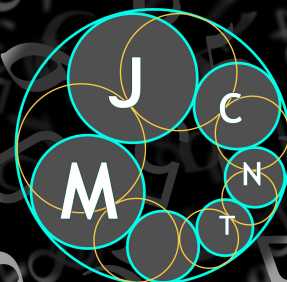


# Moscow Journal of Combinatorics and Number Theory

2020  
vol. 9 no. 1

3  
3  
3  
3  
3



# Moscow Journal of Combinatorics and Number Theory

msp.org/moscow

## EDITORS-IN-CHIEF

- Yann Bugeaud    Université de Strasbourg (France)  
bugaud@math.unistra.fr
- Nikolay Moshchevitin    Lomonosov Moscow State University (Russia)  
moshchevitin@gmail.com
- Andrei Raigorodskii    Moscow Institute of Physics and Technology (Russia)  
mraigor@yandex.ru
- Ilya D. Shkredov    Steklov Mathematical Institute (Russia)  
ilya.shkredov@gmail.com

## EDITORIAL BOARD

- Iskander Aliev    Cardiff University (United Kingdom)
- Vladimir Dolnikov    Moscow Institute of Physics and Technology (Russia)
- Nikolay Dolbilin    Steklov Mathematical Institute (Russia)
- Oleg German    Moscow Lomonosov State University (Russia)
- Michael Hoffman    United States Naval Academy
- Grigory Kabatiansky    Russian Academy of Sciences (Russia)
- Roman Karasev    Moscow Institute of Physics and Technology (Russia)
- Gyula O. H. Katona    Hungarian Academy of Sciences (Hungary)
- Alex V. Kontorovich    Rutgers University (United States)
- Maxim Korolev    Steklov Mathematical Institute (Russia)
- Christian Krattenthaler    Universität Wien (Austria)
- Antanas Laurinčikas    Vilnius University (Lithuania)
- Vsevolod Lev    University of Haifa at Oranim (Israel)
- János Pach    EPFL Lausanne (Switzerland) and Rényi Institute (Hungary)
- Rom Pinchasi    Israel Institute of Technology – Technion (Israel)
- Alexander Razborov    Institut de Mathématiques de Luminy (France)
- Joël Rivat    Université d'Aix-Marseille (France)
- Tanguy Rivoal    Institut Fourier, CNRS (France)
- Damien Roy    University of Ottawa (Canada)
- Vladislav Salikhov    Bryansk State Technical University (Russia)
- Tom Sanders    University of Oxford (United Kingdom)
- Alexander A. Sapozhenko    Lomonosov Moscow State University (Russia)
- József Solymosi    University of British Columbia (Canada)
- Andreas Strömbergsson    Uppsala University (Sweden)
- Benjamin Sudakov    University of California, Los Angeles (United States)
- Jörg Thuswaldner    University of Leoben (Austria)
- Kai-Man Tsang    Hong Kong University (China)
- Maryna Viazovska    EPFL Lausanne (Switzerland)
- Barak Weiss    Tel Aviv University (Israel)

## PRODUCTION

- Silvio Levy    (Scientific Editor)  
production@msp.org

Cover design: Blake Knoll, Alex Scorpan and Silvio Levy

See inside back cover or [msp.org/moscow](http://msp.org/moscow) for submission instructions.

The subscription price for 2020 is US \$310/year for the electronic version, and \$365/year (+\$20, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Moscow Journal of Combinatorics and Number Theory (ISSN 2640-7361 electronic, 2220-5438 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

MJCNT peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY  
 **mathematical sciences publishers**  
nonprofit scientific publishing  
<http://msp.org/>  
© 2020 Mathematical Sciences Publishers

## Complete generalized Fibonacci sequences modulo primes

Mohammad Javaheri and Nikolai A. Krylov

We study generalized Fibonacci sequences  $F_{n+1} = PF_n - QF_{n-1}$  with initial values  $F_0 = 0$  and  $F_1 = 1$ . Let  $P, Q$  be relatively prime nonzero integers such that  $P^2 - 4Q$  is not a perfect square. We show that if  $Q = \pm 1$  then the sequence  $\{F_n\}_{n=0}^{\infty}$  misses a congruence class modulo every large enough prime. If  $Q \neq \pm 1$ , we prove under the GRH that the sequence  $\{F_n\}_{n=0}^{\infty}$  hits every congruence class modulo infinitely many primes.

### 1. Introduction

A generalized Fibonacci sequence with integer parameters  $(P, Q)$  is a second-order homogeneous difference equation generated by

$$F_{n+1} = PF_n - QF_{n-1}, \quad (1)$$

$n \geq 1$ , with initial values  $F_0 = 0$  and  $F_1 = 1$ ; we denote this sequence by  $F = [P, Q]$ . In this paper, we are interested in studying the completeness problem for generalized Fibonacci sequences modulo primes.

**Definition 1.** A sequence  $\{F_n\}_{n=0}^{\infty}$  is said to be complete modulo a prime  $p$  if the map  $\epsilon: \mathbb{N}_0 \rightarrow \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$  defined by  $\epsilon(n) = F_n + p\mathbb{Z}$  is onto. In other words, the sequence is complete modulo  $p$  if and only if

for all  $k \in \mathbb{Z}$ , there exists  $n \geq 0$  such that  $F_n \equiv k \pmod{p}$ .

The completeness problem for the Fibonacci sequence (with parameters  $P = 1$  and  $Q = -1$ ) was first studied by Shah [1968], who showed that the Fibonacci sequence is not complete modulo primes  $p \equiv 1, 9 \pmod{10}$ . Bruckner [1970] proved that the Fibonacci sequence is not complete modulo every prime  $p > 7$ . Somer [1988] proved that if  $p \nmid (P^2 + 4)$  then  $[P, -1]$  is not complete modulo  $p$  for every  $p > 7$  with  $p \not\equiv 1, 9 \pmod{20}$ , and Schinzel [1990] improved Somer's result for all other congruence classes; see also [Li 2000].

A primitive root modulo a prime  $p$  is any integer that generates the multiplicative group modulo  $p$ . Li [2000, Proposition 4.4] showed that if  $Q$  is a primitive root modulo prime  $p$  and  $P^2 - 4Q$  is not a quadratic residue modulo  $p$ , then  $[P, Q]$  is complete modulo  $p$  (we improve Li's result in Theorem 8). Artin's conjecture states that if  $Q \neq -1$  and  $Q$  is not a perfect square, then  $Q$  is a primitive root modulo infinitely many primes. It follows, as Somer [1988, Theorem 3] remarks, that if  $Q \neq -1$  and  $Q$  is not a perfect square, and if Artin's conjecture is correct, then there exist infinitely many primes  $p$  for which an integer  $P$  (depending on  $p$ ) exists such that  $[P, Q]$  is complete modulo  $p$ . In our main Theorem 2, under the GRH (which implies Artin's conjecture, as shown in [Hooley 1967]), we establish a dichotomy regarding completeness modulo infinitely many primes.

MSC2010: primary 11B39; secondary 11B50.

Keywords: generalized Fibonacci sequence, complete sequence.

**Theorem 2.** *Let  $P, Q$  be relatively prime nonzero integers and suppose that  $P^2 - 4Q$  is not a perfect square. Then the following statements hold.*

- (i) *If  $Q = \pm 1$  then  $[P, Q]$  is complete modulo only finitely many primes.*
- (ii) *(GRH) If  $Q \neq \pm 1$ , then  $[P, Q]$  is complete modulo infinitely many primes.*

To prove Theorem 2, we first show that if (a)  $P^2 - 4Q$  is a quadratic nonresidue modulo a prime  $p$  and (b)  $Q$  is either a primitive root or the square of a primitive root modulo  $p$ , then  $[P, Q]$  is complete modulo  $p$  (see Theorem 8). Condition (a) can be guaranteed by a congruence condition on  $p$ . A careful use of a theorem by Lenstra [1977a, Theorem 5.1] on primitive roots modulo primes in an arithmetic progression will allow us to find infinitely many primes  $p$  for which both conditions (a) and (b) are satisfied. Lenstra's theorem (which we will restate for convenience as Theorem 9) is a conditional result, and so our proof of part (ii) of Theorem 2 is conditional upon the GRH.

In case (ii) of Theorem 2, one can find (under the GRH) a lower bound for the counting function for primes  $p$  such that  $[P, Q]$  is complete modulo  $p$ . Let  $\Lambda(x; P, Q)$  denote the set of primes  $p \leq x$  such that  $[P, Q]$  is complete modulo  $p$ . If  $Q \neq \pm 1$  and  $P^2 - 4Q$  is not a perfect square, then for all  $x$  large enough

$$\#\Lambda(x; P, Q) \geq \eta(P, Q) \frac{x}{\log x},$$

where  $\eta(P, Q) > 0$  is computable in terms of  $P$  and  $Q$ . For a more detailed discussion, see the end of Section 3.

**Organization of paper.** In Section 2, we briefly discuss the cases when  $PQ = 0$  or  $P^2 - 4Q$  is a perfect square. As we stated before, Schinzel [1990] proved part (i) of Theorem 2 for the case  $Q = -1$ . We prove part (i) for the case  $Q = 1$  in Section 3, where we show that  $[P, 1]$  is complete modulo a prime  $p > 3$  if and only if  $P \equiv \pm 2 \pmod{p}$  (Theorem 7).

In Section 3, we prove part (ii) of Theorem 2 (see Lemmas 10, 12, and 13). In addition, we show that under certain conditions (that conditionally hold for infinitely many primes), the sequence  $[P, Q]$  is somewhat uniformly distributed modulo  $p$  in the sense that it contains every nonzero element the same number of times over the full period (see Theorem 8 for details).

Finally, in Section 4, we consider complete generalized Fibonacci sequences with parameters  $(P, Q) \in \{1, \dots, p-1\}^2$  for a fixed prime  $p$  and derive the following asymptotic result.

**Theorem 3.** *Let  $\Lambda_p$  denote the set of pairs  $(P, Q) \in \{1, \dots, p-1\}^2$  such that  $[P, Q]$  is complete modulo  $p$ . Then*

$$\limsup_{p \rightarrow \infty} \frac{|\Lambda_p|}{p^2} = \frac{1}{2}.$$

## 2. Preliminary results

Let  $P, Q$  be integers. By a simple induction, one can show that the solution  $F = [P, Q]$  of (1) can be written as the following analog of Binet's formula [Elaydi 2005, §2.3]:

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{for all } n \geq 0, \tag{2}$$

where

$$\alpha = \frac{1}{2}(P + \sqrt{\Delta}), \quad \beta = \frac{1}{2}(P - \sqrt{\Delta}) \quad (3)$$

are the roots of the characteristic polynomial  $x^2 - Px + Q$ , and  $\Delta = P^2 - 4Q \neq 0$  is its discriminant. One has

$$\alpha + \beta = P, \quad \alpha\beta = Q. \quad (4)$$

The difference equation (1) has the following generalization which follows from (2) and (4) by a straightforward calculation:

$$F_n = F_a F_{n+1-a} - Q F_{a-1} F_{n-a} \quad \text{for all } n \geq 1, \text{ for all } a \in \{1, \dots, n\}. \quad (5)$$

Given a prime  $p > 2$ , let  $\widehat{F} \in \{0, \dots, p-1\}$  denote the residue class of an integer  $F$  modulo  $p$ . As we will see later in this section, where we discuss the three cases for the discriminant  $\Delta$ , the sequence  $\{\widehat{F}_n\}_{n=0}^{\infty}$  modulo  $p$  is a periodic sequence unless  $P \equiv Q \equiv 0 \pmod{p}$ . A period of  $[P, Q]$  modulo  $p$  is an integer  $n$  such that  $F_{n+k} \equiv F_k \pmod{p}$  for all  $k \geq 0$ . The *Pisano period*  $\pi(p)$  is the smallest period of  $[P, Q]$  modulo  $p$ , and it divides every period of  $[P, Q]$ . We call the finite sequence  $\{\widehat{F}_i : 1 \leq i \leq \pi(p)\}$  the *full period* of  $[P, Q]$  modulo  $p$ .

**Example 4.** Let  $P = 1$ ,  $Q = 4$ , and  $p = 7$ . Then  $\pi(p) = 24$  and

$$\{\widehat{F}_i : 1 \leq i \leq 24\} = \{1, 1, 4, 0, 5, 5, 6, 0, 4, 4, 2, 0, 6, 6, 3, 0, 2, 2, 1, 0, 3, 3, 5, 0\}$$

is the full period of  $[P, Q]$  modulo  $p = 7$ .

Regarding the discriminant  $\Delta$ , there are three cases.

(I)  $\Delta$  is a nonzero quadratic residue modulo  $p$ . In this case, the characteristic polynomial  $x^2 - Px + Q$  has two distinct roots modulo  $p$  that we again denote by  $\alpha$  and  $\beta$ . Binet's formula (2) still holds, where all the operations involved are carried out in the field  $\mathbb{Z}_p$ . By Fermat's little theorem, we have

$$F_{n+p-1} = \frac{\alpha^{n+p-1} - \beta^{n+p-1}}{\alpha - \beta} = \frac{\alpha^n - \beta^n}{\alpha - \beta} = F_n$$

in  $\mathbb{Z}_p$ . It follows that  $\pi(p) \mid (p-1)$ ; hence the sequence  $[P, Q]$  is not complete modulo  $p$  in this case.

(II)  $\Delta \equiv 0 \pmod{p}$ . In this case, the characteristic polynomial  $x^2 - Px + Q$  has the repeated root  $\alpha = \beta = \frac{1}{2}P$ . A simple induction shows

$$F_n \equiv n\left(\frac{1}{2}P\right)^{n-1} \quad \text{for all } n \geq 1. \quad (6)$$

If  $P \not\equiv 0 \pmod{p}$ , by letting  $n = (p-1)k + 1$  for an arbitrary integer  $k$  and using Fermat's little theorem again, we conclude that  $F_n \equiv -k + 1 \pmod{p}$ ; hence  $[P, Q]$  is complete modulo  $p$ . If  $P \equiv 0 \pmod{p}$ , then  $Q \equiv 0 \pmod{p}$ , and the sequence  $[P, Q]$  modulo  $p$  becomes  $0, 1, 0, 0, \dots$ , which is complete modulo  $p$  only if  $p = 2$ .

(III)  $\Delta$  is a quadratic nonresidue modulo  $p$ . We consider the field extension

$$\mathbb{F}_{p^2} = \{a + b\sqrt{\Delta} : a, b \in \mathbb{Z}_p\}.$$

Binet's formula (2) still holds with all the operations carried out in the field  $\mathbb{F}_{p^2}$ . Given an element  $\gamma \in \mathbb{F}_{p^2}$ , the order of  $\gamma$ , denoted by  $\text{ord}_p(\gamma)$  is the smallest positive integer  $t$  such that  $\gamma^t = 1$ . In

particular, if  $\gamma \in \mathbb{Z}_p$ , then  $\text{ord}_p(\gamma) \mid (p-1)$ . Generally  $\text{ord}_p(\gamma) \mid (p^2-1)$  since the multiplicative group  $\mathbb{F}_{p^2}^*$  has order  $p^2-1$ . In particular, for  $\alpha, \beta$  defined by (3), one has  $\alpha^{p^2-1} = \beta^{p^2-1} = 1$  in  $\mathbb{F}_{p^2}$ , and so  $F_{n+p^2-1} \equiv F_n \pmod{p}$  by Binet's formula (2). Therefore,  $\pi(p) \mid (p^2-1)$ , which is improved in the following lemma.

**Lemma 5.** *Suppose that  $P, Q$  are integers and  $p$  is an odd prime such that  $\Delta = P^2 - 4Q$  is a quadratic nonresidue modulo  $p$ . Let  $\alpha, \beta$  be the roots of  $x^2 - Px + Q = 0$  in  $\mathbb{F}_{p^2}$  given by (3). Then*

(i)  $\alpha^{p+1} = \beta^{p+1} = Q$  in  $\mathbb{F}_{p^2}$ .

(ii)  $\pi(p) \mid (p+1) \text{ord}_p(Q)$ . Moreover, if  $\text{ord}_p(Q)$  is even, then  $(p+1) \text{ord}_p(Q) / \pi(p)$  is an odd integer.

*Proof.* (i) Let  $\alpha = u + v\sqrt{\Delta}$ , where  $u = \frac{1}{2}P$ ,  $v = \frac{1}{2}$ . We note that  $(\sqrt{\Delta})^{p+1} = \Delta^{(p-1)/2} \Delta = -\Delta$  by Euler's criterion. It follows from the binomial theorem modulo  $p$  and Fermat's little theorem that

$$\begin{aligned} \alpha^{p+1} &= u^{p+1} + u^p v \sqrt{\Delta} + uv^p (\sqrt{\Delta})^p + v^{p+1} (\sqrt{\Delta})^{p+1} \\ &= u^2 + uv\sqrt{\Delta} - uv\sqrt{\Delta} - v^2 \Delta \\ &= u^2 - v^2 \Delta = \frac{1}{4}P^2 - \frac{1}{4}(P^2 - 4Q) = Q, \end{aligned}$$

where all of the operations are carried out in the field  $\mathbb{F}_{p^2}$ . Similarly,  $\beta^{p+1} = Q$  in  $\mathbb{F}_{p^2}$ .

(ii) Let  $t = \text{ord}_p(Q)$  such that  $Q^t \equiv 1 \pmod{p}$ . It follows from part (i) that  $\alpha^{(p+1)t} = \beta^{(p+1)t} = Q^t = 1$ , and so  $F_{(p+1)t+k} \equiv F_k \pmod{p}$  for all  $k \geq 0$ , which implies  $\pi(p) \mid (p+1)t$ .

If  $t$  is even, then  $\alpha^{(p+1)t/2} = \beta^{(p+1)t/2} = Q^{t/2} = -1$ . It follows again from Binet's formula (2) that  $F_{(p+1)t/2+k} = -F_k$  for all  $k \geq 0$ . In particular,  $\pi(p) \nmid \frac{1}{2}(p+1)t$ , and therefore,  $(p+1)t / \pi(p)$  is odd.  $\square$

In the rest of this section, we briefly discuss the cases when  $PQ = 0$  or  $P^2 - 4Q$  is a perfect square.

(i)  $P = 0$ . Then  $F_{2k} = 0$  and  $F_{2k+1} = (-Q)^k$  for all  $k \geq 0$ . Therefore,  $[0, Q]$  is complete modulo  $p > 2$  if and only if  $-Q$  is a primitive root modulo  $p$ .

(ii)  $Q = 0$ . Then  $F_n = P^n$  for all  $n \geq 1$ . Therefore,  $[P, 0]$  is complete modulo  $p > 2$  if and only if  $P$  is a primitive root modulo  $p$ .

(iii)  $P^2 - 4Q = 0$ . If  $P \equiv 0 \pmod{p}$ , the sequence is clearly not complete modulo  $p > 2$ . If  $P \not\equiv 0 \pmod{p}$ , then the sequence  $F = [P, Q]$  satisfies (6); hence it is complete modulo  $p$  as shown earlier in case II.

(iv)  $P^2 - 4Q$  is a nonzero perfect square. Then by Binet's formula (2) and Fermat's little theorem, the sequence  $[P, Q]$  is not complete modulo  $p$  for all primes  $p$  greater than the largest prime factor of  $\Delta$ , as shown earlier in case I.

Therefore, we have the following corollary of Theorem 2.

**Corollary 6.** (GRH) *Let  $P, Q$  be relatively prime integers. Then the sequence  $[P, Q]$  is complete modulo infinitely many primes if and only if one of the following statements is true:*

(i)  $P \neq 0$  and  $P^2 - 4Q = 0$ .

(ii)  $Q = 0$  and  $P \neq \pm 1$  and  $P$  is not a perfect square.

(iii)  $Q \neq \pm 1$  and  $P^2 - 4Q$  is not a perfect square.

### 3. Proof of the main theorem

First, we consider generalized Fibonacci sequences  $[P, 1]$ .

**Theorem 7.** *Let  $P$  be an integer and  $p > 3$  be a prime. Then the sequence  $[P, 1]$  is complete modulo  $p$  if and only if  $P \equiv \pm 2 \pmod{p}$ .*

*Proof.* If  $P^2 - 4$  is zero or a nonzero quadratic residue modulo  $p$ , the claim follows from our analysis of the three cases (I)–(III) in Section 2. Thus, suppose that  $P^2 - 4$  is a quadratic nonresidue modulo  $p$  and  $F = [P, 1]$  is complete modulo  $p$ , and we derive a contradiction. It follows from part (i) of Lemma 5 that in this case  $\alpha^{p+1} = \beta^{p+1} = 1$ . Therefore, for  $r = \frac{1}{2}(p+1)$ , we have  $\alpha^r, \beta^r \in \{1, -1\}$ . Since  $\alpha\beta = Q = 1$ , one has  $\alpha^r \beta^r = (\alpha\beta)^r = 1$ ; hence  $\alpha^r = \beta^r \in \{1, -1\}$ . If  $\alpha^r = \beta^r = 1$ , then  $F_{r+n} \equiv F_n \pmod{p}$  for all  $n \geq 0$ ; hence  $\pi(p) \mid r$  and so the sequence  $[P, 1]$  is not complete modulo  $p$ . Therefore, suppose that  $\alpha^r = \beta^r = -1$ . Then for all  $n \geq 0$ ,

$$F_{r+n} = \frac{\alpha^{r+n} - \beta^{r+n}}{\alpha - \beta} = \frac{-\alpha^n + \beta^n}{\alpha - \beta} = -F_n$$

in  $\mathbb{Z}_p$ . In particular, by our assumption that  $[P, 1]$  is complete, we must have  $\{\pm F_1, \dots, \pm F_{r-1}\} = \{1, \dots, p-1\}$  modulo  $p$ . It follows that

$$F_1^2 + \dots + F_{r-1}^2 \equiv 1^2 + \dots + (r-1)^2 \equiv 0 \pmod{p} \quad (7)$$

for  $p > 3$ . On the other hand,

$$\begin{aligned} \sum_{i=1}^{r-1} F_i^2 &= \frac{1}{(\alpha - \beta)^2} \sum_{i=1}^{r-1} (\alpha^i - \beta^i)^2 \\ &= \frac{1}{(\alpha - \beta)^2} \left( \frac{\alpha^{2r} - \alpha^2}{\alpha^2 - 1} - 2 \sum_{i=1}^{r-1} Q^i + \frac{\beta^{2r} - \beta^2}{\beta^2 - 1} \right) \\ &= \frac{1}{\Delta} \left( -2 - 2 \sum_{i=1}^{r-1} 1 \right) = -\frac{1}{\Delta}, \end{aligned}$$

which contradicts (7). □

Part (i) of Theorem 2 follows from Schinzel's result [1990] for  $Q = -1$  and from Theorem 7 for  $Q = 1$ . Note that Theorem 7 implies that if  $\Delta = P^2 - 4 \neq 0$  then  $[P, 1]$  is not complete modulo any  $p \geq |P| + 3$ .

The *rank of apparition*  $\mu = \mu(p)$  is the smallest positive integer  $n$  such that  $F_n \equiv 0 \pmod{p}$ , or equivalently  $\alpha^n = \beta^n$  in  $\mathbb{F}_{p^2}$ . If  $\alpha^m = \beta^m$  in  $\mathbb{F}_{p^2}$  for an integer  $m$ , then  $\mu \mid m$ . One can arrange the full period  $\{\widehat{F}_i : 1 \leq i \leq \pi(p)\}$  in a  $(\pi/\mu) \times \mu$  matrix, where the  $ij$ -th entry is given by  $\widehat{F}_{(i-1)\mu+j}$ ,  $1 \leq i \leq \pi/\mu$ ,  $1 \leq j \leq \mu$ ; We call this matrix the *period matrix* of  $[P, Q]$  modulo  $p$ . Since  $F_t \equiv 0 \pmod{p}$  if and only if  $\mu \mid t$ , the last column of the period matrix is a zero column and all other entries are nonzero modulo  $p$ . It follows that 0 appears exactly  $\pi/\mu$  times in the full period.

In Theorem 8, we show that if  $Q$  is a primitive root or the square of a primitive root modulo  $p$ , then every nonzero element appears the same number of times in the full period. As an illustration, consider

the following two examples. First, let  $(P, Q) = (12, 5)$  and  $p = 19$ . In this case  $\mu(19) = 5$ ,  $\text{ord}_{19}(5) = 9$ ,  $\pi(19) = 45$ , and  $u = \alpha^5 = 103566 + 18601\sqrt{31} \equiv 16 \pmod{19}$ . The period matrix is given by

$$\begin{pmatrix} 1 & 12 & 6 & 12 & 0 \\ 16 & 2 & 1 & 2 & 0 \\ 9 & 13 & 16 & 13 & 0 \\ 11 & 18 & 9 & 18 & 0 \\ 5 & 3 & 11 & 3 & 0 \\ 4 & 10 & 5 & 10 & 0 \\ 7 & 8 & 4 & 8 & 0 \\ 17 & 14 & 7 & 14 & 0 \\ 6 & 15 & 17 & 15 & 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 16 \\ 9 \\ 11 \\ 5 \\ 4 \\ 7 \\ 17 \\ 6 \end{pmatrix} (1 \ 12 \ 6 \ 12 \ 0) \pmod{19}.$$

The first and the third columns of the period matrix list exactly all of the nonzero quadratic residues modulo 19, while the second and the fourth columns list exactly all of the quadratic nonresidues modulo 19. In particular, each nonzero element in the period matrix is repeated exactly two times.

Next, let  $(P, Q) = (1, 4)$  and  $p = 13$ . Then  $\text{ord}_{13}(4) = 6$ ,  $\pi(13) = 84$ , and  $\mu(13) = 7$ . The period matrix in this case is given by

$$\begin{pmatrix} 1 & 1 & 10 & 6 & 5 & 7 & 0 \\ 11 & 11 & 6 & 1 & 3 & 12 & 0 \\ 4 & 4 & 1 & 11 & 7 & 2 & 0 \\ 5 & 5 & 11 & 4 & 12 & 9 & 0 \\ 3 & 3 & 4 & 5 & 2 & 8 & 0 \\ 7 & 7 & 5 & 3 & 9 & 10 & 0 \\ 12 & 12 & 3 & 7 & 8 & 6 & 0 \\ 2 & 2 & 7 & 12 & 10 & 1 & 0 \\ 9 & 9 & 12 & 2 & 6 & 11 & 0 \\ 8 & 8 & 2 & 9 & 1 & 4 & 0 \\ 10 & 10 & 9 & 8 & 11 & 5 & 0 \\ 6 & 6 & 8 & 10 & 4 & 3 & 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 11 \\ 4 \\ 5 \\ 3 \\ 7 \\ 12 \\ 2 \\ 9 \\ 8 \\ 10 \\ 6 \end{pmatrix} (1 \ 1 \ 10 \ 6 \ 5 \ 7 \ 0) \pmod{13},$$

where each nonzero entry is repeated six times.

**Theorem 8.** *Let  $p$  be an odd prime such that  $p \nmid P$  and  $P^2 - 4Q$  is a quadratic nonresidue modulo  $p$ . Suppose that  $\text{ord}_p(Q) = (p-1)/k$  for some  $k \in \{1, 2\}$ . Then the generalized Fibonacci sequence  $[P, Q]$  is complete modulo  $p$ . More precisely, the following statements hold:*

- (a) *If  $p \equiv 1 \pmod{4}$ , or  $p \equiv 3 \pmod{4}$  and  $\mu(p)$  is even, then zero appears in the full period  $\{\widehat{F}_i : 1 \leq i \leq \pi(p)\}$  exactly  $p-1$  times, while each nonzero element of  $\mathbb{Z}_p$  appears exactly  $\mu-1$  times.*
- (b) *If  $p \equiv 3 \pmod{4}$  and the rank of apparition  $\mu$  is odd, then*
  - (i) *either zero appears in the full period exactly  $p-1$  times, while each nonzero element of  $\mathbb{Z}_p$  appears  $\mu-1$  times, or*
  - (ii) *zero appears in the full period exactly  $\frac{1}{2}(p-1)$  times, while each nonzero element of  $\mathbb{Z}_p$  appears exactly  $\frac{1}{2}(\mu-1)$  times.*

*Proof.* (a) Let  $u = \alpha^\mu = F_{\mu+1} \in \mathbb{Z}_p$ . We first show that  $u$  is a primitive root modulo  $p$ . Since  $F_{p+1} = (\alpha^{p+1} - \beta^{p+1})/(\alpha - \beta) = 0$  by Lemma 5, we have  $\mu \mid (p+1)$ . Let  $l = (p+1)/\mu$ , and so  $u^l = Q$  in  $\mathbb{F}_{p^2}$ . If  $k = 1$ , then  $Q$  is a primitive root modulo  $p$ ; hence  $u$  is a primitive root modulo  $p$ . Thus, suppose that  $k = 2$ ; hence  $Q$  is a quadratic residue modulo  $p$ . It follows from  $u^l = Q$  that  $\text{ord}_p(u) = p-1$  or  $\frac{1}{2}(p-1)$ . Since  $(\alpha^{(p+1)/2})^2 = Q$ , and  $Q$  is a quadratic residue, we must have  $\alpha^{(p+1)/2} \in \mathbb{Z}_p \subseteq \mathbb{F}_{p^2}$ . Similarly  $\beta^{(p+1)/2} \in \mathbb{Z}_p$ . Therefore, either  $\alpha^{(p+1)/2} = \beta^{(p+1)/2}$  or  $\alpha^{(p+1)/2} = -\beta^{(p+1)/2}$ . If  $\alpha^{(p+1)/2} = -\beta^{(p+1)/2}$ , we have  $F_{(p+3)/2} = \alpha^{(p+1)/2} P/(\alpha - \beta) \in \mathbb{Z}_p$ , which is a contradiction since  $P \not\equiv 0$  modulo  $p$  and  $\alpha - \beta = \sqrt{\Delta} \notin \mathbb{Z}_p$ . Therefore, we have  $\alpha^{(p+1)/2} = \beta^{(p+1)/2}$ , and so  $\mu \mid \frac{1}{2}(p+1)$ . There are two cases.

Case 1. If  $p \equiv 1 \pmod{4}$ , then it follows from  $\mu \mid \frac{1}{2}(p+1)$  that  $\mu$  is odd and  $l$  is even. But then,  $(u^{(p-1)/2})^{l/2} = Q^{(p-1)/4} = -1$ , which implies  $\text{ord}_p(u) \neq \frac{1}{2}(p-1)$ , and so  $\text{ord}_p(u) = p-1$  in this case.

Case 2. If  $p \equiv 3 \pmod{4}$ , then  $\mu$  is even by the assumption. If  $\text{ord}_p(u) = \frac{1}{2}(p-1)$ , then  $u$  is a quadratic residue and so  $\alpha^{\mu/2}, \beta^{\mu/2} \in \mathbb{Z}_p$  since  $(\alpha^{\mu/2})^2 = (\beta^{\mu/2})^2 = u$ . It follows that  $\alpha^{\mu/2} = \pm\beta^{\mu/2}$ . However, by the definition of  $\mu$ , we cannot have  $\alpha^{\mu/2} = \beta^{\mu/2}$ . Therefore,  $\alpha^{\mu/2} = -\beta^{\mu/2}$ , which implies  $F_{\mu/2+1} = \alpha^{\mu/2} P/(\alpha - \beta)$ , which contradicts  $\alpha - \beta = \sqrt{\Delta} \notin \mathbb{Z}_p$ . It follows that  $\text{ord}_p(u) = p-1$  in this case as well.

We have so far shown that  $u = \alpha^\mu$  is a primitive root modulo  $p$ . In particular, the numbers  $F_{s\mu+1} = \alpha^{s\mu}$ ,  $1 \leq s \leq p-1$ , form a reduced residue system modulo  $p$ ; i.e., they contain every nonzero congruence class modulo  $p$ . Since for each  $1 \leq s \leq p-1$  and  $0 \leq t < \mu$ , we have

$$F_{s\mu+t} = \frac{\alpha^{s\mu+t} - \beta^{s\mu+t}}{\alpha - \beta} = \alpha^{s\mu} F_t = F_{s\mu+1} F_t,$$

and  $F_t \neq 0$  for  $1 \leq t < \mu$ , we conclude that the numbers  $F_{s\mu+t}$ ,  $1 \leq s \leq p-1$ , form a reduced residue system modulo  $p$  for each fixed  $0 < t < \mu$ . It follows that zero appears exactly  $p-1$  times among the numbers  $\widehat{F}_1, \dots, \widehat{F}_{\pi(p)}$ , and each  $k \in \{1, \dots, p-1\}$  appears exactly  $\mu-1$  times in the full period. Moreover,  $\pi(p) = \mu(p-1)$ ; i.e., each nonzero element of  $\mathbb{Z}_p$  appears exactly  $\mu-1 = (\pi(p) - p + 1)/(p-1)$  times. This completes the proof of part (a).

(b) If  $\text{ord}_p(u) = p-1$ , then again  $u$  is a primitive root modulo  $p$  and the claim follows as in the proof of part (a). Thus, suppose that  $\text{ord}_p(Q) = \text{ord}_p(u) = \frac{1}{2}(p-1)$ . Then  $\{F_{s\mu+1} = u^s : 1 \leq s \leq \frac{1}{2}(p-1)\}$  contains exactly all quadratic residues modulo  $p$ . Since  $F_{a+s\mu} = u^s F_a$ , we have

$$\left(\frac{F_a}{p}\right) = \left(\frac{F_{a+s\mu}}{p}\right).$$

Therefore, the last column of the period matrix is a zero column; moreover, every other column of the period matrix lists either exactly the set of all nonzero quadratic residues or the set of all quadratic nonresidues, depending on whether the first entry in the column is a quadratic residue or a quadratic nonresidue. Equation (5) implies  $F_a F_{\mu-(a-1)} \equiv Q F_{a-1} F_{\mu-a} \pmod{p}$ . Since  $Q$  is a quadratic residue modulo  $p$ , it follows that

$$\left(\frac{F_a}{p}\right) \left(\frac{F_{\mu-a}}{p}\right) = \left(\frac{F_{a-1}}{p}\right) \left(\frac{F_{\mu-(a-1)}}{p}\right) \quad \text{for all } a \in \{2, \dots, \mu-1\}.$$

Therefore,  $\left(\frac{F_a}{p}\right)\left(\frac{F_{\mu-a}}{p}\right)$  is independent of  $a$ , and so

$$\left(\frac{F_a}{p}\right)\left(\frac{F_{\mu-a}}{p}\right) = \left(\frac{F_{\mu-1}}{p}\right)\left(\frac{F_1}{p}\right) = -1$$

since  $u = \alpha^\mu = F_{\mu+1} = PF_\mu - QF_{\mu-1} = -QF_{\mu-1}$ , which implies

$$\left(\frac{F_{\mu-1}}{p}\right) = -1.$$

We conclude that for each  $a \in \{1, \dots, \mu - 1\}$  exactly one of the numbers  $F_a$  or  $F_{\mu-a}$  is a nonzero quadratic residue modulo  $p$ . So half of the  $(\mu - 1)$  nonzero columns of the period matrix list exactly the set of all nonzero quadratic residues and the other half list exactly the set of quadratic nonresidues. It follows that each  $k \in \{1, 2, \dots, p - 1\}$  appears  $\frac{1}{2}(\mu - 1)$  times in the full period.  $\square$

As we discussed in the Introduction, the existence of primitive roots modulo primes in a given arithmetic progression plays an important role in the proof of Theorem 2. In particular, we need the following theorem from [Lenstra 1977a, Theorem 5.1].

**Theorem 9** (Lenstra). *Let  $b, c$  be positive integers,  $(b, c) = 1$ , and let  $t \in \mathbb{Q}$ ,  $t \neq 0, \pm 1$ . Let  $\alpha(t)$  denote the discriminant of  $\mathbb{Q}(\sqrt{t})$  over  $\mathbb{Q}$ . Then the set of prime numbers  $q$  in the arithmetic progression  $b + kc$ ,  $k \in \{0, 1, 2, \dots\}$ , for which  $t$  is a primitive root is finite if and, modulo the Generalized Riemann Hypotheses, only if, one of the following conditions is satisfied:*

- (a)  $l \mid c$ ,  $b \equiv 1 \pmod{l}$ ,  $t \in \mathbb{Q}^{*l}$  for some prime number  $l$ ,
- (b)  $\alpha(t) \mid c$ ,  $\left(\frac{\alpha(t)}{b}\right) = 1$  (Kronecker symbol),
- (c)  $\alpha(t) \mid 3c$ ,  $3 \mid \alpha(t)$ ,  $\left(\frac{-\alpha(t)/3}{b}\right) = 1$ ,  $t \in \mathbb{Q}^{*3}$ ,

where  $\mathbb{Q}^{*l} = \{q^l : q \in \mathbb{Q} \setminus \{0\}\}$ .

**Lemma 10.** (GRH) *Let  $P, Q$  be integers such that  $|P^2 - 4Q|$  is not a perfect square and  $Q \neq -1$ . Suppose that either  $\frac{1}{3}(P^2 - 4Q)$  is not a perfect square or  $Q$  is not the twelfth power of an integer. Then there exist infinitely many primes  $q$  such that  $[P, Q]$  is complete modulo  $q$ .*

*Proof.* Let  $r$  be the largest integer such that  $Q$  is the  $r$ -th power of an integer. If  $r$  is odd, let  $h = r$  and  $Q_0$  be the unique integer such that  $Q = Q_0^h$ . If  $r$  is even, we write  $r = 2^\epsilon h$ , where  $h$  is odd and  $\epsilon \geq 1$ , and let  $Q_0$  be the unique negative integer such that  $Q = Q_0^{2h}$ . Also, let  $\Delta'$  and  $Q'$  be the square-free parts of  $\Delta = P^2 - 4Q$  and  $Q_0$ , respectively. Let  $\mathcal{C}$ ,  $\mathcal{H}$  and  $\mathcal{T}$  denote the sets of prime factors of  $\Delta'$ ,  $h$ , and  $Q'$  respectively.

First, suppose that  $\Delta' = 3$ ,  $3 \in \mathcal{H}$ , and  $\mathcal{T} = \emptyset$ . It follows that  $-Q_0$  is a perfect square. If  $Q$  is a perfect square, then by the definition of  $Q_0$ , we have  $Q = Q_0^{2h}$ . Since  $3 \mid h$  and  $-Q_0$  is a perfect square, it follows that  $Q$  is the twelfth power of an integer. Since  $\Delta' = 3$ , we see that  $\frac{1}{3}(P^2 - 4Q)$  is a perfect square. However, the case where  $Q$  is the twelfth power of an integer and  $\frac{1}{3}(P^2 - 4Q)$  is a perfect square is excluded from consideration in the hypotheses of Lemma 10. Thus, suppose that  $Q$  is not a perfect square, and so  $Q = Q_0^h$ . It follows that  $Q = -R^2$  for some integer  $R$  and  $P^2 - 4Q = \Delta = 3Y^2$  for some integer  $Y$ . But then  $P^2 + 4R^2 = 3Y^2$ , which has only the trivial solution  $P = R = Y = 0$  in integers by the sum of two squares theorem (see, for example, Theorem 2 in Chapter 2 of [Grosswald 1985]), a contradiction.

Next, suppose that  $\Delta' \neq 3$ , or  $3 \notin \mathcal{H}$ , or  $\mathcal{T} \neq \emptyset$ . We have two cases:

Case I. Suppose  $\Delta' \neq 3$  or  $3 \notin \mathcal{H}$ . If  $\mathcal{C} \neq \{3\}$ , let  $a \neq 3$  be the smallest prime factor of  $\Delta'$ , otherwise (i.e., when  $\Delta' = -3$  or  $\Delta' = 3$  but  $3 \notin \mathcal{H}$ ) let  $a = 3$ . For each odd  $p \in \mathcal{C} \setminus \{a\}$ , let  $X_p$  be an integer such that

$$\left(\frac{X_p}{p}\right) = (-1)^{(p-1)/2}.$$

If  $a$  is odd, choose  $X_a$  such that

$$\left(\frac{X_a}{a}\right) = -\operatorname{sgn}(\Delta)(-1)^{(a-1)/2},$$

where  $\operatorname{sgn}(\Delta) = 1$  if  $\Delta > 0$  and  $\operatorname{sgn}(\Delta) = -1$  if  $\Delta < 0$ . Moreover, without loss of generality, we can choose  $X_p$  for each  $p \in \mathcal{C} \cap \mathcal{H}$  such that  $X_p \not\equiv 1 \pmod{p}$ . Now, consider the system of congruences

$$\begin{cases} x \equiv X_p \pmod{p} & \text{for all } p \in \mathcal{C} \setminus \{2\}, \\ x \equiv 2 \pmod{p} & \text{for all } p \in \mathcal{H} \setminus \mathcal{C}, \\ x \equiv 3 \pmod{8} & \text{if } a \neq 2 \text{ or } \Delta > 0, \\ x \equiv 7 \pmod{8} & \text{if } a = 2 \text{ and } \Delta < 0. \end{cases} \quad (8)$$

Note that by our choice of  $X_p$  for  $p \in \mathcal{C} \cap \mathcal{H}$ , any solution of the system (8) satisfies  $\gcd(x-1, h) = 1$ . By the Chinese remainder theorem and Dirichlet's theorem, there exists a prime  $b > 4\Delta h$  that satisfies (8). We choose  $t \in \{Q_0, -Q_0\}$  such that  $\left(\frac{t}{b}\right) = -1$ . Theorem 9 with our  $b$  and  $t$  and  $c = 4^\delta \Delta h$  (where the integer  $\delta$  is large enough so that  $b < c$ ) implies that there exist infinitely many primes  $q \equiv b \pmod{4\Delta h}$  such that  $\operatorname{ord}_q(t) = q-1$ . Since  $\gcd(q-1, h) = 1$ , it follows that  $\operatorname{ord}_q(t^h) = q-1$ .

If  $Q$  is not a perfect square, then by our definition of  $Q_0$  and  $t$ , we have  $Q = \pm t^h$ . It follows that either  $\operatorname{ord}_q(Q) = q-1$  or  $\operatorname{ord}_q(-Q) = q-1$ . Hence,  $\operatorname{ord}_q(Q) = q-1$  or  $\frac{1}{2}(q-1)$ . If  $Q$  is a perfect square, then  $Q = Q_0^{2h}$ , and since  $Q_0$  or  $-Q_0$  is a primitive root modulo  $q$ , we have  $\operatorname{ord}_q(Q_0^2) = \frac{1}{2}(q-1)$ , and so  $\operatorname{ord}_q(Q) = \frac{1}{2}(q-1)$  since  $Q = (Q_0^2)^h$  and  $\gcd(h, q-1) = 1$ .

If  $a$  is odd, then  $\Delta'$  is odd and  $q \equiv b \equiv X_p \pmod{p}$  for all  $p \in \mathcal{C}$ . Moreover,  $q \equiv b \equiv 3 \pmod{4}$ . It follows from the quadratic reciprocity law that

$$\begin{aligned} \left(\frac{\Delta}{q}\right) &= \left(\frac{\operatorname{sgn}(\Delta)a}{q}\right) \prod_{p \in \mathcal{C} \setminus \{a\}} \left(\frac{p}{q}\right) \\ &= \operatorname{sgn}(\Delta)(-1)^{(a-1)/2} \left(\frac{q}{a}\right) \prod_{p \in \mathcal{C} \setminus \{a\}} (-1)^{(p-1)/2} \left(\frac{q}{p}\right) \\ &= \operatorname{sgn}(\Delta)(-1)^{(a-1)/2} \left(\frac{X_a}{a}\right) \prod_{p \in \mathcal{C} \setminus \{a\}} (-1)^{(p-1)/2} \left(\frac{X_p}{p}\right) = -1. \end{aligned} \quad (9)$$

A similar calculation works for the case  $a = 2$ . Therefore,  $P^2 - 4Q$  is a quadratic nonresidue modulo  $q$  and  $\operatorname{ord}_q(Q) = q-1$  or  $\frac{1}{2}(q-1)$ . It then follows from Theorem 8 that  $[P, Q]$  is complete modulo  $q$ , and the proof of the lemma is completed in case I.

