for hereditary discrepancy

In this appendix, we prove Theorem 5.1, an improved upper bound on the hereditary discrepancy of modular arithmetic progressions. We need the following lemma which gives a partial coloring bound.

Lemma A.1. *Let $X \subseteq \mathbb{Z}_n$ be a set of size $m > 0$. There exists an absolute constant c such that there is a partial coloring $\chi : X \to \{-1, 0, 1\}$ that assigns ± 1 to at least $m/10$ elements in X such that*

$$\max_{A \in \mathcal{A}_n} |\chi(A \cap X)| \leq c\phi(n)^{\frac{1}{2}} \left(\log \frac{en}{\phi(n)}\right)^{\frac{1}{2}}.$$

Assuming this lemma, we may now prove Theorem 5.1.

Proof of Theorem 5.1 assuming A.1. Let $X \subseteq \mathbb{Z}_n$ be a set of size m. We show that there exists a coloring $\chi : X \to \{1, -1\}$ such that, for some absolute constant c,

$$\max_{A \in \mathcal{A}_n} |\chi(A \cap X)| \leq c\phi(n)^{\frac{1}{2}} \left(\log \frac{en}{\phi(n)}\right)^{\frac{3}{2}}. \tag{A.1}$$

The idea is that we iteratively apply Lemma A.1 to the set of uncolored elements until there are at most $\phi(n)$ elements left, and then apply Corollary 2.3 to color the remaining elements. Let c_0, c_1 be the constants in Lemma A.1 and Corollary 2.3.

Start with $X_0 = X$. For each $i \geq 0$, we apply Lemma A.1 to X_i to get a partial coloring $\chi_i : X_i \to \{-1, 0, 1\}$, and we let $X_{i+1} = \chi_i^{-1}(0) \subseteq X_i$ to be the set of uncolored elements in i-th iteration. We continue this process until the $(k-1)$-th iteration where there are at most $\phi(n)$ elements left (i.e. $|X_k| \leq \phi(n)$). Then we apply Corollary 2.3 to get a coloring $\chi_k : X_k \to \{-1, 1\}$. Let χ be the final coloring given by $\chi(x_i) = \chi_i(x_i)$ if $x_i \in X_i \setminus X_{i+1}$ for $0 \leq i \leq k-1$, and $\chi(x_k) = \chi_k(x_k)$. We know that $|X_i| \leq 0.9|X_{i-1}|$ for all $1 \leq i \leq k$, so $|X_k| \leq (0.9)^k |X_0| = (0.9)^k m \leq (0.9)^k n$. Because we stop when there are at most $\phi(n)$ elements left, we shall see that $k \leq 1 + \log_{0.9} \frac{m}{n} \leq 10 \log \frac{en}{m}$.

Applying the bounds on the discrepancy of χ_i from Lemma A.1 and Corollary 2.3, we conclude that for any $A \in \mathcal{A}_n$,

$$\begin{aligned}
|\chi(A \cap X)| = \left|\sum_{i=0}^{k} \chi_i(X_i \cap A)\right| &\leq \sum_{i=0}^{k-1} |\chi_i(X_i \cap A)| + |\chi_k(X_k \cap A)| \\
&\leq k \cdot c_0 \phi(n)^{\frac{1}{2}} \left(\log \frac{en}{\phi(n)}\right)^{\frac{1}{2}} + c_1 |X_k|^{\frac{1}{2}} \left(\log \frac{en}{|X_k|}\right)^{\frac{1}{2}} \\
&< 10 c_0 \phi(n)^{\frac{1}{2}} \left(\log \frac{en}{m}\right)^{\frac{3}{2}} + c_1 \phi(n)^{\frac{1}{2}} \left(\log \frac{en}{m}\right)^{\frac{1}{2}} \leq c\phi(n)^{\frac{1}{2}} \left(\log \frac{en}{m}\right)^{\frac{3}{2}}
\end{aligned}$$

for $c = 10c_0 + c_1$ being an absolute constant. Since it holds for all $A \in \mathcal{A}_n$, we have (A.1). □

We are left to prove Lemma A.1. We first need a slight generalization of the partial coloring lemma in Lemma 2.1. In Lemma 2.1 we require $\Delta_S \geq 2\sqrt{|S|}$. Here we allow Δ_S to take any positive value.