Case II.  $\Delta' = 3$  and  $3 \in \mathcal{H}$  and  $\mathcal{T} \neq \emptyset$ . If  $3 \in \mathcal{T}$ , let  $a = 3$ , otherwise let  $a \in \mathcal{T}$  be arbitrary. For each odd  $p \in \mathcal{T} \setminus \{a\}$ , choose  $X_p$  such that

$$\left(\frac{X_p}{p}\right) = 1.$$

Also let  $X_a$  be an integer such that

$$\left(\frac{X_a}{a}\right) = -1.$$

Moreover, without loss of generality, we can choose  $X_p$  for each  $p \in \mathcal{C} \cap \mathcal{H}$  such that  $X_p \not\equiv 1 \pmod{p}$ . Consider the system of congruences

$$\begin{cases} x \equiv X_p \pmod{p} & \text{for all } p \in \mathcal{T} \setminus \{2\}, \\ x \equiv 2 \pmod{p} & \text{for all } p \in \mathcal{H} \setminus \mathcal{T}, \\ x \equiv 1 \pmod{8} & \text{if } a \neq 2, \\ x \equiv 5 \pmod{8} & \text{if } a = 2. \end{cases} \quad (10)$$

As in the proof of case I, we choose  $b > 4\Delta h$  to be a prime satisfying congruences (10). Let  $t = Q_0$  and  $c = 4^\delta \Delta h$ , where the integer  $\delta$  is chosen such that  $b < c$ . By Theorem 9, there exist infinitely many primes  $q$  such that  $t$  is a primitive root modulo  $q$ . A calculation similar to (9) shows that  $P^2 - 4Q$  is a quadratic nonresidue modulo  $q$ . Therefore, by Theorem 8, the sequence  $[P, Q]$  is complete modulo  $q$ , and the proof of Lemma 10 is completed.  $\square$

Next, we consider the case where  $\frac{1}{3}(P^2 - 4Q)$  is a perfect square and  $Q$  is the twelfth power of an integer. First we need a lemma.

**Lemma 11.** *Let  $P, Q$  be relatively prime integers and  $t'$  be a square-free integer. Then there exists a constant  $N$  (that depends on  $P, Q$ , and  $t'$ ) such that for the sequence  $F = [P, Q]$  we have  $F'_i \neq 1, 6, 2t', 3t'$  for all  $i > N$ , where  $F'_i$  denotes the square-free part of  $F_i$ .*

*Proof.* By [Ribenoim and McDaniel 1991, Proposition 1], each square class of  $[P, Q]$  is finite. In other words, given any  $i \geq 1$ , there exist only finitely many  $j \geq 1$  such that  $F_i F_j$  is a square. Lemma 11 follows immediately.  $\square$

In the proof of the next lemma, we will work with biquadratic residues and nonresidues. Given a prime  $p \equiv 1 \pmod{4}$ , the multiplicative group  $\mathbb{Z}_p^*$  is divided into four subsets: the subgroup generated by the fourth powers (which we call biquadratic residues) and its cosets.

**Lemma 12.** (GRH) *Let  $P, Q$  be relatively prime integers such that  $Q = Z^{12}$  and  $P^2 - 4Q = 3Y^2$  for some integers  $Z > 1$  and  $Y \neq 0$ . Then  $[P, Q]$  is complete modulo infinitely many primes.*

*Proof.* Let  $h$  be the largest odd integer such that  $Z = t^{2^\epsilon h}$ , where  $\epsilon \geq 0$  and  $t$  is not a perfect square. Let  $t'$  be the square-free part of  $t$ . Let  $F = [P, Q]$  and  $F'_i$  be the square-free part of  $F_i$ ,  $i \geq 1$ . Finally, let  $\mathcal{D}_i, \mathcal{H}$ , and  $\mathcal{T}$  denote the sets of prime factors of  $F'_i, h$ , and  $t'$  respectively,  $i \geq 1$ .

We claim that there exists a set  $\Omega \subseteq \mathcal{D}_i \cup \mathcal{T}$  that has the following properties:

- (i)  $2, 3 \notin (\mathcal{D}_i \cup \mathcal{T}) \setminus \Omega$ .
- (ii)  $\#(\mathcal{D}_i \cap \Omega)$  and  $\#(\mathcal{T} \cap \Omega)$  are odd.

We first note that  $\gcd(t', 6) = 1$ , since otherwise  $\gcd(Z, 6) \neq 1$ , and it would follow from  $P^2 - 4Z^{12} = 3Y^2$  that  $\gcd(P, Q) \neq 1$ . Therefore,  $\mathcal{T} \cap \{2, 3\} = \emptyset$ . By Lemma 11, there exists  $i \geq 1$  such that  $F'_i \neq 1, 6, 2t', 3t'$ . There are four cases:

Case 1.  $2, 3 \in \mathcal{D}_i$ . If  $\mathcal{D}_i \cap \mathcal{T} \neq \emptyset$ , let  $a \in \mathcal{D}_i \cap \mathcal{T}$  and  $\Omega = \{2, 3, a\}$ . If  $\mathcal{D}_i \cap \mathcal{T} = \emptyset$ , then since  $t' \neq 1$  and  $F'_i \neq 1, 6$ , there exists  $a \in \mathcal{T} \setminus \mathcal{D}_i$  and  $a' \in \mathcal{D}_i \setminus \mathcal{T}$ . We let  $\Omega = \{2, 3, a, a'\}$ .

Case 2.  $3 \in \mathcal{D}_i$  and  $2 \notin \mathcal{D}_i$ . If there exists  $a \in \mathcal{T} \setminus \mathcal{D}_i$ , let  $\Omega = \{3, a\}$ . If  $\mathcal{T} \setminus \mathcal{D}_i = \emptyset$ , choose  $a \in \mathcal{D}_i \cap \mathcal{T}$ . Moreover, we choose  $a' \in \mathcal{D}_i \setminus \mathcal{T}$ . Such an  $a'$  exists, otherwise  $F'_i = 3t'$ , a contradiction.

Case 3.  $2 \in \mathcal{D}_i$  and  $3 \notin \mathcal{D}_i$ . If there exists  $a \in \mathcal{T} \setminus \mathcal{D}_i$ , let  $\Omega = \{2, a\}$ . If  $\mathcal{T} \setminus \mathcal{D}_i = \emptyset$ , choose  $a \in \mathcal{D}_i \cap \mathcal{T}$ . Moreover, we choose  $a' \in \mathcal{D}_i \setminus \mathcal{T}$ . Such an  $a'$  exists, otherwise  $F'_i = 2t'$ , a contradiction.

Case 4.  $2, 3 \notin \mathcal{D}_i$ . If there exists  $a \in \mathcal{D}_i \cap \mathcal{T}$ , let  $\Omega = \{a\}$ . If  $\mathcal{D}_i \cap \mathcal{T} = \emptyset$ , choose  $a \in \mathcal{D}_i \setminus \mathcal{T}$  and  $a' \in \mathcal{T} \setminus \mathcal{D}_i$ , and let  $\Omega = \{a, a'\}$ .

Next, we define integers  $X_p$  for odd primes  $p \in \mathcal{D}_i \cup \mathcal{T}$  as follows. For each odd  $p \in (\mathcal{D}_i \cup \mathcal{T}) \setminus \Omega$ , choose an integer  $X_p$  such that

$$\left(\frac{X_p}{p}\right) = 1.$$

For odd  $p \in \Omega$ , choose an integer  $X_a$  such that

$$\left(\frac{X_a}{a}\right) = -1.$$

Moreover, we can choose  $X_p$  such that  $X_p \not\equiv 1 \pmod{p}$  if  $p \in \mathcal{H}$ . Consider the system of congruences

$$\begin{cases} x \equiv X_p \pmod{p} & \text{for all } p \in (\mathcal{D}_i \cup \mathcal{T}) \setminus \{2\}, \\ x \equiv 2 \pmod{p} & \text{for all } p \in \mathcal{H} \setminus (\mathcal{D}_i \cup \mathcal{T}), \\ x \equiv 2 \pmod{3}, \\ x \equiv 5 \pmod{8}. \end{cases} \quad (11)$$

Let  $b > 24F'_i t'$  be a prime satisfying the congruence relations (11). In particular, for any prime  $p \equiv b \pmod{24F'_i t'}$ , we have  $\gcd(b-1, 3h) = 1$  and

$$\left(\frac{t'}{p}\right) = \prod_{q \in \mathcal{T}} \left(\frac{q}{p}\right) = \prod_{q \in \Omega} \left(\frac{q}{p}\right) \prod_{q \in \mathcal{T} \setminus \Omega} \left(\frac{q}{p}\right) = -1.$$

Lenstra's theorem, Theorem 9, with  $c = 3 \cdot 4^\delta F'_i t'$  (where the integer  $\delta \geq 2$  is large enough such that  $b < c$ ) and our  $b$  and  $t$ , implies that there exist infinitely many primes  $p \equiv b \pmod{c}$  such that  $t$  is a primitive root modulo  $p$ . Since  $Q = t^{12 \cdot 2^\epsilon h}$ , we have

$$\text{ord}_p(Q) = \frac{p-1}{\gcd(p-1, 12 \cdot 2^\epsilon h)} = \frac{1}{4}(p-1).$$

Recall from the proof of Theorem 8 that  $Q = u^l$ , where  $u = \alpha^\mu$  and  $l = (p+1)/\mu$ . It follows that  $\text{ord}_p(u) \in \{p-1, \frac{1}{2}(p-1), \frac{1}{4}(p-1)\}$ . If  $\text{ord}_p(u) = p-1$ , then the numbers  $F_{s\mu+1} = u^s$  contain all nonzero elements modulo  $p$ ; hence  $[P, Q]$  is complete modulo  $p$ . If  $\text{ord}_p(u) = \frac{1}{2}(p-1)$ , then the numbers  $F_{s\mu+1} \equiv u^s \pmod{p}$  contain all quadratic residues modulo  $p$ , while the numbers  $F_{s\mu+i} \equiv u^s F_i \pmod{p}$  contain all quadratic nonresidues modulo  $p$  since  $F_i$  is a quadratic nonresidue modulo  $p$  by the calculation

$$\left(\frac{F_i}{p}\right) = \prod_{q \in \mathcal{D}_i} \left(\frac{q}{p}\right) = \prod_{q \in \Omega} \left(\frac{q}{p}\right) \prod_{q \in \mathcal{D}_i \setminus \Omega} \left(\frac{q}{p}\right) = -1,$$

and so  $[P, Q]$  is complete modulo  $p$ . Thus, suppose  $\text{ord}_p(u) = \frac{1}{4}(p-1)$ . Then the numbers  $F_{s\mu+1} = u^s$  consist of all of the biquadratic residues modulo  $p$ . Moreover, we have

$$u \equiv F_{\mu+1} \equiv PF_\mu - QF_{\mu-1} \equiv -QF_{\mu-1} \pmod{p}.$$

Since  $p \equiv 5 \pmod{8}$ , we know that  $-1$  is a quadratic residue but not a biquadratic residue modulo  $p$ . It follows from the fact that  $Q$  and  $u$  are biquadratic residues modulo  $p$  that  $F_{\mu-1}$  is a quadratic residue but not a biquadratic residue modulo  $p$ . Hence the numbers  $F_{s\mu+\mu-1} = u^s F_{\mu-1}$  consist of all of the quadratic residues that are not biquadratic residues modulo  $p$ . Moreover, since  $F_a F_{\mu-(a-1)} \equiv F_{a-1} F_{\mu-a} \pmod{p}$  for  $a \in \{2, \dots, \mu-1\}$ , one has

$$F_{\mu-a} F_a^{-1} \equiv F_{\mu-(a-1)} F_{a-1}^{-1} \pmod{p} \quad \text{for all } a \in \{2, \dots, \mu-1\},$$

which implies  $F_{\mu-a} F_a^{-1} \equiv F_{\mu-1} F_1^{-1} \equiv F_{\mu-1} \pmod{p}$ , which is a quadratic residue but not a biquadratic residue. It then follows that the numbers  $F_{s\mu+i} \equiv u^s F_i$  and  $F_{s\mu+\mu-i} \equiv u^s F_{\mu-i}$  together consist of all of the quadratic nonresidues modulo  $p$ , and the proof is completed.  $\square$

To complete the proof of Theorem 2, it remains to consider the case where  $P^2 - 4Q = -X^2$  for a nonzero integer  $X$ .

**Lemma 13.** (GRH) *Suppose that  $Q \neq \pm 1$  and  $P^2 - 4Q = -X^2$ , where  $X$  is a nonzero integer. Then  $[P, Q]$  is complete modulo infinitely many primes.*

*Proof.* There are two cases:

Case I.  $Q$  is not a perfect square. Let  $t = Q$  and note that  $Q > 0$ , otherwise  $-X^2 = P^2 - 4Q > 0$ , a contradiction. We claim that the obstructions (a), (b), and (c) in Theorem 9 (with  $b = 3$  and  $c = 4$ ) do not hold. Condition (a) fails since  $l$  must be odd and  $b = 3$ , and so  $b \not\equiv 1 \pmod{l}$  for any odd prime  $l$ . Condition (b) fails since if  $\alpha(t) \mid 4$ , then  $\alpha(t) = \pm 1, \pm 2, \pm 4$ . Since  $t = Q$  is not a perfect square and  $Q > 0$ , and  $\alpha(t)$  is a fundamental discriminant, we must have  $\alpha(t) = 2$ , and so

$$\left(\frac{\alpha(t)}{3}\right) = -1.$$

For condition (c), since  $\alpha(t) > 0$ , if  $\alpha(t) \mid 3c$  and  $3 \mid \alpha(t)$ , then  $\alpha(t) = 3, 6, 12$ , and so the power of 3 in the prime factorization of  $4Q$  is odd. But then from  $P^2 - 4Q = -X^2$ , we have  $4Q = P^2 + X^2$ , a contradiction with the sum of two squares theorem (see again [Grosswald 1985, Chapter 2]).

It then follows from Theorem 9 that there exist infinitely many primes  $p$  in the arithmetic progression  $\{4k + 3 : k \geq 0\}$  for which  $\text{ord}_p(Q) = \text{ord}_p(t) = p-1$ . On the other hand, since  $p \equiv 3 \pmod{4}$ , we have that  $P^2 - 4Q = -X^2$  is a quadratic nonresidue modulo  $p$ . Therefore, the sequence  $[P, Q]$  is complete modulo each such  $p > P$  by Theorem 8.

Case II.  $Q$  is a perfect square. Let  $Q = Z^2$  for some integer  $Z$ , and let  $t = -Q$ . In particular  $\alpha(t) = \alpha(-Z^2) = -4$ . We again see that conditions (a), (b), (c) in Theorem 9 fail with  $b = 3$  and  $c = 4$ . Condition (a) fails since  $b = 3$  and  $l$  is odd. Condition (b) fails since

$$\left(\frac{\alpha(t)}{3}\right) = \left(\frac{-4}{3}\right) = -1.$$

Condition (c) fails since  $3 \nmid \alpha(t)$ . It follows that there exist infinitely many primes  $p$  in the arithmetic progression  $\{4k + 3 : k \geq 0\}$  such that  $\text{ord}_p(t) = p - 1$ ; hence  $\text{ord}_p Q = \frac{1}{2}(p - 1)$ , and so the sequence  $[P, Q]$  is complete modulo  $p$  by Theorem 8.  $\square$

Theorem 2 follows from Theorem 7 and Lemmas 10, 12, and 13.

If we let  $\pi_t(x; c, b)$  denote the set of primes  $p \leq x$  such that  $p \equiv b \pmod{c}$  and  $t$  is a primitive root modulo  $p$ , then by a theorem of [Lenstra 1977b] (see also [Moree 1999, Theorem 2]):

$$\pi_t(x; c, b) = \delta(t, c, b) \frac{x}{\log x} + O\left(\frac{x \log \log x}{\log^2 x}\right),$$

where  $\delta(t, c, b) \geq 0$  is a constant computable in terms of  $t, c, b$  [Moree 1999, Theorem 3]. The cases where  $\delta(t, c, b) = 0$  are exactly given by the three cases (a), (b), (c) of Theorem 9. In the proofs of Lemmas 10, 12, and 13, we have excluded the possibility of  $\delta(t, c, b) = 0$  to show that there exist infinitely many primes in suitable arithmetic progressions with a suitable prescribed primitive root. In other words, throughout our proofs, we have had  $\delta(t, c, b) > 0$  in various places where we have defined  $t, c,$  and  $b$  in terms of  $P$  and  $Q$ . Therefore, we have shown under the GRH that if  $\text{gcd}(P, Q) = 1$  and  $Q \neq \pm 1$  and  $P^2 - 4Q$  is not a perfect square, then for all  $x$  large enough,

$$\#\Lambda(x; P, Q) \geq \eta(P, Q) \frac{x}{\log x},$$

where  $\eta(P, Q) > 0$  is a constant that only depends on  $P$  and  $Q$ .

#### 4. The relative size of complete pairs

In Theorem 2, we fixed the parameters  $P, Q$  and considered the primes  $p$  such that the generalized Fibonacci sequence  $[P, Q]$  was complete modulo  $p$ . In this section, we fix a prime  $p$  and consider parameters  $P, Q$  for which the sequence  $[P, Q]$  is complete. Let  $\Lambda_p$  denote the set of pairs  $(P, Q) \in \{1, \dots, p - 1\}^2$  such that  $[P, Q]$  is complete modulo  $p$ . We are particularly interested in the relative size of  $\Lambda_p$  in the set  $\{1, \dots, p - 1\}^2$ .

In what follows, let  $\mathcal{A}_p$  denote the set of primitive roots modulo  $p$  in  $\mathbb{Z}_p$ . Let  $\mathcal{B}_p$  denote the set of  $Q \in \{1, \dots, p - 1\}$  such that  $\text{ord}_p(Q) = (p - 1)/k$ , where  $k \in \{1, 2\}$ . In particular  $\mathcal{A}_p \subseteq \mathcal{B}_p$ . Finally, for each  $Q \in \{1, \dots, p - 1\}$ , let  $\mathcal{C}_Q$  denote the set of  $P \in \{1, \dots, p - 1\}$  such that  $P^2 - 4Q$  is a quadratic nonresidue.

**Lemma 14.** *For every odd prime  $p$ , one has  $|\Lambda_p| \geq \frac{1}{2}(p - 3)|\mathcal{B}_p|$ .*

*Proof.* Let  $\mathcal{X}$  be the set of  $x \in \{1, \dots, p - 1\}$  such that  $x$  is a quadratic residue and  $x - 1$  is a quadratic nonresidue, and let  $\mathcal{Y}$  be the set of  $y \in \{1, \dots, p - 1\}$  such that  $y - 1$  is a quadratic residue and  $y$  is a quadratic nonresidue modulo  $p$ . It follows from [Aladov 1896, Theorem 1] that

$$|\mathcal{X}|, |\mathcal{Y}| \geq \frac{1}{4}(p - 3). \tag{12}$$

If  $Q$  is a quadratic residue modulo  $p$ , then the map  $P \mapsto P^2/(4Q)$  is a two-to-one map from  $\mathcal{C}_Q$  onto  $\mathcal{X}$ . If  $Q$  is a quadratic nonresidue modulo  $p$ , then the map  $P \mapsto P^2/(4Q)$  is a two-to-one map from  $\mathcal{C}_Q$  onto  $\mathcal{Y}$ . In either case, it follows from the inequalities (12) that

$$|\mathcal{C}_Q| \geq \frac{1}{2}(p - 3).$$

By Theorem 8, if  $Q \in \mathcal{B}_p$  and  $P \in \mathcal{C}_Q$ , then  $[P, Q]$  is complete modulo  $p$ . Therefore, we have

$$|\Lambda_p| \geq \sum_{Q \in \mathcal{B}_p} |\mathcal{C}_Q| \geq \frac{1}{2}(p-3)|\mathcal{B}_p|. \quad \square$$

Now, we are ready to prove Theorem 3.

*Proof of Theorem 3.* By [Heath-Brown 1986, Lemma 1], there exist infinitely many primes  $p_i \equiv 3 \pmod{4}$ ,  $i \geq 1$ , such that  $\frac{1}{2}(p_i - 1)$  is either a prime or a product of two primes  $q_i, r_i$  such that  $q_i, r_i > p_i^{1/4}$ . Therefore

$$\frac{1}{2} > \frac{\phi(p_i - 1)}{p_i - 1} > \frac{1}{2} \left(1 - \frac{1}{p_i^{1/4}}\right)^2$$

for all  $i \geq 1$ . Since the number of primitive roots modulo  $p_i$  is given by  $|\mathcal{A}_{p_i}| = \phi(\phi(p_i)) = \phi(p_i - 1)$ , it follows that

$$\lim_{i \rightarrow \infty} \frac{|\mathcal{A}_{p_i}|}{p_i} = \lim_{i \rightarrow \infty} \frac{\phi(p_i - 1)}{p_i - 1} = \frac{1}{2}. \quad (13)$$

Moreover, since

$$\begin{aligned} |\mathcal{B}_p \setminus \mathcal{A}_p| &= \#\{x \in \mathbb{Z}_p^* : \text{ord}_p(x) = \frac{1}{2}(p-1)\} \\ &= \#\{1 \leq k \leq p-1 : \gcd(k, p-1) = 2\} \\ &= \phi\left(\frac{1}{2}(p-1)\right) = \phi(p-1) = |\mathcal{A}_p|, \end{aligned}$$

we have  $|\mathcal{B}_p| = |\mathcal{A}_p| + |\mathcal{B}_p \setminus \mathcal{A}_p| = 2|\mathcal{A}_p|$ , and so

$$\lim_{i \rightarrow \infty} \frac{|\mathcal{B}_{p_i}|}{p_i} = 1.$$

Therefore, by Lemma 14, we conclude that

$$\limsup_{p \rightarrow \infty} \frac{|\Lambda_p|}{p^2} \geq \limsup_{i \rightarrow \infty} \frac{|\Lambda_{p_i}|}{p_i^2} \geq \lim_{i \rightarrow \infty} \frac{\frac{1}{2}(p_i - 3)|\mathcal{B}_{p_i}|}{p_i^2} \geq \frac{1}{2}. \quad (14)$$

On the other hand, for every odd prime  $p$ , one has  $|\Lambda_p| \leq \frac{1}{2}(p^2 - 1)$ . To see this, we note that for each  $P \in \{1, \dots, p-1\}$ , the number of  $Q$  such that  $P^2 - 4Q$  is zero or a quadratic nonresidue is  $\frac{1}{2}(p+1)$ . It follows (recall case (I) of Section 2) that for at most  $\frac{1}{2}(p^2 - 1)$  pairs  $[P, Q] \in \{1, \dots, p-1\}^2$ , the sequence  $[P, Q]$  is complete modulo  $p$ , and so  $|\Lambda_p| \leq \frac{1}{2}(p^2 - 1)$ , which implies  $\limsup_{p \rightarrow \infty} |\Lambda_p|/p^2 \leq \frac{1}{2}$ . This together with (14) completes the proof of Theorem 3.  $\square$

### Acknowledgements

We are grateful to the referee for a careful reading of the original manuscript and many useful suggestions that improved the overall exposition of the paper and clarified certain details and proofs.

### References

- [Aladov 1896] N. S. Aladov, “On the distribution of quadratic residues and nonresidues of a prime number  $P$  in the sequence  $1, 2, \dots, P-1$ ”, *Mat. Sb.* **18**:1 (1896), 61–75. In Russian.
- [Bruckner 1970] G. Bruckner, “Fibonacci sequence modulo a prime  $p \equiv 3 \pmod{4}$ ”, *Fibonacci Quart.* **8**:2 (1970), 217–220. MR Zbl

- [Elaydi 2005] S. Elaydi, *An introduction to difference equations*, 3rd ed., Springer, 2005. MR Zbl
- [Grosswald 1985] E. Grosswald, *Representations of integers as sums of squares*, Springer, 1985. MR Zbl
- [Heath-Brown 1986] D. R. Heath-Brown, “Artin’s conjecture for primitive roots”, *Quart. J. Math. Oxford Ser. (2)* **37**:145 (1986), 27–38. MR Zbl
- [Hooley 1967] C. Hooley, “On Artin’s conjecture”, *J. Reine Angew. Math.* **225** (1967), 209–220. MR Zbl
- [Lenstra 1977a] H. W. Lenstra, Jr., “Artin’s conjecture on primes with prescribed primitive roots”, *Séminaire Delange–Pisot–Poitou: théorie des nombres* **18**:1 (1977), exposé 14. MR Zbl
- [Lenstra 1977b] H. W. Lenstra, Jr., “On Artin’s conjecture and Euclid’s algorithm in global fields”, *Invent. Math.* **42** (1977), 201–224. MR Zbl
- [Li 2000] H.-C. Li, “Complete and reduced residue systems of second-order recurrences modulo  $p$ ”, *Fibonacci Quart.* **38**:3 (2000), 272–281. MR Zbl
- [Moree 1999] P. Moree, “On primes in arithmetic progression having a prescribed primitive root”, *J. Number Theory* **78**:1 (1999), 85–98. MR Zbl
- [Ribenboim and McDaniel 1991] P. Ribenboim and W. L. McDaniel, “Square classes of Lucas sequences”, *Portugal. Math.* **48**:4 (1991), 469–473. MR Zbl
- [Schinzel 1990] A. Schinzel, “Special Lucas sequences, including the Fibonacci sequence, modulo a prime”, pp. 349–357 in *A tribute to Paul Erdős*, edited by A. Baker et al., Cambridge Univ. Press, 1990. MR Zbl
- [Shah 1968] A. P. Shah, “Fibonacci sequence modulo  $m$ ”, *Fibonacci Quart.* **6**:2 (1968), 139–141. MR Zbl
- [Somer 1988] L. Somer, “Primes having an incomplete system of residues for a class of second-order recurrences”, pp. 113–141 in *Applications of Fibonacci numbers* (San Jose, CA, 1986), edited by A. N. Philippou et al., Kluwer Acad. Publ., Dordrecht, 1988. MR Zbl

Received 17 Dec 2018. Revised 7 Nov 2019.

MOHAMMAD JAVAHERI:

mjavaheri@siena.edu

Department of Mathematics, Siena College, Loudonville, NY, United States

NIKOLAI A. KRYLOV:

nkrylov@siena.edu

Department of Mathematics, Siena College, Loudonville, NY, United States



## Discretized sum-product for large sets

Changhao Chen

Let  $A \subset [1, 2]$  be a  $(\delta, \sigma)$ -set with measure  $|A| = \delta^{1-\sigma}$  in the sense of Katz and Tao. For  $\sigma \in (\frac{1}{2}, 1)$  we show that

$$|A + A| + |AA| \gtrsim \delta^{-c} |A|$$

for  $c = (1 - \sigma)(2\sigma - 1)/(6\sigma + 4)$ . This improves the bound of Guth, Katz, and Zahl for large  $\sigma$ .

### 1. Introduction

Erdős and Volkmann [1966] showed that for any  $\sigma \in [0, 1]$  there exists a subgroup of reals with Hausdorff dimension  $\sigma$ , and they conjectured that this property does not hold for a subring of reals. Precisely the Erdős–Volkmann ring conjecture claims that there does not exist a subring of reals with Hausdorff dimension strictly between 0 and 1. Edgar and Miller [2003] first proved this ring conjecture via the orthogonal projections of fractal sets. Slightly later Bourgain [2003] independently proved the Erdős–Volkmann ring conjecture via the discretized ring conjecture (discretized sum-product) of [Katz and Tao 2001].

The discretized sum-product also has many other applications. For instance it is closely related to Falconer’s distance set problem and the dimension of Furstenberg sets; see [Katz and Tao 2001] for more details. Bourgain [2010] showed a different approach for the discretized sum-product, and gave applications in the projections of fractal sets and Fourier analysis. For applications of the discretized sets to projections of fractal sets see [He 2017a; Orponen 2016]. For applications of the discretized sum-product to the Fourier decay of measures see [Li 2018].

We note that Bourgain [2003; 2010] does not produce an explicit bound. Recently Guth, Katz, and Zahl [2018] gave a short proof of the discretized sum-product theorem, and they showed an explicit bound for it. They used some ideas from [Garaev 2007] and applied some discretized version of arguments from additive combinatorics.

We begin by introducing some notation of [Katz and Tao 2001]. Let  $\epsilon, \delta$  be small and positive parameters. We use  $f \lesssim g$  to denote  $|f| \leq C_\epsilon \delta^{-C_\epsilon} |g|$ ,  $f \gtrsim g$  if  $g \lesssim f$ , and  $f \approx g$  if  $f \lesssim g$  and  $g \gtrsim f$ . We say that a subset  $A \subset \mathbb{R}$  is  $\delta$ -discretized if  $A$  is the union of intervals of lengths  $\approx \delta$ . For a positive constant  $M$  we say that a subset  $A \subset (-M, M)$  is a  $(\delta, \sigma)$ -set if it is  $\delta$ -discretized and one has

$$|A \cap B(x, r)| \lesssim \delta \left(\frac{r}{\delta}\right)^\sigma$$

for all  $\delta \leq r < 1$  and  $x \in \mathbb{R}$ .

*MSC2010:* 05B99.

*Keywords:*  $(\delta, \sigma)$ -sets, sum set estimates, Fourier transform.

We note that a  $(\delta, \sigma)$ -set here may have much smaller measure than  $\delta^{1-\sigma}$ . However we ask that any  $(\delta, \sigma)$ -set have positive measure to avoid its being the empty set.

We remark that the  $(\delta, \sigma)$ -set can be considered as the discrete approximation of a set in  $\mathbb{R}$  at scale  $\delta$ . Suppose that  $F$  is a compact subset of  $\mathbb{R}$ . For each  $k \in \mathbb{Z}$  let

$$I_{k,\delta} = [k\delta, (k+1)\delta]$$

and  $F_\delta$  be the union of the interval  $I_{k,\delta}$  which intersects  $F$ ; that is,

$$F_\delta = \bigcup_{k \in \mathbb{Z}, F \cap I_{k,\delta} \neq \emptyset} I_{k,\delta}.$$

In many cases, the set  $F_\delta$  is a  $(\delta, \sigma)$ -set for some  $0 \leq \sigma \leq 1$ . Here the parameter  $\sigma$  is often related to the ‘‘fractal dimension’’ of  $F$ . For instance if  $F$  is the classical Cantor ternary set, then for any  $0 < \delta < 1$  the set  $F_\delta$  is a  $(\delta, \log 2 / \log 3)$ -set. Indeed this follows from [Falconer 2003, Chapter 3], which shows that the box dimension of the Cantor set is  $\log 2 / \log 3$ . We remark that there are various dimensions in fractal geometry; we refer to [Falconer 2003] for more details.

The above argument shows that the  $(\delta, \sigma)$ -set in  $\mathbb{R}^d$  is also important for understanding the structure of set in  $\mathbb{R}^d$ . However, in this paper we consider  $(\delta, \sigma)$ -sets on the line  $\mathbb{R}$  only.

Let  $A, B \subseteq \mathbb{R}$ . The sum set of  $A$  and  $B$  is defined as

$$A + B = \{a + b : a \in A, b \in B\},$$

and similarly the product set of  $A$  and  $B$  is defined as

$$AB = \{ab : a \in A, b \in B\}.$$

Using the above notation, Bourgain’s discretized sum-product theorem claims that for a  $(\delta, \sigma)$ -set  $A \subset [1, 2]$  with  $0 < \sigma < 1$  and measure  $|A| = \delta^{1-\sigma}$ , there exists a constant  $c = c(\sigma) > 0$  such that

$$|A + A| + |AA| \gtrsim \delta^{-c} |A|.$$

Under the same condition, Guth, Katz, and Zahl [2018] proved that for any  $c < \sigma(1-\sigma)/(4(7+3\sigma))$  one has

$$|A + A| + |AA| \gtrsim \delta^{-c} |A|.$$

By adapting the arguments of [Garaev 2007; Guth, Katz, and Zahl 2018], and the bilinear bound of [Bourgain 2010, Theorem 7], we obtain the following.

**Theorem 1.1.** *Let  $\sigma \in (\frac{1}{2}, 1)$  and  $A \subset [1, 2]$  be a  $(\delta, \sigma)$ -set with measure  $|A| = \delta^{1-\sigma}$ . Then*

$$|A + A| + |AA| \gtrsim \delta^{-\frac{(1-\sigma)(2\sigma-1)}{6\sigma+4}} |A|.$$

Note that for any  $\frac{1}{2} < \sigma < 1$ , Theorem 1.1 gives a nontrivial lower bound. Furthermore for  $\sigma > \frac{1}{9}(\sqrt{226} - 10) = 0.5703\dots$ , Theorem 1.1 improves the bound of [Guth, Katz, and Zahl 2018].

## 2. Preliminaries

We use  $\#S$  to denote the cardinality of set  $S$ . Let  $X, Y, Z \subset \mathbb{R}$  be finite sets with  $Z \neq \emptyset$ ; then the Ruzsa triangle inequality claims that

$$\#(X + Y) \leq \frac{\#(X + Z)\#(Z + Y)}{\#Z}.$$

See [Tao and Vu 2006, Chapter 2] for a proof and many other useful sum set estimates.

We need the following well-known discretized version of the Ruzsa triangle inequality. Our proof is based on [Guth, Katz, and Zahl 2018, Proof of Corollary 2.3; Orponen 2016, Remark 4.40]. For many other discretized versions of sum sets estimates see [He 2017b; Tao 2014].

We show a geometric observation first. Let  $S \subset \mathbb{R}$  be the union of disjoint intervals with length  $\gtrsim \delta$ . Then for all  $0 < c < 10$  we have

$$|S + B(0, c\delta)| \lesssim |S|. \quad (1)$$

Here we can change the parameter 10 to any other fixed positive constant.

**Lemma 2.1.** *Let  $A, B, C \subset \mathbb{R}$  be  $\delta$ -discretized sets. Then*

$$|A + B| \lesssim \frac{|A + C||C + B|}{|C|}.$$

*Proof.* Without loss of generality we may assume that each interval of  $A, B$  and  $C$  has length at least  $\delta$ . In the end we change the estimate  $\ll$  to  $\lesssim$ , and this does not change our result.

For any set  $S \subset \mathbb{R}$  let  $S_\delta = (\delta/3)\mathbb{Z} \cap S$ . For any  $a \in A, b \in B$  there exists  $a' \in A_\delta, b' \in B_\delta$  such that

$$|a + b - a' - b'| \leq \delta.$$

It follows that

$$A + B \subset A_\delta + B_\delta + B(0, \delta) \subset A + B + B(0, 2\delta). \quad (2)$$

Combining with (1) we obtain

$$|A + B| \ll \#(A_\delta + B_\delta)\delta \ll |A + B|.$$

Applying the Ruzsa triangle inequality to sets  $A_\delta, B_\delta, C_\delta$  and applying (2) to  $A + C$  and  $C + B$  we obtain the result.  $\square$

**Lemma 2.2.** *Let  $A \subset [0, 2]$  be a  $\delta$ -discretized set, and assume the intervals of  $A$  are pairwise disjoint. Then for any  $t \in [0.5, 2.1]$  and any  $x \in [-\delta, \delta]$  we have*

$$|A + tA| \lesssim |A + (t + x)A| \lesssim |A + tA|.$$

*Proof.* For any  $t \in [0.5, 2], x \in [-\delta, \delta]$ , and  $a, b \in A$  we have

$$|(a + tb) - (a + (t + x)b)| \leq 2\delta,$$

and hence

$$A + tA \subset A + (t + x)A + B(0, 2\delta) \subset A + tA + B(0, 4\delta).$$

Combining with (1) we finish the proof.  $\square$

Let  $f : \mathbb{R} \rightarrow \mathbb{R}$  be a function. The Fourier transform of the function  $f$  at  $\xi \in \mathbb{R}$  is defined as

$$\hat{f}(\xi) = \int_{\mathbb{R}} e(-x\xi) f(x) dx,$$

where throughout the paper we let  $e(x) = e^{2\pi i x}$ . Let  $\mu$  be a measure on  $\mathbb{R}$ . The Fourier transform of the measure  $\mu$  at  $\xi \in \mathbb{R}$  is defined as

$$\hat{\mu}(\xi) = \int e(-x\xi) d\mu(x).$$

For a subset  $S \subset \mathbb{R}$  we will also use  $S$  to denote the characteristic function of  $S$ . Let  $A, B \subset \mathbb{R}$  be two bounded sets. The convolution of  $A$  and  $B$  is defined as

$$(A * B)(x) = \int_{\mathbb{R}} A(x - y) B(y) dy.$$

The (additive) energy of  $A, B$  is defined as

$$E(A, B) = \int_{\mathbb{R}} (A * B)(x)^2 dx = \int_{\mathbb{R}} |\hat{A}(\xi)|^2 |\hat{B}(\xi)|^2 d\xi. \quad (3)$$

The second equality holds by applying the Plancherel identity and the convolution theorem. Clearly we have

$$\int_{\mathbb{R}} (A * B)(x) dx = |A| |B|.$$

By the Cauchy–Schwarz inequality we obtain

$$(|A| |B|)^2 \leq E(A, B) |A + B|. \quad (4)$$

We will frequently use the Plancherel identity for a set. Precisely for a bounded subset  $S \subset \mathbb{R}$  we have

$$\int_{\mathbb{R}} |\hat{S}(\xi)|^2 d\xi = |S|. \quad (5)$$

We formulate the following version of [Bourgain 2010, Theorem 7]. Note that the interval  $[0, 4]$  is not essential; in fact Lemma 2.3 holds for any bounded interval.

**Lemma 2.3.** *Let  $\mu, \nu$  be probability measures on  $[0, 4]$  such that, for all  $\delta < r \leq 1$  and all  $x \in \mathbb{R}$ ,*

$$\mu(B(x, r)) \lesssim K_1 r^\alpha \quad \text{and} \quad \nu(B(x, r)) \lesssim K_2 r^\beta.$$

*Then for  $1 \leq |\xi| \leq \delta^{-1}$  we have*

$$\int_{\mathbb{R}} \left| \int_{\mathbb{R}} e(-xy\xi) d\mu(x) \right| d\nu(y) \lesssim \sqrt{K_1 K_2} |\xi|^{-\frac{\alpha+\beta-1}{2}}.$$

We remark that the statement of [Bourgain 2010, Theorem 7] gives a bound for

$$\left| \int_{\mathbb{R}} \int_{\mathbb{R}} e(-xy\xi) d\mu(x) d\nu(y) \right|.$$

However the proof of [Bourgain 2010, Theorem 7] (see (8.3) of that paper) indeed works for the bound

$$\int_{\mathbb{R}} \left| \int_{\mathbb{R}} e(-xy\xi) d\mu(x) \right| d\nu(y),$$

which is used for bounding (22) below. Moreover the term  $\sqrt{K_1 K_2}$  appears, due to the use of the Cauchy–Schwarz inequality in the proof of [Bourgain 2010, Theorem 7].

In particular we have the following version for  $(\delta, \sigma)$ -sets, which is easier for our use.

**Lemma 2.4.** *Let  $0 < \alpha, \beta < 1$ . Let  $A \subset [0, 4]$  and  $B \subset [0, 4]$  be a  $(\delta, \alpha)$ -set and a  $(\delta, \beta)$ -set respectively. Then for any  $1 \leq \xi \leq \delta^{-1}$  we have*

$$\int_A \left| \int_B e(-xy\xi) dx \right| dy \lesssim |\xi|^{-\frac{\alpha+\beta-1}{2}} \delta^{\frac{2-\alpha-\beta}{2}} \sqrt{|A||B|}.$$

*Proof.* For  $A$  we define a measure  $\mu$  by letting

$$\mu(X) = \frac{|X \cap A|}{|A|} \quad \text{for } X \subset \mathbb{R}.$$

By the condition that  $A$  is a  $(\delta, \alpha)$ -set we obtain

$$\mu(B(x, r)) \lesssim r^\alpha \delta^{1-\alpha} |A|^{-1} \quad \text{for } \delta \leq r \leq 1. \quad (6)$$

Similarly for  $B$  we define a measure  $\nu$  by letting

$$\nu(X) = \frac{|X \cap B|}{|B|} \quad \text{for } X \subset \mathbb{R},$$

and we have

$$\nu(B(x, r)) \lesssim r^\beta \delta^{1-\beta} |B|^{-1} \quad \text{for } \delta \leq r \leq 1. \quad (7)$$

Clearly we have

$$\int_A \left| \int_B e(-xy\xi) dx \right| dy = |A||B| \int_A \left| \int_B e(-xy\xi) d\mu(x) \right| d\nu(y).$$

Then Lemma 2.4 and estimates (6), (7) give the result.  $\square$

### 3. Proof of Theorem 1.1

By adapting the arguments in [Guth, Katz, and Zahl 2018] and especially in [Garaev 2007] we obtain the following.

**Lemma 3.1.** *Let  $0 < \sigma < 1$ . Let  $A \subset [1, 2]$  be a  $(\delta, \sigma)$ -set with measure  $|A| = \delta^{1-\sigma}$ . Then there exists a  $(\delta, \sigma)$ -set  $T \subset [0.4, 2.1]$  with measure*

$$|T| \gtrsim \frac{|A|^2}{|AA|}$$

*such that for any  $t \in T$  we have*

$$|A + tA| \lesssim \frac{|A + A|^2 |AA|}{|A|^2}.$$

*Proof.* Let  $D = \{a_1, \dots, a_N\}$  be a maximal  $\delta$ -separated subset of  $A$ ; i.e., any two distinct elements of  $D$  have distance at least  $\delta$ , and furthermore for any  $a \in A$  there exists  $a_i \in D$  such that  $|a - a_i| \leq \delta$ . Note that

$$N \approx \delta^{-\sigma}, \quad (8)$$

and for all  $\delta \leq r \leq 1$  and  $x \in \mathbb{R}$ ,

$$\#(D \cap B(x, r)) \lesssim \left(\frac{r}{\delta}\right)^\sigma. \quad (9)$$

Let

$$f(x) = \sum_{i=1}^N \mathbf{1}_{a_i A}(x).$$

Then we have

$$\int_{\mathbb{R}} f(x) dx = \sum_{i=1}^N |a_i A| \geq N|A|, \quad (10)$$

$$\int_{\mathbb{R}} f(x)^2 dx = \sum_{1 \leq i, j \leq N} |a_i A \cap a_j A|. \quad (11)$$

By the Cauchy–Schwarz inequality we arrive at

$$\left(\int_{\mathbb{R}} f(x) dx\right)^2 \leq \int_{\mathbb{R}} f(x)^2 dx |\{x \in \mathbb{R} : f(x) > 0\}|. \quad (12)$$

Observe that

$$\{x \in \mathbb{R} : f(x) > 0\} \subset AA.$$

Thus together with (10), (11), and (12), we obtain

$$\sum_{1 \leq i, j \leq N} |a_i A \cap a_j A| \geq \frac{N^2 |A|^2}{|AA|}.$$

Thus there exists  $1 \leq j_0 \leq N$  such that

$$\sum_{1 \leq i \leq N} |a_i A \cap a_{j_0} A| \geq \frac{N |A|^2}{|AA|}.$$

Let

$$P = \left\{ 1 \leq i \leq N : |a_i A \cap a_{j_0} A| \geq \frac{|A|^2}{2|AA|} \right\}.$$

Then

$$\sum_{i \in P} |a_i A \cap a_{j_0} A| \geq \frac{N |A|^2}{2|AA|}.$$

Taking dyadic decomposition for  $|a_i A \cap a_{j_0} A|$  with  $i \in P$ , we obtain

$$\sum_{k=1}^K 2^{-k} \#P_k \gg \sum_{i \in P} |a_i A \cap a_{j_0} A| \geq \frac{N |A|^2}{2|AA|},$$

where

$$P_k = \{i \in P : 2^{-k-1} < |a_i A \cap a_{j_0} A| \leq 2^{-k}\},$$

and  $K$  is an integer parameter such that

$$2^{-K-1} < \frac{|A|^2}{2|AA|} \leq 2^{-K}.$$

Since the product set  $AA$  is a subset of  $[1, 4]$ , we have  $|AA| \ll 1$ . It follows that

$$K \ll \log\left(\frac{1}{\delta}\right).$$

Thus there exist  $\tau$  and  $D_\tau \subset P$  such that

$$\tau \# D_\tau \gtrsim \sum_{k=1}^K 2^{-k} \# P_k \gg \frac{N|A|^2}{|AA|},$$

and for any  $i \in D_\tau$  we have

$$\tau \leq |a_i A \cap a_{j_0} A| \leq 2\tau. \quad (13)$$

Since  $\tau \leq |A|$  and  $\# D_\tau \leq N$ , we obtain

$$\tau \gtrsim \frac{|A|^2}{|AA|}, \quad (14)$$

$$\# D_\tau \gtrsim \frac{N|A|}{|AA|}. \quad (15)$$

Now we intend to bound the measure of the set  $a_i A + a_{j_0} A$  for each  $i \in D_\tau$ . For this purpose we introduce some notation first.

For each  $k \in \mathbb{Z}$  let  $J_{k,\delta} = [k\delta, (k+1)\delta)$ . For each  $1 \leq i \leq N$  let

$$U_i = \bigcup_{k \in \mathbb{Z}, a_i A \cap J_{k,\delta} \neq \emptyset} J_{k,\delta}.$$

Note that

$$a_i A \subseteq U_i \subseteq a_i A + B(0, \delta), \quad (16)$$

and the intersection  $U_i \cap U_j$  is a  $\delta$ -discretized set for  $1 \leq i, j \leq N$ . Moreover for each  $i \in D_\tau$  by (13), (14) we have

$$|U_i \cap U_{j_0}| \geq |a_i A \cap a_{j_0} A| \gtrsim \frac{|A|^2}{|AA|}. \quad (17)$$

For any  $i \in D_\tau$ , applying the Ruzsa triangle inequality Lemma 2.1 for the sets  $a_i A$ ,  $a_{j_0} A$  and  $U_i \cap U_{j_0}$ , we derive

$$|a_i A + a_{j_0} A| \lesssim \frac{|a_i A + U_i \cap U_{j_0}| |U_i \cap U_{j_0} + a_{j_0} A|}{|U_i \cap U_{j_0}|}. \quad (18)$$

By (16) we have

$$a_i A + U_i \cap U_{j_0} \subseteq a_i A + a_i A + B(0, \delta).$$

Since  $1 \leq a_i \leq 2$  and the simpler fact (1) we obtain

$$|a_i A + U_i \cap U_{j_0}| \ll |A + A|.$$

Similarly, we have

$$|a_{j_0}A + U_i \cap U_{j_0}| \ll |A + A|.$$

Combining with (17) and (18) we arrive at

$$|a_iA + a_{j_0}A| \lesssim \frac{|A + A|^2 |AA|}{|A|^2}.$$

Applying Lemma 2.2 we obtain that for any  $i \in D_\tau$  and  $x \in (-\delta, \delta)$  we have

$$\left| A + \left( \frac{a_i}{a_{j_0}} + x \right) A \right| \lesssim \frac{|A + A|^2 |AA|}{|A|^2}.$$

Let

$$T = \bigcup_{i \in D_\tau} B\left(\frac{a_i}{a_{j_0}}, \frac{\delta}{2}\right).$$

We ask that  $\delta$  is a small positive parameter, and hence  $T \subset [0.4, 2.1]$ . Furthermore, the estimates (8), (15) imply

$$|T| \gg \#D_\tau \delta \gtrsim \frac{|A|^2}{|AA|}.$$

By (9) we obtain that  $T$  is a  $(\delta, \sigma)$ -set, which finishes the proof.  $\square$

Applying Lemma 2.4 we obtain the following upper bound of the mean value of energies  $E(A, tA)$ .

**Lemma 3.2.** *Fix  $\frac{1}{2} < \sigma < 1$ . Let  $T \subset [0.4, 2.1]$  be a  $(\delta, \sigma)$ -set with the measure  $|T| \geq \delta$ . Let  $A \subset [1, 2]$  be a  $(\delta, \sigma)$ -set with measure  $|A| = \delta^{1-\sigma}$ . Then*

$$\int_T E(A, tA) dt \lesssim |A|^3 |T| (|A|^{\frac{2\sigma}{1+2\sigma}} |T|^{-\frac{1}{1+2\sigma}} + \delta(|A||T|)^{-1}).$$

*Proof.* For each  $t \in \mathbb{R}$  and  $\xi \in \mathbb{R}$  we have

$$t\widehat{A}(\xi) = t\hat{A}(t\xi).$$

Thus by (3) and the condition  $T \subset [0.4, 2.1]$  we conclude that

$$\int_T E(A, tA) dt \ll \int_T \int_{\mathbb{R}} |\hat{A}(\xi)|^2 |\hat{A}(t\xi)|^2 dt d\xi. \quad (19)$$

Let  $0 < L < 1/\delta$  be a parameter which will be determined later. We decompose  $\mathbb{R}$  into three parts, and then bound (19) by three corresponding parts. Precisely,

$$(19) \ll I_0 + I_1 + I_2, \quad (20)$$

where

$$I_0 = \int_T \int_{|\xi| \leq L} |\hat{A}(\xi)|^2 |\hat{A}(t\xi)|^2 dt d\xi,$$

$$I_1 = \int_T \int_{L \leq |\xi| \leq \delta^{-1}} |\hat{A}(\xi)|^2 |\hat{A}(t\xi)|^2 dt d\xi,$$

and

$$I_2 = \int_T \int_{|\xi| \geq \delta^{-1}} |\hat{A}(\xi)|^2 |\hat{A}(t\xi)|^2 dt d\xi.$$

For  $I_0$ , we use the trivial bound  $|\hat{A}(\xi)| \leq |A|$ , and we obtain

$$I_0 \leq |A|^4 |T| L. \quad (21)$$

For  $I_1$ , clearly the trivial bound  $|\hat{A}(\xi)| \leq |A|$  gives

$$\int_T |\hat{A}(\xi t)|^2 dt \leq |A| \int_T |\hat{A}(\xi t)| dt. \quad (22)$$

Applying Lemma 2.4, and the condition  $|A| = \delta^{1-\sigma}$ , we obtain

$$\int_T |\hat{A}(\xi t)| dt \lesssim |A|^{\frac{3}{2}} |T|^{\frac{1}{2}} |\xi|^{-\frac{2\sigma-1}{2}}.$$

Thus we arrive at

$$(22) \lesssim |A|^{\frac{5}{2}} |T|^{\frac{1}{2}} |\xi|^{-\frac{2\sigma-1}{2}}.$$

Combining with Fubini's theorem and the condition  $\sigma > \frac{1}{2}$ , we have

$$\begin{aligned} I_1 &\lesssim |A|^{\frac{5}{2}} |T|^{\frac{1}{2}} \int_{L \leq |\xi| \leq \delta^{-1}} |\hat{A}(\xi)|^2 |\xi|^{-\frac{2\sigma-1}{2}} d\xi \\ &\lesssim |A|^{\frac{5}{2}} |T|^{\frac{1}{2}} L^{-\frac{2\sigma-1}{2}} \int_{L \leq |\xi| \leq \delta^{-1}} |\hat{A}(\xi)|^2 d\xi. \end{aligned}$$

The Plancherel identity (5) implies

$$\int_{L \leq |\xi| \leq \delta^{-1}} |\hat{A}(\xi)|^2 d\xi \leq |A|.$$

Thus we arrive at

$$I_1 \lesssim |A|^{\frac{7}{2}} |T|^{\frac{1}{2}} L^{-\frac{2\sigma-1}{2}}. \quad (23)$$

Now we optimize the choice of the parameter  $L$  to find the smallest upper bound for the parts  $I_0, I_1$ . Recall that we assumed  $0 < L < 1/\delta$ . In the end, the parameter  $L_0$ , which makes the right-hand sides of (21), (23) “comparable”, satisfies our need. Thus we derive

$$L_0 = (|A||T|)^{-\frac{1}{1+2\sigma}}. \quad (24)$$

Indeed the conditions  $|A| = \delta^{1-\sigma}$ ,  $|T| \geq \delta$ , and  $\frac{1}{2} < \sigma < 1$  imply that  $L_0 \leq \delta^{-1}$ . It follows that

$$I_0, I_1 \lesssim |A|^4 |T| L_0 \lesssim |A|^3 |T| (|A|^{\frac{2\sigma}{1+2\sigma}} |T|^{-\frac{1}{1+2\sigma}}). \quad (25)$$

Now we turn to the estimate for  $I_2$ . By changing variables and applying the Plancherel identity we obtain

$$\int_{\mathbb{R}} |\hat{A}(t\xi)|^2 dt \leq |A| |\xi|^{-1}.$$

Again by applying the Plancherel identity we have

$$I_2 \leq \int_{|\xi| \geq \delta^{-1}} |\hat{A}(\xi)|^2 |A| |\xi|^{-1} d\xi \ll |A|^2 \delta.$$

Combining with (20), (21), (24), (25), we obtain the desired bound.  $\square$

Now we turn to the proof of Theorem 1.1. Suppose that

$$\max\{|A + A|, |AA|\} = K|A|.$$

By Lemma 3.1 there exists a  $(\delta, \sigma)$ -set  $T \subset [0.4, 2]$  such that

$$|T| \gtrsim \frac{|A|}{K}, \quad (26)$$

and for each  $t \in T$  we have

$$|A + tA| \lesssim K^3 |A|. \quad (27)$$

Applying Lemma 3.2 to  $A$  and  $T$ , we conclude that there exists a  $t_0 \in T$  such that

$$E(A, t_0 A) \lesssim |A|^3 (|A|^{\frac{2\sigma}{1+2\sigma}} |T|^{-\frac{1}{1+2\sigma}} + \delta(|A||T|)^{-1}).$$

By (4) and estimates (26), (27), we obtain

$$\begin{aligned} |A| &\lesssim (|A|^{\frac{2\sigma}{1+2\sigma}} |T|^{-\frac{1}{1+2\sigma}} + \delta(|A||T|)^{-1}) |A + t_0 A| \\ &\lesssim |A|^{\frac{2\sigma-1}{2\sigma+1}} |A| K^{\frac{6\sigma+4}{2\sigma+1}} + |A|^{-1} \delta K^4. \end{aligned}$$

It follows that

$$K \gtrsim \min\left\{\delta^{-\frac{(1-\sigma)(2\sigma-1)}{6\sigma+4}}, \delta^{-\frac{2\sigma-1}{4}}\right\}.$$

Note that for  $\frac{1}{2} < \sigma < 1$  we have

$$\frac{(1-\sigma)(2\sigma-1)}{6\sigma+4} \leq \frac{2\sigma-1}{4},$$

and hence

$$K \gtrsim \delta^{-\frac{(1-\sigma)(2\sigma-1)}{6\sigma+4}},$$

which gives the result.

### Acknowledgement

The author is grateful to Igor Shparlinski for his comments on the initial draft. The author would especially like to thank the anonymous referee for carefully reading the manuscript and giving excellent comments, and thus improving the quality of this article.

This work was supported in part by ARC grant DP170100786.

## References

- [Bourgain 2003] J. Bourgain, “On the Erdős–Volkman and Katz–Tao ring conjectures”, *Geom. Funct. Anal.* **13**:2 (2003), 334–365. MR Zbl
- [Bourgain 2010] J. Bourgain, “The discretized sum-product and projection theorems”, *J. Anal. Math.* **112** (2010), 193–236. MR Zbl
- [Edgar and Miller 2003] G. A. Edgar and C. Miller, “Borel subrings of the reals”, *Proc. Amer. Math. Soc.* **131**:4 (2003), 1121–1129. MR Zbl
- [Erdős and Volkmann 1966] P. Erdős and B. Volkmann, “Additive Gruppen mit vorgegebener Hausdorffscher Dimension”, *J. Reine Angew. Math.* **221** (1966), 203–208. MR Zbl
- [Falconer 2003] K. Falconer, *Fractal geometry: mathematical foundations and applications*, 2nd ed., John Wiley & Sons, Hoboken, NJ, 2003. MR Zbl
- [Garaev 2007] M. Z. Garaev, “An explicit sum-product estimate in  $\mathbb{F}_p$ ”, *Int. Math. Res. Not.* **2007**:11 (2007), art. id. rnm035. MR Zbl
- [Guth, Katz, and Zahl 2018] L. Guth, N. H. Katz, and J. Zahl, “On the discretized sum-product problem”, preprint, 2018. arXiv
- [He 2017a] W. He, “Orthogonal projections of discretized sets”, preprint, 2017. arXiv
- [He 2017b] W. He, *Sums, products and projections of discretized sets*, Ph.D. thesis, Université Paris-Saclay, 2017, <https://tel.archives-ouvertes.fr/tel-01680114/document>.
- [Katz and Tao 2001] N. H. Katz and T. Tao, “Some connections between Falconer’s distance set conjecture and sets of Furstenberg type”, *New York J. Math.* **7** (2001), 149–187. MR Zbl
- [Li 2018] J. Li, “Discretized sum-product and Fourier decay in  $\mathbb{R}^n$ ”, preprint, 2018. arXiv
- [Orponen 2016] T. Orponen, “An improved bound on the packing dimension of Furstenberg sets in the plane”, preprint, 2016. To appear in *J. Eur. Math. Soc.* arXiv
- [Tao 2014] T. Tao, “Metric entropy analogues of sum set theory”, blog post, 19 March 2014, <https://terrytao.wordpress.com/tag/metric-entropy/>.
- [Tao and Vu 2006] T. Tao and V. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics **105**, Cambridge University Press, 2006. MR Zbl

Received 17 Jun 2019. Revised 3 Oct 2019.

CHANGHAO CHEN:

[changhao.chenm@gmail.com](mailto:changhao.chenm@gmail.com)

School of Mathematics and Statistics, University of New South Wales, Sydney, NSW, Australia



# Positive semigroups and generalized Frobenius numbers over totally real number fields

Lenny Fukshansky and Yingqi Shi

The Frobenius problem and its many generalizations have been extensively studied in several areas of mathematics. We study semigroups of totally positive algebraic integers in totally real number fields, defining analogues of the Frobenius numbers in this context. We use a geometric framework recently introduced by Aliev, De Loera and Louveaux to produce upper bounds on these Frobenius numbers in terms of a certain height function. We discuss some properties of this function, relating it to absolute Weil height and obtaining a lower bound in the spirit of Lehmer's conjecture for algebraic vectors satisfying some special conditions. We also use a result of Borosh and Treybig to obtain bounds on the size of representations and number of elements of bounded height in such positive semigroups of totally real algebraic integers.

## 1. Introduction

Let  $n \geq 2$  be an integer and let

$$1 < a_1 < \cdots < a_n \tag{1}$$

be relatively prime integers. We say that a positive integer  $t$  is *representable* by the  $n$ -tuple  $\mathbf{a} := (a_1, \dots, a_n)$  if

$$t = a_1x_1 + \cdots + a_nx_n \tag{2}$$

for some nonnegative integers  $x_1, \dots, x_n$ , and we call each such a solution  $\mathbf{x} := (x_1, \dots, x_n)$  of (2) a *representation for  $t$  in terms of  $\mathbf{a}$* . Let  $s \geq 0$  be an integer; then the  *$s$ -Frobenius number* of this  $n$ -tuple,  $g_s(\mathbf{a})$ , as defined in [Beck and Robins 2004], is the largest positive integer that has at most  $s$  distinct representations in terms of  $\mathbf{a}$ . This is a generalization of the classical Frobenius number  $g_0(\mathbf{a})$ , i.e., the largest positive integer that has no such representations. The Frobenius number has been studied extensively by a variety of authors, starting as early as late 19th century; see [Ramírez Alfonsín 2005] for a detailed account and bibliography. The condition

$$\gcd(a_1, \dots, a_n) = 1 \tag{3}$$

implies that  $g_s(\mathbf{a})$  exists for every  $s$ . The algorithmic *Frobenius problem*, known to be NP-hard, is to determine  $g_0$  (or more generally  $g_s$  for  $s \geq 1$ ) given  $n$  and the relatively prime  $n$ -tuple  $a_1, \dots, a_n$  on the

---

Fukshansky was partially supported by the Simons Foundation grant #519058.

MSC2010: 11D07, 11H06, 52C07, 11D45, 11G50.

Keywords: linear Diophantine problem of Frobenius, lattice points in polyhedra, affine semigroups, totally real number fields, heights.

input. The hardness of this problem in particular implies that no general closed form formulas for the Frobenius numbers exist, sparking interest in upper and lower bounds.

A geometric approach to the classical Frobenius problem was pioneered in the influential paper of R. Kannan [1992], leading to a polynomial-time algorithm to find the Frobenius number for each fixed  $n$ . Bounds on the classical Frobenius number stemming from further geometry-of-numbers applications were obtained in [Fukshansky and Robins 2007; Aliev and Gruber 2007]. These ideas were also extended to the more general  $s$ -Frobenius problem in [Fukshansky and Schürmann 2011; Aliev et al. 2012]. A higher-dimensional analogue of the Frobenius problem was also considered in recent years by several authors, notably in [Aliev and Henk 2010; Aliev et al. 2013; 2016].

This note is inspired by the work of Aliev, De Loera and Louveaux [Aliev et al. 2016]. We use the geometric setup and results of that paper (described in Section 2) to define a natural extension of the Frobenius problem to totally real number fields and to give bounds on the  $s$ -Frobenius numbers in this context. Let  $K$  be a totally real number field of degree  $d$  over  $\mathbb{Q}$  with embeddings  $\sigma_1, \dots, \sigma_d : K \rightarrow \mathbb{R}$ . Let

$$\Sigma := (\sigma_1, \dots, \sigma_d) : K \rightarrow \mathbb{R}^d$$

be the Minkowski embedding of  $K$ . Let  $\mathcal{O}_K$  be the ring of integers of  $K$ , and  $\mathcal{O}_K^+$  the additive semigroup of totally positive elements in  $\mathcal{O}_K$ ; i.e.,

$$\mathcal{O}_K^+ := \{\alpha \in \mathcal{O}_K : \sigma_i(\alpha) \geq 0 \text{ for all } 1 \leq i \leq d\}.$$

Let  $n > d$  and let  $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K^+$  be a collection of elements so that

$$\mathcal{O}_K = \text{span}_{\mathbb{Z}}\{\alpha_1, \dots, \alpha_n\}. \quad (4)$$

Such a collection always exists, since there exist bases for  $\mathcal{O}_K$  in  $\mathcal{O}_K^+$ . Indeed, let  $\omega_1, \dots, \omega_d$  be a  $\mathbb{Z}$ -basis for  $\mathcal{O}_K$ , where  $\omega_1 = 1$ , and suppose it is not in  $\mathcal{O}_K^+$ . Let

$$M = \left[ \max_{1 \leq i, j \leq d} |\sigma_i(\omega_j)| \right] + 1,$$

where  $[ \ ]$  stands for integer part. Then  $1, M + \omega_2, \dots, M + \omega_d \in \mathcal{O}_K^+$  and it is still a  $\mathbb{Z}$ -basis for  $\mathcal{O}_K$ . Write  $\alpha = (\alpha_1, \dots, \alpha_n)$ . Define the semigroup generated by  $\alpha$  to be

$$\text{Sg}(\alpha) := \left\{ \sum_{i=1}^n \alpha_i x_i : \mathbf{x} \in \mathbb{Z}_{\geq 0}^n \right\},$$

and the rational cone spanned by  $\alpha$  to be

$$\mathcal{C}_{\mathbb{Q}}(\alpha) := \left\{ \sum_{i=1}^n \alpha_i x_i : \mathbf{x} \in \mathbb{Q}_{\geq 0}^n \right\}.$$

Then it is clear that  $\text{Sg}(\alpha) \subseteq \mathcal{C}_{\mathbb{Q}}(\alpha) \cap \mathcal{O}_K \subseteq \mathcal{O}_K^+$ , and  $\text{Sg}(\alpha)$  is not necessarily equal to  $\mathcal{C}_{\mathbb{Q}}(\alpha) \cap \mathcal{O}_K$ .

**Example 1.** Indeed, consider for instance the real quadratic field  $K = \mathbb{Q}(\sqrt{2})$  and take

$$\alpha_1 = 1, \quad \alpha_2 = 4 + \sqrt{2}, \quad \alpha_3 = 6 + 2\sqrt{2}.$$

One easily checks that these three elements are in  $\mathcal{O}_K^+$  and

$$\mathcal{O}_K = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} = \{(a - 4b)\alpha_1 + b\alpha_2 : a, b \in \mathbb{Z}\}.$$

Then

$$\text{Sg}(\boldsymbol{\alpha}) = \{(x_1 + 4x_2 + 6x_3) + (x_2 + 2x_3)\sqrt{2} : x_1, x_2, x_3 \in \mathbb{Z}_{\geq 0}\}.$$

On the other hand,

$$3 + \sqrt{2} = \frac{1}{2}\alpha_3 \in \mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha}) \cap \mathcal{O}_K,$$

but it is clearly not in  $\text{Sg}(\boldsymbol{\alpha})$ .

Further, for each  $s \geq 1$  let  $\text{Sg}_s(\boldsymbol{\alpha})$  be the set of all points  $\beta \in \text{Sg}(\boldsymbol{\alpha})$  for which there are at least  $s$  distinct points  $\mathbf{x} \in \mathbb{Z}_{>0}^n$  such that  $\sum_{i=1}^n \alpha_i x_i = \beta$ ; then  $\text{Sg}(\boldsymbol{\alpha}) = \text{Sg}_1(\boldsymbol{\alpha})$ .

Now, let  $\beta \in \mathcal{O}_K^+$  be in the interior of the cone  $\mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha})$  and take the ray  $t\beta$  as  $t \in \mathbb{Z}_{>0}$ . Shifting the cone  $\mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha})$  along this ray and intersecting it with  $\mathcal{O}_K$  we will eventually land in the semigroup  $\text{Sg}(\boldsymbol{\alpha})$  (this observation will follow from our results). In other words, there exists a positive integer  $t$  such that

$$\text{int}(t\beta + \mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha})) \cap \mathcal{O}_K \subseteq \text{Sg}(\boldsymbol{\alpha}).$$

More precisely, for each  $s \geq 1$  we can define

$$g_s(\boldsymbol{\alpha}, \beta) := \min\{t \in \mathbb{Z}_{>0} : \text{int}(t\beta + \mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha})) \cap \mathcal{O}_K \subseteq \text{Sg}_s(\boldsymbol{\alpha})\},$$

and let

$$g_s(\boldsymbol{\alpha}) := \max\{g_s(\boldsymbol{\alpha}, \beta) : \beta \in \text{int}(\mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha})) \cap \mathcal{O}_K^+\}.$$

We refer to  $g_s(\boldsymbol{\alpha})$  as the *s-Frobenius number of  $\boldsymbol{\alpha}$* .

We can see that when  $K = \mathbb{Q}$  this construction reduces to the usual  $s$ -Frobenius numbers. Indeed, if  $K = \mathbb{Q}$  then  $\mathcal{O}_K = \mathbb{Z}$  and  $\mathcal{O}_K^+ = \mathbb{Z}_{\geq 0}$ , and (4) simply means that  $\alpha_1, \dots, \alpha_n$  are positive relatively prime integers. Then  $\text{Sg}(\boldsymbol{\alpha})$  is the semigroup of all positive integers representable by  $\boldsymbol{\alpha}$ ,  $\mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha}) = \mathbb{Q}_{\geq 0}$ , and so  $\mathcal{C}_{\mathbb{Q}}(\boldsymbol{\alpha}) \cap \mathbb{Z}_{\geq 0} = \mathbb{Z}_{\geq 0}$ . Then

$$\max_{\beta \in \mathbb{Z}_{\geq 0}} \min\{t \in \mathbb{Z}_{>0} : \text{int}(t\beta + \mathbb{Q}_{\geq 0}) \cap \mathbb{Z} \subseteq \text{Sg}_s(\boldsymbol{\alpha})\} \leq \min\{t \in \mathbb{Z}_{>0} : \text{int}(t + \mathbb{Q}_{\geq 0}) \cap \mathbb{Z} \subseteq \text{Sg}_s(\boldsymbol{\alpha})\}$$

is precisely the smallest integer  $t$  so that all integers  $> t$  have at least  $s$  representations by  $\boldsymbol{\alpha}$ .

We present an upper bound on  $g_s(\boldsymbol{\alpha})$ . To state it, we need to introduce a certain measure of arithmetic complexity of  $\boldsymbol{\alpha}$ . Let us write  $[n] := \{1, \dots, n\}$  and define  $\mathcal{J}(n, d) := \{I \subset [n] : |I| = d\}$ . For each  $I = \{i_1, \dots, i_d\} \in \mathcal{J}(n, d)$ , let us write  $\text{disc}(\boldsymbol{\alpha}_I)$  for the discriminant of the subcollection  $\alpha_{i_1}, \dots, \alpha_{i_d}$ . We also write  $\Delta_K$  for the discriminant of  $K$ , and define

$$\mathcal{D}(\boldsymbol{\alpha}) := \frac{1}{|\Delta_K|} \sum_{I \in \mathcal{J}(n, d)} |\text{disc}(\boldsymbol{\alpha}_I)|. \quad (5)$$

Notice that absolute values in this definition are not necessary in the case of a real number field, since all the quantities are positive; we put them there so that this definition can be naturally extended to any number field. We now state our theorem.

**Theorem 1.1.** *With notation as above,*

$$g_s(\boldsymbol{\alpha}) \leq \frac{1}{2\sqrt{n-d+1}} ((n-d)\mathcal{D}(\boldsymbol{\alpha}) + (s-1)^{1/(n-d)}\mathcal{D}(\boldsymbol{\alpha})^{(n-d+1)/(2(n-d))}).$$

We prove Theorem 1.1 in Section 2. Now suppose that  $\beta \in \text{Sg}(\boldsymbol{\alpha})$ ; hence there exists  $\mathbf{x} \in \mathbb{Z}_{\geq 0}^n$  such that  $\sum_{i=1}^n \alpha_i x_i = \beta$ . It is natural to ask for the smallest such representation for  $\beta$ . In other words, given  $\beta \in \text{Sg}(\boldsymbol{\alpha})$  we want to find  $\mathbf{x} \in \mathbb{Z}_{\geq 0}^n$  such that  $\sum_{i=1}^n \alpha_i x_i = \beta$  with  $|\mathbf{x}| := \max\{x_i : 1 \leq i \leq n\}$  as small as possible. This is our next result. To state it, let  $\boldsymbol{\alpha}(\beta) := (\alpha_1, \dots, \alpha_n, \beta) \in K^{n+1}$  and define

$$\mathcal{M}(\boldsymbol{\alpha}, \beta) := \frac{1}{|\Delta_K|^{1/2}} \max_{I \in \mathcal{J}(n+1, d)} |\text{disc}(\boldsymbol{\alpha}(\beta)_I)|^{1/2}. \quad (6)$$

We also briefly recall the definition of a standard Weil-type height on  $K$ . Let us write  $M(K)$  for the set of places of  $K$ , and for each  $v \in M(K)$  let  $d_v := [K_v : \mathbb{Q}_v]$  be the local degree of  $K$  at  $v$ ; in particular,  $\sum_{v|u} d_v = d$  for each  $u \in M(\mathbb{Q})$ . Let us normalize absolute values so that the product formula reads

$$\prod_{v \in M(K)} |a|_v = 1$$

for all nonzero  $a \in K$ . Then the usual *inhomogeneous height function*  $H_K : K^n \rightarrow \mathbb{R}$ , which extends Weil height on  $K$ , is defined as

$$H_K(\boldsymbol{\alpha}) = \prod_{v \in M(K)} \max\{1, |\alpha_1|_v, \dots, |\alpha_n|_v\}. \quad (7)$$

We can now state our next result.

**Theorem 1.2.** *With notation as above, let  $\beta \in \text{Sg}(\boldsymbol{\alpha})$ . Then there exists  $\mathbf{x} \in \mathbb{Z}_{\geq 0}^n$  such that  $\sum_{i=1}^n \alpha_i x_i = \beta$ , and for any such  $\mathbf{x}$  we have*

$$\frac{1}{n} \left( \frac{H_K(\beta)}{H_K(\boldsymbol{\alpha})} \right)^{1/d} \leq |\mathbf{x}| \leq \mathcal{M}(\boldsymbol{\alpha}, \beta).$$

We discuss some properties of  $\mathcal{D}(\boldsymbol{\alpha})$  and  $\mathcal{M}(\boldsymbol{\alpha}, \beta)$  in Section 3, viewing them as kinds of height functions. We use these properties along with Theorem 1.1 to obtain a lower bound on absolute Weil height of  $\boldsymbol{\alpha}$  in the spirit of Lehmer's conjecture on heights of algebraic numbers.

We use a result of [Borosh and Treybig 1976] to prove Theorem 1.2 in Section 4. This theorem also allows us to obtain a counting estimate on the number of points of bounded height in the positive semigroup  $\text{Sg}(\boldsymbol{\alpha})$ .

**Theorem 1.3.** *With notation as above, let  $T_1, T_2 \in \mathbb{R}_{\geq 0}$  with  $T_1 < T_2$ , and define*

$$\text{Sg}_s(\boldsymbol{\alpha}, T_1, T_2) = \{\beta \in \text{Sg}_s(\boldsymbol{\alpha}) : T_1 \leq H_K(\beta) \leq T_2\}.$$

*Additionally, for each  $\beta \in \text{Sg}(\boldsymbol{\alpha})$  define  $r(\beta) = \max\{s : \beta \in \text{Sg}_s(\boldsymbol{\alpha})\}$ . Then*

$$\sum_{\beta \in \text{Sg}_1(\boldsymbol{\alpha}, T_1, T_2)} r(\beta) \leq \left( \frac{d! H_K(\boldsymbol{\alpha})}{|\Delta_K|^{1/2}} T_2 + 1 \right)^n - \left[ \frac{T_1^{1/d}}{n H_K(\boldsymbol{\alpha})^{1/d}} \right]^n.$$

In particular,

$$|\text{Sg}_s(\boldsymbol{\alpha}, T_1, T_2)| \leq \frac{1}{s} \left\{ \left( \frac{d! H_K(\boldsymbol{\alpha})}{|\Delta_K|^{1/2}} T_2 + 1 \right)^n - \left[ \frac{T_1^{1/d}}{n H_K(\boldsymbol{\alpha})^{1/d}} \right]^n \right\}. \quad (8)$$

On the other hand, for  $T \geq 1$ ,

$$\sum_{\beta \in \text{Sg}_1(\boldsymbol{\alpha}, 1, T)} r(\beta) \geq \left[ \frac{T_1^{1/d}}{n H_K(\boldsymbol{\alpha})^{1/d}} \right]^n.$$

Theorem 1.3 is also proved in Section 4. It is instructive to compare the bounds of Theorem 1.3 to the known estimates on the number of algebraic integers of bounded height in a fixed number field. A result attributed to S. Lang (see [Widmer 2016] for details) asserts that in our case of a totally real number field  $K$ ,

$$|\{\beta \in \mathcal{O}_K : H_K(\beta) \leq T\}| = O(T^{d^2} (\log T)^{d-1}).$$

This implies that our bound (8) is nontrivial when  $n \leq d^2$ . We are now ready to proceed.

## 2. Polyhedral semigroups and proof of Theorem 1.1

We start by briefly describing the setup and some results of [Aliev et al. 2016]. Let  $A$  be a  $d \times n$  integer matrix, and for each set  $I \in \mathcal{J}(n, d)$  let  $A_I$  be the  $d \times d$  submatrix of  $A$  whose columns are indexed by  $I$ . Assume that

- (1)  $\gcd(\det(A_I) : I \in \mathcal{J}(n, d)) = 1$ ,
- (2)  $\{\mathbf{x} \in \mathbb{R}_{\geq 0}^n : A\mathbf{x} = \mathbf{0}\} = \{\mathbf{0}\}$ .

Define the additive semigroup

$$\text{Sg}(A) := \{\mathbf{b} \in \mathbb{Z}^d : \mathbf{b} = A\mathbf{x} \text{ for some } \mathbf{x} \in \mathbb{Z}_{\geq 0}^n\},$$

and for each  $s \geq 1$  let  $\text{Sg}_s(A)$  be the set of all points  $\mathbf{b} \in \text{Sg}(A)$  for which there are at least  $s$  distinct points  $\mathbf{x} \in \mathbb{Z}_{\geq 0}^n$  such that  $A\mathbf{x} = \mathbf{b}$ . Thus  $\text{Sg}(A) = \text{Sg}_1(A)$ . Let

$$\mathcal{C}_{\mathbb{R}}(A) = \{A\mathbf{x} : \mathbf{x} \in \mathbb{R}_{\geq 0}^n\}$$

be the convex polyhedral cone spanned by the column vectors of  $A$ . Then it is clear that

$$\text{Sg}(A) \subseteq \mathcal{C}_{\mathbb{R}}(A) \cap \mathbb{Z}^d,$$

and this containment is often proper; i.e., in general  $\text{Sg}(A) \neq \mathcal{C}_{\mathbb{R}}(A) \cap \mathbb{Z}^d$ . For each  $\mathbf{b} \in \text{int}(\mathcal{C}_{\mathbb{R}}(A)) \cap \mathbb{Z}^d$ , define

$$g_s(A, \mathbf{b}) = \min\{t \in \mathbb{Z}_{>0} : \text{int}(t\mathbf{b} + \mathcal{C}_{\mathbb{R}}(A)) \cap \mathbb{Z}^d \subseteq \text{Sg}_s(A)\},$$

and let

$$g_s(A) := \max\{g_s(\boldsymbol{\alpha}, \beta) : \beta \in \text{int}(\mathcal{C}_{\mathbb{R}}(A)) \cap \mathbb{Z}^d\}.$$

This is the  $s$ -Frobenius number of  $A$  as defined in [Aliev et al. 2016]. The upper bound on  $g_s(A)$  proved in that paper (Theorem 2) is

$$g_s(A) \leq \frac{1}{2\sqrt{n-d+1}} ((n-d) \det(AA^\top) + (s-1)^{1/(n-d)} \det(AA^\top)^{(n-d+1)/(2(n-d))}). \quad (9)$$

We can now use this result to prove our Theorem 1.1. Our strategy is straightforward: we use the Minkowski embedding to convert our setup into that of a lattice in a Euclidean space, prove that our resulting ingredients satisfy the hypotheses of Theorem 2 of [Aliev et al. 2016], apply their bound (9), and then reinterpret it in terms of the original setup in the number field.

*Proof of Theorem 1.1.* Let the setup be as in Section 1. Let  $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K^+$  be a collection of elements satisfying (4), and let us fix  $\omega_1, \dots, \omega_d$ , a  $\mathbb{Z}$ -basis for  $\mathcal{O}_K$ . Then there exist integers  $a_{ij}$ , where  $1 \leq i \leq n$ ,  $1 \leq j \leq d$  so that

$$\alpha_i = \sum_{j=1}^d a_{ij} \omega_j.$$

Let us write  $A = (a_{ij})^\top$  for the  $d \times n$  matrix of these integer coefficients. Let

$$B = (\Sigma(\omega_1) \ \cdots \ \Sigma(\omega_d)).$$

Then  $\Delta_K = \det(B)^2$  and

$$C := (\Sigma(\alpha_1) \ \cdots \ \Sigma(\alpha_n)) = BA.$$

Since  $\alpha_1, \dots, \alpha_n$  satisfy (4), we must have  $\Sigma(\mathcal{O}_K) = C\mathbb{Z}^n$ . On the other hand, certainly  $\Sigma(\mathcal{O}_K) = B\mathbb{Z}^d$ ; hence  $B\mathbb{Z}^d = B(A\mathbb{Z}^n)$ , which means that  $A\mathbb{Z}^n = \mathbb{Z}^d$ . This implies that row vectors of  $A$  are extendable to a basis for  $\mathbb{Z}^n$ . By Lemma 2 on p. 15 of [Cassels 1959], this is equivalent to the condition that

$$\gcd(\det(A_I) : I \in \mathcal{J}(n, d)) = 1.$$

Now suppose  $\mathbf{x} \in \mathbb{R}_{\geq 0}^n$  and assume  $A\mathbf{x} = \mathbf{0}$ . Then

$$C\mathbf{x} = B(A\mathbf{x}) = \mathbf{0},$$

but entries of  $C$  are of the form  $\sigma_i(\alpha_j)$ , which are all positive real numbers, since  $\alpha_j \in \mathcal{O}_K^+$ . Therefore  $\mathbf{x}$  must be equal to  $\mathbf{0}$ , and so

$$\{\mathbf{x} \in \mathbb{R}_{\geq 0}^n : A\mathbf{x} = \mathbf{0}\} = \{\mathbf{0}\}.$$

Thus matrix  $A$  satisfies conditions (1) and (2) above, and so we can apply (9) to get a bound on  $g_s(A)$ .

Now notice that  $\Sigma(C_{\mathbb{Q}}(\boldsymbol{\alpha})) = BC_{\mathbb{Q}}(A)$ , where

$$C_{\mathbb{Q}}(A) := \{A\mathbf{x} : \mathbf{x} \in \mathbb{Q}_{\geq 0}^n\},$$

and  $\text{int}(C_{\mathbb{R}}(A)) \cap \mathbb{Z}^d = \text{int}(C_{\mathbb{Q}}(A)) \cap \mathbb{Z}^d$ . Indeed, it is clear that

$$\text{int}(C_{\mathbb{Q}}(A)) \cap \mathbb{Z}^d \subseteq \text{int}(C_{\mathbb{R}}(A)) \cap \mathbb{Z}^d,$$

so let us show containment in the opposite direction. Suppose  $\mathbf{z} \in \text{int}(C_{\mathbb{R}}(A)) \cap \mathbb{Z}^d$ . Then there exists  $\mathbf{x} \in \mathbb{R}_{\geq 0}^n$  such that

$$A\mathbf{x} = \mathbf{z}.$$

In fact, this equation defines a hyperplane in  $\mathbb{R}^n$ , which is defined over  $\mathbb{Q}$  (since  $A$  and  $\mathbf{z}$  have integer coordinates), and hence points with rational coordinates are dense in it. Thus taking a sufficiently small open ball in this hyperplane centered at  $\mathbf{x}$ , we can find a rational point with positive coordinates satisfying the same equation. This means that  $\mathbf{z} \in \text{int}(C_{\mathbb{Q}}(A)) \cap \mathbb{Z}^d$ .

With this setup in mind, let  $\beta \in \text{int}(\mathcal{C}_{\mathbb{Q}}(\alpha)) \cap \mathcal{O}_K^+$  and let  $\mathbf{b} \in \mathbb{Z}^d$  be such that  $\Sigma(\beta) = B\mathbf{b}$ . Then for  $t \in \mathbb{Z}_{>0}$  we have

$$\begin{aligned} \text{int}(t\beta + \mathcal{C}_{\mathbb{Q}}(\alpha)) \cap \mathcal{O}_K &\subseteq \text{Sg}_s(\alpha) \iff \text{int}(tB\mathbf{b} + BC_{\mathbb{Q}}(A)) \cap B\mathbb{Z}^d \subseteq B \text{Sg}_s(A) \\ &\iff \text{int}(t\mathbf{b} + C_{\mathbb{R}}(A)) \cap \mathbb{Z}^d \subseteq \text{Sg}_s(A). \end{aligned}$$

This implies that  $g_s(\alpha) = g_s(A)$ , and so we only need to express  $\det(AA^\top)$  in terms of  $\alpha$ . Notice that

$$\det(AA^\top) = \det((B^{-1}C)(B^{-1}C)^\top) = \frac{1}{\det(B)^2} \det(CC^\top).$$

Now,  $\det(B)^2 = \Delta_K$ , and by the Cauchy–Binet formula

$$\det(CC^\top) = \sum_{I \in \mathcal{J}(n,d)} \det(C_I)^2,$$

where for each  $I = \{i_1, \dots, i_d\}$ ,

$$\det(C_I)^2 = \det(\Sigma(\alpha_{i_1}) \cdots \Sigma(\alpha_{i_d}))^2 = \text{disc}(\alpha_I).$$

Combining these observations with (9) completes the proof.  $\square$

### 3. Height functions

In this section we study some basic properties of the functions  $\mathcal{D}(\alpha)$  and  $\mathcal{M}(\alpha, \beta)$  that we introduced in (5) and (6), respectively. Since we view these functions as certain measures of arithmetic complexity, it makes sense to compare them to a traditional height function on number fields.

Until further notice, let  $K$  be any number field of degree  $d$ , not necessarily totally real as above. As in (7) above, we write  $H_K$  for the inhomogeneous height on  $K$ . We can also define the absolute version of Weil height by  $H(\alpha) = H_K(\alpha)^{1/d}$ : this height no longer depends on the field of definition. Let us establish some basic properties of  $\mathcal{D}$  and  $\mathcal{M}$  as defined in (5) and (6), respectively.

**Lemma 3.1.** *Let  $K$  be a number field of degree  $d$  over  $\mathbb{Q}$ ,  $n \geq d$ , and let  $\alpha \in K^n$ ,  $\beta \in K$ . Then the following are true:*

- (1)  $\mathcal{D}(\alpha) = 0$  if and only if  $\text{span}_{\mathbb{Q}} \alpha \neq K$ , and  $\mathcal{M}(\alpha, \beta) = 0$  if and only if  $\text{span}_{\mathbb{Q}} \alpha(\beta) \neq K$ .
- (2) If  $\alpha \in \mathcal{O}_K^n$ , then either  $\mathcal{D}(\alpha) = 0$ , or  $\mathcal{D}(\alpha) \geq 1$ ; similarly, if  $\beta \in \mathcal{O}_K$ , then either  $\mathcal{M}(\alpha, \beta) = 0$ , or  $\mathcal{M}(\alpha, \beta) \geq 1$ . Furthermore,  $\mathcal{D}(\alpha), \mathcal{M}(\alpha, \beta) \in \mathbb{Z}_{\geq 0}$ .

$$(3) \quad \mathcal{D}(\alpha) \leq \frac{(d!)^2}{|\Delta_K|} \binom{n}{d} H_K(\alpha)^2, \quad \mathcal{M}(\alpha, \beta) \leq \frac{d!}{|\Delta_K|^{1/2}} H_K(\alpha) H_K(\beta).$$

*Proof.* To prove (1), notice that  $\mathcal{D}(\alpha) = 0$  if and only if the discriminant of every  $d$ -tuple of coordinates of  $\alpha$  is equal to 0. This happens if and only if every  $d$ -tuple of coordinates of  $\alpha$  is linearly dependent over  $\mathbb{Q}$ , meaning that  $\text{span}_{\mathbb{Q}} \alpha \neq K$ . Similarly,  $\mathcal{M}(\alpha, \beta) = 0$  if and only if the discriminant of every  $d$ -tuple of coordinates of the vector  $\alpha(\beta)$  is equal to 0, which happens if and only if  $\text{span}_{\mathbb{Q}} \alpha(\beta) \neq K$ .

To prove (2), assume that  $\alpha \in \mathcal{O}_K^n$  and  $\mathcal{D}(\alpha) \neq 0$ . Then there exists some  $I = \{i_1, \dots, i_d\} \in \mathcal{J}(n, d)$  such that  $\text{disc}(\alpha_I) \neq 0$ . Since coordinates of  $\alpha$  are algebraic integers, it must be true that for each  $1 \leq j \leq d$

$$\alpha_{i_j} = u_{j1}\omega_1 + \dots + u_{jd}\omega_d,$$

where  $\omega_1, \dots, \omega_d$  is a  $\mathbb{Z}$ -basis for  $\mathcal{O}_K$  and  $u_{jk}$  are integers such that the matrix  $U = (u_{jk})_{1 \leq j, k \leq d}$  is nonsingular. Therefore  $\text{disc}(\alpha_I) = \Delta_K \det(U)^2$ , and hence

$$\mathcal{D}(\alpha) \geq \frac{|\text{disc}(\alpha_I)|}{|\Delta_K|} = \det(U)^2 \in \mathbb{Z}_{>0}.$$

The argument for  $\mathcal{M}(\alpha, \beta)$  is analogous, replacing  $\alpha$  with  $(\alpha, \beta)$  and  $\mathcal{J}(n, d)$  with  $\mathcal{J}(n+1, d)$ , and then observing that  $\mathcal{M}(\alpha, \beta) \geq |\text{disc}(\alpha(\beta)_I)|/\Delta_K^{1/2} \in \mathbb{Z}_{>0}$ . In particular,  $\mathcal{D}(\alpha), \mathcal{M}(\alpha, \beta) \in \mathbb{Z}_{\geq 0}$ .