Lemma A.2 (Section 4.6 in [9])**.** *Let (V, C) be a set system on n elements, and let a number $\Delta_S > 0$ be given for each set $S \in C$. Suppose that*

$$\sum_{S \in C : S \neq \emptyset} g\left(\frac{\Delta_S}{\sqrt{|S|}}\right) \leq \frac{n}{5} \tag{A.2}$$

where

$$g(\lambda) = \begin{cases} 10e^{-\lambda^2/4} & \text{if } \lambda \geq 2, \\ 10 \log(1 + 2\lambda^{-1}) & \text{if } 0 < \lambda < 2. \end{cases} \tag{A.3}$$

Then there exists a partial coloring χ that assigns ± 1 to at least $n/10$ variables (and 0 to the rest), satisfying $|\chi(S)| \le \Delta_S$ for each $S \in C$.

We now prove Lemma A.1.

Proof of Lemma A.1. We use the same decomposition as in Lemma 2.2 to get the family C_2 of nonempty subsets of X. From the argument in Lemma 2.2, we know that sets in C_2 are of size 2^i for $2^i \le m$. If $\chi : X \to \{-1, 0, 1\}$ is such that for all $0 \le i \le \log_2 m$ we have $\chi(S) \le \Delta_i$ for any set $S \in C_2$ of size 2^i, then

$$\max_{A \in \mathcal{A}_n} |\chi(A \cap X)| \le 4 \sum_{0 \le i \le \log_2 m} \Delta_i. \tag{A.4}$$

Then we apply a better bound on the number of sets in C_2 of size 2^i, which we shall denote as f_i. The notations here are the same as in Lemma 2.2. For each $1 \le d < n$ and $0 \le a < \gcd(d, n)$, the number of choices of t in (2.5) is $\lfloor l_{d,a}/2^i \rfloor$. Yet note that $l_{d,a} \le \frac{n}{\gcd(d,n)}$. Hence if $\gcd(d, n) > \frac{n}{2^i}$, then there are no such sets included in the set $X_{d,a}$. Therefore we have the following better bound on f_i:

$$f_i \le \sum_{1 \le d \le n-1 : \gcd(d,n) \le \frac{n}{2^i}} \sum_{a=0}^{\gcd(d,n)-1} \left\lfloor \frac{l_{d,a}}{2^i} \right\rfloor = \sum_{1 \le d \le n-1 : \gcd(d,n) \le \frac{n}{2^i}} \frac{m}{2^i} \le \sum_{1 \le l \le \frac{n}{2^i} : l \mid n} \phi(n/l) \cdot \frac{m}{2^i}.$$

Because $\phi(ab) \ge \phi(a)\phi(b)$ for all $a, b \in \mathbb{N}$, we know that $\phi(n/l) \le \phi(n)/\phi(l)$ for all l that divides n. Also note that $0 < \phi(n)/\phi(l)$ for all l that does not divide n. By Landau [8, p. 184], for any $x \ge 1$, $\sum_{l \le x} 1/\phi(l) \le c_0 \log ex$ for some absolute constant c_0. Hence we have

$$f_i \le \frac{m}{2^i} \sum_{1 \le l \le \frac{n}{2^i} : l \mid n} \phi(n/l) \le \frac{m}{2^i} \phi(n) \sum_{1 \le l \le \frac{n}{2^i}} \frac{1}{\phi(l)} \le c_0 \frac{m}{2^i} \phi(n) \log \frac{en}{2^i}. \tag{A.5}$$