To prove (3), let  $I = \{i_1, \dots, i_d\} \in \mathcal{J}(n, d)$  and consider the matrix

$$\Sigma(\alpha_I) := \begin{pmatrix} \sigma_1(\alpha_{i_1}) & \cdots & \sigma_1(\alpha_{i_d}) \\ \vdots & \ddots & \vdots \\ \sigma_d(\alpha_{i_1}) & \cdots & \sigma_d(\alpha_{i_d}) \end{pmatrix}.$$

The archimedean absolute values on  $K$  are  $v_1, \dots, v_d$ , given by  $|a|_{v_i} = |\sigma_i(a)|^{d_{v_i}}$  for each  $a \in K$ . Hence

$$\begin{aligned} |\text{disc}(\alpha_I)|^{1/2} &= |\det(\Sigma(\alpha_I))| = \left| \sum_{\tau \in S_d} \text{sgn}(\tau) \sigma_1(\alpha_{i_{\tau(1)}}) \cdots \sigma_d(\alpha_{i_{\tau(d)}}) \right| \\ &\leq \sum_{\tau \in S_d} |\sigma_1(\alpha_{i_{\tau(1)}})| \cdots |\sigma_d(\alpha_{i_{\tau(d)}})| \\ &\leq d! \prod_{j=1}^d \max\{1, |\sigma_j(\alpha_{i_1})|^{d_{v_j}}, \dots, |\sigma_j(\alpha_{i_d})|^{d_{v_j}}\} \\ &= d! \prod_{v|\infty} \max\{1, |\alpha_{i_1}|_v, \dots, |\alpha_{i_d}|_v\}, \end{aligned} \tag{10}$$

where  $\text{sgn}(\tau) = \pm 1$  is the sign of the permutation  $\tau$ . Therefore

$$\begin{aligned} \mathcal{D}(\alpha) &= \frac{1}{|\Delta_K|} \sum_{I \in \mathcal{J}(n, d)} |\text{disc}(\alpha_I)| \leq \frac{(d!)^2}{|\Delta_K|} \binom{n}{d} \left( \prod_{v|\infty} \max\{1, |\alpha_1|_v, \dots, |\alpha_n|_v\} \right)^2 \\ &\leq \frac{(d!)^2}{|\Delta_K|} \binom{n}{d} \left( \prod_{v \in M(K)} \max\{1, |\alpha_1|_v, \dots, |\alpha_n|_v\} \right)^2 = \frac{(d!)^2}{|\Delta_K|} \binom{n}{d} H_K(\alpha)^2. \end{aligned}$$

This gives the desired bound on  $\mathcal{D}(\alpha)$  in terms of  $H_K(\alpha)$ . Now, in a manner completely analogous to (10), we can obtain

$$\begin{aligned} |\text{disc}(\alpha(\beta)_I)|^{1/2} &\leq d! \prod_{v|\infty} \max\{1, |\alpha_1|_v, \dots, |\alpha_n|_v, |\beta|_v\} \\ &\leq d! \prod_{v \in M(K)} (\max\{1, |\alpha_1|_v, \dots, |\alpha_n|_v\} \max\{1, |\beta|_v\}) = d! H_K(\alpha) H_K(\beta), \end{aligned}$$

and so

$$\mathcal{M}(\alpha, \beta) \leq \frac{d!}{|\Delta_K|^{1/2}} H_K(\alpha) H_K(\beta). \quad \square$$

Part (3) of Lemma 3.1 and its proof show that  $\mathcal{D}(\alpha)$  and  $\mathcal{M}(\alpha, \beta)$  measure the arithmetic complexity of  $\alpha$  and  $\alpha(\beta)$ , respectively, at the archimedean places, allowing for a comparison to the more traditional height function  $H_K(\alpha)$ . Notice, however, that  $\mathcal{D}(\alpha)$  and  $\mathcal{M}(\alpha, \beta)$  are different from traditional heights in the sense that they do not take into account information at the nonarchimedean places and do not satisfy Northcott's finiteness property, as does  $H_K(\alpha)$ : For each  $c \in \mathbb{R}_{>0}$ , the set  $\{\alpha \in K^n : H_K(\alpha) \leq c\}$  is finite, but, say, the set  $\{\alpha \in K^n : \mathcal{D}(\alpha) \leq c\}$  is not. Well, clearly  $\mathcal{D}(\alpha) = 0$  for any  $\alpha$  with  $\text{span}_{\mathbb{Q}} \alpha \neq K$  (part (1) of Lemma 3.1 above), but even sets like

$$\{\alpha \in (\mathcal{O}_K^+)^n : \text{span}_{\mathbb{Z}} \alpha = \mathcal{O}_K, \mathcal{D}(\alpha) \leq c\}$$

do not have to be finite.

**Example 2.** Indeed, let for instance  $K = \mathbb{Q}(\sqrt{2})$ ,  $t \geq 2$  be a rational integer, and

$$\alpha_1 = 1 \in \mathcal{O}_K^+, \quad \alpha_2 = t + \sqrt{2} \in \mathcal{O}_K^+, \quad \alpha_3 = 2t + 2\sqrt{2} \in \mathcal{O}_K^+.$$

It is easy to see that  $\sqrt{2} = \alpha_2 - t\alpha_1$ ; hence

$$\mathcal{O}_K = \text{span}_{\mathbb{Z}}\{\alpha_1, \alpha_2, \alpha_3\}$$

for every  $t$ . On the other hand,

$$\mathcal{D}(\alpha) = \frac{1}{8}(8 + 32 + 0) = 5,$$

also for every nonzero  $t \in \mathbb{Z}$ . Hence the set

$$\{\alpha \in (\mathcal{O}_K^+)^3 : \text{span}_{\mathbb{Z}} \alpha = \mathcal{O}_K, \mathcal{D}(\alpha) \leq 5\}$$

in this case is infinite.

**Remark.** One can think of  $\mathcal{D}(\alpha)$  as Euclidean norm of the vector of Grassmann coordinates of the matrix  $\Sigma(\alpha)$ , normalized by the discriminant  $\Delta_K$ . The transpose of such a matrix can be viewed as a basis matrix for a lattice of rank  $d$  in  $\mathbb{R}^n$ , and choosing any other basis for this lattice does not change the value of  $\mathcal{D}(\alpha)$ . Indeed, rewriting Example 2 in the notation of Section 2, we have  $\Sigma(\alpha) = C = BA$ , where

$$B = (\Sigma(1) \ \Sigma(\sqrt{2})) = \begin{pmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{pmatrix}, \quad A = \begin{pmatrix} 1 & t & 2t \\ 0 & 1 & 2 \end{pmatrix},$$

and so

$$A^{\top} = \begin{pmatrix} 1 & 0 \\ t & 1 \\ 2t & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$$

is a basis matrix of the lattice

$$\text{span}_{\mathbb{Z}} \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} \right\},$$

where  $\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \in \text{GL}_2(\mathbb{Z})$  is just a change of basis matrix. More generally, if  $\Sigma(\alpha) = BA$  then for any matrix  $U \in \text{GL}_d(\mathbb{Z})$  the matrix  $C = B(A^{\top}U)^{\top} = B(U^{\top}A)$  is equal to  $\Sigma(\alpha')$  for some  $\alpha' \in \mathcal{O}_K$  with  $\mathcal{D}(\alpha') = \mathcal{D}(\alpha)$ ; hence there are infinitely many such  $\alpha'$ . Choosing  $U$  carefully, it is easy to construct such examples with  $\alpha' \in \mathcal{O}_K^+$ . An analogous observation also applies to the function  $\mathcal{M}(\alpha, \beta)$ .

The above observations in particular imply that there cannot exist a general lower bound on  $\mathcal{D}(\alpha)$  in terms of  $H_K(\alpha)$ : if such a bound existed, we would have

$$\{\alpha \in K^n : \mathcal{D}(\alpha) \leq c_1\} \subseteq \{\alpha \in K^n : H_K(\alpha) \leq c_2\}$$

for some appropriate constants  $c_1, c_2$ . It is therefore interesting to obtain lower bounds on  $\mathcal{D}(\alpha)$  besides the trivial one in part (2) of Lemma 3.1. Hence, in situations when, say,  $g_1(\alpha)$  is known (with the setup of Section 1), one can conversely think of Theorem 1.1 as providing a lower bound on  $\mathcal{D}(\alpha)$ :

$$\mathcal{D}(\alpha) \geq \frac{2\sqrt{n-d+1}}{n-d} g_1(\alpha).$$

For instance, in a situation when  $n = d + 1$  and  $g_1(\alpha) \geq 1$  (a rather common situation, as in Example 1, for instance), we obtain  $\mathcal{D}(\alpha) \geq 2\sqrt{2}$  (and hence  $\mathcal{D}(\alpha) \geq 4$ , since it is an integer), which is already better than that of part (2) of Lemma 3.1. In fact,  $g_1(\alpha) \geq 1$  whenever  $\text{Sg}(\alpha) \neq \mathcal{C}_{\mathbb{Q}}(\alpha) \cap \mathcal{O}_K$ , and hence we have the following immediate corollary.

**Corollary 3.2.** *Let the notation be as in Theorem 1.1 and assume that  $\text{Sg}(\alpha) \neq \mathcal{C}_{\mathbb{Q}}(\alpha) \cap \mathcal{O}_K$ . Then*

$$\mathcal{D}(\alpha) \geq \max \left\{ 1, \frac{2\sqrt{n-d+1}}{n-d} \right\}.$$

*This lower bound is greater than 1 as long as  $n \leq d + 4$ .*

Combining Corollary 3.2 with part (3) of Lemma 3.1, we also obtain the following lower bound on the absolute Weil height of  $\alpha$ .

**Corollary 3.3.** *Let the notation be as in Theorem 1.1 and assume that  $\text{Sg}(\alpha) \neq \mathcal{C}_{\mathbb{Q}}(\alpha) \cap \mathcal{O}_K$ . Then*

$$H(\alpha) \geq \left( \frac{2|\Delta_K| \sqrt{n-d+1} (n-d-1)!}{d! n!} \right)^{1/(2d)}.$$

The lower bound of Corollary 3.3 is greater than 1 when  $|\Delta_K|$  is large in comparison to  $n$ . For instance, in the case  $K$  is a quadratic number field and  $n = 3$ , we have

$$H(\alpha) \geq \left( \frac{|\Delta_K|}{3\sqrt{2}} \right)^{1/4},$$

while  $|\Delta_K|$  can be arbitrarily large (for a general totally real field, Minkowski's bound guarantees that  $|\Delta_K| \geq (d^d/d!)^2$ ).

These observations should be viewed in light of Lehmer's problem on the lower bound for absolute Weil height of algebraic numbers and the great amount of work done in this direction (see [Mossinghoff 2011] for detailed information). Lehmer's conjecture dating back to 1933 states that there exists a constant  $c > 1$  such that for every algebraic number  $\alpha$  of degree  $d$ ,  $H(\alpha) > c^{1/d}$ . While the conjecture is still open, there is a great number of partial results and generalizations in a variety of special cases. Our lower bound on  $H(\alpha)$  for the special types of algebraic  $n$ -tuples  $\alpha$  is a small contribution in that general direction.

#### 4. Proofs of Theorems 1.2 and 1.3

Let us start by reviewing what we may call a “positive” version of Siegel’s lemma as established in [Borosh and Treybig 1976]. The name Siegel’s lemma often refers to results about the size of solutions of systems of linear equations. The particular version we are interested in is concerned with nonnegative solutions to inhomogeneous integer linear systems. Let  $A$  be a  $d \times n$  integer matrix such that the equation  $A\mathbf{x} = \mathbf{0}$  has no nonzero solutions  $\mathbf{x} \in \mathbb{Z}_{\geq 0}^n$ . Let  $\mathbf{b} \in \mathbb{Z}^d$  and let  $(A \ \mathbf{b})$  be the augmented  $d \times (n+1)$  matrix. Define

$$\mathcal{M}(A, \mathbf{b}) = \max\{|\det((A \ \mathbf{b})_I)| : I \in \mathcal{J}(n+1, d)\}.$$

Theorem 4 of [Borosh and Treybig 1976] asserts that every  $\mathbf{x} \in \mathbb{Z}_{\geq 0}^n$  such that  $A\mathbf{x} = \mathbf{b}$  satisfies

$$|\mathbf{x}| \leq \mathcal{M}(A, \mathbf{b}). \quad (11)$$

We now use this result to prove Theorem 1.2.

*Proof of Theorem 1.2.* Let  $\beta \in \text{Sg}(\boldsymbol{\alpha})$ ; then for some  $\mathbf{x} \in \mathbb{Z}_{\geq 0}^n$  we have  $\sum_{i=1}^n x_i \alpha_i = \beta$ . This means that

$$\Sigma(\beta) = \sum_{i=1}^n x_i \Sigma(\alpha_i) = \Sigma(\boldsymbol{\alpha})\mathbf{x}.$$

Using the same notation as in Section 2 above, we write  $C = \Sigma(\boldsymbol{\alpha}) = BA$ , and so

$$\beta = C\mathbf{x} = BA\mathbf{x} = B\mathbf{b},$$

where  $\mathbf{b} \in \mathbb{Z}^m$ ; hence  $A\mathbf{x} = \mathbf{b}$ . Suppose now that for some  $\mathbf{y} \in \mathbb{Z}_{\geq 0}^n$  we have  $A\mathbf{y} = \mathbf{0}$ . Then

$$BA\mathbf{y} = C\mathbf{y} = \Sigma\left(\sum_{i=1}^n y_i \alpha_i\right) = \mathbf{0},$$

which implies that  $\sum_{i=1}^n y_i \alpha_i = \mathbf{0}$ . Since  $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K^+$ , this is only possible if  $\mathbf{y} = \mathbf{0}$ . Then every  $\mathbf{x} \in \mathbb{Z}_{\geq 0}^n$  such that  $A\mathbf{x} = \mathbf{b}$  satisfies (11), and for each such  $\mathbf{x}$  we have  $\beta = \sum_{i=1}^n \alpha_i x_i$ . Observe also that for each  $I \in \mathcal{J}(n+1, d)$ ,

$$|\det((A \ \mathbf{b})_I)| = |\det((B^{-1}C \ B^{-1}\Sigma(\beta))_I)| = \frac{|\det((\Sigma(\boldsymbol{\alpha}) \ \Sigma(\beta))_I)|}{|\det(B)|} = \left| \frac{\text{disc}(\boldsymbol{\alpha}(\beta)_I)}{\Delta_K} \right|^{1/2},$$

which implies that  $\mathcal{M}(A, \mathbf{b}) = \mathcal{M}(\boldsymbol{\alpha}, \beta)$ . This completes the proof of the upper bound of the theorem.

To establish the lower bound, let  $\boldsymbol{\alpha} \in K^n$  and  $\mathbf{x} \in \mathbb{Z}^n$ , and let  $\beta = \sum_{i=1}^n \alpha_i x_i$ . We will prove

$$H_K(\beta) \leq n^d |\mathbf{x}|^d H_K(\boldsymbol{\alpha}). \quad (12)$$

Indeed, if  $v \mid \infty$  in  $M(K)$ , then

$$|\beta|_v \leq \sum_{i=1}^n |\alpha_i|_v |x_i|_v \leq n |\mathbf{x}| \max\{|\alpha_1|_v, \dots, |\alpha_n|_v\}.$$

If  $v \nmid \infty$  in  $M(K)$ , then

$$|\beta|_v \leq \max_{1 \leq i \leq n} |\alpha_i|_v |x_i|_v \leq \max\{|\alpha_1|_v, \dots, |\alpha_n|_v\},$$

since  $\mathbf{x} \in \mathbb{Z}^n \subseteq \mathcal{O}_K^n$ , and so  $|x_i|_v \leq 1$  for every  $v \nmid \infty$  and  $1 \leq i \leq n$ . Therefore

$$\begin{aligned} H_K(\beta) &= \prod_{v \in M(K)} \max\{1, |\beta|_v\} \\ &\leq \prod_{v|\infty} (n|\mathbf{x}| \max\{1, |\alpha_1|_v, \dots, |\alpha_n|_v\}) \times \prod_{v \nmid \infty} (\max\{1, |\alpha_1|_v, \dots, |\alpha_n|_v\}) \\ &\leq n^d |\mathbf{x}|^d H_K(\boldsymbol{\alpha}). \end{aligned}$$

The lower bound of Theorem 1.2 now follows from (12).  $\square$

*Proof of Theorem 1.3.* Let  $1 \leq T_1 < T_2$  be real numbers. Then for each  $\mathbf{x} \in \mathbb{Z}_{\geq 0}^n$  such that  $\beta = \sum_{i=1}^n \alpha_i x_i \in \text{Sg}_1(\boldsymbol{\alpha}, T_1, T_2)$ , by Theorem 1.2 and Lemma 3.1 we have

$$\frac{1}{n} \left( \frac{T_1}{H_K(\boldsymbol{\alpha})} \right)^{1/d} \leq \frac{1}{n} \left( \frac{H_K(\beta)}{H_K(\boldsymbol{\alpha})} \right)^{1/d} \leq |\mathbf{x}| \leq \mathcal{M}(\boldsymbol{\alpha}, \beta) \leq \frac{d!}{|\Delta_K|^{1/2}} H_K(\boldsymbol{\alpha}) H_K(\beta) \leq \frac{d! H_K(\boldsymbol{\alpha})}{|\Delta_K|^{1/2}} T_2.$$

Now, let

$$\mathbb{Z}_+(\boldsymbol{\alpha}, T_1, T_2) = \left\{ \mathbf{x} \in \mathbb{Z}_{\geq 0}^n : \frac{1}{n} \left( \frac{T_1}{H_K(\boldsymbol{\alpha})} \right)^{1/d} \leq |\mathbf{x}| \leq \frac{d! H_K(\boldsymbol{\alpha})}{|\Delta_K|^{1/2}} T_2 \right\},$$

and notice that

$$|\mathbb{Z}_+(\boldsymbol{\alpha}, T_1, T_2)| \leq \left( \frac{d! H_K(\boldsymbol{\alpha})}{|\Delta_K|^{1/2}} T_2 + 1 \right)^n - \left[ \frac{T_1^{1/d}}{n H_K(\boldsymbol{\alpha})^{1/d}} \right]^n. \quad (13)$$

To each  $\beta \in \text{Sg}_1(\boldsymbol{\alpha}, T_1, T_2)$  there correspond  $r(\beta)$  vectors in  $\mathbb{Z}_+(\boldsymbol{\alpha}, T_1, T_2)$ . Therefore

$$|\text{Sg}_1(\boldsymbol{\alpha}, T_1, T_2)| \leq \sum_{\beta \in \text{Sg}_1(\boldsymbol{\alpha}, T_1, T_2)} r(\beta) \leq |\mathbb{Z}_+(\boldsymbol{\alpha}, T_1, T_2)|. \quad (14)$$

Further, for each  $\beta \in \text{Sg}_s(\boldsymbol{\alpha}, T_1, T_2)$  there are at least  $s$  distinct  $\mathbf{x}$  in the set  $\mathbb{Z}_+(\boldsymbol{\alpha}, T_1, T_2)$ , and so

$$|\text{Sg}_s(\boldsymbol{\alpha}, T_1, T_2)| \leq \frac{1}{s} |\mathbb{Z}_+(\boldsymbol{\alpha}, T_1, T_2)|. \quad (15)$$

On the other hand, for  $T > 1$  and each  $\beta \in \text{Sg}_1(\boldsymbol{\alpha}, 1, T)$  there are  $r(\beta)$  points in the set

$$\left\{ \mathbf{x} \in \mathbb{Z}_{\geq 0}^n : |\mathbf{x}| \leq \frac{1}{n} \left( \frac{T}{H_K(\boldsymbol{\alpha})} \right)^{1/d} \right\},$$

and so

$$\sum_{\beta \in \text{Sg}_1(\boldsymbol{\alpha}, 1, T)} r(\beta) \geq \left[ \frac{T^{1/d}}{n H_K(\boldsymbol{\alpha})^{1/d}} \right]^n. \quad (16)$$

The theorem now follows upon combining (13) with (14), (15) and (16).  $\square$

### Acknowledgement

We thank the referee for a careful reading of our paper and helpful suggestions that improved the quality of presentation.

## References

- [Aliev and Gruber 2007] I. M. Aliev and P. M. Gruber, “An optimal lower bound for the Frobenius problem”, *J. Number Theory* **123**:1 (2007), 71–79. MR Zbl
- [Aliev and Henk 2010] I. Aliev and M. Henk, “Feasibility of integer knapsacks”, *SIAM J. Optim.* **20**:6 (2010), 2978–2993. MR Zbl
- [Aliev et al. 2012] I. Aliev, L. Fukshansky, and M. Henk, “Generalized Frobenius numbers: bounds and average behavior”, *Acta Arith.* **155**:1 (2012), 53–62. MR Zbl
- [Aliev et al. 2013] I. Aliev, M. Henk, and E. Linke, “Integer points in knapsack polytopes and  $s$ -covering radius”, *Electron. J. Combin.* **20**:2 (2013), art.id. P42. MR Zbl
- [Aliev et al. 2016] I. Aliev, J. A. De Loera, and Q. Louveaux, “Parametric polyhedra with at least  $k$  lattice points: their semigroup structure and the  $k$ -Frobenius problem”, pp. 753–778 in *Recent trends in combinatorics*, edited by A. Beveridge et al., IMA Vol. Math. Appl. **159**, Springer, 2016. MR Zbl
- [Beck and Robins 2004] M. Beck and S. Robins, “A formula related to the Frobenius problem in two dimensions”, pp. 17–23 in *Number theory* (New York, 2003), edited by D. Chudnovsky et al., Springer, 2004. MR Zbl
- [Borosh and Treybig 1976] I. Borosh and L. B. Treybig, “Bounds on positive integral solutions of linear Diophantine equations”, *Proc. Amer. Math. Soc.* **55**:2 (1976), 299–304. MR Zbl
- [Cassels 1959] J. W. S. Cassels, *An introduction to the geometry of numbers*, Grundlehren der Mathematischen Wissenschaften **99**, Springer, 1959. MR Zbl
- [Fukshansky and Robins 2007] L. Fukshansky and S. Robins, “Frobenius problem and the covering radius of a lattice”, *Discrete Comput. Geom.* **37**:3 (2007), 471–483. MR Zbl
- [Fukshansky and Schürmann 2011] L. Fukshansky and A. Schürmann, “Bounds on generalized Frobenius numbers”, *European J. Combin.* **32**:3 (2011), 361–368. MR Zbl
- [Kannan 1992] R. Kannan, “Lattice translates of a polytope and the Frobenius problem”, *Combinatorica* **12**:2 (1992), 161–177. MR Zbl
- [Mossinghoff 2011] M. Mossinghoff, “Lehmer’s problem”, website, 2011, available at <http://www.cecm.sfu.ca/~mjm/Lehmer/>.
- [Ramírez Alfonsín 2005] J. L. Ramírez Alfonsín, *The Diophantine Frobenius problem*, Oxford Lecture Series in Mathematics and its Applications **30**, Oxford University Press, Oxford, 2005. MR Zbl
- [Widmer 2016] M. Widmer, “Integral points of fixed degree and bounded height”, *Int. Math. Res. Not.* **2016**:13 (2016), 3906–3943. MR Zbl

Received 30 Jul 2019. Revised 3 Nov 2019.

LENNY FUKSHANSKY:

[lenny@cmc.edu](mailto:lenny@cmc.edu)

Department of Mathematical Sciences, Claremont McKenna College, Claremont, CA, United States

YINGQI SHI:

[yshi20@students.claremontmckenna.edu](mailto:yshi20@students.claremontmckenna.edu)

Department of Mathematical Sciences, Claremont McKenna College, Claremont, CA, United States



# The sum-of-digits function on arithmetic progressions

Lukas Spiegelhofer and Thomas Stoll

Let  $s_2$  be the sum-of-digits function in base 2, which returns the number of nonzero binary digits of a nonnegative integer  $n$ . We study  $s_2$  along arithmetic subsequences and show that — up to a shift — the set of  $m$ -tuples of integers that appear as an arithmetic subsequence of  $s_2$  has full complexity.

## 1. Results

The binary sum-of-digits function  $s_2$  is an elementary object studied in number theory. It is defined by the equation

$$s_2(\varepsilon_\nu 2^\nu + \cdots + \varepsilon_0 2^0) = \varepsilon_\nu + \cdots + \varepsilon_0,$$

where  $\varepsilon_i \in \{0, 1\}$  for  $0 \leq i \leq \nu$ . Despite the simplicity of definition, the behaviour of  $s_2$  on arithmetic progressions is not fully understood. Cusick’s conjecture on the sum-of-digits function [Drmota et al. 2016; Spiegelhofer 2019] concerns this area of research: for an integer  $t \geq 0$ , we define the limit

$$c_t = \lim_{N \rightarrow \infty} \frac{1}{N} |\{n : 0 \leq n < N, s_2(n+t) \geq s_2(n)\}|.$$

(The limit exists; see for example [Bésineau 1972]. In fact, the set in this definition is periodic with period  $2^k$  for some  $k$ .) Cusick’s conjecture states that

$$c_t > \frac{1}{2} \tag{1-1}$$

for all  $t \geq 0$ . Drmota, Kauers, and the first author [Drmota et al. 2016] proved that  $c_t > \frac{1}{2}$  for *almost all*  $t$  in the sense of asymptotic density; we also wish to note [Emme and Prikhod’ko 2017; Emme and Hubert 2018; 2019], and the recent partial result [Spiegelhofer 2019].

For  $t \geq 0$  and  $k \in \mathbb{Z}$ , we consider the quantity

$$\delta(k, t) = \lim_{N \rightarrow \infty} \frac{1}{N} |\{n : 0 \leq n < N, s_2(n+t) - s_2(n) = k\}|$$

(as was the case for  $c_t$ , this asymptotic density exists [Bésineau 1972]). The family  $\delta(\cdot, t)$  defines a probability distribution with mean 0. Clearly, Cusick’s conjecture states that

$$\delta(0, t) + \delta(1, t) + \cdots > \frac{1}{2}. \tag{1-2}$$

---

The authors acknowledge support by the project MuDeRa, which is a joint project between the FWF (Austrian Science Fund) and the ANR (Agence Nationale de la Recherche). Moreover, Spiegelhofer was supported by the FWF project F5502-N26, which is a part of the Special Research Program “Quasi Monte Carlo methods: theory and applications”; Stoll was supported by the project ANR-18-CE40-0018.

MSC2010: 11A63, 11B25.

Keywords: sum-of-digits function, arithmetic progression, Cusick’s conjecture.

Numerical computation, using the recurrence for the values  $\delta(k, t)$  presented below, reveals that indeed  $c_t > \frac{1}{2}$  for all  $t < 2^{30}$ . Moreover, since the sum (1-2) involves the summand  $\delta(0, t)$ , and the associated probability distribution is usually close to a normal distribution [Emme and Hubert 2019], the strict inequality  $c_t > \frac{1}{2}$  is plausible. In fact the statement  $\frac{1}{2}\delta(0, t) + \delta(1, t) + \delta(2, t) + \dots > \frac{1}{2}$  is not true in general ( $t = 27$  being the first counterexample); moreover the statement  $\tilde{c}_t \leq \frac{1}{2}$ , where  $\tilde{c}_t = c_t - \delta(0, t)$ , is true for  $t < 2^{30}$  and for almost all  $t$  with respect to asymptotic density [Drmota et al. 2016].

In the current note, motivated by Cusick's conjecture, we are concerned with the  $(m+1)$ -tuple

$$(s_2(n), s_2(n+t), \dots, s_2(n+mt)),$$

where  $t \geq 0$  and  $m \geq 1$  are integers. We aim to understand the set of tuples that can occur, as  $n$  and  $t$  run. In fact, our theorem states that, up to a shift, all tuples occur.

**Theorem 1.1.** *Assume that  $k_1, \dots, k_m \in \mathbb{Z}$ . There exist  $n$  and  $t$  such that for  $1 \leq \ell \leq m$ ,*

$$k_\ell = s_2(n + \ell t) - s_2(n).$$

This is a generalization of the statement that the Thue–Morse sequence  $\mathbf{t}$  has full *arithmetic complexity*, meaning that every finite word  $\omega \in \{0, 1\}^L$  occurs as an arithmetic subsequence of  $\mathbf{t}$ . This was first proved in [Avgustinovich et al. 2003] and also follows from [Müllner and Spiegelhofer 2017; Konieczny 2019]. Our theorem should be compared to the results proved in [Sanna 2012], who considered pairwise different values of  $s_2(n + 0t), \dots, s_2(n + \ell t)$ .

Theorem 1.1 is not hard to prove for  $m = 1$ . We present three arguments leading to this fact:

(1) Assume first that  $k \geq 0$ . Set  $n = 2^{k+1}$  and  $t = 2^k - 1$ . Then  $s_2(n+t) = k+1$  and  $s_2(n) = 1$ , yielding  $k = s_2(n+t) - s_2(n)$ . If  $k < 0$ , we set  $n = 2^{-k+1} - 1$  and  $t = 1$ . Then  $s_2(n) = -k+1$  and  $s_2(n+t) = 1$ , which yields  $s_2(n+t) - s_2(n) = k$ .

Alternatively, we may also write, as in the case  $m = 2$  presented below,  $t = 2^c - 1$  and  $n = 2^{c-1}(2^a - 1)$  for positive integers  $a$  and  $c$ . We obtain  $s_2(n+t) = c$  and  $s_2(n) = a$ , and clearly the difference  $c - a$  runs through all integers.

(2) We have  $s_2(n+1) - s_2(n) = 1 - v_2(n+1) \leq 1$ , where  $v_2(m) = \max\{k \geq 0 : 2^k \mid m\}$  for  $m \geq 1$  is the 2-adic valuation of  $m$ . This formula follows by considering the number of 1s with which the binary expansion of  $n$  ends. Since  $s_2(2^\ell) = 1$  and  $s_2(2^{\ell+1} - 1) = \ell + 1$ , we obtain the fact that  $s_2(n)$  attains all values in  $\{1, \dots, \ell + 1\}$  as  $n$  varies in  $\{2^\ell, \dots, 2^{\ell+1} - 1\}$ . Let  $k \in \mathbb{Z}$  be given and set  $\ell = 2|k|$ . Choose  $n \in \{2^\ell, \dots, 2^{\ell+1} - 1\}$  such that  $s_2(n) = |k| + 1$  and  $n' \in \{2^{\ell+1}, \dots, 2^{\ell+2} - 1\}$  such that  $s_2(n') = |k| + 1 + k$ . Then  $s_2(n') - s_2(n) = k$ , which implies the statement.

(3) The quantities  $\delta(k, t)$  satisfy the following recurrence [Drmota et al. 2016]:

$$\delta(k, 1) = \begin{cases} 2^{k-2}, & k \leq 1, \\ 0 & \text{otherwise,} \end{cases}$$

$$\delta(k, 2t) = \delta(k, t),$$

$$\delta(k, 2t+1) = \frac{1}{2}\delta(k-1, t) + \frac{1}{2}\delta(k+1, t+1).$$

From this, it is very easy to show that  $\delta(k, t) > 0$  for all  $k \leq s_2(t)$ . For  $k$  given, choose  $t$  in such a way that  $s_2(t) \geq k$ ; the positivity of the density  $\delta(k, t)$  implies that there exists an  $n$  such that  $s_2(n+t) - s_2(n) = k$ .

For  $m = 2$ , it is also possible to obtain the statement by elementary considerations: consider integers  $a, c \geq 1$ ,  $b, d \geq 0$  and choose the integers  $n$  and  $t$  in such a way that the binary expansions look as follows:

$$\begin{array}{r} n : \overbrace{1 \cdots 1}^a 1 0 \cdots 0 \overbrace{1 \cdots 1}^b 0 \cdots 0 \\ t : \quad \quad \quad \underbrace{1 1 \cdots 1}_c 0 \cdots 0 \underbrace{1 \cdots 1}_d 1. \end{array}$$

The sums of digits of  $n$ ,  $n + t$ , and  $n + 2t$  respectively are  $a + b$ ,  $b + c + d$ , and  $c + d$  respectively. By varying the variables, we can obtain the statement for all integers  $k_1$  and  $k_2$  such that  $k_2 \leq k_1$ . For the case  $k_1 < k_2$ , we use the following configuration of the integers  $n$  and  $t$ , where  $a, d \geq 1$  and  $c \geq 0$ :

$$\begin{array}{r} n : \quad \quad \quad \overbrace{1 \cdots 1}^a 1 0 \cdots 0 \\ t : \underbrace{1 \cdots 1}_c 0 \cdots 0 \underbrace{1 1 \cdots 1}_d. \end{array}$$

The sums of digits of  $n$ ,  $n + t$ , and  $n + 2t$  are  $a$ ,  $d$ , and  $c + d$  respectively, and we see that we obtain all pairs  $(k_1, k_2) \in \mathbb{Z}^2$  such that  $k_1 \leq k_2$ .

However, the method quickly experiences difficulties, as multiplication by 3 is not a shift of the binary digits anymore. While we believe that the case  $m = 3$  can be done with some effort, a general principle is not apparent. Therefore we choose a different approach.

We prove Theorem 1.1 by induction on  $m$ , the cases  $m = 1, 2$  having been discussed above. Assume that  $m \geq 3$  and let  $k_1, \dots, k_m \in \mathbb{Z}$  be given. By induction hypothesis, there exist  $t_0$  and  $n_0$  such that

$$k_\ell = s_2(n_0 + \ell t_0) - s_2(n_0 + (\ell - 1)t_0) \quad \text{for } 1 \leq \ell < m.$$

Set

$$k'_m = s_2(n_0 + m t_0) - s_2(n_0 + (m - 1)t_0).$$

We are going to show that we may vary  $k'_m$  by steps of  $\pm 1$ , thus yielding the full statement.

By concatenation of binary expansions, it is sufficient to show the following statement:

There exist  $t_1, n_1$  such that  $s_2(n_1 + \ell t_1) - s_2(n_1 + (\ell - 1)t_1) = 0$  for  $1 \leq \ell < m$   
and  $s_2(n_1 + m t_1) - s_2(n_1 + (m - 1)t_1) = \pm 1$ . (1-3)

This concatenation is straightforward and summarized in the following lemma, which we will also use again in a moment.

**Lemma 1.2.** *Let  $\ell \geq 1$ ,  $m \geq 1$ ,  $n_0, \dots, n_{k-1}$ , and  $t_0, \dots, t_{k-1}$  be nonnegative integers. There exist nonnegative integers  $n$  and  $t$  such that*

$$s_2(n + \ell t) - s_2(n + (\ell - 1)t) = \sum_{0 \leq j < k} (s_2(n_j + \ell t_j) - s_2(n_j + (\ell - 1)t_j))$$

for  $1 \leq \ell \leq m$ .

*Proof.* The base case  $k = 1$  is trivial; it is sufficient to prove the statement for  $k = 2$ , the general case following easily from repeated application of this case.

Let  $N$  be so large that  $n_0 + mt_0 < 2^N$ , and set  $n = 2^N n_1 + n_0$  and  $t = 2^N t_1 + t_0$ . Since no carry propagation between the digits below and above  $N$  occurs, we can add up the contribution of the two blocks in order to yield the statement.  $\square$

We reduce the problem further, using this block representation again: choose  $t_j = 1$  for all  $0 \leq j < k$ ; it is sufficient to find a  $k \geq 1$  and nonnegative integers  $n_j$  for  $0 \leq j < k$  such that

$$\sum_{0 \leq j < k} (s_2(n_j + \ell) - s_2(n_j + \ell - 1)) = \begin{cases} 0 & \text{if } 1 \leq \ell < m, \\ \pm 1 & \text{if } \ell = m. \end{cases} \quad (1-4)$$

In order to show (1-4), we use the telescoping sum

$$\sum_{a \leq j < a+2^L} g(j) = s_2(a + 2^L) - s_2(a) = g\left(\left\lfloor \frac{a}{2^L} \right\rfloor\right),$$

where  $g(j) = s_2(j + 1) - s_2(j)$ . This representation yields for  $1 \leq \ell \leq m$ , where  $L$  is chosen such that  $2^L \leq m < 2^{L+1}$ ,

$$\begin{aligned} \sum_{2 \cdot 2^L - m + \ell \leq j < 3 \cdot 2^L - m + \ell} g(j) &= g\left(2 + \left\lfloor \frac{-m + \ell}{2^L} \right\rfloor\right) = \begin{cases} g(1) = 0 & \text{if } 1 \leq \ell < m, \\ g(2) = 1 & \text{if } \ell = m, \end{cases} \\ \sum_{2^L - m + \ell \leq j < 2 \cdot 2^L - m + \ell} g(j) &= g\left(1 + \left\lfloor \frac{-m + \ell}{2^L} \right\rfloor\right) = \begin{cases} g(0) = 1 & \text{if } 1 \leq \ell < m, \\ g(1) = 0 & \text{if } \ell = m, \end{cases} \\ \sum_{3 \cdot 2^{L+1} + \ell \leq j < 4 \cdot 2^{L+1} + \ell} g(j) &= g(3) = -1 \quad \text{for } 1 \leq \ell \leq m. \end{aligned}$$

The first of these three identities yields the “+”-part of (1-4) by choosing  $k = 2^L$  and  $n_j = 2 \cdot 2^L - m + j$  for  $0 \leq j < k$ .

The “-”-part is obtained from the second and third identities: by considering the disjoint union  $J = [2^L - m, 2 \cdot 2^L - m) \cup [3 \cdot 2^{L+1}, 4 \cdot 2^{L+1})$ , we have

$$\sum_{j \in J} (s_2(j + \ell) - s_2(j + \ell - 1)) = \begin{cases} 0 & \text{if } 1 \leq \ell < m, \\ -1 & \text{if } \ell = m. \end{cases}$$

The statement follows by merging the two intervals and choosing  $n_j$  accordingly. This finishes the proof of our theorem.

## 2. Possible extensions

From our proof, it is possible to effectively construct integers  $n$  and  $t$  such that  $s_2(n + \ell t) - s_2(n) = k_\ell$  for  $1 \leq \ell \leq m$ . In particular, this yields integers  $n$  and  $t$  such that  $t_{n+\ell t} = \omega_\ell$  for  $1 \leq \ell \leq m$ , where  $(\omega_1, \dots, \omega_m) \in \{0, 1\}^m$  and  $t$  is the Thue–Morse sequence on  $\{0, 1\}$ . (Note that we also used  $t(2^\lambda + n) = 1 - t(n)$  for  $n < 2^\lambda$ .) This gives a constructive result concerning the problem of full arithmetic complexity of the Thue–Morse sequence considered in [Avgustinovich et al. 2003; Konieczny 2019; Müllner and Spiegelhofer 2017].

As an extension of the presented line of research, we are interested in the proportion of cases in which  $s_2(n + \ell t) - s_2(n) = k_\ell$  occurs (for  $1 \leq \ell \leq m$ ). For this, we define more generally

$$\delta(\mathbf{k}, \boldsymbol{\varepsilon}, t) = \text{dens}\{n \in \mathbb{N} : s_2(n + \ell t + \varepsilon_\ell) - s_2(n) = k_\ell \text{ for } 1 \leq \ell \leq m\},$$

where  $\mathbf{k} = (k_1, \dots, k_m) \in \mathbb{Z}^m$  and  $\boldsymbol{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_m) \in \mathbb{N}^m$ . This generalizes the array  $\delta$  defined before. As in the one-dimensional case, the densities in this definition actually exist, and they satisfy the following recurrence relation:

$$\delta(\mathbf{k}, \boldsymbol{\varepsilon}, 2t) = \frac{1}{2}\delta(\mathbf{k}', \boldsymbol{\varepsilon}', t) + \frac{1}{2}\delta(\mathbf{k}'', \boldsymbol{\varepsilon}'', t),$$

where

$$\begin{aligned} k'_\ell &= k_\ell - (\varepsilon_\ell \bmod 2), & \varepsilon'_\ell &= \lfloor \frac{1}{2}\varepsilon_\ell \rfloor, \\ k''_\ell &= k_\ell + 1 - ((\varepsilon_\ell + 1) \bmod 2), & \varepsilon''_\ell &= \lfloor \frac{1}{2}(\varepsilon_\ell + 1) \rfloor; \end{aligned}$$

moreover,

$$\delta(\mathbf{k}, \boldsymbol{\varepsilon}, 2t + 1) = \frac{1}{2}\delta(\mathbf{k}', \boldsymbol{\varepsilon}', t) + \frac{1}{2}\delta(\mathbf{k}'', \boldsymbol{\varepsilon}'', t),$$

where

$$\begin{aligned} k'_\ell &= k_\ell - ((\varepsilon_\ell + \ell) \bmod 2), & \varepsilon'_\ell &= \lfloor \frac{1}{2}(\varepsilon_\ell + \ell) \rfloor, \\ k''_\ell &= k_\ell + 1 - ((\varepsilon_\ell + \ell + 1) \bmod 2), & \varepsilon''_\ell &= \lfloor \frac{1}{2}(\varepsilon_\ell + \ell + 1) \rfloor. \end{aligned}$$

This recurrence is the reason for the introduction of  $\boldsymbol{\varepsilon}$  in the definition of  $\delta(\mathbf{k}, \boldsymbol{\varepsilon}, t)$ . To our knowledge, these identities are new; we give the idea of proof. We have

$$\begin{aligned} \delta(\mathbf{k}, \boldsymbol{\varepsilon}, 2t) &= \frac{1}{2} \text{dens}\{n \in \mathbb{N} : s(2n + 2\ell t + \varepsilon_\ell) - s(2n) = k_\ell \text{ for } 1 \leq \ell \leq m\} \\ &\quad + \frac{1}{2} \text{dens}\{n \in \mathbb{N} : s(2n + 2\ell t + \varepsilon_\ell + 1) - s(2n + 1) = k_\ell \text{ for } 1 \leq \ell \leq m\}, \end{aligned}$$

and using the identities  $s(2n) = s(n)$  and  $s(2n + 1) = s(n) + 1$ , we obtain

$$s(2n + 2\ell t + \varepsilon_\ell) = s(2(n + \ell t + \lfloor \frac{1}{2}\varepsilon_\ell \rfloor) + (\varepsilon_\ell \bmod 2)) = s(n + \ell t + \varepsilon'_\ell) + (\varepsilon_\ell \bmod 2);$$

therefore  $s(2n + 2\ell t + \varepsilon_\ell) - s(2n) = k_\ell$  is equivalent to  $s(n + \ell t + \varepsilon'_\ell) - s(n) = k'_\ell$ . Analogous computations are valid for  $\varepsilon_\ell$  replaced by  $\varepsilon_\ell + 1$ ,  $\varepsilon_\ell + \ell$ , and  $\varepsilon_\ell + \ell + 1$  respectively, which yields the claim.

This recurrence can be used to prove statements on the densities  $\delta(\mathbf{k}, \boldsymbol{\varepsilon}, t)$ . The general intuitive idea is that the differences  $s(n + jt) - s(n)$ , for  $1 \leq j \leq m$ , should be *almost independent for most  $t$* ; in light of this consideration, we consider generalizations of Cusick's conjecture and of the result of [Emme and Hubert 2019]. On the one hand, we may ask for multidimensional generalizations of (1-1), relating the relative sizes of the values  $s_2(n), s_2(n + t), \dots, s_2(n + mt)$  to one another. We propose the following conjecture, extending (1-1).

**Conjecture 1.** Assume that  $m \geq 1$  is an integer. For an integer  $t \geq 0$ , define

$$c_t^{(m)} = \text{dens}\{n \in \mathbb{N} : s(n) \leq s(n + jt) \text{ for } 1 \leq j \leq m\}.$$

Then for all  $t \geq 0$ ,

$$c_t^{(m)} > \frac{1}{2^m}.$$

The statement is wrong for any larger constant in place of  $1/2^m$ . Also, define

$$C_t^{(m)} = \text{dens}\{n \in \mathbb{N} : s(n) \leq s(n + t) \leq s(n + 2t) \leq \dots \leq s(n + mt)\}.$$

Then for all  $t \geq 0$ ,

$$C_t^{(m)} > \frac{1}{2^m m!}.$$

The constant  $1/(2^m m!)$  is maximal.

On the other hand, we could ask for the overall shape of the  $m$ -dimensional probability distribution defined by  $\delta(\cdot, \mathbf{\epsilon}, t)$ .

**Problem 1.** Prove a multidimensional generalization of the theorem in [Emme and Hubert 2019]: for most  $t$ , the densities  $\text{dens}\{n \in \mathbb{N} : s_2(n + \ell t) - s_2(n) = k_\ell \text{ for } 1 \leq \ell \leq m\}$  should define a probability distribution that is close to a multivariate Gaussian law.

We can now understand the intuition behind the constants in Conjecture 1: a bivariate normal distribution with mean  $(0, 0)$  has one quarter of its total weight in the quadrant  $\{(x, y) \in \mathbb{R}^2 : 0 \leq x, 0 \leq y\}$ , and analogous considerations hold for higher dimensions. Concerning the values  $C_t^{(2)}$ , a bivariate normal distribution with mean  $(0, 0)$  has one *eighth* of its total weight in the octant  $\{(x, y) \in \mathbb{R}^2 : 0 \leq x \leq y\}$ , which corresponds to the complex closed region  $\{re^{2\pi i x} : r \geq 0, \frac{1}{8} \leq x \leq \frac{1}{4}\}$ . Noting the fact that  $s(n + 2t) \geq s(n + t)$  if and only if  $s(n + 2t) - s(n) \geq s(n + t) - s(n)$ , we see the link between the densities  $\delta(\mathbf{k}, \mathbf{\epsilon}, t)$  with  $\mathbf{k}$  lying in this octant and the values  $C_t^{(2)}$ . Concerning higher dimensions, we note that the  $m!$  sets

$$\{x \in \mathbb{R}^m : \|x\| \leq 1, 0 \leq x_{\sigma(1)} \leq x_{\sigma(2)} \leq \dots \leq x_{\sigma(m)}\},$$

where  $\sigma$  is a permutation of  $\{1, \dots, m\}$ , are unions of line segments  $[0, z]$ , where  $\|z\| = 1$ ; they are pairwise congruent (using a linear transformation that is a permutation matrix in the canonical base); an intersection of two distinct sets of this form has measure zero, and their union makes up a fraction  $1/2^m$  of the unit ball in  $m$  dimensions.

We implemented the computation of the densities  $\delta(\mathbf{k}, \mathbf{\epsilon}, t)$  for two dimensions in the Sage computer algebra system [SageMath 2017], and the resulting Sage worksheet is available from the website of Spiegelhofer.<sup>1</sup> We obtain

$$c_t^{(2)} \geq c_{951}^{(2)} = \frac{94299}{262144} = 0.3597\dots > \frac{1}{4} \quad \text{for } t \leq 2^{10}$$

and

$$c_t^{(2)} \geq c_{991}^{(2)} = \frac{43947}{262144} = 0.1676\dots > \frac{1}{8} \quad \text{for } t \leq 2^{10}.$$

The implementation involves nine two-dimensional arrays of rational numbers (corresponding to the nine possibilities  $(\epsilon_1, \epsilon_2) \in \{0, 1, 2\}^2$ ) and each of these calculations took about 5 minutes on a standard machine. We note that we did not optimize the Sage code, and certainly this computation can be sped up significantly.

Other conjectures similar to Conjecture 1 are conceivable: what about the other octants and quadrants  $A$  in the plane (including the borders)? Is it always true that  $\frac{1}{8}$ , resp.  $\frac{1}{4}$ , is a lower bound for the density  $\text{dens}\{n \in \mathbb{N} : (s(n + t) - s(n), s(n + 2t) - s(n)) \in A\}$ ? We leave this question open for future discussion, but we note that the analogous problem in one dimension is true for almost all  $t$ : we also have

$$\tilde{c}_t = \text{dens}\{n \in \mathbb{N} : s(n + t) \leq s(n)\} > \frac{1}{2}$$

<sup>1</sup><https://dmg.tuwien.ac.at/spiegelhofer/>

for  $t$  in a set having asymptotic density 1 [Drmota et al. 2016]. In other words, usually the median of the probability distribution defined by  $\delta(\cdot, t)$  is very close to the mean value (which is 0). We believe that  $\tilde{c}_t \geq \frac{1}{2}$  is true for all  $t$ , which complements Cusick’s conjecture (1-1) (note that  $\tilde{c}_1 = \frac{1}{2}$ ; thus there is no strict inequality).

We expect that nontrivial statements on both Conjecture 1 and Problem 1, at least for small  $m$ , can be obtained by extending the study of moments set forward in [Emme and Hubert 2019]. This is certainly not easy and will introduce technical difficulties that have to be surmounted.

## References

- [Avgustinovich et al. 2003] S. V. Avgustinovich, D. G. Fon-Der-Flaass, and A. E. Frid, “Arithmetical complexity of infinite words”, pp. 51–62 in *Words, languages & combinatorics, III* (Kyoto, 2000), edited by M. Ito and T. Imaoka, World Sci. Publ., River Edge, NJ, 2003. MR
- [Bésineau 1972] J. Bésineau, “Indépendance statistique d’ensembles liés à la fonction “somme des chiffres””, *Acta Arith.* **20** (1972), 401–416. MR Zbl
- [Drmota et al. 2016] M. Drmota, M. Kauers, and L. Spiegelhofer, “On a conjecture of Cusick concerning the sum of digits of  $n$  and  $n + t$ ”, *SIAM J. Discrete Math.* **30**:2 (2016), 621–649. MR Zbl
- [Emme and Hubert 2018] J. Emme and P. Hubert, “Normal distribution of correlation measures of binary sum-of-digits functions”, preprint, 2018. arXiv
- [Emme and Hubert 2019] J. Emme and P. Hubert, “Central limit theorem for probability measures defined by sum-of-digits function in base 2”, *Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)* **19**:2 (2019), 757–780. MR
- [Emme and Prikhod’ko 2017] J. Emme and A. Prikhod’ko, “On the asymptotic behavior of density of sets defined by sum-of-digits function in base 2”, *Integers* **17** (2017), art. id. A58. MR Zbl
- [Konieczny 2019] J. Konieczny, “Gowers norms for the Thue–Morse and Rudin–Shapiro sequences”, *Ann. Inst. Fourier (Grenoble)* **69**:4 (2019), 1897–1913. MR Zbl
- [Müllner and Spiegelhofer 2017] C. Müllner and L. Spiegelhofer, “Normality of the Thue–Morse sequence along Piatetski–Shapiro sequences, II”, *Israel J. Math.* **220**:2 (2017), 691–738. MR Zbl
- [SageMath 2017] The Sage Developers, *SageMath, the Sage Mathematics Software System*, Version 8.1, 2017, available at <http://www.sagemath.org>.
- [Sanna 2012] C. Sanna, “On arithmetic progressions of integers with a distinct sum of digits”, *J. Integer Seq.* **15**:8 (2012), art. id. 12.8.1. MR Zbl
- [Spiegelhofer 2019] L. Spiegelhofer, “Approaching Cusick’s conjecture on the sum-of-digits function”, *Integers* **19** (2019), art. id. A59. Zbl

Received 19 Sep 2019. Revised 26 Nov 2019.

LUKAS SPIEGELHOFER:

lukas.spiegelhofer@tuwien.ac.at

Institute of Discrete Mathematics and Geometry, Vienna University of Technology, Vienna, Austria

THOMAS STOLL:

thomas.stoll@univ-lorraine.fr

Institut Élie Cartan, Université de Lorraine, Vandœuvre-lès-Nancy, France



## A convexity criterion for unique ergodicity of interval exchange transformations

René Rühr

A criterion for unique ergodicity for points of a curve in the space of interval exchange transformation is given.

There is a metaconjecture in metric number theory that states that any Diophantine property that holds for generic vectors in  $\mathbb{R}^n$  should hold for generic vectors on nondegenerate submanifolds; see [Kleinbock 2001, Section 4]. Mahler asked for example whether almost all points on the curve  $s \mapsto (s, s^2, \dots, s^d)$  are very well approximable. This has been answered affirmatively by Sprindzuk. It is believed that an analogue of this phenomenon holds also for the unique ergodicity property for interval exchange transformations. Minsky and Weiss [2014] provided a general condition for unique ergodicity to hold. In this note we provide an easy-to-check criterion for their condition to be satisfied.

Let  $\sigma$  denote a permutation of  $d$  elements. Let  $\Omega$  denote the antisymmetric matrix

$$\Omega_{ij} = \begin{cases} 1 & i > j, \sigma(i) < \sigma(j), \\ -1 & i < j, \sigma(i) > \sigma(j), \\ 0 & \text{otherwise.} \end{cases}$$

Let  $\mathbf{a} = (a_1, \dots, a_d) \in \mathbb{R}_+^d$  be a row vector with positive entries  $a_i > 0$  and the associated interval be  $I_{\mathbf{a}} = [0, \sum a_i)$ , which is divided into  $d$  subintervals  $I_i = [x_{i-1}, x_i)$ , where  $x_i = \sum_{j \leq i} a_j$  are called discontinuities. Also introduce  $x'_i = \sum_{j \leq i} a_{\sigma^{-1}(j)}$ . An *interval exchange transformation*  $T : I_{\mathbf{a}} \rightarrow I_{\mathbf{a}}$  defined by the data  $(\sigma, \mathbf{a})$  is the map

$$T(x) = x + (\mathbf{a}\Omega)_j = x - x_j + x'_{\sigma(j)} \quad \text{for } x \in I_j.$$

In words,  $T$  permutes the intervals  $I_j$  of length  $a_j$  according to  $\sigma$ . The form  $\Omega_{ij}$  captures the exchange of two intervals  $I_i, I_j$  relative to each other.

We shall always assume that the permutation  $\sigma$  is irreducible in the sense that if  $\{1, \dots, k\} \subset \mathcal{A} = \{1, \dots, d\}$  is invariant under  $\sigma$  then  $k = d$ .

Masur [1982] and Veech [1982] proved independently that for almost all  $\mathbf{a} \in \mathbb{R}_+^d$ , the interval exchange transformation  $T$  associated to  $(\sigma, \mathbf{a})$  is uniquely ergodic; that is, the only  $T$ -invariant probability measure on  $I$  is Lebesgue measure.

Motivated by a conjecture of Mahler in the theory of Diophantine approximation, Minsky and Weiss [2014] proved the following theorem.

---

This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program (grant agreement no. 754475).

MSC2010: 28D10.

Keywords: uniquely ergodic interval exchange transformation, translation surface suspension.

**Theorem 1** (Minsky–Weiss). *Let  $\sigma = (d, \dots, 1)$  and  $\mathbf{a}(s) = (s, s^2, \dots, s^d)$ . Then for Lebesgue almost all  $s > 0$ , the interval exchange transformation associated to  $(\sigma, \mathbf{a}(s))$  is uniquely ergodic.*

We extend the theorem of Minsky and Weiss to arbitrary permutations by means of a simple convexity criterion.

We first recall the theorem from which Theorem 1 is deduced, which requires us to introduce more definitions. A connection of  $T$  is a triple  $(m, x_i, x_j)$  for which  $T^m(x_i) = x_j$ . As noted by Keane, if the coordinates  $a_k$  of  $\mathbf{a}$  are rationally independent then  $T$  has no connections. We shall restrict to curves  $\mathbf{a}(s)$  for which this is the case for almost all  $s$ . This implies that there are no  $T$ -invariant atomic probability measures.

Let  $\mathbf{b} = (b_1, \dots, b_d) \in \mathbb{R}^d$  be a row vector, which we will take to be  $\mathbf{b} = \dot{\mathbf{a}}$ , the derivative of a curve  $\mathbf{a}(s)$ . Define  $y_i = \sum_{j \leq i} b_j$  and  $y'_i = \sum_{j \leq i} b_{\sigma^{-1}(j)}$ . We put

$$L(x) = (\Omega \mathbf{b}^T)_i = y_i - y'_{\sigma(i)} \quad \text{for } x \in I_i.$$

We call  $(\mathbf{a}, \mathbf{b}) \in \mathbb{R}_+^d \times \mathbb{R}^d$  a positive pair if  $\mu(L) > 0$  for any  $T$ -invariant probability measure  $\mu$ . The following is a simplified statement of Theorem 6.2 in [Minsky and Weiss 2014].

**Theorem 2** (Minsky–Weiss). *If  $\mathbf{a} : A \rightarrow \mathbb{R}_+^d$  is a  $C^2$ -curve defined on an interval  $A \subset \mathbb{R}$  and  $\sigma$  is a permutation for which  $(\mathbf{a}(s), \dot{\mathbf{a}}(s))$  is positive for Lebesgue almost all  $s \in A$  then  $T$  associated to  $(\sigma, \mathbf{a}(s))$  is uniquely ergodic for almost all  $s \in A$ .*

While the condition seems hard to check—involved all  $T$ -invariant  $\mu$ 's (from which we want to deduce that there is only one!)—we see however that a sufficient criterion for positivity is  $L(x) > 0$  pointwise for every  $x \in I$ .

Let us now explain a suspension construction of Masur for an interval exchange transformation  $T$  associated to  $(\sigma, \mathbf{a})$ . Let  $\mathbf{b} \in \mathbb{R}^d$  be a “height vector” (associated to the “length vector”  $\mathbf{a}$ ) and define  $\zeta_i$  to be  $(a_i, b_i) \in \mathbb{R}^2$  and their slopes to be  $\kappa_i = b_i/a_i$ .

Let  $\Gamma_t$  be the curve obtained by connecting the points

$$C_0 = C'_0 = (0, 0), \quad C'_1 = \zeta_1, \quad C'_2 = \zeta_1 + \zeta_2, \quad \dots, \quad C_d = C'_d = \sum_{i=1}^d \zeta_i$$

and  $\Gamma_b$  be the curve obtained by connecting

$$C_0 = C^b_0, \quad C^b_1 = \zeta_{\sigma^{-1}(1)}, \quad C^b_2 = \zeta_{\sigma^{-1}(1)} + \zeta_{\sigma^{-1}(2)}, \quad \dots, \quad C_d = C^b_d.$$

If  $\zeta_1$  lies above  $\zeta_{\sigma^{-1}(1)}$ , i.e., if  $\kappa_1 > \kappa_{\sigma^{-1}(d)}$ , then we call  $\Gamma_t$  the top curve and  $\Gamma_b$  the bottom curve. They have common endpoints  $C_0$  and  $C_d$ . We denote their union by  $\Gamma$ . If there are no further intersections,  $\Gamma$  bounds a polygon. In this case, we are identifying the line segment  $[C^t_{k-1}, C^t_k]$  of  $\Gamma_t$  with segment  $[C^b_{j-1}, C^b_j]$  in  $\Gamma_b$ , where  $k = \sigma^{-1}(j)$ . One obtains a closed topological surface  $S$  which outside of the corners of the polygon inherits a flat structure from  $\mathbb{R}^2$ . This means that there is an atlas of charts  $\{(U, \psi)\}$  with  $U$  open and  $\psi : U \rightarrow \mathbb{R}^2$  continuous such that for any two charts  $\psi_i : U_i \rightarrow \mathbb{R}^2$  over a common point  $p$ , we find a translation  $v \in \mathbb{R}^2$  such that  $\psi_1 = \psi_2 + v$  for all points around  $p$ . It is possible to complement to an atlas defined on all of  $M$  by considering the complex multiplication on  $\mathbb{R}^2 = \mathbb{C}$  with maps of the form  $\psi = \phi^{\alpha+1}$  for a homeomorphism  $\phi : U \rightarrow \mathbb{C}$  that contains 0 in its range. The points with  $\alpha > 0$  are called the singularities of  $M$ .

$M$  is endowed with a dynamical system, the vertical straight line flow that preserves the natural area form coming from the flat metric. We note that the interval  $I$  embeds into  $M$  as a horizontal line starting from the origin. The vertical straight line flow defines a suspension of the interval exchange transformation  $T$  by considering the induced transformation on  $I$ , namely the first return map of  $I \rightarrow I$ . We can now understand the meaning of  $L(x)$ : it is the return time of  $x$  to  $I$ , and as such positive.

Self-intersections of the curves  $\Gamma_t$  and  $\Gamma_b$  give rise to a “nonsensical picture”; see depictions on page 247 of [Minsky and Weiss 2014]. We observe here that one can make sense of the picture even if the curve  $\Gamma$  has self-intersection, by attaching a half-translation structure to it, but we have not tried to follow up on this direction. Instead, we shall restrict ourselves to a criterion that avoids self-intersections.

**Lemma 3.** *Let  $\mathbf{a} \in \mathbb{R}^d$  be a length vector,  $\mathbf{b} \in \mathbb{R}^d$  be a height vector and  $\Gamma_t : I \rightarrow \mathbb{R}^2$  be the top curve constructed by concatenating the vectors  $\zeta_i = (a_i, b_i) \in \mathbb{R}^2$ , i.e.,  $\Gamma_t(\sum_{i \leq j} a_i) = C_j^t$ . Suppose the slopes  $\kappa_i = b_i/a_i$  of  $\zeta_i$  are strictly monotonically decreasing so that  $\Gamma_t$  is convex. Then for any irreducible permutation  $\sigma$  and bottom curve  $\Gamma_b$  constructed from vectors  $\zeta_{\sigma^{-1}(1)}, \dots, \zeta_{\sigma^{-1}(d)}$ , the closed curve  $\Gamma = \Gamma_t \cup \Gamma_b$  has no self-intersections. In particular,  $(\mathbf{a}, \mathbf{b})$  defines a positive pair if connection-free.*

*Proof.* We shall argue by induction on the number of symbols  $d$ . The base case is on two elements  $d = 2$ . By monotonicity  $\kappa_1 > \kappa_2$  and by irreducibility  $\sigma = (2, 1)$ . Then  $\Gamma_t \cup \Gamma_b$  bounds a parallelogram.

Assume now that for all  $d' < d$  the lemma is true. Let  $\Gamma_{b,j}$  the curve from concatenating  $C_0, C_1^b, \dots, C_j^b$  from left to right, i.e., restricting  $\Gamma_b : I \rightarrow \mathbb{R}^2$  to  $\bigcup_{i=1}^j I_{\sigma^{-1}(i)}$ . We now start another induction and assume that for all  $j' < j$ ,  $\Gamma_{b,j'}$  does not intersect  $\Gamma_t$ . For the base of the induction  $j = 1$ , there is nothing to check.

If  $\Gamma_{b,j}$  intersects  $\Gamma_t$  then by the induction hypothesis it does so with its final line segment  $[C_{j-1}^b, C_j^b]$ . We put  $k = \sigma^{-1}(j)$  such that  $C_{j-1}^b + \zeta_k = C_j^b$ , intersecting, say, the  $i$ -th segment  $[C_{i-1}^t, C_i^t]$  of  $\Gamma_t$ . Then  $\kappa_k > \kappa_i$ . By monotonicity,  $\zeta_k$  has to appear to the left of  $\zeta_i$  in  $\Gamma_t$ ; i.e.,  $k < i$ .

We now describe a procedure of removing  $[C_{j-1}^b, C_j^b]$  to obtain a smaller permutation to apply the induction hypothesis on  $d'$ .

Observe that if  $K \subset \sigma^{-1}(\{1, \dots, j\})$ , we can define the curves  $\Gamma_{t,K}, \Gamma_{b,j,K}$  that one obtains from taking  $\Gamma_t$  and removing the line segments  $[C_{k-1}^t, C_k^t]$  for  $k \in K$  from  $\Gamma_t$  and taking  $\Gamma_{b,j}$  and removing the line segments  $[C_{\sigma^{-1}(j'-1)}^b, C_{\sigma^{-1}(j')}^b]$  from  $\Gamma_{b,j}$  for  $\sigma^{-1}(j') \in K$ . Below, we shall have the additional property that  $K \subset \{1, \dots, i-1\}$ . We obtain a new permutation  $\sigma_K$  obtained by removing the symbols  $k \in K$ . If it is no longer irreducible then the maximal invariant subset  $\{1, \dots, \ell\}$  must be contained in  $\sigma^{-1}(\{1, \dots, j-1\})$  (or else  $\sigma$  is already reducible). By removing the subpermutation on  $(1, \dots, \ell)$  from  $\sigma_K$ , we can allow ourselves to only consider the irreducible component  $\sigma'$  of  $\sigma_K$  containing  $i$ .

We now choose  $K = \{k' = \sigma^{-1}(j') : j' \leq j \text{ and } \kappa_{k'} \geq \kappa_k\}$ . We note that  $k' \in K$  implies  $k' \leq k = \sigma^{-1}(j)$  and that  $i \notin K$ . Hence the curve  $\Gamma_{t,K}$  is only changed to the left of its line segment  $[C_{i-1}^t, C_i^t]$ , and most importantly, the curve  $\Gamma_{b,j,K}$  still intersects  $[C_{i-1}^t, C_i^t]$ . To see this, divide the plane into two half-planes with boundary  $\partial$  containing  $\zeta_k$  attached to the right endpoint of  $\Gamma_{b,j,K}$ , and we see that  $\Gamma_{b,j,K}$  stays to the upper-left half-plane. Since  $[C_{i-1}^t, C_i^t]$  intersects  $\partial$ , it also intersects  $\Gamma_{b,j,K}$  as claimed.

If  $\sigma_K$  is no longer irreducible then we proceed with the irreducible restriction  $\sigma'$  as described above, supported on, say,  $\mathcal{B} \subset \mathcal{A}$ . Consider the associated pair  $(\mathbf{a}', \mathbf{b}')$ , where  $\mathbf{a}', \mathbf{b}' \in \mathbb{R}^{|\mathcal{B}|}$  by restricting to the support of  $\sigma'$ . These give still monotone slopes, and the induction hypothesis on  $d' < d$  applies; i.e., there are no self-intersections. By construction, however, the curve defined by  $\mathbf{a}', \mathbf{b}'$  and  $\sigma'$  has at least one self-intersection.  $\square$

**Remark 4.** We have an analogous criterion if  $\kappa_i$  are increasing in  $i$ , in which case  $\Gamma_b(\sum_{i \leq j} a_j) = C_j^t$ , and we apply the argument of Lemma 3 with roles of  $\Gamma_t$  and  $\Gamma_b$  exchanged.

**Remark 5.** Barak Weiss has informed us of a topological proof of Lemma 3, which we invite the reader to find herself.

**Corollary 6.** *Theorem 1 holds for any irreducible permutation.*

*Proof.* The slopes associated to  $\mathbf{a}(s) = (s, s^2, \dots, s^d)$  are  $\kappa_i = is^{i-1}/s^i = i/s$ , monotone in  $i$ .  $\square$

## References

- [Kleinbock 2001] D. Kleinbock, “Some applications of homogeneous dynamics to number theory”, pp. 639–660 in *Smooth ergodic theory and its applications* (Seattle, WA, 1999), edited by A. Katok et al., Proc. Sympos. Pure Math. **69**, Amer. Math. Soc., Providence, RI, 2001. MR Zbl
- [Masur 1982] H. Masur, “Interval exchange transformations and measured foliations”, *Ann. of Math. (2)* **115**:1 (1982), 169–200. MR Zbl
- [Minsky and Weiss 2014] Y. Minsky and B. Weiss, “Cohomology classes represented by measured foliations, and Mahler’s question for interval exchanges”, *Ann. Sci. Éc. Norm. Supér. (4)* **47**:2 (2014), 245–284. MR Zbl
- [Veech 1982] W. A. Veech, “Gauss measures for transformations on the space of interval exchange maps”, *Ann. of Math. (2)* **115**:1 (1982), 201–242. MR Zbl

Received 13 Nov 2019.

RENÉ RÜHR:

rener@campus.technion.ac.il

Department of Mathematics, Technion – Israel Institute of Technology, Haifa, Israel

## Long monochromatic paths and cycles in 2-edge-colored multipartite graphs

József Balogh, Alexandr Kostochka, Mikhail Lavrov and Xujun Liu

We solve four similar problems: for every fixed  $s$  and large  $n$ , we describe all values of  $n_1, \dots, n_s$  such that for every 2-edge-coloring of the complete  $s$ -partite graph  $K_{n_1, \dots, n_s}$  there exists a monochromatic (i) cycle  $C_{2n}$  with  $2n$  vertices, (ii) cycle  $C_{\geq 2n}$  with at least  $2n$  vertices, (iii) path  $P_{2n}$  with  $2n$  vertices, and (iv) path  $P_{2n+1}$  with  $2n + 1$  vertices.

This implies a generalization for large  $n$  of the conjecture by Gyárfás, Ruszinkó, Sárközy and Szemerédi that for every 2-edge-coloring of the complete 3-partite graph  $K_{n,n,n}$  there is a monochromatic path  $P_{2n+1}$ . An important tool is our recent stability theorem on monochromatic connected matchings.

### 1. Introduction

A *connected matching* in a graph  $G$  is a matching whose edges are all in the same component of  $G$ . By  $M_n$  we will always denote a connected matching with  $n$  edges and by  $P_n$  the path with  $n$  vertices. Also by  $C_n$  we denote the cycle with  $n$  vertices, and by  $C_{\geq n}$  a cycle of length at least  $n$ .

For graphs  $G_0, \dots, G_k$  we write  $G_0 \mapsto (G_1, \dots, G_k)$  if for every  $k$ -coloring of the edges of  $G_0$ , for some  $i \in [k]$  there is a copy of  $G_i$  with all edges of color  $i$ . The *Ramsey number*  $R(G_1, \dots, G_k)$  is the minimum  $N$  such that  $K_N \mapsto (G_1, \dots, G_k)$ , and  $R_k(G) = R(G_1, \dots, G_k)$ , where  $G_1 = \dots = G_k = G$ .

Gerencsér and Gyárfás [1967] proved that the  $n$ -vertex path  $P_n$  satisfies  $R_2(P_n) = \lfloor \frac{1}{2}(3n - 2) \rfloor$ . They actually proved a stronger result:

**Theorem 1** [Gerencsér and Gyárfás 1967]. *For any two positive integers  $k \geq \ell$ ,  $R(P_k, P_\ell) = k - 1 + \lfloor \frac{1}{2}\ell \rfloor$ .*

Many significant results bounding  $R_k(P_n)$  for  $k \geq 3$  and  $R_k(C_n)$  for even  $n$  were proved in [Benevides et al. 2012; Benevides and Skokan 2009; Bondy and Erdős 1973; DeBiasio and Krueger 2018; DeBiasio et al. 2020; Faudree and Schelp 1974; Figaj and Łuczak 2007; 2018; Gyárfás et al. 2007a; Knierim and Su 2019; Łuczak 1999; Łuczak et al. 2012; Sárközy 2016]. Many proofs used the Szemerédi Regularity Lemma [1978] and a number of them used the idea of connected matchings in regular partitions due to [Łuczak 1999].

Ramsey-type problems when the host graphs are not complete but complete bipartite were studied by Gyárfás and Lehel [1973], Faudree and Schelp [1975], DeBiasio, Gyárfás, Krueger, Ruszinkó, and

---

Balogh was supported in part by NSF grants DMS-1500121, DMS-1764123, the Arnold O. Beckman Research Award 18132 of the UIUC Campus Research Board and the Langan Scholar Fund (UIUC). Kostochka was supported in part by NSF grant DMS-1600592, Award RB17164 of the UIUC Campus Research Board, and grants 18-01-00353 and 19-01-00682 of the Russian Foundation for Basic Research. Liu was supported in part by Award RB17164 of the UIUC Campus Research Board.

*MSC2010:* 05C15, 05C35, 05C38.

*Keywords:* Ramsey number, Regularity Lemma, paths and cycles.

Sárközy [Gyárfás et al. 2007a], DeBiasio and Krueger [2018], Bucić, Letzter, and Sudakov [Bucić et al. 2019a; 2019b], and Zhang, Sun, and Wu [Zhang et al. 2013], and when the host graphs are complete 3-partite by Gyárfás, Ruszinkó, Sárközy, and Szemerédi [Gyárfás et al. 2007b]. The main result in [Faudree and Schelp 1975] and [Gyárfás and Lehel 1973] was:

**Theorem 2** [Faudree and Schelp 1975; Gyárfás and Lehel 1973]. *For every positive integer  $n$ ,  $K_{n,n} \mapsto (P_{2\lceil n/2 \rceil}, P_{2\lceil n/2 \rceil})$ . Furthermore,  $K_{n,n} \not\mapsto (P_{2\lceil n/2 \rceil+1}, P_{2\lceil n/2 \rceil+1})$ .*

DeBiasio and Krueger [2018] extended the result from paths  $P_{2\lceil n/2 \rceil}$  to cycles of length at least  $2\lfloor \frac{1}{2}n \rfloor$  for large  $n$ .

The main result in [Gyárfás et al. 2007b] was:

**Theorem 3** [Gyárfás et al. 2007b]. *For every positive integer  $n$ ,  $K_{n,n,n} \mapsto (P_{2n-o(n)}, P_{2n-o(n)})$ .*

The following exact bound was also conjectured:

**Conjecture 4** [Gyárfás et al. 2007b]. *For every positive integer  $n$ ,  $K_{n,n,n} \mapsto (P_{2n+1}, P_{2n+1})$ .*

The goal of this paper is to prove for large  $n$  Conjecture 4 and similar exact bounds for paths  $P_{2n}$  (parity matters here) and cycles  $C_{2n}$ . We do it in a more general setting: for multipartite graphs with possibly different part sizes. In the next section, we discuss extremal examples, define some notions and state our main results. In Section 3, we describe our tools. In Sections 4–8, we prove the main part, namely, the result for even cycles  $C_{2n}$ . In Sections 9–11 we use the main result to derive similar results for cycles  $C_{\geq 2n}$  and paths  $P_{2n}$  and  $P_{2n+1}$ .

## 2. Examples and results

For a graph  $G$  and disjoint sets  $A, B \subset V(G)$ , by  $G[A]$  we denote the subgraph of  $G$  induced by  $A$ , and by  $G[A, B]$  the bipartite subgraph of  $G$  with parts  $A$  and  $B$  formed by all edges of  $G$  connecting  $A$  with  $B$ .

Our edge-colorings always will be with red (color 1) and blue (color 2).

We consider necessary restrictions on  $n_1 \geq n_2 \geq \dots \geq n_s$  providing that each 2-edge-coloring of  $K_{n_1, n_2, \dots, n_s}$  contains (a) a monochromatic path  $P_{2n}$ , (b) a monochromatic path  $P_{2n+1}$ , (c) a monochromatic cycle  $C_{2n}$  and (d) a monochromatic cycle  $C_{\geq 2n}$ . Each condition we add is motivated by an example showing that the condition is necessary.

First, recall that each of  $P_{2n}$ ,  $P_{2n+1}$ ,  $C_{2n}$ , and  $C_{\geq 2n}$  contains a connected matching  $M_n$ . Thus a graph with no  $M_n$  also contains neither  $P_{2n}$  nor  $P_{2n+1}$  nor  $C_{\geq 2n}$ .

**2.1. Example with no monochromatic  $M_n$ : too few vertices.** Let  $G = K_{3n-2}$ . Clearly,  $G \supseteq K_{n_1, n_2, \dots, n_s}$  for each  $n_1, \dots, n_s$  with  $n_1 + \dots + n_s = 3n - 2$ . Partition  $V(G)$  into sets  $U_1$  and  $U_2$  with  $|U_1| = 2n - 1$  and  $|U_2| = n - 1$ . Color the edges of  $G[U_1, U_2]$  with red and the rest of the edges with blue. Since neither  $K_{2n-1}$  nor  $K_{n-1, 2n-1}$  contains  $M_n$ , we conclude  $G \not\mapsto (M_n, M_n)$ ; see Figure 1.

To rule out this example, we add the condition

$$N := n_1 + \dots + n_s \geq 3n - 1. \tag{1}$$

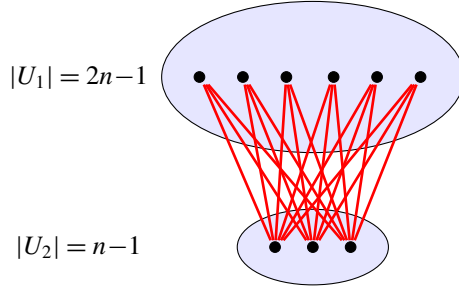


Figure 1. Section 2.1.

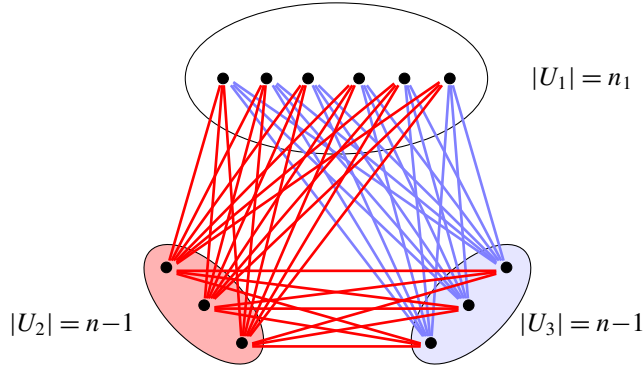


Figure 2. Section 2.2.

**2.2. Example with no monochromatic  $M_n$ : too few vertices outside  $V_1$ .** Choose any  $n_1$  and let  $N = n_1 + 2n - 2$ . Let  $G$  be obtained from  $K_N$  by deleting the edges inside a vertex subset  $U_1$  with  $|U_1| = n_1$ . Graph  $G$  contains every  $K_{n_1, n_2, \dots, n_s}$  with  $n_2 + \dots + n_s = 2n - 2$ . Partition  $V(G) - U_1$  into sets  $U_2$  and  $U_3$  with  $|U_2| = |U_3| = n - 1$ . Color all edges incident with  $U_2$  red, and the remaining edges of  $G$  blue. Since the red and blue subgraphs of  $G$  have vertex covers of size  $n - 1$  (namely,  $U_2$  and  $U_3$ ), neither of them contains  $M_n$ . Thus  $G \not\rightarrow (M_n, M_n)$ ; see Figure 2.

To rule out this example, we add the condition

$$N - n_1 = n_2 + \dots + n_s \geq 2n - 1. \tag{2}$$

**2.3. Example with no red  $M_n$  and no blue  $P_{2n+1}$ : too few vertices.** Let  $G = K_{3n-1}$ . Partition  $V(G)$  into sets  $U_1$  and  $U_2$  with  $|U_1| = 2n$  and  $|U_2| = n - 1$ . Color the edges of  $G[U_1, U_2]$  red and the rest of the edges blue. Since the red subgraph of  $G$  has vertex cover  $U_2$  with  $|U_2| = n - 1$ , it does not contain  $M_n$ . Since each component of the blue subgraph of  $G$  has fewer than  $2n + 1$  vertices, it does not contain  $P_{2n+1}$ .

Therefore

$$R(P_{2n}, P_{2n+1}) \geq R(M_n, P_{2n+1}) \geq 3n,$$

which yields for  $P_{2n+1}$  the following strengthening of (1):

$$\text{for } P_{2n+1}, \quad N \geq 3n. \tag{3}$$

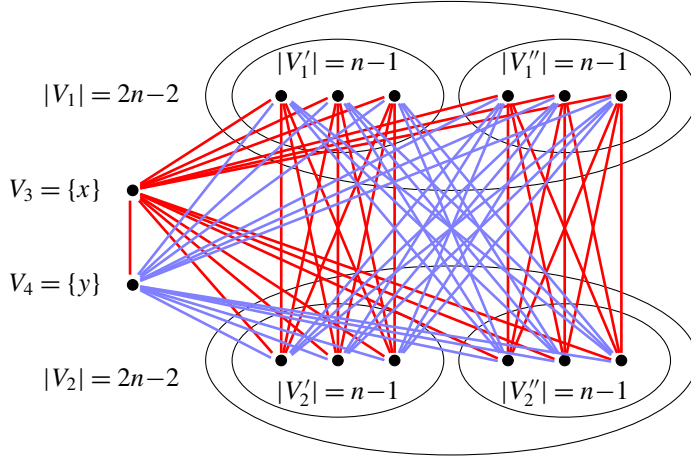


Figure 3. Section 2.4.

**2.4. Example with no monochromatic  $C_{\geq 2n}$  when  $N - n_1 - n_2 \leq 2$ .** This example, and all the ones that follow, show that additional restrictions are necessary when  $G$  is bipartite or close to bipartite.

Let  $G = K_{n_1, \dots, n_s}$  satisfy (1) and (2) with  $N - n_1 - n_2 \leq 2$  such that  $n_1 \leq 2n - 2$ . Then also  $n_2 \leq 2n - 2$ , so  $G \subseteq K_{2n-2, 2n-2, 1, 1}$ . Thus we assume  $G = K_{2n-2, 2n-2, 1, 1}$ , with  $V_1 = \{v_1, \dots, v_{2n-2}\}$ ,  $V_2 = \{u_1, \dots, u_{2n-2}\}$ ,  $V_3 = \{x\}$ , and  $V_4 = \{y\}$ . Let  $V_1' = \{v_1, \dots, v_{n-1}\}$ ,  $V_1'' = V_1 - V_1'$ ,  $V_2' = \{u_1, \dots, u_{n-1}\}$ ,  $V_2'' = V_2 - V_2'$ . Color the edges in  $G[V_1', V_2']$ ,  $G[V_1'', V_2'']$  and in  $G[V_3, V_1 \cup V_2 \cup V_4]$  red, and all other edges blue. Then the red graph  $G_1$  has cut vertex  $x$ , and the components of  $G_1 - x$  have sizes  $2n - 2$ ,  $2n - 2$ , and 1, so  $G_1$  has no  $C_{\geq 2n}$ . Similarly,  $G_2$  contains no  $C_{\geq 2n}$ ; see Figure 3.

To rule out this example, we add the condition

$$\text{for } C_{\geq 2n}, \quad \text{if } N - n_1 - n_2 \leq 2, \quad \text{then } n_1 \geq 2n - 1. \quad (4)$$

**2.5. Example with no monochromatic  $C_{\geq 2n}$  when  $N - n_1 - n_2 \leq 1$ .** Let  $G = K_{n_1, \dots, n_s}$  satisfy (1), (2) and (4) with  $N - n_1 - n_2 \leq 1$  such that  $N + n_1 \leq 6n - 3$ . Since by (4),  $n_1 \geq 2n - 1$ , we get  $N - n_1 \leq (6n - 3) - 2(2n - 1) = 2n - 1$ , but (2) implies  $N - n_1 \geq 2n - 1$ ; therefore both inequalities are tight and  $N - n_1 = n_1 = 2n - 1$ . Hence  $G \subseteq K_{2n-1, 2n-2, 1}$ , which is a subgraph of the graph  $K_{2n-2, 2n-2, 1, 1}$  considered in Section 2.4.

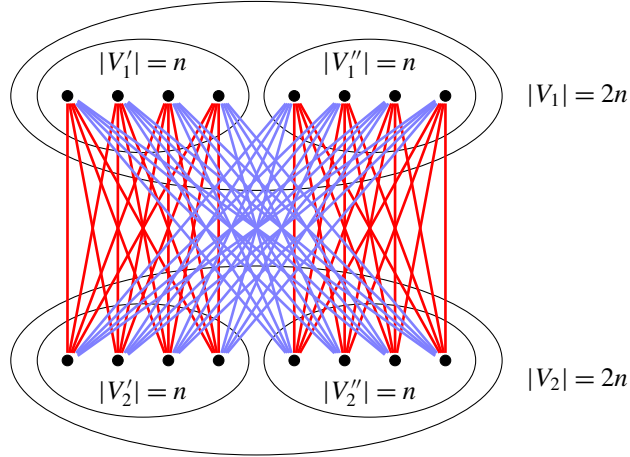
This example is not ruled out by (4), so we add the condition

$$\text{for } C_{\geq 2n}, \quad \text{if } N - n_1 - n_2 \leq 1, \quad \text{then } n_1 + N \geq 6n - 2. \quad (5)$$

**2.6. Example with no monochromatic  $P_{2n+1}$  when  $G$  is bipartite.** Suppose  $n_3 = 0$  and  $n_1 \leq 2n$ . Then  $n_2 \leq 2n$  as well, so  $G \subseteq K_{2n, 2n}$ . Thus we assume  $G = K_{2n, 2n}$  with  $V_1 = \{v_1, \dots, v_{2n}\}$  and  $V_2 = \{u_1, \dots, u_{2n}\}$ . Let  $V_1' = \{v_1, \dots, v_n\}$ ,  $V_1'' = V_1 - V_1'$ ,  $V_2' = \{u_1, \dots, u_n\}$ ,  $V_2'' = V_2 - V_2'$ . Color the edges in  $G(V_1', V_2')$  and  $G(V_1'', V_2'')$  red, and all other edges blue. Then each component in the red graph and each component in the blue graph has  $2n$  vertices and thus does not contain  $P_{2n+1}$ ; see Figure 4.

To rule out this example, we add the condition

$$\text{for } P_{2n+1}, \quad \text{if } n_3 = 0, \quad \text{then } n_1 \geq 2n + 1. \quad (6)$$



**Figure 4.** Section 2.5.

**2.7. Example with no monochromatic  $C_{2n}$  when  $N - n_1 - n_2 \leq 2$ .** Let  $G = K_{n_1, \dots, n_s}$  satisfy (1), (2) and (4) with  $N - n_1 - n_2 = 2$  such that  $N \leq 4n - 2$ . By (4),  $N - n_1 \leq 2n - 1$ . Now (2) implies  $N - n_1 = 2n - 1 = n_1$ . Hence  $G \subseteq K_{2n-1, 2n-3, 1, 1}$ . Thus we assume  $G = K_{2n-1, 2n-3, 1, 1}$  with  $V_1 = \{v_1, \dots, v_{2n-1}\}$ ,  $V_2 = \{u_1, \dots, u_{2n-3}\}$ ,  $V_3 = \{x\}$ , and  $V_4 = \{y\}$ . Define  $A = \{v_2, v_3, \dots, v_n\}$ ,  $B = \{v_{n+1}, v_{n+2}, \dots, v_{2n-1}\}$ ,  $C = \{u_1, u_2, \dots, u_{n-1}\}$ , and  $D = \{u_n, u_{n+1}, \dots, u_{2n-3}\}$ . We assign the colors to the edges of  $G$  as follows:

- (1)  $G[A, C]$  and  $G[B, D]$  are complete bipartite red graphs.
- (2)  $G[A, D]$  and  $G[B, C]$  are complete bipartite blue graphs.
- (3)  $v_1$  has all blue edges to  $V_2$ .
- (4)  $x$  has all red edges to  $V_1 \cup V_2 \cup \{y\}$ .
- (5)  $y$  has all red edges to  $B \cup D \cup \{x\}$  and all blue edges to  $A \cup C \cup \{v_1\}$ .

We claim that  $G$  has no monochromatic cycle of length  $2n$ . Indeed, consider first the red graph  $G_1$ . The graph  $G_1 - x$  has three components: (a)  $A \cup C$  of size  $2n - 2$ , (b)  $\{v_1\}$  of size 1, and (c)  $B \cup D \cup \{y\}$  of size  $2n - 2$ . Thus  $G$  has no red cycle of length  $2n$  since the largest block of  $G_1$  has order  $2n - 1$ .

Consider now the blue graph  $G_2$ . We ignore  $x$  since it is isolated. Suppose  $G_2$  contains a  $2n$ -cycle  $F$ . Since  $v_1$  is a cut vertex of  $G_2 - \{y\}$  with the components of  $G_2 - \{y, v_1\}$  of order  $2n - 3$  and  $2n - 2$ ,  $F$  contains  $y$ .