For simplicity we denote $M = \phi(n) \log \frac{en}{\phi(n)}$. We define $b : (0, n] \to \mathbb{R}$, given by

$$b(s) = \begin{cases} c_1 \sqrt{s} \cdot \left(\frac{s}{M}\right)^{-1} & \text{if } s \ge M, \\ c_1 \sqrt{s} \cdot \left(\frac{s}{M}\right)^{-0.1} & \text{if } s < M, \end{cases} \tag{A.6}$$

where $c_1 > 2$ is an absolute constant to be determined later. We would like to show that there exists a partial coloring that colors at least $m/10$ elements in X, such that for any $S \in C_2$,

$$|\chi(S)| \le b(|S|). \tag{A.7}$$

In order to apply Lemma A.2, it suffices to verify that

$$\sum_{S \in C_2} g\left(\frac{b(s)}{\sqrt{|S|}}\right) = \sum_{i=0}^{\lfloor \log_2 m \rfloor} f_i \cdot g\left(b(2^i) 2^{-i/2}\right) \le m/5. \tag{A.8}$$

For fixed i, we denote $\tau = 2^i/M$, so $2^i = \tau M \ge \tau \phi(n)$. Observe that

$$f_i \le c_0 m \cdot \tau^{-1} \cdot \frac{\log \frac{en}{2^i}}{\log \frac{en}{\phi(n)}} \le c_0 m \tau^{-1} \frac{\log \frac{en}{\tau\phi(n)}}{\log \frac{en}{\phi(n)}} = c_0 m \tau^{-1} \left(1 + \frac{\log \tau^{-1}}{\log \frac{en}{\phi(n)}}\right).$$

When $\tau < 1$, we have $b(2^i) 2^{-i/2} = c_1 \tau^{-0.1}$ and

$$f_i \le c_0 m \tau^{-1} \left(1 + \frac{\log \tau^{-1}}{\log \frac{en}{\phi(n)}}\right) \le c_0 m \tau^{-1} (1 + \log \tau^{-1}).$$

When $\tau \geq 1$, we have $b(2^i)2^{-i/2} = c_1\tau^{-1}$ and

$$f_i \leq c_0 m\tau^{-1}\left(1 + \frac{\log \tau^{-1}}{\log \frac{en}{\phi(n)}}\right) \leq c_0 m\tau^{-1}.$$

Therefore if we write the summation in (A.8) in terms of τ, we have

$$\sum_{i=0}^{\lfloor \log_2 m \rfloor} f_i \cdot g\left(b(2^i)2^{-i/2}\right) = c_0 m\left(\sum_{\tau \geq 1} \tau^{-1} g(c_1\tau^{-1}) + \sum_{\tau<1} \tau^{-1}(1+\log \tau^{-1}) g(c_1\tau^{-0.1})\right), \tag{A.9}$$

where the summation of τ is over a geometric sequence with ratio 2. By definition of g in (A.3), g is monotonically decreasing. Let T be a large absolute constant to be determined later. We have

$$\sum_{\tau \geq T} \tau^{-1} g(c_1\tau^{-1}) \leq \sum_{\tau \geq T} \tau^{-1} g(2\tau^{-1}) = \sum_{\tau \geq T} \tau^{-1} \cdot 10 \log(1+\tau).$$

Since $\sum_{\tau \geq 1} \tau^{-1} \cdot 10\log(1+\tau)$ converges, there exists sufficiently large constant T satisfying

$$\sum_{\tau \geq T} \tau^{-1} g(c_1\tau^{-1}) \leq \frac{1}{20c_0}. \tag{A.10}$$

We bound the second term on the right hand side of (A.9) similarly. We have

$$\sum_{\tau<T^{-1}} \tau^{-1}(1+\log \tau^{-1}) g(c_1\tau^{-0.1}) \leq \sum_{\tau<T^{-1}} \tau^{-1}(1+\log \tau^{-1}) g(2\tau^{-0.1}) = \sum_{\tau<T^{-1}} \tau^{-1}(1+\log \tau^{-1}) \cdot 10 e^{-\tau^{-0.2}}.$$