If we delete from  $G_2$  all edges in  $G_2[\{y\}, C]$ , then both blocks in the remaining blue graph will be of order  $2n - 1$ ; thus  $F$  contains an edge from  $y$  to  $C$ , say  $yz$ . Furthermore, if  $yz$  is the only edge in  $F$  connecting  $y$  to  $C$ , then all other edges in  $F$  belong to the bipartite graph  $H = G_2[A \cup B \cup \{v_1\}, D \cup \{y\} \cup C]$ . But this bipartite graph  $H$  cannot have a path of odd length  $2n - 1$  between the vertices  $y$  and  $z$  in the same part.

Thus,  $F$  has to use two edges from  $y$  to  $C$ , say  $yz_1$  and  $yz_2$ . Then the problem is reduced to finding a blue path from  $z_1$  to  $z_2$  of length  $2n - 2$  in  $G_2[C, B \cup \{v_1\}]$ . However, it is impossible because  $|C| = n - 1$  and the longest path from  $z_1$  to  $z_2$  in  $G_2[C, B \cup \{v_1\}]$  has  $2n - 3$  vertices.

Note that this example has cycles of length greater than  $2n - 1$ , but all such cycles are odd.

To rule out this example, we add the condition

$$\text{for } C_{2n}, \quad \text{if } N - n_1 - n_2 \leq 2, \quad \text{then } N \geq 4n - 1. \quad (7)$$

**2.8. Results.** Our key result is that for large  $n$ , the necessary conditions (1), (2) and (7) for the presence in a 2-edge-colored  $K_{n_1, \dots, n_s}$  of a monochromatic  $C_{2n}$  together are also sufficient for this.

**Theorem 5.** *Let  $s \geq 2$  and  $n$  be sufficiently large. Let  $n_1 \geq \dots \geq n_s$  and  $N = n_1 + \dots + n_s$  satisfy (1), (2) and (7). Then for each 2-edge-coloring  $f$  of the complete  $s$ -partite graph  $K_{n_1, \dots, n_s}$ , there exists a monochromatic cycle  $C_{2n}$ .*

Based on Theorem 5, we derive our other results. The first of them is on cycles of length at least  $2n$  (it extends a result of [DeBiasio and Krueger 2018]). Recall that (7) is not necessary for the existence of a monochromatic  $C_{\geq 2n}$ , but (1), (2), (4) and (5) are.

**Theorem 6.** *Let  $s \geq 2$  and  $n$  be sufficiently large. Let  $n_1 \geq \dots \geq n_s$  and  $N = n_1 + \dots + n_s$  satisfy (1), (2), (4) and (5). Then for each 2-edge-coloring  $f$  of the complete  $s$ -partite graph  $K_{n_1, \dots, n_s}$ , there exists a monochromatic cycle  $C_{\geq 2n}$ .*

The results for paths of even and odd lengths are somewhat different. The first of them shows that for large  $n$ , the necessary conditions (1) and (2) for the presence in a 2-edge-colored  $K_{n_1, \dots, n_s}$  of a monochromatic connected matching  $M_n$  together are sufficient for the presence of the monochromatic path  $P_{2n}$ .

**Theorem 7.** *Let  $s \geq 2$  and  $n$  be sufficiently large. Let  $n_1 \geq \dots \geq n_s$  and  $N = n_1 + \dots + n_s$  satisfy (1) and (2). Then for each 2-edge-coloring  $f$  of the complete  $s$ -partite graph  $K_{n_1, \dots, n_s}$ , there exists a monochromatic path  $P_{2n}$ .*

Our last result implies Conjecture 4:

**Theorem 8.** *Let  $s \geq 2$  and  $n$  be sufficiently large. Let  $n_1 \geq \dots \geq n_s$  and  $N = n_1 + \dots + n_s$  satisfy (2), (3) and (6). Then for each 2-edge-coloring  $f$  of the complete  $s$ -partite graph  $K_{n_1, \dots, n_s}$ , there exists a monochromatic path  $P_{2n+1}$ .*

In the next section, we describe our main tools: the Szemerédi Regularity Lemma, connected matchings, and theorems on the existence of Hamiltonian cycles in dense graphs. In Section 4 we set up and describe the structure of the proof of Theorem 5, and in the next four sections we present this proof. In the last three sections we prove Theorems 6, 7 and 8.

### 3. Tools

As in many recent papers on Ramsey numbers of paths (see [Benevides et al. 2012; Benevides and Skokan 2009; DeBiasio and Krueger 2018; Figaj and Łuczak 2007; Gyárfás et al. 2007a; Knierim and Su 2019; Łuczak et al. 2012; Sárközy 2016]), our proof heavily uses the Szemerédi Regularity Lemma [1978] and the idea of connected matchings in regular partitions of reduced graphs due to [Łuczak 1999].

**3.1. Regularity.** We say that a pair  $(V_1, V_2)$  of two disjoint vertex sets  $V_1, V_2 \subseteq V(G)$  is  $(\epsilon, G)$ -regular if

$$\left| \frac{|E(X, Y)|}{|X||Y|} - \frac{|E(V_1, V_2)|}{|V_1||V_2|} \right| < \epsilon$$

for all  $X \subseteq V_1$  and  $Y \subseteq V_2$  with  $|X| > \epsilon|V_1|$  and  $|Y| > \epsilon|V_2|$ .

We use a 2-color version of the Regularity Lemma, following Gyárfás, Ruszinkó, Sárközy, and Szemerédi [Gyárfás et al. 2007a].

**Lemma 9** (2-color version of the Szemerédi Regularity Lemma). *For every  $\epsilon > 0$  and integer  $m > 0$ , there are positive integers  $M$  and  $n_0$  such that for  $n \geq n_0$  the following holds. For all graphs  $G_1$  and  $G_2$  with  $V(G_1) = V(G_2) = V$ ,  $|V| = n$ , there is a partition of  $V$  into  $L + 1$  disjoint classes (clusters)  $(V_0, V_1, V_2, \dots, V_L)$  such that*

- $m \leq L \leq M$ ,
- $|V_1| = |V_2| = \dots = |V_L|$ ,
- $|V_0| < \epsilon n$ ,
- Apart from at most  $\epsilon \binom{L}{2}$  exceptional pairs, the pairs  $\{V_i, V_j\}$  are  $(\epsilon, G_q)$ -regular for  $q = 1$  and  $2$ .

Additionally, if  $G_1 \cup G_2$  is a multipartite graph with partition  $V = V_1^* \cup V_2^* \cup \dots \cup V_s^*$ , with  $s < 6$ , we can guarantee that each of the clusters  $V_1, V_2, \dots, V_L$  is contained entirely in a single part of this partition.

To do so, for a given  $\epsilon > 0$ , we begin by arbitrarily partitioning each  $V_i^*$  into parts  $V_{i,1}^*, V_{i,2}^*, \dots$ , each of size  $\lfloor \frac{1}{10}\epsilon n \rfloor$ , with a part  $V_{i,0}^*$  of size at most  $\frac{1}{10}\epsilon n$  left over. This is an equitable partition of  $V - \bigcup_{i=1}^k V_{i,0}^*$ , a set of at least  $(1 - \frac{9}{10}\epsilon)n$  vertices. The Regularity Lemma allows us to refine any equitable partition into one that satisfies the conclusions of Lemma 9. Working with the subgraphs of  $G_1$  and  $G_2$  excluding the vertices in  $\bigcup_{i=1}^k V_{i,0}^*$ , take such a refinement with parameters  $\frac{1}{9}\epsilon$  and  $m$ , then add  $\bigcup_{i=1}^k V_{i,0}^*$  to its exceptional cluster  $V_0$ . The resulting exceptional cluster still has size at most  $\epsilon n$ , so we have obtained a partition satisfying the conditions of Lemma 9 in which each of  $V_1, V_2, \dots, V_L$  is entirely contained in one of  $V_1^*, V_2^*, \dots, V_k^*$ .

**3.2. Connected matchings.** Let  $\alpha'(G)$  denote the size of a largest matching and  $\alpha'_*(G)$  denote the size of a largest connected matching in  $G$ . Let  $\alpha(G)$  denote the independence number and  $\beta(G)$  denote the size of a smallest vertex cover in  $G$ .

Łuczak [1999] was the first to use the fact that the existence of large connected matchings in the reduced graph of a regular partition of a large graph  $G$  implies the existence of long paths and cycles in  $G$ . A flavor of it is illustrated by the following fact.

**Lemma 10** [Łuczak et al. 2012, Lemma 8; Knierim and Su 2019, Lemma 1]. *Let a real number  $c > 0$  and a positive integer  $k$  be given. If for every  $\epsilon > 0$  there exists a  $\delta > 0$  and an  $n_0$  such that for every even  $n > n_0$  and each graph  $G$  with  $v(G) > (1 + \epsilon)cn$  and  $e(G) \geq (1 - \delta)\binom{v(G)}{2}$  each  $k$ -edge-coloring of  $G$  has a monochromatic connected matching  $M_{n/2}$ , then for large  $N$ , we have  $R_k(C_N) \leq (c + o(1))N$  (and hence  $R_k(P_N) \leq (c + o(1))N$ ).*

We use the following property of  $(\epsilon, G)$ -regular pairs:

**Lemma 11** [Gyárfás et al. 2007a, Lemma 3]. *For every  $\delta > 0$  there exist  $\epsilon > 0$  and  $t_0$  such that the following holds. Let  $G$  be a bipartite graph with bipartition  $(V_1, V_2)$  such that  $|V_1| = |V_2| = t \geq t_0$ , and let the pair  $(V_1, V_2)$  be  $(\epsilon, G)$ -regular. Moreover, assume that  $\deg_G(v) > \delta t$  for all  $v \in V(G)$ .*

*Then for every pair of vertices  $v_1 \in V_1, v_2 \in V_2$ , the graph  $G$  contains a Hamiltonian path with endpoints  $v_1$  and  $v_2$ .*

Since we are aiming at an exact bound, we need a stability version of a result similar to Lemma 10. To state it, we need some definitions.

**Definition 12.** For  $\epsilon > 0$ , an  $N$ -vertex  $s$ -partite graph  $G$  with parts  $V_1, \dots, V_s$  of sizes  $n_1 \geq n_2 \geq \dots \geq n_s$ , and a 2-edge-coloring  $E = E_1 \cup E_2$  is  $(n, s, \epsilon)$ -suitable if the conditions

$$N = n_1 + \dots + n_s \geq 3n - 1, \quad (\text{S1})$$

$$n_2 + n_3 + \dots + n_s \geq 2n - 1 \quad (\text{S2})$$

hold, and if  $\tilde{V}_i$  is the set of vertices in  $V_i$  of degree at most  $N - \epsilon n - n_i$  and  $\tilde{V} = \bigcup_{i=1}^s \tilde{V}_i$ , then

$$|\tilde{V}| = |\tilde{V}_1| + \dots + |\tilde{V}_s| < \epsilon n. \quad (\text{S3})$$

We do not require  $E_1 \cap E_2 = \emptyset$ ; an edge can have one or both colors. We write  $G_i = G[E_i]$  for  $i = 1, 2$ .

Our stability theorem gives a partition of the vertices of near-extremal graphs called a  $(\lambda, i, j)$ -bad partition. There are two types of bad partitions.

**Definition 13.** For  $i \in \{1, 2\}$ ,  $\lambda > 0$ , and an  $(n, s, \epsilon)$ -suitable graph  $G$ , a partition  $V(G) = W_1 \cup W_2$  of  $V(G)$  is  $(\lambda, i, 1)$ -bad if the following hold:

- (i)  $(1 - \lambda)n \leq |W_2| \leq (1 + \lambda)n_1$ .
- (ii)  $|E(G_i[W_1, W_2])| \leq \lambda n^2$ .
- (iii)  $|E(G_{3-i}[W_1])| \leq \lambda n^2$ .

**Definition 14.** For  $i \in \{1, 2\}$ ,  $\lambda > 0$ , and an  $(n, s, \epsilon)$ -suitable graph  $G$ , a partition  $V(G) = V_j \cup U_1 \cup U_2$ ,  $j \in [s]$ , of  $V(G)$  is  $(\lambda, i, 2)$ -bad if the following hold:

- (i)  $|E(G_i[V_j, U_1])| \leq \lambda n^2$ .
- (ii)  $|E(G_{3-i}[V_j, U_2])| \leq \lambda n^2$ .
- (iii)  $n_j = |V_j| \geq (1 - \lambda)n$ .
- (iv)  $(1 - \lambda)n \leq |U_1| \leq (1 + \lambda)n$ .
- (v)  $(1 - \lambda)n \leq |U_2| \leq (1 + \lambda)n$ .

Our stability theorem is:

**Theorem 15** [Balogh et al. 2019, Theorem 9]. *Let  $0 < \epsilon < 10^{-3}\gamma < 10^{-6}$ ,  $n \geq s \geq 2$ , and  $n > 100/\gamma$ . Let  $G$  be an  $(n, s, \epsilon)$ -suitable graph. If  $\max\{\alpha'_*(G_1), \alpha'_*(G_2)\} \leq n(1 + \gamma)$ , then for some  $i \in [2]$  and  $j \in [2]$ ,  $V(G)$  has a  $(68\gamma, i, j)$ -bad partition.*

### 3.3. Theorems on Hamiltonian cycles in bipartite graphs.

**Theorem 16** ([Chvátal 1972]; see also [Berge 1976, Corollary 5 in Chapter 10]). *Let  $H$  be a  $2n$ -vertex bipartite graph with vertices  $u_1, u_2, \dots, u_n$  on one side and  $v_1, v_2, \dots, v_n$  on the other such that  $d(u_1) \leq \dots \leq d(u_n)$  and  $d(v_1) \leq \dots \leq d(v_n)$ .*

*If  $d_H(u_i) \leq i < n$  implies  $d_H(v_{n-i}) \geq n - i + 1$ , then  $H$  is Hamiltonian.*

**Theorem 17** [Berge 1976]. *Let  $H$  be a  $2m$ -vertex bipartite graph with vertices  $u_1, u_2, \dots, u_m$  on one side and  $v_1, v_2, \dots, v_m$  on the other such that  $d(u_1) \leq \dots \leq d(u_m)$  and  $d(v_1) \leq \dots \leq d(v_m)$ . Suppose that for the smallest two indices  $i$  and  $j$  such that  $d(u_i) \leq i+1$  and  $d(v_j) \leq j+1$ , we have  $d(u_i) + d(v_j) \geq m+2$ .*

*Then  $H$  is Hamiltonian biconnected: for every  $i$  and  $j$ , there is a Hamiltonian path with endpoints  $u_i$  and  $v_j$ .*

**Theorem 18** ([Las Vergnas 1970]; see also [Berge 1976, Theorem 11 on page 214]). *Let  $H$  be a  $2n$ -vertex bipartite graph with vertices  $u_1, u_2, \dots, u_n$  on one side and  $v_1, v_2, \dots, v_n$  on the other such that  $d(u_1) \leq \dots \leq d(u_n)$  and  $d(v_1) \leq \dots \leq d(v_n)$ . Let  $q$  be an integer,  $0 \leq q \leq n-1$ .*

*If, whenever  $u_i v_j \notin E(H)$ ,  $d(u_i) \leq i+q$ , and  $d(v_j) \leq j+q$ , we have*

$$d(u_i) + d(v_j) \geq n + q + 1,$$

*then each set of  $q$  edges that form vertex-disjoint paths is contained in a Hamiltonian cycle of  $G$ .*

**3.4. Using the tools.** Our strategy to prove Theorem 5 is: We first apply a 2-colored version of the Regularity Lemma to  $G$  to obtain a reduced graph  $G^r$ . If  $G^r$  has a large monochromatic connected matching then we find a long monochromatic cycle using Lemma 10. If  $G^r$  does not have a large monochromatic connected matching, then we use Theorem 15 to obtain a bad partition of  $G^r$ . We then transfer the bad partition of  $G^r$  to a bad partition of  $G$  and work with this partition. In some important cases, theorems on Hamiltonian cycles help to find a monochromatic cycle  $C_{2n}$  in  $G$ .

#### 4. Setup of the proof of Theorem 5

Formally, we need to prove the theorem for every  $N$ -vertex complete  $s$ -partite graph  $G$  with parts  $(V_1^*, V_2^*, \dots, V_s^*)$  such that the numbers  $n_i = |V_i^*|$  satisfy  $n_1 \geq n_2 \geq \dots \geq n_s$  and the three conditions

$$N = n_1 + \dots + n_s \geq 3n - 1, \quad (\text{S1}')$$

$$N - n_1 = n_2 + \dots + n_s \geq 2n - 1, \quad (\text{S2}')$$

$$\text{if } N - n_1 - n_2 \leq 2, \quad \text{then } N \geq 4n - 1. \quad (\text{S3}')$$

For a given large  $n$ , we consider a possible counterexample with the minimum  $N + s$ . In view of this, it is enough to consider the lists  $(n_1, \dots, n_s)$  satisfying (S1'), (S2') and (S3') such that:

- (a) For each  $1 \leq i \leq s$ , if  $n_i > n_{i+1}$ , then the list  $(n_1, \dots, n_{i-1}, n_i - 1, n_{i+1}, \dots, n_s)$  does not satisfy some of (S1'), (S2') and (S3').
- (b) If  $s \geq 4$ , then the list  $(n_1, \dots, n_{s-2}, n_{s-1} + n_s)$  (possibly with the entries rearranged into a non-increasing order) does not satisfy some of (S1'), (S2') and (S3').

**Case 1:**  $N - n_1 - n_2 \geq 3$  and  $N > 3n - 1$ . Then (S3') holds by default. If  $n_1 > n_2$ , then the list  $(n_1 - 1, n_2, n_3, \dots, n_s)$  still satisfies the conditions (S1'), (S2') and (S3'), a contradiction to (a). Hence  $n_1 = n_2$ . Choose the maximum  $i$  such that  $n_1 = n_i$ . If  $N - n_1 > 2n - 1$ , consider the list  $(n_1, \dots, n_{i-1}, n_i - 1, n_{i+1}, \dots, n_s)$ . In this case (S1') and (S2') still are satisfied for this list; so by (a), (S3') fails for it. As we assumed  $N - n_1 - n_2 \geq 3$ , we must have  $i \geq 3$  and  $N - n_1 - n_2 = 3$  for (S3') to fail for this list; this further implies  $n_1 = n_i \leq 3$ , so  $N = n_1 + n_2 + 3 \leq 9$ , a contradiction. Thus in this case  $N - n_1 = 2n - 1$ . Therefore,  $n_1 = N - (N - n_1) \geq 3n - (2n - 1) = n + 1$  and hence  $n_2 \geq n + 1$ ,

so  $N - n_1 - n_2 \leq (2n - 1) - (n + 1) = n - 2$ . Then the list  $(n_1, n_1, N - 2n_1)$  satisfies (S1')–(S3'). Summarizing, we get

$$\text{if } N - n_1 - n_2 \geq 3 \text{ and } N > 3n - 1, \text{ then } s = 3, n_2 + n_3 = 2n - 1, \text{ and } n_1 = n_2. \quad (8)$$

**Case 2:**  $N - n_1 - n_2 \geq 3$  and  $N = 3n - 1$ . Again (S3') holds by default. By (S2'),  $n_1 \leq n$ ; hence  $N - n_1 - n_2 \geq n - 1$ . If  $s \geq 4$  and  $n_{s-1} + n_s \leq n$ , then let  $L$  be the list obtained from  $(n_1, \dots, n_s)$  by replacing the two entries  $n_{s-1}$  and  $n_s$  with  $n_{s-1} + n_s$  and then possibly rearrange the entries into nonincreasing order. By construction,  $L$  satisfies (S1')–(S3'), a contradiction to (b). Hence  $n_{s-1} + n_s \geq n + 1$ . We also have  $n_{s-1} + n_s \geq n + 1$  if  $s = 3$ , since in this case  $n_{s-1} + n_s = N - n_1 \geq 2n - 1$ . If  $s \geq 6$ , then  $N \geq 3(n_{s-1} + n_s) \geq 3n + 3$ , contradicting  $N = 3n - 1$ . Thus

$$\text{if } N - n_1 - n_2 \geq 3 \text{ and } N = 3n - 1, \text{ then } n_1 \leq n, s \leq 5, n_{s-1} + n_s \geq n + 1. \quad (9)$$

**Case 3:**  $N - n_1 - n_2 \leq 2$ . Then  $N \leq 2n_1 + 2$ , so by (S3'),  $2n_1 + 2 \geq N \geq 4n - 1$ , implying  $n_1 \geq 2n - 1$ . If  $n_1 \geq 2n$ , then (S2') implies  $G \supseteq K_{2n, 2n-1}$ . If  $n_1 = 2n - 1$ , then by (S3'),  $N - n_1 \geq 2n$ , so again  $G \supseteq K_{2n, 2n-1}$ . Thus we can assume that

$$\text{if } N - n_1 - n_2 \leq 2, \text{ then } G = K_{2n, 2n-1}. \quad (10)$$

As we have seen,

$$\text{in each of Cases 1, 2 and 3 we have } s \leq 5. \quad (11)$$

Fix an arbitrary 2-edge-coloring  $E(G) = E_1 \cup E_2$  of  $G$ . For  $i \in [2]$  and  $v \in V(G)$ , let  $G_i := (V(G), E_i)$  and  $d_i(v)$  denote the degree of  $v$  in  $G_i$ .

## 5. Regularity

**5.1. Applying the 2-colored version of the Regularity Lemma.** We first choose parameter  $\alpha$  so that  $0 < \alpha < 10^{-10}$  and then choose  $\epsilon$  such that  $\epsilon < 10^{-20}$  and  $0 < 10^6 \epsilon < \alpha$  so that the pair  $(\frac{1}{2}\alpha, 3\epsilon)$  satisfies the relation of  $(\delta, \epsilon)$  in Lemma 11 with  $\frac{1}{2}\alpha$  playing the role of  $\delta$ . Here,  $\epsilon$  is the parameter for the Regularity Lemma, and  $\alpha$  is our cutoff for the edge density at which we give an edge of the reduced graph a color.

We apply Lemma 9 to obtain a partition  $(V_0, V_1, \dots, V_L)$  of  $V(G)$ , with each of  $V_1, V_2, \dots, V_L$  contained entirely in one of  $V_1^*, V_2^*, \dots, V_k^*$ . Define the  $k$ -partite *reduced graph*  $G^r$  as follows:

- The vertices of  $G^r$  are  $v_i$  for  $i = 1, 2, \dots, L$ . A  $k$ -partition  $(V'_1, V'_2, \dots, V'_k)$  of  $V(G^r)$  is induced by the  $k$ -partition of  $G$ , and reordered if necessary so that  $|V'_1| \geq |V'_2| \geq \dots \geq |V'_k|$ .
- There is an edge between  $v_i$  and  $v_j$  if and only if  $v_i$  and  $v_j$  are in different parts of the  $k$ -partition and the pair  $\{V_i, V_j\}$  is  $(\epsilon, G_q)$ -regular for both  $q = 1$  and  $q = 2$ .
- The reduced graph  $G^r$  is missing at most  $\epsilon \binom{L}{2}$  edges between distinct pairs  $\{V'_i, V'_j\}$ .
- We give  $G^r$  a 2-edge-multicoloring: two graphs  $(G_1^r, G_2^r)$  whose union includes every edge of  $G^r$ , but are not necessarily edge-disjoint. We add edge  $v_i v_j \in E(G^r)$  to  $G_q^r$  if  $G_q$  contains at least  $\alpha |V_i| |V_j|$  of the edges between  $V_i$  and  $V_j$ . Since  $G = G_1 \cup G_2$  contains all  $|V_i| |V_j|$  edges between  $V_i$  and  $V_j$ , each edge of  $G^r$  is added to either  $G_1^r$  or  $G_2^r$ , and possibly to both.

Let  $t = |V_1| = |V_2| = \dots = |V_L|$ ,  $\ell_i = |V'_i|$  for  $i = 1, \dots, k$ , and  $\ell := (n - \epsilon N)/t$ ; since  $N \leq 4n - 1$ , we have  $\ell t \geq (1 - 5\epsilon)n$ .

Because  $|V_0| \leq \epsilon N$ , we have  $(1 - \epsilon)N \leq Lt \leq N$  and  $n_i - \epsilon N \leq \ell_i t \leq n_i$ . Therefore:

- $Lt \geq (1 - \epsilon)N \geq 3n - 1 - \epsilon N = 3(\ell t + \epsilon N) - 1 - \epsilon N \geq 3\ell t - 1 + 2\epsilon n$ , which means  $L \geq 3\ell - 1$ .
- $Lt \leq N \leq 4n - 1 = 4(\ell t + \epsilon N) - 1 \leq 5\ell t$ , which means  $L \leq 5\ell$ .
- $Lt - \ell_1 t \geq N - n_1 - \epsilon N \geq 2n - 1 - \epsilon N \geq 2(\ell t + \epsilon N) - 1 - \epsilon N \geq 2\ell t - 1 + \epsilon N$ , which means  $L - \ell_1 \geq 2\ell - 1$ .

Recall that  $G^r$  is missing at most  $\epsilon \binom{L}{2} \leq \epsilon \frac{1}{2} L^2 < 16\epsilon L^2$  edges between distinct pairs  $\{V'_i, V'_j\}$ . Since the number of  $V_i$ 's missing at least  $4\sqrt{\epsilon}\ell$  edges is less than  $4\sqrt{\epsilon}\ell$ , we know  $G^r$  is  $(\ell, k, 4\sqrt{\epsilon})$ -suitable. We apply Theorem 15 to the graph  $G^r$  with  $\gamma$  such that  $10^{-6} > \gamma > 1000\alpha$  and  $\gamma > 4000\sqrt{\epsilon}$ . Then we conclude that either  $G^r$  has a monochromatic connected matching of size  $(1 + \gamma)\ell$ , or else  $V(G)$  has a  $(68\gamma, i, j)$ -bad partition for some  $i \in [2]$  and  $j \in [2]$ .

**5.2. Handling a large connected matching in the reduced graph.** For every edge  $v_i v_j \in G_1^r$ , the corresponding pair  $(V_i, V_j)$  is  $(\epsilon, G_1)$ -regular and contains at least  $\alpha t^2$  edges of  $G_1$ . Let  $X_{ij} \subseteq V_i$  be the set of all vertices of  $V_i$  with fewer than  $\frac{1}{2}\alpha t$  edges of  $G_1$  to  $V_j$ , and let  $Y_{ij} \subseteq V_j$  be the set of all vertices of  $V_j$  with fewer than  $\frac{1}{2}\alpha t$  edges of  $G_1$  to  $V_i$ . Note we have  $Y_{ij} = X_{ji}$  but we keep using the notation  $Y_{ij}$  for emphasizing they are in different parts. Then

$$\frac{|E(X_{ij}, V_j)|}{|X_{ij}||V_j|} \leq \frac{\alpha}{2},$$

so  $|X_{ij}| \leq \epsilon t$  to avoid violating  $(\epsilon, G_1)$ -regularity; similarly,  $|Y_{ij}| \leq \epsilon t$ . Call vertices of  $V_i \cup V_j$  which are not in  $X_{ij} \cup Y_{ij}$  *typical* for the pair  $(V_i, V_j)$  (or for the edge  $v_i v_j$  of  $G_1$ ).

Let  $\mathcal{M}$  be a connected matching in  $G_1^r$  of size  $(1 + \gamma)\ell$ . Give the edges in  $\mathcal{M}$  an arbitrary cyclic ordering.

If  $v_{i_1} v_{j_1}$  and  $v_{i_2} v_{j_2}$  are edges of  $\mathcal{M}$  which are consecutive in the ordering, we shall find a path  $P(j_1, i_2)$  in  $G_1$  joining a vertex of  $V_{j_1} \setminus Y_{i_1 j_1}$  to a vertex of  $V_{i_2} \setminus X_{i_2 j_2}$ . To do so, we begin by finding a path  $P^r$  from  $v_{j_1}$  to  $v_{i_2}$  in  $G_1^r$ , then find a realization of that path in  $G_1$ . Pick a starting point of  $P(j_1, i_2)$  typical both for the edge  $v_{i_1} v_{j_1}$  and for the first edge of  $P^r$ . Next, choose the path greedily, making sure to satisfy the following conditions:

- Choose a neighbor of the previous vertex chosen which is typical for the next edge of  $P^r$  (or for  $v_{i_2} v_{j_2}$  when we reach the end of  $P^r$ ).
- Choose a vertex which has not been chosen for any previous paths.

As we construct  $P(j_1, i_2)$ , the last vertex we have chosen is always typical for the edge of  $P^r$  we are about to realize; therefore we have at least  $\frac{1}{2}\alpha t$  options for its neighbors. At most  $\epsilon t$  of them are eliminated because they are not typical for the next edge, and at most  $L^2$  are eliminated because they have been chosen for previous paths. Since  $L$  is upper bounded by  $M$  which is independent of  $n$ , and  $\epsilon < 10^{-6}\alpha$ , we can always choose such a vertex.

Moreover, we may choose the paths such that their total length has the same parity as  $|\mathcal{M}|$ . If the component of  $G_1^r$  containing  $\mathcal{M}$  is not bipartite, then each path can be chosen to have any parity we like. If the component of  $G_1^r$  containing  $\mathcal{M}$  is bipartite, then this condition is satisfied automatically:

if we join the paths of  $P^r$  we chose by the edges of  $\mathcal{M}$ , we get a closed walk, which must have even length.

Once all these paths are chosen, we combine them into a long even cycle in  $G_1$ . For each edge  $v_i v_j$  in the matching  $\mathcal{M}$ , we have vertices  $x \in V_i$  and  $y \in V_j$ , both typical for  $(V_i, V_j)$ , which are the endpoints of two paths we have constructed. We show that we can find a path from  $x$  to  $y$  using only edges of  $G_1$  between  $V_i$  and  $V_j$  of any odd length between  $t - 1$  and  $(1 - 3\epsilon)2t - 1$ .

To do so, we choose any  $X \subseteq V_i$  with  $|X| \geq \frac{1}{2}t$  that contains  $x$  and at least  $\frac{1}{2}\alpha t$  neighbors of  $y$ ; similarly, we choose  $Y \subseteq V_j$  with  $|Y| = |X|$  that contains  $y$  and at least  $\frac{1}{2}\alpha t$  neighbors of  $x$ . If we want the path to have length  $2Ct - 1$ , where  $C \in [\frac{1}{2}, 1 - 3\epsilon]$ , we begin by choosing  $X$  and  $Y$  of size  $(C + 3\epsilon)t$ . The pair  $(X, Y)$  is  $(2\epsilon, G_1)$ -regular with density at least  $\alpha - \epsilon$ , so there are at most  $2\epsilon$  vertices in each of  $X$  and  $Y$  which have fewer than  $\frac{1}{2}\alpha t$  neighbors on the other side; by our construction of  $X$  and  $Y$ ,  $x$  and  $y$  are not among them.

Let  $X' \subseteq X$  and  $Y' \subseteq Y$  be the subsets obtained by deleting these low-degree vertices, leaving at least  $(C + \epsilon)t$  vertices on each side, and then deleting enough vertices from each part to make  $|X'| = |Y'| = Ct$ . The pair  $(X', Y')$  is  $(3\epsilon, G_1)$ -regular, and all vertices have minimum degree at least  $(\alpha - 3\epsilon)t$ , so by Lemma 11, there is a path from  $x$  to  $y$  using all vertices of  $X'$  and  $Y'$ , which has the desired length  $2Ct - 1$ .

If we use  $C = 1 - 3\epsilon$  for each edge  $v_i v_j$  in the matching  $\mathcal{M}$ , then the cycle contains at least  $2(1 - 3\epsilon)t$  vertices for each edge of  $\mathcal{M}$ , even ignoring the paths we constructed between them, while  $|\mathcal{M}| \geq (1 + 10\epsilon)\ell$ ; therefore the total length is at least

$$2(1 - 3\epsilon)(1 + 10\epsilon)\ell t \geq 2(1 - 3\epsilon)(1 + 10\epsilon)(1 - 5\epsilon)n \geq (1 + \epsilon)2n.$$

If we use  $C = \frac{1}{2}$  each edge  $v_i v_j$ , then the cycle contains only  $t$  vertices for each edge of  $\mathcal{M}$ , giving approximately half as many edges. Up to parity, we are free to choose any length in this range, and therefore it is possible to construct a path in  $G_1$  of length exactly  $2n$ .

**5.3. Handling a bad partition of the reduced graph.** We will show in Sections 6 and 7 how to find a long monochromatic cycle in a bad partition of  $G$ . In this subsection, we show that a bad partition of  $G^r$  corresponds to a bad partition of  $G$ .

- (1) If  $X \subseteq V(G^r)$  has size  $C\ell$ , then the corresponding set of vertices in  $G$  is  $\bigcup_{v_i \in X} V_i$ . It has size  $C\ell t$ , which is in the range  $[(1 - 5\epsilon)Cn, Cn]$ .
- (2) If  $|E_{G_i^r}(X)| \leq \lambda\ell^2$ , then each of those  $\lambda\ell^2$  edges of  $G_i^r$  corresponds to at most  $t^2$  edges of  $G_i$  for  $\lambda\ell^2 t^2 \leq \lambda n^2$  edges.

Additionally, edges not in  $G_i^r$  may appear in  $G_i$ ; across all of  $G_i$  there are at most  $\alpha t^2 \binom{L}{2} \leq \frac{1}{2}\alpha N^2 \leq 10\alpha n^2$  edges that occur in this way.

Moreover, edges from at most  $\epsilon \binom{L}{2}$  exceptional pairs may appear in  $G_i$ , contributing at most  $10\epsilon n^2$  edges in total by the same calculation.

To summarize, there are at most  $(\lambda + 10\alpha + 10\epsilon)n^2$  edges in  $G_i$  corresponding to  $E_{G_i^r}(X)$ . A similar argument applies to a bound on  $|E_{G_i^r}(X, Y)|$  for  $X, Y \subseteq V(G^r)$ .

- (3) There are fewer than  $\epsilon N \leq 5\epsilon n$  vertices from the exceptional part  $V_0$ , which can generally be assigned to any part of any bad partition without changing the approximate structure.

Thus, for  $10^{-3} > \lambda > 1000\alpha > 10^9\epsilon > 0$ , if  $G^r$  has a  $(\lambda, i, 1)$ -bad partition ( $i \in [2]$ )  $V(G^r) = W_1^r \cup W_2^r$ , then  $G$  has a corresponding  $(2\lambda, i, 1)$ -bad partition with:

- (0)  $W_1 := (\bigcup_{v_i \in W_1^r} V_i) \cup V_0$  and  $W_2 := \bigcup_{v_i \in W_2^r} V_i$ .
- (i)  $(1 - 2\lambda)n \leq (1 - \lambda)(1 - 5\epsilon)n \leq (1 - \lambda)\ell t \leq |W_2| \leq (1 + \lambda)\ell_1 t \leq (1 + \lambda)n_1$ .
- (ii)  $|E(G_i[W_1, W_2])| \leq (\lambda + 10\alpha + 10\epsilon + 5\epsilon)n^2 \leq 2\lambda n^2$ .
- (iii)  $|E(G_{3-i}[W_1])| \leq (\lambda + 10\alpha + 10\epsilon + 5\epsilon + \frac{25}{2}\epsilon^2)n^2 \leq 2\lambda n^2$ .

If  $G^r$  has a  $(\lambda, i, 2)$ -bad partition ( $i \in [2]$ )  $V(G^r) = V_j^r \cup U_1^r \cup U_2^r$  then  $G$  has a corresponding  $(2\lambda, i, 2)$ -bad partition with:

- (0)  $U_1 := \bigcup_{v_i \in U_1^r} V_i \cup (V_0 - V_j^*)$  and  $U_2 := \bigcup_{v_i \in U_2^r} V_i$ .
- (i)  $|E(G_i[V_j^*, U_1])| \leq (\lambda + 10\alpha + 10\epsilon + 5\epsilon)n^2 \leq 2\lambda n^2$ .
- (ii)  $|E(G_{3-i}[V_j, U_2])| \leq (\lambda + 10\alpha + 10\epsilon + 5\epsilon)n^2 \leq 2\lambda n^2$ .
- (iii)  $n_j = |V_j^*| \geq \ell_j t \geq (1 - \lambda)\ell t \geq (1 - \lambda)(1 - 5\epsilon)n \geq (1 - 2\lambda)n$ .
- (iv)  $(1 + 2\lambda)n \geq (1 + \lambda)n + 5\epsilon n \geq (1 + \lambda)\ell t + 5\epsilon n \geq |U_1| \geq (1 - \lambda)\ell t \geq (1 - \lambda)(1 - 5\epsilon)n \geq (1 - 2\lambda)n$ .
- (v)  $(1 + \lambda)n \geq (1 + \lambda)\ell t \geq |U_2| \geq (1 - \lambda)\ell t \geq (1 - \lambda)(1 - 5\epsilon)n \geq (1 - 2\lambda)n$ .

Therefore, a  $(68\gamma, i, j)$ -bad partition of  $G^r$  corresponds to a  $(136\gamma, i, j)$ -bad partition of  $G$  for some  $i \in [2]$  and  $j \in [2]$ . In the next three sections we show how to find a monochromatic cycle of length exactly  $2n$  when  $G$  has a  $(\lambda, i, j)$ -bad partition for some  $i \in [2]$  and  $j \in [2]$ , where  $\lambda = 136\gamma$ .

## 6. Dealing with $(\lambda, i, 1)$ -bad partitions when $N - n_1 - n_2 \geq 3$

**6.1. Setup.** Without loss of generality, let  $i = 1$ . Recall that  $d_k(v)$  is the degree of  $v$  in  $G_k$ , where  $k \in [2]$ . We assume that for some  $\lambda < 0.01$ , there is a partition  $V(G) = W_1 \cup W_2$  such that

$$(1 - \lambda)n \leq |W_2| \leq (1 + \lambda)n_1, \quad (12)$$

$$|E(G_1[W_1, W_2])| \leq \lambda n^2, \quad (13)$$

$$|E(G_2[W_1])| \leq \lambda n^2. \quad (14)$$

If  $G$  has at least four parts then  $n_1 \leq n$  by (8) and (9). If  $G$  is tripartite, then we could have  $n_1$  much larger than  $n$ , but in this section, we will assume  $n_1 < \frac{5}{3}n$ . The alternative, that  $G$  is tripartite and  $n_1 \geq \frac{5}{3}n$ , is handled in Section 6.2.

We know that  $|W_1| \geq N - (1 + \lambda)n_1 \geq 2n - 1 - \lambda n_1 \geq (2 - 5\lambda)n$  since  $n_1 \leq 2n$ . For any vertex  $x$ , fewer than  $\frac{5}{3}n$  vertices of  $W_1$  can be in the same part  $V_i$  of  $G$  as  $x$ , so at least  $(\frac{1}{3} - 5\lambda)n > \frac{1}{4}n$  are in other parts of  $G$ . In other words, we have  $d(x, W_1) \geq \frac{1}{4}n$  for all  $x \in V(G)$ .

We call a vertex  $x \in V(G)$   $W_1$ -typical if  $d_1(x, W_1) \geq \frac{3}{4}d(x, W_1)$ , and  $W_2$ -typical if  $d_1(x, W_1) < \frac{3}{4}d(x, W_1)$ .

If  $x$  is  $W_1$ -typical, then  $d_1(x, W_1) \geq \frac{3}{4} \cdot \frac{1}{4}n = \frac{3}{16}n$ . Since

$$\sum_{x \in W_2} d_1(x, W_1) = |E(G_1[W_1, W_2])| \leq \lambda n^2,$$

the number of  $W_1$ -typical vertices in  $W_2$  is at most

$$\frac{\lambda n^2}{\frac{3}{16}n} < 6\lambda n.$$

Similarly, if  $x$  is  $W_2$ -typical, then  $d_2(x, W_1) \geq \frac{1}{4} \cdot \frac{1}{4}n = \frac{1}{16}n$ . Since

$$\sum_{x \in W_1} d_2(x, W_1) = 2|E(G_2[W_1])| \leq 2\lambda n^2,$$

the number of  $W_2$ -typical vertices in  $W_1$  is at most

$$\frac{2\lambda n^2}{\frac{1}{16}n} = 32\lambda n.$$

Let  $W'_1$  be the set of all  $W_1$ -typical vertices and  $W'_2$  be the set of all  $W_2$ -typical vertices. The partition  $(W'_1, W'_2)$  is almost exactly the same as the partition  $(W_1, W_2)$ : at most  $40\lambda n$  vertices have been moved from one part to the other part to obtain  $(W'_1, W'_2)$  from  $(W_1, W_2)$ . Therefore, if  $x \in W'_1$ , we still have  $d_1(x, W'_1) \geq \frac{3}{4}d(x, W_1) - 40\lambda n$ , and if  $x \in W'_2$ , we still have  $d_1(x, W'_1) < \frac{3}{4}d(x, W_1) + 40\lambda n$ . In either case, we still have  $d(x, W'_1) \geq \frac{1}{4}n - 40\lambda n$  for all  $x$ .

Moreover,  $W'_1$  and  $W'_2$  still satisfy similar conditions to  $W_1$  and  $W_2$ :

- (1)  $(1 - 41\lambda)n \leq |W'_2| \leq (1 + \lambda)n_1 + 40\lambda n \leq (1 + 81\lambda)n_1$  (since  $n_1 \geq \frac{1}{2}n$  in all cases).
- (2)  $|E(G_1[W'_1, W'_2])| \leq \lambda n^2 + N \cdot (40\lambda n) \leq 161\lambda n^2$ , since we move at most  $40\lambda n$  vertices with degree less than  $N$ .
- (3)  $|E(G_2[W'_1])| \leq \lambda n^2 + N \cdot (6\lambda n) \leq 25\lambda n^2$ , since we move at most  $6\lambda n$  vertices with degree less than  $N$  into  $W'_1$ .

For convenience, let  $\delta = 200\lambda$ , which is at least as large as all multiples of  $\lambda$  used above.

Our goal is to find a cycle of length  $2n$  in either  $G_1$  or  $G_2$ . We decide which type of cycle we will attempt to find based on the relative sizes of  $W'_1$  and  $W'_2$ .

Suppose that  $|W'_1| \geq 2n$  and, moreover,  $|W'_1 \setminus V_i| \geq n$  for all  $i$ . In this case, we find a cycle of length  $2n$  in  $G_1$ ; this is done in Section 6.3.

Otherwise, we must have  $|W'_2| \geq n$ : either  $|W'_1| \leq 2n - 1$  and  $|W'_2| = N - |W'_1| \geq n$ , or else  $|W'_1 \setminus V_i| \leq n - 1$  for some  $i$ , and

$$|W'_2| \geq |W'_2 \setminus V_i| = |V \setminus V_i| - |W'_1 \setminus V_i| \geq (N - n_i) - (n - 1) \geq (2n - 1) - (n - 1) = n.$$

In this case, we find a cycle of length  $2n$  in  $G_2$ ; this is done in Section 6.4.

We use the following lemma to pick out “well-behaved” vertices in  $W'_1$  and  $W'_2$ . For example, we commonly apply it to  $G_2[W'_1]$  or to  $G_1[W'_1, W'_2]$ .

**Lemma 19.** *Let  $H$  be an  $n$ -vertex graph with at most  $\epsilon n^2$  edges for some  $\epsilon > 0$  and let  $S \subseteq V(H)$ . If  $S' \subseteq S$  is any subset that excludes the  $k$  vertices of  $S$  with the highest degree, then every  $v \in S'$  satisfies  $d_H(v) < 2\epsilon n^2/k$ .*

*Additionally, when  $H$  is bipartite, and  $S$  is entirely contained in one part of  $H$ , every  $v \in S'$  satisfies  $d_H(v) < \epsilon n^2/k$ .*

*Proof.* In the first case, if we have  $d_H(v) \geq 2\epsilon n^2/k$  for any  $v \in S'$ , then we also have  $d_H(v) \geq d$  for the  $k$  vertices of  $S$  with the highest degree, which we excluded from  $S'$ . The sum of degrees of these  $k+1$  vertices exceeds  $2\epsilon n^2$ , so it is greater than twice the number of edges in  $H$ , a contradiction.