Since $\sum_{\tau<1} \tau^{-1}(1+\log \tau^{-1}) \cdot 10 e^{-\tau^{-0.2}}$ converges, there exists sufficiently large constant T satisfying

$$\sum_{\tau<T^{-1}} \tau^{-1}(1+\log \tau^{-1}) g(c_1\tau^{-0.1}) \leq \frac{1}{20c_0}. \tag{A.11}$$

Hence, there exists constant T such that whenever $c_1 > 2$, (A.10) and (A.11) hold. Note that there are at most $(1+\log_2 T)$ terms in each of the ranges $1 \leq \tau < T$ and $T^{-1} \leq \tau < 1$, and that $g(x)$ is monotonically decreasing and tends to zero as x goes to infinity. We can choose $c_1 > 2$ sufficiently large so that

$$\sum_{1 \leq \tau < T} \tau^{-1} g(c_1\tau^{-1}) \leq (1+\log_2 T) \cdot g(c_1 T^{-1}) \leq \frac{1}{20c_0} \tag{A.12}$$

and

$$\sum_{T^{-1} \leq \tau < 1} \tau^{-1}(1+\log \tau^{-1}) g(c_1\tau^{-0.1}) \leq (1+\log_2 T) \cdot T(1+\log T) g(c_1) \leq \frac{1}{20c_0}. \tag{A.13}$$

Combining inequalities (A.10), (A.11), (A.12) and (A.13), there exists a constant c_1 such that

$$\sum_{\tau \geq 1} \tau^{-1}(1+\log \tau) g(c_1\tau^{-1}) + \sum_{\tau<1} \tau^{-1} g(c_1\tau^{-0.1}) \leq \frac{1}{5c_0}. \tag{A.14}$$

We use this constant c_1 to define the function $b(\cdot)$ in (A.6). Combining (A.9) and (A.14), we have

$$\sum_{i=0}^{\lfloor \log_2 m \rfloor} f_i \cdot g\left(b(2^i)2^{-i/2}\right) \leq c_0 m \cdot \frac{1}{5c_0} = \frac{m}{5}.$$

Therefore (A.8) holds. By Lemma A.2, there exists a partial coloring $\chi : X \to \{-1, 0, 1\}$ that assigns ± 1 to at least $m/10$ elements in X such that (A.7) holds. For this coloring χ, we may choose $\Delta_i = b(2^i)$ in (A.4). Again we denote $\tau = 2^i/M$, or equivalently $2^i = \tau M$. We have

$$\Delta_i = b(2^i) = \begin{cases} c_1\sqrt{M} \cdot \tau^{-0.5} & \text{if } \tau \geq 1, \\ c_1\sqrt{M} \cdot \tau^{0.4} & \text{if } \tau < 1. \end{cases}$$

Put this in (A.4). We know that χ satisfies that

$$\max_{A \in \mathcal{A}_n} |\chi(A \cap X)| \leq 4 \sum_{0 \leq i \leq \log_2 m} \Delta_i = 4c_1\sqrt{M} \left(\sum_{\tau \geq 1} \tau^{-0.5} + \sum_{\tau < 1} \tau^{0.4} \right).$$

Note that summation of τ is over a geometric sequence with ratio 2. Hence we have

$$\sum_{\tau \geq 1} \tau^{-0.5} \leq \frac{1}{1 - 2^{-0.5}} \quad \text{and} \quad \sum_{\tau < 1} \tau^{0.4} \leq \frac{1}{1 - 2^{-0.4}}.$$

Therefore we conclude that we can find χ that assigns ± 1 to at least $m/10$ elements in X and satisfies

$$\max_{A \in \mathcal{A}_n} |\chi(A \cap X)| \leq 4c_1\sqrt{M} \left(\frac{1}{1 - 2^{-0.5}} + \frac{1}{1 - 2^{-0.4}} \right) \leq c\sqrt{M} = c\phi(n)^{\frac{1}{2}} \left(\log \frac{en}{\phi(n)} \right)^{\frac{1}{2}}$$

for some appropriate absolute constant c. □

Department of Mathematics, Stanford University, Stanford, CA, USA

Email address: {jacobfox,maxxu,yunkunzhou}@stanford.edu