In the second case, if we have  $d_H(v) \geq \epsilon n^2/k$  for any  $v \in S'$ , the same sum of degrees exceeds  $\epsilon n^2$ . But since the vertices of  $S$  are all on one side of the bipartition of  $H$ , this sum of degrees cannot be greater than the number of edges in  $H$ , which is again a contradiction.  $\square$

**6.2. The nearly bipartite subcase.** In this subsection, we assume that  $G$  is tripartite with  $n_1 \geq \frac{5}{3}n$ . Recall that when  $G$  is tripartite we have  $n_1 = n_2$  and  $n_1 + n_3 = n_2 + n_3 = 2n - 1$ , and that throughout Section 6 we assume  $N - n_1 - n_2 \geq 3$ , or in this case that  $n_3 \geq 3$ .

Case 1:  $|W_1 \cap V_i| \geq (1 + 10\lambda)n$  for  $i = 1$  or  $i = 2$ . We assume  $i = 1$ ; the proof for the case  $i = 2$  is the same. In this case, let  $X$  be an  $n$ -vertex subset of  $V_1 \cap W_1$  avoiding the  $5\lambda n$  vertices of  $V_1 \cap W_1$  with the most edges of  $G_2$  to  $W_1 \setminus V_1$  and the  $5\lambda n$  vertices of  $V_1 \cap W_1$  with the most edges of  $G_1$  to  $W_2 \setminus V_1$ .

For any vertex  $v \in X$ , we have

$$d_2(v, W_1 \setminus V_1) \leq \frac{\lambda n^2}{5\lambda n} = \frac{n}{5} \quad \text{and} \quad d_1(v, W_2 \setminus V_1) \leq \frac{n}{5}$$

by Lemma 19.

We partition  $V_2 \cup V_3$  into sets  $Y_1$  and  $Y_2$  by the following procedure:

- (1) The  $2\lambda n$  vertices of  $W_1 \setminus V_1$  with the most edges of  $G_2$  to  $X$  are set aside, and the remaining vertices of  $W_1 \setminus V_1$  are assigned to  $Y_1$ .  
By Lemma 19, any vertex  $v$  assigned to  $Y_1$  in this step has  $d_2(v, X) \leq \frac{1}{2}n$ .
- (2) The  $2\lambda n$  vertices of  $W_2 \setminus V_1$  with the most edges of  $G_1$  to  $X$  are set aside, and the remaining vertices of  $W_2 \setminus V_1$  are assigned to  $Y_2$ .  
By Lemma 19, any vertex  $v$  assigned to  $Y_2$  in this step has  $d_1(v, X) \leq \frac{1}{2}n$ .
- (3) Each remaining vertex  $v$  is assigned to  $Y_1$  if  $d_1(v, X) \geq \frac{1}{2}n$  and to  $Y_2$  otherwise (in which case  $d_2(v, X) \geq \frac{1}{2}n$ ).

Since  $|V_2 \cup V_3| = 2n - 1$ , we must have  $|Y_1| \geq n$  or  $|Y_2| \geq n$ . Let  $Y'_j$  be an  $n$ -vertex subset of  $Y_j$ , where  $j \in [2]$  and  $|Y'_j| \geq n$ . We apply Theorem 16 to find a Hamiltonian cycle in the bipartite graph  $H = G_j[X, Y'_j]$ .

The minimum  $H$ -degree in  $X$  is  $\frac{4}{5}n - 2\lambda n$ , since each  $v \in X$  had at most  $\frac{1}{5}n$  edges to  $W_j \setminus V_1$  which were not in  $G_j$ , and at most  $2\lambda n$  vertices of  $Y'_j$  did not come from  $W_j \setminus V_1$  originally. The minimum  $H$ -degree in  $Y'_j$  is  $\frac{1}{2}n$ , so the condition of Theorem 16 is satisfied: whenever  $d_H(u_i) \leq i$ , we have  $i \geq (\frac{4}{5} - 2\lambda)n$ , so  $d_H(v_{n-i}) \geq \frac{1}{2}n \geq (\frac{1}{5} + 2\lambda)n + 1$ .

Case 2:  $|V_i \cap W_1| < (1 + 10\lambda)n$  for  $i = 1$  and  $i = 2$ . By (12), we must have  $|W_1| \geq N - (1 + \lambda)n_1 = 2n - 1 - \lambda n_1 > 2n - 3\lambda n$ . Since  $n_1 = n_2 \geq \frac{5}{3}n$  and  $n_2 + n_3 = 2n - 1$ , fewer than  $\frac{1}{3}n$  vertices of  $W_1$  are in  $V_3$ , so at least  $(\frac{5}{3} - 3\lambda)n$  of them are in  $V_1 \cup V_2$ ; therefore  $|W_1 \cap V_1| > (\frac{2}{3} - 13\lambda)n$  and  $|W_1 \cap V_2| > (\frac{2}{3} - 13\lambda)n$ .

Because  $2n > n_1 = n_2 \geq \frac{5}{3}n$ , we have  $(\frac{2}{3} - 10\lambda)n < |V_i \cap W_2| < (\frac{4}{3} + 13\lambda)n$  for  $i = 1, 2$ , as well.

Next, we choose subsets  $X_{ij} \subseteq V_i \cap W_j$  with  $|X_{11}| = |X_{21}| = |X_{12}| = |X_{22}| = \frac{1}{2}n + 10$ . To choose  $X_{11}$  and  $X_{21}$ , avoid the  $\frac{1}{20}n$  vertices with the most edges in  $G_1$  to  $W_2$  and the  $\frac{1}{20}n$  vertices with the most edges in  $G_2$  to  $W_1$ , so that each chosen vertex has at most  $20\lambda n$  edges of each kind by Lemma 19. To

choose  $X_{12}$  and  $X_{22}$ , avoid the  $\frac{1}{10}n$  vertices with the most edges in  $G_1$  to  $W_1$ , so that each chosen vertex has at most  $10\lambda n$  such edges by Lemma 19.

First, we observe that if  $H$  is any of the graphs  $G_1[X_{11}, X_{21}]$ ,  $G_2[X_{12}, X_{21}]$ , or  $G_2[X_{11}, X_{22}]$ , then given any vertices  $v, w$  in  $H$ , we can find a  $(v, w)$ -path in  $H$  on  $m$  vertices, provided that  $n - 10 \leq m \leq n + 10$  (this is not optimal, but it is more than we need) and that the parity of  $m$  is correct.

To do so, we apply Theorem 18. If  $v$  and  $w$  are on the same side of  $H$ , add a vertex  $x$  to the other side adjacent to all vertices in the side containing  $v$  and  $w$ ; if not, add an edge  $vw$ . Then take a subgraph containing  $\lceil \frac{1}{2}m \rceil$  vertices from each side, making sure to include  $v, w$  and if applicable  $x$ . In this subgraph, the minimum degree is at least  $\lceil \frac{1}{2}m \rceil - 20\lambda n$ , so we can use Theorem 18 to find a Hamiltonian cycle in this graph containing either the edge  $vw$  or the edges  $vx$  and  $xw$ . Deleting the vertex  $x$  or the edge  $vw$ , whichever applies, creates a  $(v, w)$ -path in  $H$  of the correct length.

Suppose that  $G_2[X_{12}, X_{22}]$  contains a matching  $M = \{u_1u_2, v_1v_2\}$  of size 2, where  $u_1, v_1 \in X_{12}$  and  $u_2, v_2 \in X_{22}$ . In that case, we can find a  $(u_1, v_1)$ -path  $P$  in  $G_2[X_{12}, X_{21}]$  on  $2\lceil \frac{1}{2}n \rceil + 1$  vertices and a  $(u_2, v_2)$ -path  $Q$  in  $G_2[X_{11}, X_{22}]$  on  $2\lfloor \frac{1}{2}n \rfloor - 1$  vertices by the previous observation. Joining the paths  $P$  and  $Q$  using the edges of the matching  $M$ , we find a cycle of length  $2n$  in  $G_2$ .

Now we assume  $G_2[X_{12}, X_{22}]$  does not contain a matching of size 2. If the size of a maximum matching in this graph is 1, then there is a vertex cover of size 1 since  $G_2[X_{12}, X_{22}]$  is bipartite. We delete this vertex cover from  $X_{12}$  or  $X_{22}$  (it depends on where this vertex cover is). Having changed  $X_{12}$  and  $X_{22}$  in this way,  $G_1[X_{12}, X_{22}]$  is a complete bipartite graph, so it also has the property that any two vertices in it can be joined by a path on  $m$  vertices, provided that  $n - 10 \leq m \leq n + 10$  and that the parity of  $m$  is correct.

Note that there are at least three vertices in  $V_3$ .

We say that a vertex  $v \in V_3$

- is *j-adjacent* to a set  $S$  if it has at least two edges in  $G_j$  to  $S$ ,
- *S-connects*  $G_j$  if it is *j-adjacent* to both  $X_{11}$  and  $X_{12}$ , or if it is *j-adjacent* to both  $X_{21}$  and  $X_{22}$  (“S-connects” because it is *j-adjacent* to two sets in the *same* part of  $V_1$  or  $V_2$ ),
- *C-connects*  $G_1$  if it is 1-adjacent to both  $X_{11}$  and  $X_{22}$ , or if it is 1-adjacent to both  $X_{12}$  and  $X_{21}$  (“C-connects” because the *j-adjacency crosses* from  $V_1$  to  $V_2$ ),
- *C-connects*  $G_2$  if it is 2-adjacent to both  $X_{11}$  and  $X_{21}$ , or if it is 2-adjacent to both  $X_{12}$  and  $X_{22}$ ,
- *folds into*  $G_1$  if it is 1-adjacent to both  $X_{11}$  and  $X_{21}$ , or if it is 1-adjacent to both  $X_{12}$  and  $X_{22}$ ,
- *folds into*  $G_2$  if it is 2-adjacent to both  $X_{11}$  and  $X_{22}$ , or if it is 2-adjacent to both  $X_{12}$  and  $X_{21}$ .

Some comments on these definitions: first, a vertex that is *j-adjacent* to at least three of  $X_{11}, X_{12}, X_{21}, X_{22}$  is guaranteed to both S-connect and C-connect  $G_j$ . Second, a vertex that is *j-adjacent* to only two of  $X_{11}, X_{12}, X_{21}, X_{22}$  for each value of  $j$  may S-connect both  $G_1$  and  $G_2$ , or C-connect  $G_1$  and fold into  $G_2$ , or C-connect  $G_2$  and fold into  $G_1$ . In particular, each vertex either S-connects or C-connects some  $G_j$ .

If there are two vertices in  $V_3$  that both S-connect  $G_j$ , or both C-connect  $G_j$ , then we can find a cycle of length  $2n$  in  $G_j$ . The cases are all symmetric; without loss of generality, suppose  $v, w \in V_3$  both S-connect  $G_1$ . We can find a path  $P$  in  $G_1[X_{11}, X_{21}]$  on  $2\lceil \frac{1}{2}n \rceil - 1$  vertices that starts at a  $G_1$ -neighbor of  $v$  and ends at a  $G_1$ -neighbor of  $w$ , and a path  $Q$  in  $G_1[X_{12}, X_{22}]$  on  $2\lfloor \frac{1}{2}n \rfloor - 1$  vertices that starts at

a  $G_1$ -neighbor of  $v$  and ends at a  $G_1$ -neighbor of  $w$ . Joining  $P$  and  $Q$  via  $v$  at one endpoint and via  $w$  on the other creates a cycle of length  $2n$  in  $G_1$ .

If we cannot find two vertices as in the previous paragraph, then the best we can do is to find, for some  $j$ , a vertex  $v \in V_3$  that S-connects  $G_j$  and another vertex  $w \in V_3$  that C-connects  $G_j$ . Since  $v$  does not C-connect  $G_j$ , it must also S-connect  $G_{3-j}$ .

There is at least one more vertex  $x \in V_3$ . By assumption, it does not S-connect  $G_{3-j}$  and neither S-connects nor C-connects  $G_j$ , so it must fold into  $G_j$  (and C-connect  $G_{3-j}$ ).

Without loss of generality, suppose that  $j = 1$  and  $x$  has a  $G_1$ -neighbor in both  $X_{11}$  and  $X_{21}$ . We add an artificial edge  $e_x$  between a pair of such neighbors of  $x$ .

As before, we can find a path  $P$  in  $G_1[X_{11}, X_{21}]$  joining a neighbor of  $v$  to a different neighbor of  $w$ ; we add the requirement that it uses the edge  $e_x$ , which is still possible by Theorem 18. We can also find a path  $Q$  in  $G_1[X_{12}, X_{22}]$  joining a neighbor of  $v$  to a different neighbor of  $w$ . Since  $v$  S-connects  $G_1$  and  $w$  C-connects  $G_1$ , one of these paths will have even length and the other will have odd length, but we can choose them to have  $2n - 3$  vertices total.

Now join the paths  $P$  and  $Q$  using the vertices  $v$  and  $w$ , then replace the artificial edge  $e_x$  by two edges to  $x$  from its endpoints. The result is a cycle of length  $2n$  in  $G_1$ .

**6.3. Finding a cycle in  $G_1$ .** In this subsection, we are considering a 2-edge-colored graph  $G$  and a partition  $W'_1 \cup W'_2$  of  $V(G)$  satisfying the following properties:

- (1)  $G$  is a complete  $s$ -partite graph with parts  $V_1, V_2, \dots, V_s$  of sizes  $n_1, n_2, \dots, n_s$ , with  $s \geq 3$  and  $n_1 + \dots + n_s \leq 4n$ .
- (2)  $(1 - \delta)n \leq |W'_2| \leq (1 + \delta)n_1$ .
- (3)  $|E(G_1[W'_1, W'_2])| \leq \delta n^2$  and  $|E(G_2[W'_1])| \leq \delta n^2$ .
- (4) If  $x \in W'_1$ , then  $d_1(x, W'_1) \geq \frac{3}{4}d(x, W_1) - \delta n$ .
- (5)  $|W'_1| \geq 2n$  and  $|W'_1 \setminus V_i| \geq n$  for all  $i$ . (This is the assumption that leads to this subsection as opposed to Section 6.4.)

We can deduce a further degree condition that holds for all vertices  $x \in W'_1$ :

- (6) By properties (1) and (2),  $|W'_1| = |V(G)| - |W'_2| \leq 4n - (1 - \delta)n = (3 + \delta)n$ , so  $d(x, W'_1) \leq (3 + \delta)n$ .  
By property (4), we have  $d_2(x, W_1) \leq \frac{1}{4}(3 + \delta)n + \delta n \leq (\frac{3}{4} + 2\delta)n$ .

To find a cycle of length  $2n$  in  $G_1$ , we will choose two disjoint sets  $X, Y \subseteq W'_1$  of size  $n$ , then apply Theorem 16 to find a Hamiltonian cycle in  $H = G_1[X, Y]$ .

Let  $a, b \in \{1, 2, \dots, s\}$  be such that  $V_a \cap W'_1$  is the largest part of  $G_1[W'_1]$  and  $V_b \cap W'_1$  is the second-largest part of  $G_1[W'_1]$ . To define  $X$  and  $Y$ , we begin by assigning  $V_a \cap W'_1$  to  $X$  and  $V_b \cap W'_1$  to  $Y$ . If either of these exceeds  $n$  vertices, we choose  $n$  of the vertices arbitrarily.

Continue by assigning the parts  $V_i \cap W'_1$  to either  $X$  or  $Y$  arbitrarily for as long as this does not make  $|X|$  or  $|Y|$  exceed  $n$ . Once this is no longer possible, then:

- If there are still at least two parts  $V_i \cap W'_1$  left unassigned, then each of them must have more than  $\max\{n - |X|, n - |Y|\}$  vertices. Therefore we can add vertices from one of them to  $X$  to make  $|X| = n$  (if necessary), and add vertices from the other to  $Y$  to make  $|Y| = n$  (if necessary).

- If there is only one part of  $G_1[W'_1]$  left unassigned, call it  $V_{\text{split}} \cap W'_1$ . We assign  $n - |X|$  vertices of  $V_{\text{split}} \cap W'_1$  to  $X$  and  $n - |Y|$  other vertices of  $V_{\text{split}} \cap W'_1$  to  $Y$ .
- If there are no parts left unassigned, then we must have  $|X| = |Y| = n$ .

We must show that we do not run out of vertices in either of the last two cases. If  $|V_a \cap W'_1| \leq n$ , then we do not run out because  $|W'_1| \geq 2n$  (by property (5)) and all vertices in  $W'_1 \setminus V_{\text{split}}$  are assigned to either  $X$  or  $Y$ , so either  $V_{\text{split}} \cap W'_1$  must contain enough vertices to fill  $X$  and  $Y$  or  $X$  and  $Y$  are already full. If  $|V_a \cap W'_1| > n$ , then we do not run out because  $|W'_1 \setminus V_a| \geq n$  (again, by property (5)), and after  $V_a \cap W'_1$  is assigned, all vertices of  $W'_1$  are added to  $Y$  until it is full.

The most difficult case for us is the one in which some part  $V_{\text{split}} \cap W'_1$  is divided between  $X$  and  $Y$ . To handle all cases at once, we assume this happens; if necessary, we choose some part  $V_i \cap W'_1$  ( $i \neq a, b$ ) to be a degenerate instance of  $V_{\text{split}}$  which is entirely in  $X$  or  $Y$ .

Let  $n_x = |V_{\text{split}} \cap X|$  and  $n_y = |V_{\text{split}} \cap Y|$ . We assigned the largest part of  $G[W'_1]$  to  $X$  and the second-largest to  $Y$ ; therefore  $X$  and  $Y$  both contain at least  $n_x + n_y$  vertices not in  $V_{\text{split}}$ . Since  $|X| = |Y| = n$ , we must have  $n_x + (n_x + n_y) \leq n$  and  $n_y + (n_x + n_y) \leq n$ ; therefore  $n_x + n_y \leq \frac{2}{3}n$ , while individually  $n_x \leq \frac{1}{2}n$  and  $n_y \leq \frac{1}{2}n$ .

We first prove some bounds on  $d_1(x, Y)$  for  $x \in X$  (and, by symmetry,  $d_1(y, X)$  for  $y \in Y$ ). If  $x \notin V_{\text{split}}$ , then  $d(x, Y) = n$  (since there are no vertices of  $Y$  in the same part of  $G$  as  $x$ ), while  $d_2(x, W'_1) \leq (\frac{3}{4} + 2\delta)n$  by property (6), so  $d_1(x, Y) \geq (\frac{1}{4} - 2\delta)n$ . If  $x \in V_{\text{split}}$ , then  $d(x, W'_1) = (n - n_x) + (n - n_y)$ , since all vertices of  $W'_1$  outside  $V_{\text{split}}$  have been assigned to either  $X$  or  $Y$ , so  $d_2(x, W'_1) \leq \frac{1}{4}(2n - n_x - n_y) + \delta n$  by property (4). This leaves  $d_1(x, Y) \geq \frac{1}{2}n - \frac{3}{4}n_y - \delta n \geq (\frac{1}{8} - \delta)n$ .

If we exclude the  $\frac{1}{10}n$  vertices of  $X$  with the most edges to  $W'_1$  in  $G_2$ , then by Lemma 19, the remaining vertices  $x \in X$  have  $d_2(x, W'_1) \leq 20\delta n$ . If  $x \notin V_{\text{split}}$ , this means  $d_1(x, Y) \geq (1 - 20\delta)n$ , and if  $x \in V_{\text{split}}$ , this means that  $d_1(x, Y) \geq n - n_y - 20\delta n$ .

Let  $H = G_1[X, Y]$ , let  $u_1, u_2, \dots, u_n$  be the vertices of  $X$  ordered so that  $d_H(u_1) \leq \dots \leq d_H(u_n)$ , and let  $v_1, v_2, \dots, v_n$  be the vertices of  $Y$  ordered so that  $d_H(v_1) \leq \dots \leq d_H(v_n)$ .

Suppose  $u_i \in X$  satisfies  $d_H(u_i) \leq i < n$ . We have shown  $d_1(x, Y) \geq (\frac{1}{8} - \delta)n$ , so among  $u_1, u_2, \dots, u_i$ , there must be a vertex not among the  $\frac{1}{10}n$  vertices of  $X$  with the most edges to  $W'_1$  in  $G_2$ . For such a vertex,  $d_1(x, Y) \geq n - n_y - 20\delta n$ , so in particular  $d_H(u_i) \geq n - n_y - 20\delta n$ , which means  $i \geq n - n_y - 20\delta n$ .

If we had  $d_H(v_{n-i}) \leq n - i$ , then by repeating this argument for vertices in  $Y$ , we would have  $d_H(v_{n-i}) \geq n - n_x - 20\delta n$ , which would mean  $n - i \geq n - n_x - 20\delta n$ . Adding this to the inequality on  $i$ , we would get  $n \geq 2n - n_x - n_y - 40\delta n$ , which is impossible since  $n_x + n_y \leq \frac{2}{3}n$ . So we must have  $d_H(v_{n-i}) \geq n - i + 1$ , and by Theorem 16,  $H$  contains a Hamiltonian cycle. This gives a cycle of length  $2n$  in  $G_1$ .

**6.4. Finding a cycle in  $G_2$ .** In this subsection, we are considering a 2-edge-colored graph  $G$  and a partition  $W'_1 \cup W'_2$  of  $V(G)$  satisfying the following properties:

- (1)  $G$  is a complete  $s$ -partite graph with parts  $V_1, V_2, \dots, V_s$  of size  $n_1, n_2, \dots, n_s$ , with  $s \geq 3$  and  $n_1 + \dots + n_s \leq 4n$ . Moreover,  $\frac{5}{3}n > n_1 \geq \dots \geq n_s$ ; we considered the case  $n_1 \geq \frac{5}{3}n$  in Section 6.2.
- (2) Either  $N - n_1 > 2n - 1$  and  $|V_i| \leq n$  for all  $i$ , or  $n_1 = n_2 \geq n$ ,  $s = 3$ , and  $N - n_1 = N - n_2 = 2n - 1$ .
- (3)  $|E(G_1[W'_1, W'_2])| \leq \delta n^2$  and  $|E(G_2[W'_1])| \leq \delta n^2$ .
- (4) If  $x \in W'_2$ , then  $d(x, W'_1) \geq \frac{1}{4}n - \delta n$ , and  $d_2(x, W'_1) \geq \frac{1}{4}d(x, W_1) - \delta n$ .

(5)  $n \leq |W'_2| \leq (1 + \delta)n_1$ . (The lower bound is the assumption that leads to this subsection as opposed to Section 6.3.)

Let Bad consist of the  $\sqrt{\delta}n$  vertices of  $W'_2$  that maximize  $d_1(x, W'_1)$ ; let  $\text{Good} = W'_2 \setminus \text{Bad}$ . By Lemma 19,  $d_1(x, W'_1) \leq \sqrt{\delta}n$  for all  $x \in \text{Good}$ .

Our strategy is to handle the vertices in Bad: first by finding short vertex-disjoint paths containing the vertices in Bad, then by combining them into a single path. Finally, we extend this path to a cycle of length  $2n$  in  $G_2[W'_1, W'_2]$ .

**6.4.1. Constructing paths containing each vertex of Bad.** For every vertex  $x \in \text{Bad}$ , we find a four-edge path  $P(x)$  in  $G_2$ , which contains  $x$ , but begins and ends at a vertex of Good. We construct these paths one at a time; for each vertex  $x$ , we must keep in mind that in each of  $W'_1$  and  $W'_2$ , up to  $2\sqrt{\delta}n$  vertices may have been used for previously chosen paths.

This is not always possible; when it is not, we find a cycle of length  $2n$  in another way.

**Lemma 20.** *One of the following holds:*

- (1)  $G_2$  contains a collection  $\{P(x) : x \in \text{Bad}\}$  of vertex-disjoint paths of length 4 such that, for all  $x \in \text{Bad}$ ,  $P(x)$  begins and ends at a vertex of Good, and also contains  $x$  and two vertices in  $W'_1$ .
- (2)  $G_2$  contains a cycle of length  $2n$ .

*Proof.* We attempt to find the collection of vertex-disjoint paths, one vertex of Bad at a time.

By property (4) at the beginning of this section, even if  $x \in \text{Bad}$ , we have  $d(x, W'_1) \geq (\frac{1}{4} - \delta)n$  and  $d_2(x, W'_1) \geq \frac{1}{4}d(x, W'_1) - \delta n$ , so  $d_2(x, W'_1) \geq (\frac{1}{16} - \frac{5}{4}\delta)n$ . There is a part  $V_i$  with  $d_2(x, W'_1 \cap V_i) \geq (\frac{1}{64} - \frac{5}{16}\delta)n$ .

First we consider the first case of property (2). That is, suppose  $N - n_1 > 2n - 1$ ; then we have  $|V_i| = n_i \leq n_1 \leq n$ , so  $|W'_2 \cap V_i| \leq (\frac{63}{64} + \frac{5}{16}\delta)n$ . But  $|W'_2| \geq n$  in total, so there must be another part  $V_j$  with  $|W'_2 \cap V_j| \geq \frac{1}{4}(\frac{1}{64} - \frac{5}{16}\delta)n$ . We can choose two vertices  $v, w \in V_j$  to use as the endpoints of  $P(x)$ : ruling out the vertices of  $V_j \cap \text{Bad}$  (at most  $\sqrt{\delta}n$ ) and previously used vertices of  $W'_2$  in  $V_j$  (at most  $2\sqrt{\delta}n$ ) we still have a number of choices linear in  $n$ .

Now we know not just the center vertex  $x$  of the path  $P(x)$  but also its two endpoints  $v$  and  $w$ . To complete  $P(x)$ , we must find a common neighbor of  $v$  and  $x$ , and another common neighbor of  $w$  and  $x$ . This is possible, since there are at least  $(\frac{1}{64} - \frac{5}{16}\delta)n$  neighbors of  $x$  in  $W'_1 \cap V_i$ ;  $v$  and  $w$  have edges in  $G_2$  to all but at most  $\sqrt{\delta}n$  of them, and we exclude at most  $2\sqrt{\delta}n$  more that have been already used.

We call the method above of choosing the collection  $\{P(x) : x \in \text{Bad}\}$  the *greedy strategy*. As we have seen, it always works in the first case of property (2); it remains to see when it works in the second case. Now, we assume that  $G$  is tripartite,  $n_1 = n_2 \geq n$ , and  $N - n_1 = N - n_2 = 2n - 1$ .

The greedy strategy continues to work if we can always choose the part  $V_j$  from which to pick the endpoints of  $P(x)$ . For this choice to always be possible, it is enough that at least two parts of  $G$  contain  $3\sqrt{\delta}n$  vertices of  $W'_2$ : both of them will have vertices outside Bad not previously chosen for any path, and one of them will not be the same as  $V_i$ .

If this does not occur, then one part  $V_a$  of  $G$  contains all but  $6\sqrt{\delta}n$  vertices of  $W'_2$ , and each of the other two parts contains fewer than  $3\sqrt{\delta}n$  vertices of  $W'_2$ . If  $V_a$  contains fewer than  $\frac{1}{20}n$  vertices of  $W'_1$ , then the greedy strategy still works: for any  $x \in \text{Bad}$ , we have  $d_2(x, W'_1) \geq (\frac{1}{16} - \frac{5}{4}\delta)n > |V_a \cap W'_1| + 2\sqrt{\delta}n$ , so we can always choose a part of  $G$  other than  $V_a$  to play the part of  $V_i$ . In this case, it does not matter

that only  $V_a$  contains many vertices of  $W'_2$ , because we only need to choose the endpoints of  $P(x)$  from vertices in  $V_a$ .

The greedy strategy fails in the remaining case: when  $V_a$  contains all but  $6\sqrt{\delta}n$  vertices of  $W'_2$  and at least  $\frac{1}{20}n$  vertices of  $W'_1$ . Then  $|V_a| > n$ , so without loss of generality,  $V_a = V_2$ . In this case, we do not try to find the paths  $P(x)$  and instead find a cycle of length  $2n$  in  $G_1$  or  $G_2$  directly.

We have a lower bound on  $n_1 = n_2 = |V_2|$ : it is  $|V_2 \cap W'_1| + |V_2 \cap W'_2| \geq (1 + \frac{1}{20} - 6\sqrt{\delta})n$ . Since  $|V_1 \cap W'_2| \leq 3\sqrt{\delta}n$ , we have  $|V_1 \cap W'_1| \geq (\frac{21}{20} - 9\sqrt{\delta})n > n$ .

Let  $Y_1$  be a subset of exactly  $n$  vertices of  $V_1 \cap W'_1$ , chosen to avoid the  $\sqrt{\delta}n$  vertices of  $V_1 \cap W'_1$  with largest degree in  $G_1[W'_1, W'_2]$  and the  $\sqrt{\delta}n$  vertices of  $V_1 \cap W'_1$  with largest degree in  $G_2[V_1 \cap W'_1, W'_1 \setminus V_1]$ . (This is possible since  $(\frac{21}{20} - 11\sqrt{\delta})n > n$  as well.) In both cases, if a vertex  $x \in Y_1$  has degree  $d$  in the corresponding graph, we get at least  $\sqrt{\delta}nd$  edges in either  $G_1[W'_1, W'_2]$  or  $G_2[W'_1]$  by looking at the vertices we deleted; therefore  $\sqrt{\delta}nd \leq \delta n^2$  and  $d \leq \sqrt{\delta}n$ .

Redistribute vertices of  $V_2 \cup V_3$  into two parts  $(X_1, X_2)$  as follows:

- All vertices of  $W'_1 \setminus V_1$ , except the  $\sqrt{\delta}n$  vertices  $v$  maximizing  $d_2(v, Y_1)$ , are put in  $X_1$ . A vertex  $v$  of this type is guaranteed to have  $d_2(v, Y_1) \leq \sqrt{\delta}n$ .
- All vertices of  $W'_2 \setminus V_1$ , except the vertices in *Bad*, are put in  $X_2$ . A vertex  $v$  of this type is guaranteed to have  $d_1(v, Y_1) \leq \sqrt{\delta}n$ .
- The remaining vertices, of which there are at most  $2\sqrt{\delta}n$ , are assigned to  $X_1$  or  $X_2$  based on their edges to  $Y_1$ . If  $d_1(v, Y_1) \geq \frac{1}{2}n$ , then  $v$  is put into  $X_1$ ; otherwise,  $d_2(v, Y_1) \geq \frac{1}{2}n$ , and  $v$  is put into  $X_2$ .

The sets  $X_1, X_2, Y_1$  satisfy the following properties. For any  $v \in X_1$  we have  $d_1(v, Y_1) \geq \frac{1}{2}n$ . For any  $v \in X_2$  we have  $d_2(v, Y_1) \geq \frac{1}{2}n$ . For any  $v \in Y_1$  we have  $d_2(v, X_1) \leq 4\sqrt{\delta}n$ , since  $d_2(v, W'_1) \leq \sqrt{\delta}n$  and  $X_1$  contains at most  $3\sqrt{\delta}n$  vertices of  $W'_2$ ; similarly, for any  $v \in Y_1$  we have  $d_1(v, X_2) \leq 4\sqrt{\delta}n$ .

Since  $|X_1| + |X_2| = |V_2 \cup V_3| = 2n - 1$ , either  $|X_1| \geq n$  or  $|X_2| \geq n$ .

If  $|X_1| \geq n$ , then we let  $X'_1$  be a subset of exactly  $n$  vertices of  $X_1$ , and find a cycle of length  $2n$  in  $H = G_1[X'_1, Y_1]$  by applying Theorem 16. The hypotheses of the theorem are satisfied by the minimum degree conditions above: for  $u \in X'_1$  we have  $d_H(u) \geq \frac{1}{2}n$ , and for  $v \in Y_1$  we have  $d_H(v) \geq (1 - 4\sqrt{\delta})n$ .

Similarly, if  $|X_2| \geq n$ , we let  $X'_2$  be a subset of exactly  $n$  vertices of  $X_2$  and find a cycle of length  $2n$  in  $H = G_2[X'_2, Y_1]$  by applying Theorem 16. The argument is the same as in the previous paragraph.  $\square$

**6.4.2. Finding a cycle using Theorem 18.** Applying Lemma 20, each of the  $\sqrt{\delta}n$  vertices  $x \in \text{Bad}$  is the center of a length-4 path  $P(x)$ . Let  $A$  be the  $2\sqrt{\delta}n$  vertices of  $W'_1$  in these paths and  $B$  be the  $3\sqrt{\delta}n$  vertices of  $W'_2$  in these paths (including the vertices in *Bad*). Additionally, let  $C$  be the set of  $\sqrt{\delta}n$  vertices of  $W'_1 \setminus A$  with the most edges to  $W'_2$  in  $G_1$ ; by Lemma 19, every  $x \in W'_1 \setminus (A \cup C)$  satisfies  $d_1(x, W'_2) \leq \sqrt{\delta}n$ .

Next, we will construct a bipartite graph  $H$  by choosing subsets  $W''_1 \subseteq W'_1 \setminus (A \cup C)$  of size  $n - 2\sqrt{\delta}n$ , and  $W''_2 \subseteq W'_2 \setminus B$  of size  $n - 3\sqrt{\delta}n$ ; the edges of  $H$  are the edges of  $G_2[W''_1 \cup A, W''_2 \cup B]$ , except that we artificially join every internal vertex of every path  $P(x)$  to every vertex on the other side of  $H$ . We will apply Theorem 18 to find a Hamiltonian cycle in  $H$  containing all  $q = 4\sqrt{\delta}n$  edges belonging to the paths  $P(x)$ , after choosing  $W''_1$  and  $W''_2$  to make sure that the hypotheses of this theorem hold.

In terms of our future choice of  $(W''_1, W''_2)$ , let  $n_{i,j} = |V_i \cap W''_j|$ . If  $u \in V_i \cap W''_1$ , then the degree of  $u$  in  $H$  is at least  $n - n_{i,2} - \sqrt{\delta}n$ :  $u$  has at most  $\sqrt{\delta}n$  edges to  $W''_2$  that are in  $G_1$ , not  $G_2$ , and its degree is

further reduced by the  $n_{i,2}$  vertices of  $W_2''$  that are also in  $V_i$ . Similarly, if  $v \in V_i \cap W_2''$ , then the degree of  $v$  in  $H$  is at least  $n - n_{i,1} - \sqrt{\delta}n$ .

Let  $n_{*,1} \geq n_{**,1}$  be the two largest values of  $n_{i,1}$  and let  $n_{*,2} \geq n_{**,2}$  be the two largest values of  $n_{i,2}$ . As in the statement of Theorem 18 let  $u_1, u_2, \dots, u_n$  be the vertices of  $W_1'' \cup A$  and let  $v_1, v_2, \dots, v_n$  be the vertices of  $W_2'' \cup B$ , ordered by degree in  $H$ .

We begin with a lemma showing that some choices of  $(W_1'', W_2'')$  are guaranteed to satisfy the conditions of Theorem 18:

**Lemma 21.** *Theorem 18 can be applied, letting us find a cycle of length  $2n$  in  $H$ , if we can choose  $W_1''$  and  $W_2''$  to satisfy the following two conditions:*

- (1) For each  $i$ , either  $n_{i,1} + n_{i,2} \leq n - 10\sqrt{\delta}n$ , or  $n_{i,1} = 0$ .
- (2) For either  $j = 1$  or  $j = 2$ , at most one value of  $n_{i,j}$  exceeds  $(\frac{1}{2} - 10\sqrt{\delta})n$ .

*Proof.* Suppose that  $u_i \in W_1'' \cup A$  and  $d(u_i) \leq i + q = i + 4\sqrt{\delta}n$ . The minimum  $H$ -degree of vertices in  $W_1'' \cup A$  is  $n - n_{*,2} - \sqrt{\delta}n$ , so we must have  $i \geq n - n_{*,2} - 5\sqrt{\delta}n$ . By condition (1), at most  $n - n_{*,2} - 10\sqrt{\delta}n$  vertices in  $W_1''$  are in the same part as the largest part of  $W_2''$ ; at most  $2\sqrt{\delta}n$  vertices are endpoints of paths  $P(x)$ , so together these make up at most  $n - n_{*,2} - 8\sqrt{\delta}n < i$  vertices. Therefore some of the vertices  $u_1, \dots, u_i$  are vertices of  $W_1''$  in a different part, and therefore  $d(u_i) \geq n - n_{**,2} - \sqrt{\delta}n$ .

Similarly, suppose that  $v_j \in W_2'' \cup B$  and  $d(v_j) \leq j + q \leq j + 4\sqrt{\delta}n$ . The minimum  $H$ -degree of vertices in  $W_2'' \cup B$  is  $n - n_{*,1} - \sqrt{\delta}n$ , so we must have  $j \geq n - n_{*,1} - 5\sqrt{\delta}n$ . By condition (1), at most  $n - n_{*,1} - 10\sqrt{\delta}n + |B|$  vertices in  $W_2''$  are in the same part as the largest part of  $W_1''$ , which is fewer than  $j$ . Therefore some of the vertices  $v_1, \dots, v_j$  are vertices of  $W_2''$  in a different part, and hence  $d(v_j) \geq n - n_{**,1} - \sqrt{\delta}n$ .

In such a case, we have  $d(u_i) + d(v_j) \geq 2n - n_{**,1} - n_{**,2} - 2\sqrt{\delta}n$ . We have  $n_{**,1}, n_{**,2} \leq \frac{1}{2}n$ , and additionally by condition (2),  $n_{**,j} \leq \frac{1}{2}n - 10\sqrt{\delta}n$  for some  $j$ . Therefore  $d(u_i) + d(v_j) \geq n + 8\sqrt{\delta}n \geq n + 4\sqrt{\delta}n + 1$ , and the hypothesis of Theorem 18 holds.  $\square$

It remains to choose  $W_1''$  and  $W_2''$  so that they satisfy the conditions of Lemma 21, or to deal separately with the cases where this is impossible.

First, we consider the case in which all parts of  $G$  have size at most  $\frac{5}{4}n$ . (By property (2), this automatically holds when  $G$  has more than three parts: if so, all parts of  $G$  have size at most  $n$ .) Choose  $W_2''$  arbitrarily.  $W_1''$  must contain at least  $N - (1 + \delta)n_1 \geq N - n_1 - \delta n_1 \geq 2n - 1 - 2\delta n$  vertices, of which only  $2\sqrt{\delta}n$  vertices have been used by paths and  $\sqrt{\delta}n$  more have been thrown away as  $C$ ; therefore we have at least  $2n - 1 - 3\sqrt{\delta}n - 2\delta n$  choices for vertices in  $W_1''$ .

We set aside vertices of  $W_1''$  which we forbid from being in  $W_1''$ . From each part,  $V_i$ , forbid either at least  $|V_i| - (1 - 10\sqrt{\delta})n$  vertices, or else all vertices of  $V_i \cap W_1''$ , whichever is smaller. This forbids at most  $(\frac{1}{4} + 10\sqrt{\delta})n$  vertices from each part, and at most  $10\sqrt{\delta}n$  vertices in the case  $n_i \leq n$ . There are at most two parts with  $n_i > n$ , so we forbid at most  $(\frac{1}{2} + 50\sqrt{\delta})n$  vertices. Now condition (1) of Lemma 21 will be satisfied no matter what: for each part  $i$ , we will either have  $n_{i,1} + n_{i,2} \leq (1 - 10\sqrt{\delta})n$ , or else  $n_{i,1} = 0$ .

Next, we attempt to ensure that condition (2) of Lemma 21 holds. Call a part  $V_i$  of  $G$   $W_1''$ -rich if, after excluding the forbidden vertices, and vertices of  $A \cup C$ , there are still at least  $20\sqrt{\delta}n$  vertices of  $W_1''$  left in  $V_i$ ; call it  $W_1''$ -poor otherwise.

If there are at least three  $W_1''$ -rich parts, then we can choose  $20\sqrt{\delta}n$  vertices from each of them for  $W_1''$ , and complete the choice of  $W_1''$  arbitrarily. Condition (2) of Lemma 21 must now hold for  $j = 1$ : if we had  $n_{*,1} \geq (\frac{1}{2} - 10\sqrt{\delta})n$  and  $n_{**,1} \geq (\frac{1}{2} - 10\sqrt{\delta})n$ , then together these two parts would contain all but  $20\sqrt{\delta}n$  vertices of  $W_1''$ . This is impossible, since there is a third  $W_1''$ -rich part containing at least that many vertices of  $W_1''$ .

If there are not at least three  $W_1''$ -rich parts, we give up on Lemma 21, and satisfy the conditions of Theorem 18 by a different strategy.

If  $V_i$  is  $W_1''$ -poor, it must have many vertices of  $W_2''$ . More precisely,  $V_i$  has at least  $\min\{n, n_i\} - 10\sqrt{\delta}n$  vertices that we have not forbidden. Among these, there are up to  $3\sqrt{\delta}n$  vertices which are in  $A \cup C$ , up to  $3\sqrt{\delta}n$  vertices which are in  $B$ , and fewer than  $20\sqrt{\delta}n$  vertices that can be added to  $W_1''$ , so the remaining  $\min\{n, n_i\} - 36\sqrt{\delta}n$  vertices must be in  $W_2' \setminus B$ .

Moreover, when  $G$  is tripartite,  $n_i \geq \frac{3}{4}n - 1$  for any part, so if a part is  $W_1''$ -poor, it contains at least  $\frac{3}{4}n - 36\sqrt{\delta}n - 1$  vertices of  $W_2' \setminus B$ . When  $G$  has more than three parts, at least two parts must be  $W_1''$ -poor; any two parts  $V_i, V_j$  have  $n_i + n_j > n$ , so together, two  $W_1''$ -poor parts have at least  $n - 72\sqrt{\delta}n$  vertices of  $W_2' \setminus B$ . In either case, there are one or two  $W_1''$ -poor parts which together contain at least  $\frac{2}{3}n$  vertices of  $W_2' \setminus B$ .

We change our choice of  $W_2''$ , if necessary, to include at least  $\frac{2}{3}n$  vertices from this  $W_1''$ -poor part or parts; otherwise, the choice is still arbitrary. Meanwhile, we choose no vertices from these parts from  $W_1''$ ; this rules out at most  $40\sqrt{\delta}n$  vertices in addition to our previous restrictions. Completing the choice of  $W_1''$  arbitrarily, we are left with a pair  $(W_1'', W_2'')$  that satisfies condition (1) of Lemma 21, but possibly not condition (2).

From condition (1), we know that if  $v_j \in W_2''$  satisfies  $d(v_j) \leq j + q$ , we have  $d(v_j) \geq n - n_{**,2} - \sqrt{\delta}n \geq \frac{1}{2}n - \sqrt{\delta}n$ . Additionally, we know that for any  $u_i \in W_1''$ ,  $d(u_i) \geq \frac{2}{3}n - \sqrt{\delta}n$ , since there are at least  $\frac{2}{3}n$  vertices of  $W_2''$  in a different part of  $G$ . Then  $d(u_i) + d(v_j) \geq \frac{7}{6}n - 2\sqrt{\delta}n \geq n + q + 1$ , satisfying the hypothesis of Theorem 18.

*Next, we consider the case where  $G$  has at most three parts and  $n_1 > \frac{5}{4}n$ .* By (9),  $N > 3n - 1$ . Hence by (8) we know that  $n_1 = n_2$  and  $N - n_1 = 2n - 1$ . The case of  $n_1 \geq \frac{5}{3}n$  was handled in Section 6.2. Thus, we may assume  $n_1 < \frac{5}{3}n$ , so  $n_3 = (2n - 1) - n_2 > \frac{1}{3}n - 1$ .

Assume first that one of  $W_1' \setminus (A \cup C)$  or  $W_2' \setminus B$  intersects each part of  $G$  in at least  $20\sqrt{\delta}n$  vertices, and the other has at least  $30\sqrt{\delta}n$  vertices outside each part of  $G$ ; we will consider departures from this assumption later. This implies that for  $j = 1$  or  $j = 2$ , we can choose  $20\sqrt{\delta}n$  vertices from each part to add to  $W_j''$ , and match these by choosing  $60\sqrt{\delta}n$  vertices to add to  $W_{3-j}''$  with no more than  $30\sqrt{\delta}n$  of these from one part. (No  $V_i$  has more than  $50\sqrt{\delta}n$  vertices chosen from it at this point.)

Then proceed by an iterative strategy. At each step, choose one vertex from  $W_1' \setminus (A \cup C)$  not previously added to  $W_1''$ , and a vertex from  $W_2' \setminus B$  not previously added to  $W_2''$ , so that these vertices are in different parts of  $G$ . Then add them to  $W_1''$  and  $W_2''$  respectively. This step is always possible when  $|W_1'' \cup A|, |W_2'' \cup B| < n$ : in this case, at least two parts still have unchosen vertices, since  $|V_1|, |V_2| \geq \frac{5}{4}n$  but fewer than  $n$  vertices have been chosen. Additionally, choosing a pair of vertices, one from  $W_1'$  and

one from  $W'_2$ , is only impossible if  $W'_2 \setminus B$  has no more vertices, in which case  $W''_2$  has reached its desired size.

Stop when  $|W''_2 \cup B| = n$ . When this happens,  $W''_1$  still needs  $\sqrt{\delta n}$  more vertices, and these can be chosen arbitrarily.

This process guarantees that conditions (1) and (2) of Lemma 21 hold. Before we begin iterating, we have chosen  $60\sqrt{\delta n}$  vertices, but at most  $50\sqrt{\delta n}$  from each part. After we begin iterating, we add at most one vertex from each part at each step. Therefore in the end,  $n_{i,1} + n_{i,2} \leq n - 10\sqrt{\delta n}$  for each  $i$ , satisfying condition (1). Moreover, for some  $j$ , we added at least  $20\sqrt{\delta n}$  vertices from each part to  $W''_j$ , ensuring that at most one value of  $n_{i,j}$  can exceed  $(\frac{1}{2} - 10\sqrt{\delta})n$  and satisfying condition (2).

Now we consider alternatives to our initial assumptions in this case. We cannot have  $W'_1 \setminus (A \cup C)$  have fewer than  $30\sqrt{\delta n}$  vertices outside  $V_i$  for any  $i$ , since it contains at least  $2n - 1 - 4\sqrt{\delta n} - 2\delta n$  vertices, and no  $V_i$  is larger than  $\frac{5}{3}n$ . But it is possible that one of  $V_1$  or  $V_2$  contains all but  $30\sqrt{\delta n}$  vertices of  $W'_2 \setminus B$ ; without loss of generality, it is  $V_1$ .

In this case, if  $|V_1 \cap W'_2 \setminus B| > n$ , then let  $W''_2$  be any  $n$ -element subset of  $V_1 \cap W'_2 \setminus B$ ; otherwise, let  $W''_2$  be any  $n$ -element subset of  $W'_2 \setminus B$  containing  $V_1 \cap W'_2 \setminus B$ . The set  $V_2 \cup V_3$  has  $2n - 1$  vertices, at most  $30\sqrt{\delta n} + |B| = 33\sqrt{\delta n}$  of which are in  $W'_2$ , so we can pick all  $n$  vertices of  $W''_1$  from  $V_2 \cup V_3$ . Choose at least  $10\sqrt{\delta n}$  of them from  $V_3$  to satisfy condition (1) of Lemma 21 for  $i = 2$ . Condition (1) also holds for  $i = 1$  (since  $n_{i,1} = 0$ ) and  $i = 3$  (since  $n_3 < \frac{3}{4}n$ ); condition (2) holds for  $j = 2$ .

Finally, we also violate the assumptions at the beginning of this case when neither  $W'_1 \setminus (A \cup C)$  nor  $W'_2 \setminus B$  have at least  $20\sqrt{\delta n}$  vertices from each part of  $G$ . It is impossible that both of them have at most  $20\sqrt{\delta n}$  vertices from  $V_3$ , so one of them has at most  $20\sqrt{\delta n}$  vertices from one of  $V_1$  or  $V_2$ .

If one of them (without loss of generality,  $V_1$ ) contains at most  $20\sqrt{\delta n}$  vertices of  $W'_1 \setminus (A \cup C)$ , it must have at least  $n$  vertices of  $W'_2 \setminus B$ , since  $|V_1| \geq \frac{5}{4}n$ , so choose all remaining vertices out of  $W'_2$  from there. Outside  $V_1$ , we have at least  $(2n - 1 - 4\sqrt{\delta n} - 2\delta n) - 20\sqrt{\delta n}$  vertices of  $W'_1 \setminus (A \cup C)$ , which leaves at most  $24\sqrt{\delta n} + 2\delta n$  vertices we *cannot* choose for  $W''_1$ . Choose  $n$  vertices outside  $V_1$  for  $W''_1$ , including at least  $10\sqrt{\delta n}$  vertices of  $V_3$ . This satisfies condition (1) for  $i = 1$  (since  $n_{i,1} = 0$ ),  $i = 2$  (since  $n_{i,1} = 0$  and  $n_{i,2} < n - 10\sqrt{\delta n}$ ), and  $i = 3$  (since  $n_3 < \frac{3}{4}n$ ); condition (2) holds for  $j = 2$ .

If one of  $V_1$  or  $V_2$  (without loss of generality,  $V_1$ ) contains at most  $20\sqrt{\delta n}$  vertices of  $W'_2 \setminus B$ , choose  $n - 30\sqrt{\delta n}$  vertices of  $W''_1$  from  $V_1$  (satisfying condition (1) for  $i = 1$  and condition (2) by taking  $j = 1$ ). If  $V_3$  contains at least  $30\sqrt{\delta n}$  vertices of  $W'_1 \setminus (A \cup C)$ , take the remaining vertices of  $W''_1$  from  $W_3$ . Otherwise,  $V_3$  contains at least  $60\sqrt{\delta n}$  vertices of  $W'_2 \setminus B$ ; choosing as many vertices as possible from  $V_1 \cup V_3$  to add to  $W''_2$ , and the remaining vertices of  $W''_1$  arbitrarily, we end up choosing no more than  $n - 10\sqrt{\delta n}$  vertices from  $V_2$ . So condition (1) holds for  $i = 2$  either because  $n_{i,1} = 0$  or because  $n_{i,1} + n_{i,2} \leq n - 10\sqrt{\delta n}$ ; condition (1) holds for  $i = 3$  because  $n_3 < \frac{3}{4}n$ .

## 7. Dealing with $(\lambda, i, 2)$ -bad partitions when $N - n_1 - n_2 \geq 3$

A *cherry* is a path on three vertices. The *center* of a cherry is the vertex with degree 2.

Suppose  $N - n_1 - n_2 \geq 3$ . By (8)–(10), we have two cases:

- (1)  $N > 3n - 1$ ,  $s = 3$ ,  $n_2 + n_3 = 2n - 1$  and  $n_1 = n_2$  (i.e., (8) holds), or
- (2)  $N = 3n - 1$ ,  $n_1 \leq n$ ,  $s \leq 5$ , and if  $s \geq 4$ , then  $n_{s-1} + n_s \geq n + 1$  (i.e., (9) holds).

**7.1. The case when (8) holds.** By (8),  $n_1 = n_2 > n$ ,  $s = 3$ , and  $0 < n_3 = 2n - 1 - n_2 < n$ .

**Lemma 22.** *Let  $G = K_{n_1, n_2, n_3}$  with  $n_1 = n_2$  and  $n_2 + n_3 = 2n - 1$  be 2-edge-colored with a  $(\lambda, i, 2)$ -bad partition. Then  $G$  has a monochromatic cycle of length  $2n$ .*

In this section, we prove Lemma 22, but postpone technical details of how the monochromatic cycles are constructed in each of four cases; these details are given in Claims 23–26.

*Proof of Lemma 22.* Without loss of generality, let  $i = 2$ ; we call color 1 red, color 2 blue, and use  $d_1$  ( $d_2$ ) to denote the red (blue) degree.

We begin by assuming that in the  $(\lambda, 2, 2)$ -bad partition  $(V_j, U_1, U_2)$ ,  $j = 3$ . Later, in Section 7.1.5, we discuss the modifications to the proof when  $j \neq 3$ .

Since  $(V_j, U_1, U_2)$  is a 2-bad partition, we know the following conditions hold:

- (i)  $|V_3| \geq (1 - \lambda)n$ .
- (ii)  $(1 - \lambda)n \leq |U_1| \leq (1 + \lambda)n$ .
- (iii)  $(1 - \lambda)n \leq |U_2| \leq (1 + \lambda)n$ .
- (iv)  $E(G_2[V_3, U_1]) \leq \lambda n^2$ .
- (v)  $E(G_1[V_3, U_2]) \leq \lambda n^2$ .

If a vertex  $u_1$  in  $U_1$  has blue degree at least  $\frac{1}{2}n_3$  to  $V_3$  then we move  $u_1$  to  $U_2$ . If a vertex  $u_2$  in  $U_2$  has red degree at least  $\frac{1}{2}n_3$  to  $V_3$  then we move  $u_2$  to  $U_1$ . Since there are at most  $3\lambda n$  vertices in  $U_1$  with blue degree at least  $\frac{1}{2}n_3$  to  $V_3$  and there are at most  $3\lambda n$  vertices in  $U_2$  with red degree at least  $\frac{1}{2}n_3$  to  $V_3$ , we moved at most  $3\lambda n$  vertices out of  $U_1$  and  $U_2$  respectively and moved at most  $3\lambda n$  vertices into  $U_1$  and  $U_2$  respectively. Thus, we may assume  $|U_1| \geq |U_2|$ ,  $|U_1| = n + a_1$ ,  $|U_2| = n + a_2$ , and  $a_1 \geq 0$ .

Note that (iv) and (v) change to:

- (iv)  $|E(G_2[V_3, U_1])| \leq 4\lambda n^2$ .
- (v)  $|E(G_1[V_3, U_2])| \leq 4\lambda n^2$ .

Let  $|V_3| = n - a_3$ , where  $a_3 \leq 10\lambda n$ . Let  $B$  be the set of vertices in  $V_3$  with blue degree at least  $0.9n$  to  $U_1$  and  $|B| = b$ . Let  $R$  be the set of vertices in  $V_3$  with blue degree at most  $0.05n$  to  $U_1$ . By condition (iv), we know

$$|B| \leq 5\lambda n \quad \text{and} \quad |R| \geq n - a_3 - 80\lambda n.$$

Let  $C$  be a maximum collection of vertex-disjoint red cherries with center in  $U_2$  and leaves in  $U_1$ . If there are at least  $m := a_3 + b$  cherries in  $C$ , then we use them, together with the edges between  $U_1$  and  $V_3$ , to find a red cycle of length  $2n$ ; this is done in Claim 23.

Otherwise, we assume that  $|C| \leq m - 1$ : there are at most  $m - 1$  red cherries from  $U_2$  to  $U_1$ . Every vertex in  $U_2 - V(C)$  has red degree at most  $2m - 1$  to  $U_1$ , since otherwise we have a larger collection of red cherries.

When  $|U_2| = n + a_2 \geq n - b$ , we can find a blue cycle using edges between  $U_2$  and  $V_3$ , as well as enough edges between  $U_1$  and  $B$  to make up for the size of  $U_2$  when  $|U_2| < n$ . This is done in Claim 24.

Otherwise, we assume that  $|U_2| \leq n - b - 1$ ; in other words,

$$a_2 \leq -(b + 1). \tag{15}$$

Our goal is now to use edges within  $U_1$  to find a monochromatic cycle. Without loss of generality, we may assume that  $|U_1 \cap V_1| \geq |U_1 \cap V_2|$ . We first argue that  $U_1 \cap V_2$  cannot be too small.

Earlier, we defined  $|U_1| = n + a_1$ ,  $|U_2| = n + a_2$ ,  $|V_3| = n - a_3$ . Since  $|V_1| + |V_3| = |V_2| + |V_3| = 2n - 1$  and  $U_1 \cup U_2 = V_1 \cup V_2$ , we have

$$2n + a_1 + a_2 = |V_1| + |V_2| = 4n - 2 - 2|V_3| = 2n + 2a_3 - 2$$

or

$$a_1 + a_2 = 2a_3 - 2. \quad (16)$$

Therefore

$$\begin{aligned} |U_1 \cap V_2| &\geq |U_1| - |V_1| = |U_1| - \frac{1}{2}(|U_1| + |U_2|) = n + a_1 - n - \frac{1}{2}(a_1 + a_2) \\ &= \frac{1}{2}(a_1 - a_2) = a_3 - a_2 - 1 = (b + a_3) + (-b - a_2) - 1. \end{aligned}$$

There are two possibilities for the vertices of  $U_1 \cap V_2$ :

- There are at least  $m = b + a_3$  vertices in  $U_1 \cap V_2$  which have red degree at least  $0.1n$  to  $U_1 \cap V_1$ . In this case, we use Claim 25 to find a red cycle of length exactly  $2n$ .
- There are at least  $m' := -b - a_2$  vertices in  $U_1 \cap V_2$  which have blue degree at least  $|U_1 \cap V_1| - 0.1n \geq 0.4n$  to  $U_1 \cap V_1$ . In this case, we use Claim 26 to find a blue cycle of length exactly  $2n$ .

One of these must hold, since  $|U_1 \cap V_2| \geq m + m' - 1$ , while by (15),  $m' = -b - a_2 \geq 1$ : therefore there are either  $m$  vertices for Claim 25 or  $m'$  vertices for Claim 26. In either case, we obtain a monochromatic cycle of length exactly  $2n$ , completing the proof.  $\square$

**7.1.1. The case of many cherries:**  $|C| \geq m$ . Recall that  $C$  is a maximum collection of vertex-disjoint red cherries with centers in  $U_2$  and leaves in  $U_1$ ;  $m = b + a_3$ , where  $b = |B|$  and  $a_3 = n - |V_3|$ .

**Claim 23.** *If  $|C| \geq m$ , then we have a red cycle of length exactly  $2n$ .*

*Proof.* We do the following steps. Let  $C' \subseteq C$  be a collection of  $m$  red cherries with centers in  $U_2$  and leaves in  $U_1$ . Let  $\{u_1, \dots, u_m\} = V(C') \cap U_2$  and  $\{v_1, \dots, v_{2m}\} = V(C') \cap U_1$  such that each  $v_{2i-1}u_iv_{2i}$  is a cherry with center  $u_i$ , where  $1 \leq i \leq m$ .

To find a cycle of length  $2n$  in  $G_1$  that contains the edges of  $C'$ , we will apply Theorem 18 to an appropriately chosen bipartite graph.

First, create an auxiliary graph  $G'_1$  by starting with  $G_1$  and adding every edge between  $\{u_1, \dots, u_m\}$  and  $U_1$ . This will help us to satisfy the degree conditions of Theorem 18; however, these artificial edges will never be used by a cycle containing all the edges of  $C'$ , since each of  $\{u_1, \dots, u_m\}$  already has degree 2 in  $C'$ .

Second, let  $X = (V_3 - B) \cup \{u_1, u_2, \dots, u_m\}$  (a set of  $n$  vertices total) and let  $Y \subseteq U_1$  be any set of size  $n$  such that  $\{v_1, \dots, v_{2m}\} \subseteq Y$ . We check that the hypotheses of Theorem 18 apply to  $G'_1[X, Y]$ .

Order vertices in  $X$  and  $Y$  separately by their degree from smallest to largest. Since vertices in  $Y$  have red degree at least  $0.04n$  to  $X$ , the smallest index  $k$  such that  $d_1(y_k) \leq k + q$  satisfies  $d_1(y_k) \geq 0.95n$ . Since vertices in  $X$  have blue degree at most  $0.9n$  to  $U_1$ , they have red degree at least  $n - 0.9n = 0.1n \gg 0.09n$  to  $Y$ . The smallest index  $j$  such that  $d_1(x_j) \leq j + q$  satisfies  $d_1(x_j) \geq 0.09n$ . By Theorem 18 and  $0.09n + 0.95n \gg n + q + 1$ , we can find a Hamiltonian cycle in  $G'_1[X, Y]$  of length  $2n$  containing the edges of  $C'$ , which is a cycle of length  $2n$  in  $G_1$ .  $\square$

**7.1.2.** *The case of large  $U_2$ :  $|U_2| \geq n - b$ .* Recall that  $|U_2| = n + a_2$ ,  $B$  is the set of vertices in  $V_3$  with blue degree at least  $0.9n$  to  $U_1$ , and  $b = |B|$ .

**Claim 24.** *If  $b \geq -a_2$  (in other words, if  $|U_2| = n + a_2 \geq n - b$ ), then we have a blue cycle of size exactly  $2n$ .*

*Proof.* Let  $c := |C|$ ; let  $V(C) \cap U_2 = \{u_1, \dots, u_c\}$  and  $V(C) \cap U_1 = \{v_1, v_2, \dots, v_{2c}\}$ . Let  $B_2$  be the collection of vertices in  $V_3 - B$  with red degree at most  $0.1n$  to  $U_2$ . By condition (v),

$$q := |B_2| \geq n - a_3 - 40\lambda n - b.$$

Since  $2n_1 = |U_1| + |U_2| = 2n + a_1 + a_2$ , we know

$$|U_2 \cap V_2| = n_1 - |U_1 \cap V_2| \geq n_1 - \frac{1}{2}(n + a_1) = n + \frac{1}{2}(a_1 + a_2) - \frac{1}{2}n - \frac{1}{2}a_1 = \frac{1}{2}(n + a_2)$$

and thus

$$|U_2 \cap V_1| \leq n + a_2 - \frac{1}{2}(n + a_2) = \frac{1}{2}(n + a_2). \quad (17)$$

**Step 1:** We first find a path to include  $0.8n$  vertices in  $V_3$  and  $0.8n$  vertices in  $U_2$  (all of  $U_2 \cap V_1$  and  $V(C)$ ) by Theorem 17.

**Details:** Since  $|B_2| \geq n - a_3 - 40\lambda n - b$ , we take a set  $X \subseteq B_2$  such that  $|X| = 0.8n$ . By (17), we can take a set  $Y \subseteq U_2$  such that  $U_2 \cap V_1 \subseteq Y$ ,  $V(C) \cap U_2 \subset Y$ , and  $|Y| = 0.8n$ .

Now we consider  $G_2[X, Y]$  and we order vertices in  $X$  and  $Y$  separately by their degree from smallest to largest. Since vertices in  $Y$  have blue degree at least  $0.8n - \frac{1}{2}n_3 > 0.2n$  to  $X$ , the smallest index  $k$  such that  $d_2(y_k) \leq k + 1$  satisfies  $d_2(y_k) \geq 0.2n$ . Since vertices in  $X$  have red degree at most  $0.1n$  to  $U_2$ , they have blue degree at least  $0.8n - 0.1n = 0.7n$  to  $Y$ . The smallest index  $j$  such that  $d_2(x_j) \leq j + 1$  satisfies  $d_2(x_j) \geq 0.7n$ . By Theorem 17 and  $0.7n + 0.2n > 0.8n + 2$ , we can find a Hamiltonian red path  $P'_1$  from  $x \in X$  to some vertex  $y \in Y - V_1 - V(C)$  in  $G_2[X, Y]$  of length  $1.6n - 1$ .

Since  $x \in X \subseteq B_2$ ,

$$d_2(x, U_2 - Y) \geq n + a_2 - 0.8n - 0.1n > 0.05n.$$

We extend the path  $P'_1$  to  $P_1$  of length  $1.6n$  by adding a blue edge  $xy'$  such that  $y' \in U_2 - Y$ .

**Step 2:** Use  $\min\{0, -a_2\}$  vertices in  $B$  to obtain a blue path. (We can skip this step if  $a_2 \geq 0$ .)

**Details:** Assume  $a_2 < 0$ ; since  $b \geq -a_2$ , let  $Z := \{z_1, \dots, z_{|a_2|}\} \subseteq B$ .

Since

$$|U_1 \cap V_1| \geq \frac{1}{2}(n + a_1) \geq |U_1 \cap V_2|,$$

each vertex in  $B$  has blue degree at least  $0.9n - |U_1 \cap V_2|$  to  $U_1 \cap V_1$ . Therefore,

$$0.9n - |U_1 \cap V_2| \geq 0.9n - (n + a_1 - |U_1 \cap V_1|) = |U_1 \cap V_1| - a_1 - 0.1n \geq \frac{3}{4}|U_1 \cap V_1|.$$

We can find for each pair  $(z_i, z_{i+1})$  a common neighbor  $r_i \in U_1 \cap V_1 - V(C)$ , where  $1 \leq i \leq |a_2| - 1$ , a blue neighbor  $r_0$  of  $z_1$ , and a blue neighbor  $r_{|a_2|}$  of  $z_{|a_2|}$  such that  $r_0, \dots, r_{|a_2|}$  are all distinct.

We obtain a blue path

$$P_2 = r_0 z_1 r_1 \cdots z_i r_i \cdots z_{|a_2|} r_{|a_2|}$$

of length  $2|a_2|$ .

Since  $y'$  has at most one red neighbor to  $U_1 - V(C)$ , at least one of  $\{r_0, r_{|a_2|}\}$  is a blue neighbor of  $y'$ . We may assume  $r_{|a_2|}y'$  is blue.

**Step 3:** Include the rest of vertices in  $U_2$  to  $U_1$ .

**Details:** We proceed differently depending on whether  $a_2 < 0$  or  $a_2 \geq 0$ .

- If  $a_2 < 0$  then we do the following. Let  $K := (U_2 - Y - \{y'\}) \cup \{y\} = \{y, f_1, \dots, f_{k-1}\}$ . Note that  $k = |K| = n + a_2 - 0.8n = 0.2n + a_2$  and  $K \subseteq U_2 \cap V_2 - V(C)$ . Since each vertex in  $K$  has at most one red neighbor to  $U_1 - V_2 - V(C) - \{r_0, r_1, \dots, r_{|a_2|}\}$ , we find for  $(y, f_1)$  a blue common neighbor  $h_0 \in U_1 - V_2 - V(C) - \{r_0, r_1, \dots, r_{|a_2|}\}$  and each pair  $(f_i, f_{i+1})$  a distinct blue common neighbor,  $h_i$ , in  $U_1 - V_2 - V(C) - \{r_0, r_1, \dots, r_{|a_2|}\}$ , where  $1 \leq i \leq k - 2$ . We obtain a blue path

$$P_3 = yh_0f_1 \cdots f_ih_if_{i+1} \cdots f_{k-1}$$

of length  $2k - 2 = 0.4n + 2a_2 - 2$ .

We may assume  $f_{k-1}r_0$  is blue since  $f_{k-1}$  has only one red neighbor to  $U_1 \cap V_1 - V(C)$  and there are many choices when we choose  $r_0$  to connect with  $z_1$ .

Finally, we connect  $P_2$  and  $P_1$  by adding the edge  $r_{|a_2|}y'$ , glue the paths  $P_1$  and  $P_3$  at  $y$ , then add the edge  $f_{k-1}r_0$  to complete a blue cycle of length exactly

$$2|a_2| + 1 + 1.6n + 0.4n + 2a_2 - 2 + 1 = 2n.$$

- If  $a_2 \geq 0$  then in the previous argument we take  $K = \{y, y', f_1, \dots, f_{k-2}\}$  of size  $0.2n + 1$  and find common neighbors  $h_0$  for  $(y, f_1)$ ,  $h_i$  for  $(f_i, f_{i+1})$ , where  $1 \leq i \leq k - 3$ , and  $h_{k-2}$  for  $(f_{k-2}, y')$ .

In either case, we obtain a path

$$P_3 = yh_0f_1 \cdots f_ih_if_{i+1} \cdots f_{k-2}h_{k-2}y'$$

of length  $2k - 2 = 0.4n$ . We glue  $P_1$  and  $P_3$  at  $y$  and  $y'$  to obtain a blue cycle of length exactly  $1.6n + 0.4n = 2n$ .  $\square$

**7.1.3. Handling many vertices in  $U_1 \cap V_2$  incident to red edges.** We will find a red cycle. Note that the size of  $U_1 \cap V_2$  is at least  $n + a_1 - n_1$ .

**Claim 25.** *If there are at least  $m = b + a_3$  vertices in  $U_1 \cap V_2$  of red degree at least  $0.1n$  to  $U_1 \cap V_1$ , then we have a red cycle of length exactly  $2n$ .*

*Proof.* Let  $B'$  be the collection of vertices in  $U_1$  with blue degree at least  $0.05n$  to  $V_3$ . By (iv), we have

$$|B'| \leq 80\lambda n.$$

**Step 1:** We first find a collection of red cherries  $C_3$  with center in  $U_1 \cap V_2$  and leaves in  $U_1 \cap V_1 - B'$  of size  $b + a_3 =: m$ .

**Details:** Since there are at least  $m$  vertices in  $U_1 \cap V_2$  of red degree at least  $0.1n$  to  $U_1 \cap V_1$  and  $0.1n - 80\lambda n \gg 2m$ , we can find a collection of red cherries  $C_3$  with centers in  $U_1 \cap V_2$  and leaves in  $U_1 \cap V_1 - B'$  of size  $m$ . Let  $V(C_3) \cap V_2 = \{u_1, \dots, u_m\}$  and  $V(C_3) \cap V_1 = \{v_1, \dots, v_{2m}\}$ .

Recall that  $R \subseteq V_3$  is the collection of vertices in  $V_3$  with blue degree at most  $0.05n$  to  $U_1$ .

**Step 2:** Then by Hall's theorem we find a matching  $M$  for  $V(C_3) \cap V_1$  to  $R$  and then find a common neighbor back to connect those vertices.

**Details:** Since  $\{v_2, \dots, v_{2m}\} \cap B' = \emptyset$ , each of them has red degree at least  $n - a_3 - 0.05n - 80\lambda n > 0.9n$  to  $R$ . Thus, we can find a matching  $M$  for  $\{v_2, \dots, v_{2m}\}$  such that  $V(M) \cap V_3 = \{w_2, \dots, w_{2m}\}$  and each  $v_i w_i$  is a matching edge, where  $2 \leq i \leq 2m$ .

Since  $V(M) \cap V_3 \subseteq R$ , we can find for each pair  $(w_{2i}, w_{2i+1})$  a common red neighbor  $g_i \in U_1$ , where  $1 \leq i \leq m - 1$ .

Therefore, we obtained a path

$$P_1 = v_1 u_1 v_2 w_2 g_1 w_3 v_3 u_2 v_4 w_4 \cdots v_{2m-1} u_m v_{2m} w_{2m}$$

of length  $6m - 3$ .

**Step 3:** We use Theorem 17 to get a path saturating all vertices left in  $V_3 - B - V(M)$ .

**Details:** Let  $X = V_3 - B - \{w_2, \dots, w_{2m-1}\}$  and we know

$$|X| = n - a_3 - b - (2m - 2) = n - 3m + 2.$$

Choose  $Y \subseteq U_1 - \{u_1, \dots, u_m\} - \{v_2, \dots, v_{2m}\} - \{g_1, \dots, g_{m-1}\}$  such that  $v_1 \in Y$ . By (16),

$$a_1 = -a_2 + 2a_3 - 2 \geq b + 1 + a_3 + a_3 - 2 = m + a_3 - 1 \geq m \quad (18)$$

and thus

$$n + a_1 - m - (2m - 1) - (m - 1) \geq n - 3m + 2.$$

Hence we can require  $|Y| = n - 3m + 2$ .

Now we consider  $G_1[X, Y]$  and we order vertices in  $X$  and  $Y$  separately by their degree from smallest to largest. Since vertices in  $U_1$  have red degree at least  $\frac{1}{2}n_3$  to  $V_3$ , they have red degree at least  $\frac{1}{2}n_3 - b - (2m - 2) > 0.4n$  to  $X$ .

By condition (iv), there are at most  $80\lambda n$  vertices in  $U_1$  with blue degree at least  $0.05n$  to  $V_3$ . Thus, at least  $|Y| - 80\lambda n$  vertices in  $Y$  have red degree at least  $|X| - 0.05n > 0.94n$  to  $X$ , the smallest index  $k$  such that  $d_1(y_k, X) \leq k + 1$  satisfies  $d_1(y_k, X) \geq 0.94n - 1$ . Since vertices in  $X$  have blue degree at most  $0.9n$  to  $U_1$ , they have red degree at least  $n + a_1 - m - (2m - 1) - (m - 1) - 0.9n > 0.09n$  to  $Y$ . The smallest index  $j$  such that  $d_1(x_j, Y) \leq j + 1$  satisfies  $d_1(x_j, Y) \geq 0.09n$ . By Theorem 17 and  $0.09n + 0.94n \gg n + 2$ , we can find a Hamiltonian red path  $P_2$  from  $v_1$  to  $w_{2m}$  in  $G_1[X, Y]$  of length

$$2(n - 3m + 2) - 1 = 2n - 6m + 3.$$

We glue  $P_1$  and  $P_2$  at  $v_1$  and  $w_{2m}$  to obtain a red cycle of size exactly

$$6m - 3 + 2n - 6m + 3 = 2n. \quad \square$$

**7.1.4. Handling many vertices in  $U_1 \cap V_2$  incident to blue edges.** In this case, there are many disjoint blue cherries inside  $U_1$ , and we will find a blue cycle. Recall that  $C$  is a collection of at most  $m - 1$  cherries with centers in  $U_2$  and leaves in  $U_1$ , which is defined three paragraphs ahead of (15).

**Claim 26.** *If there are at least  $-a_2 - b$  vertices in  $U_1 \cap V_2$  of blue degree at least  $|U_1 \cap V_1| - 0.1n \geq 0.4n$  to  $U_1 \cap V_1$ , then we find a blue cycle of length exactly  $2n$ .*

*Proof. Step 1:* We find  $m' = -a_2 - b$  blue cherries with centers in  $U_1 \cap V_2$  and leaves in  $U_1 \cap V_1$ . Possibly avoiding bad vertices. Then find common neighbors in  $U_2 \cap V_2$  to connect those cherries.

Details: Since vertices in  $U_2 \cap V_2 - V(C)$  have red degree at most 1 to  $U_1 \cap V_1 - V(C)$ , there are at most  $|U_2 \cap V_2| \leq \lambda n^2$  red edges between  $U_2 \cap V_2 - V(C)$  and  $U_1 \cap V_1 - V(C)$ . Therefore, there are at most  $20\lambda n$  vertices in  $U_1 \cap V_1 - V(C)$  with red degree at least  $0.05n$  to  $U_2 \cap V_2 - V(C)$  and at least  $|U_1 \cap V_1| - |V(C) \cap U_1| - 20\lambda n$  vertices in  $U_1 \cap V_1 - V(C)$  with blue degree at least  $|U_2 \cap V_2| - |V(C)| - 0.05n > \frac{3}{4}|U_2 \cap V_2|$  to  $U_2 \cap V_2 - V(C)$ ; we call those vertices  $B_3$ .

Since there are  $m'$  vertices in  $U_1 \cap V_2$  of blue degree at least  $|U_1 \cap V_1| - 0.1n - |V(C)| - 20\lambda n > 0.3n$  to  $B_3$ , we find  $m'$  blue cherries,  $C_4$ , with center in  $U_1 \cap V_2$  and leaves in  $B_3$ . Let  $V(C_4) \cap V_2 = \{u_1, \dots, u_{m'}\}$  and  $V(C_4) \cap V_1 = \{v_1, \dots, v_{2m'}\}$ .

We can find for each pair  $(v_{2i}, v_{2i+1})$  a common blue neighbor,  $w_i$ , in  $U_2 \cap V_2 - V(C)$ , where  $1 \leq i \leq m' - 1$ . We also find for  $v_1$  a blue neighbor  $w_0$  and  $v_{2m'}$  a blue neighbor  $w_{m'}$  distinct from  $\{w_1, \dots, w_{m'-1}\}$  and  $V(C)$ .

We obtain a blue path

$$P_1 = w_0 v_1 u_1 v_2 w_1 \cdots v_{2m'-1} u_{m'} v_{2m'} w_{m'}$$

of length  $4m'$ .

Step 2: We find for vertices in  $B$  common neighbors in  $U_1 \cap V_1$ , avoiding vertices already used.

Details: Since

$$|U_1 \cap V_1| \geq \frac{1}{2}(n + a_1) \geq |U_1 \cap V_2|, \quad (19)$$

each vertex in  $B$  has blue degree at least  $0.9n - 2m' - |U_1 \cap V_2| - |V(C) \cap U_1|$  to  $U_1 \cap V_1 - V(C)$ . Therefore,

$$\begin{aligned} 0.9n - 2m' - |U_1 \cap V_2| - |V(C) \cap U_1| &\geq 0.9n - 2m' - (n + a_1 - |U_1 \cap V_1|) - 2(m - 1) \\ &= |U_1 \cap V_1| - a_1 - 2m' - 0.1n - 2m + 2 \geq \frac{3}{4}|U_1 \cap V_1|. \end{aligned}$$

Let  $B = \{z_1, \dots, z_b\}$ . We can find for each pair  $(z_i, z_{i+1})$  a common neighbor  $r_i$ , where  $1 \leq i \leq b - 1$ , a blue neighbor  $r_0$  of  $z_1$ , and a blue neighbor  $r_b$  of  $z_b$  such that  $r_0, \dots, r_b$  are all distinct and in  $U_1 \cap V_1 - V(C)$ .

We obtain a blue path

$$P_2 = r_0 z_1 r_1 \cdots z_i r_i \cdots z_b r_b$$

of length  $2b$ .

Step 3: Take  $0.9n$  vertices in  $V_3$  and  $0.9n$  vertices in  $U_2$  including  $U_2 \cap V_1$  and  $V(C)$ . Use Theorem 17 to find a path.

Details: Recall that  $B_2$  is the collection of vertices in  $V_3$  with red degree at most  $0.1n$  to  $U_2$  and  $|B_2| \geq n - a_3 - 40\lambda n - b$ . Since  $|B_2| \geq n - a_3 - 40\lambda n - b$ , we take a set  $X \subseteq B_2$  such that  $|X| = 0.9n$ . By (19),  $|U_2 \cap V_1| \leq 0.6n$  and we can take a set  $Y \subseteq U_2 - \{w_0, w_1, \dots, w_{m'-1}\}$  such that  $U_2 \cap V_1 \subseteq Y$ ,  $V(C) \subseteq Y$ ,  $w_{m'} \in Y$ , and  $|Y| = 0.9n$ .

First we find a blue edge  $v'u'$  with  $v' \in X$  and  $u' \in U_2 - Y$ . Now we consider  $G_2[X, Y]$  and we order vertices in  $X$  and  $Y$  separately by their degree from smallest to largest. Since vertices in  $Y$  have blue degree at least  $0.9n - \frac{1}{2}n_3 > 0.3n$  to  $X$ , the smallest index  $k$  such that  $d_2(y_k, X) \leq k + 1$  satisfies

$d_2(y_k, X) \geq 0.3n$ . Since vertices in  $X$  have red degree at most  $0.1n$  to  $U_2$ , they have blue degree at least  $0.9n - 0.1n = 0.8n$  to  $Y$ . The smallest index  $j$  such that  $d_2(x_j, Y) \leq j + 1$  satisfies  $d_2(x_j, Y) \geq 0.8n$ . By Theorem 17 and  $0.8n + 0.3n > 0.9n + 2$ , we can find a Hamiltonian blue path  $P'_3$  from  $w_{m'}$  to  $v'$  in  $G_2[X, Y]$  of length  $1.8n - 1$ . We then extend the path  $P'_3$  to  $P_3$  by adding the edge  $v'u'$ . Thus, the path  $P_3$  has length  $1.8n$ .

Step 4: Finally, the rest of the vertices in  $U_2 \cap V_2$  have large blue degree to  $U_1 \cap V_1$ , and we find common neighbors to include them.

Details: Let  $K := (U_2 - Y - \{w_0, w_1, \dots, w_{m'-1}\}) = \{u', f_1, \dots, f_{k-1}\}$ . Note that  $k = |K| = n + a_2 - 0.9n - m' = 0.1n + a_2 - m'$  and  $K \subseteq U_2 \cap V_2 - V(C)$ . Since each vertex in  $K$  has at most one red neighbor to  $U_1 \cap V_1 - V(C) - \{v_1, \dots, v_{2m'}\} - \{r_0, \dots, r_b\}$ , we find for  $(u', f_1)$  a distinct blue common neighbor  $h_0$ , and for each pair  $(f_i, f_{i+1})$  a distinct blue common neighbor,  $h_i$ , in  $U_1 \cap V_1 - V(C) - \{v_1, \dots, v_{2m'}\} - \{r_0, \dots, r_b\}$ , where  $1 \leq i \leq k - 2$ . We may assume that  $r_0 f_{k-1}$  is blue (since  $f_{k-1}$  has at most one red neighbor to  $U_1 \cap V_1$  and  $z_1$  has very large blue degree to  $U_1 \cap V_1$ , if  $r_0 f_{k-1}$  is not blue then we choose  $r_0$  such that  $r_0 f_{k-1}$  is blue).

We obtain a blue path

$$P_4 = u' h_0 f_1 \cdots f_i h_i f_{i+1} \cdots h_{k-2} f_{k-1}$$

of size  $2k - 2 = 0.2n + 2a_2 - 2m' - 2$ .

Finally, we add the edge  $r_b w_0$  to connect  $P_2$  and  $P_1$ , glue  $P_1$  and  $P_3$  at  $w_{m'}$ , glue  $P_3$  and  $P_4$  at  $u'$ , and add the edge  $r_0 f_{k-1}$  to complete the cycle of length

$$1 + 4m' + 2b + 1.8n + 0.2n + 2a_2 - 2m' + 1 = 2n. \quad \square$$

**7.1.5. Changes of the proof when  $j \neq 3$ .** When  $j \neq 3$ , essentially the same proof works, with minor modifications.

Without loss of generality, we assume  $j = 1$ . We use the same setup as in the case when  $j = 3$  but replace every place of  $V_3$  by  $V_1$  and  $n_3$  by  $n_1$ .

Case 1:  $n_1 \geq n + b$ .

Since  $n_1 \geq n + b$  and  $|U_1| \geq n$ , we take a set of vertices  $X \subseteq V_1 - B$  of size  $n$  and a set of vertices  $Y \subseteq U_1$  of size  $n$ .

Now we consider  $G_1[X, Y]$  and we order vertices in  $X$  and  $Y$  separately by their degree from smallest to largest. Since vertices in  $Y$  have red degree at least  $0.5n_1$  to  $X$  and there are at most  $80\lambda n$  vertices with blue degree at least  $0.05n$  to  $V_1$ , the smallest index  $k$  such that  $d_1(y_k, X) \leq k + 1$  satisfies  $d_1(y_k, X) \geq 0.95n$ . Since vertices in  $X$  have blue degree at most  $0.9n$  to  $U_1$ , they have red degree at least  $0.1n$  to  $Y$ . The smallest index  $j$  such that  $d_1(x_j, Y) \leq j + 1$  satisfies  $d_1(x_j, Y) \geq 0.1n$ . By Theorem 18 and  $0.1n + 0.95n \gg n + 1$ , there is a Hamiltonian cycle in  $G_1[X, Y]$  of length  $2n$ .

Case 2:  $n + 1 \leq n_1 \leq n + b - 1$ .

We still assume  $n_1 = n - a_3$  with  $a_3 < 0$ . It is included in Case 1 by replacing  $n_3$  with  $n_1$ ,  $V_3$  with  $V_1$ ,  $V_1$  with  $V_2$ , and  $V_2$  with  $V_3$ . Note that in this case we have

$$n + a_1 + n + a_2 = 2n - 1$$

and thus

$$a_1 + a_2 = -1. \quad (20)$$

Equation (17) changes to

$$|U_2 \cap V_3| = n_3 - |U_1 \cap V_3| \geq 2n - 1 - n + a_3 - \frac{1}{2}(n + a_1) = \frac{1}{2}n - 1 + a_3 - \frac{1}{2}a_1$$

and thus

$$|U_2 \cap V_2| \leq n + a_2 - \left(\frac{1}{2}n - 1 + a_3 - \frac{1}{2}a_1\right) = \frac{1}{2}n + 1 + a_2 - a_3 + \frac{1}{2}a_1 = \frac{1}{2}n - a_3 - \frac{1}{2}a_1.$$

Moreover, by  $a_3 < 0$ , the inequality  $a_1 \geq m$  in (18) still holds under the assumption  $a_2 \leq -b - 1$  since

$$a_1 = -1 - a_2 \geq b \geq b + a_3 = m.$$

When choosing between Claims 25 and 26, we still have by (20)

$$|U_1| - |V_2| \geq n + a_1 - n + a_3 = a_1 + a_3 = -1 - a_2 + a_3 = (b + a_3) + (-b - a_2) - 1$$

and therefore one of the two claims can still be applied.

## 7.2. The case when (9) holds.

**7.2.1. Statement and setup of the main lemma.** In this case, we have

$$n_1 + n_2 + \cdots + n_s = 3n - 1 \tag{21}$$

and

$$n_2 + \cdots + n_s \geq 2n - 1. \tag{22}$$

By (11),  $s \leq 5$ . Our main lemma in this subsection is:

**Lemma 27.** *Let  $G = K_{n_1, n_2, \dots, n_s}$  satisfying (21) and (22) be 2-edge-colored with a  $(\lambda, i, 2)$ -bad partition. Then  $G$  has a monochromatic cycle of length  $2n$ .*

*Proof.* Without loss of generality, let  $i = 2$ . By the definition of a  $(\lambda, i, 2)$ -bad partition, there is a  $j \in [s]$  such that:

- (i)  $n \geq |V_j| \geq (1 - \lambda)n$ .
- (ii)  $(1 - \lambda)n \leq |U_1| \leq (1 + \lambda)n$ .
- (iii)  $(1 - \lambda)n \leq |U_2| \leq (1 + \lambda)n$ .
- (iv)  $E(G_2[V_j, U_1]) \leq \lambda n^2$ .
- (v)  $E(G_1[V_j, U_2]) \leq \lambda n^2$ .

Our plan is as follows. In this and the next three subsections we handle the case  $s = 4$  and renumber the parts so that  $j = 1$  and  $n_2 \geq n_3 \geq n_4$ . Later, in Section 7.2.5, we return to the original numbering of the parts ( $n_1 \geq \cdots \geq n_s$ ) and describe modifications to the proof for  $s \neq 4$ .

Since (9) holds, we have  $n_i \leq n$  for all  $i$ ; we also know that  $n_2 \geq n_3 \geq n_4$ ,  $n_1 = |V_j| \geq (1 - \lambda)n$ , and

$$|U_1| + |U_2| = n_2 + n_3 + n_4 = 3n - 1 - n_1 \leq 2n + \lambda n - 1,$$

so  $n_2 \geq \frac{1}{3}(n_2 + n_3 + n_4) \geq \frac{2}{3}n$ .

We move vertices as we did in the previous section so that for each  $u \in U_1$  we have  $d_1(u, V_1) \geq \frac{1}{2}n_1$  and for each  $v \in U_2$  we have  $d_2(v, V_1) \geq \frac{1}{2}n_1$ . Note that (iv) and (v) change to (iv)  $|E(G_2[V_1, U_1])| \leq 4\lambda n^2$  and (v)  $|E(G_1[V_1, U_2])| \leq 4\lambda n^2$ .

Let  $|U_1| = n + a_1$ ,  $|U_2| = n + a_2$ , and  $|V_1| = n - a_3$ . Let  $B$  be the set of vertices in  $V_1$  with blue degree at least  $0.9n$  to  $U_1$ , and let  $b := |B|$ . By condition (iv), we know  $b \leq 5\lambda n$ .

Let  $C$  be a maximum collection of vertex-disjoint red cherries with center in  $U_2$  and leaves in  $U_1$ . If there are at least  $m := a_3 + b$  cherries in  $C$ , then we use them, together with the edges between  $U_1$  and  $V_1$ , to find a red cycle of length  $2n$ . This is done in exactly the same way as in Claim 23, except with  $V_1$  playing the role of  $V_3$ .

Otherwise, we assume that  $c := |C| \leq m - 1$ , which means every vertex in  $U_2 - V(C)$  has red degree at most  $2m - 1$  to  $U_1$ .

When  $|U_2| = n + a_2 \geq n - b$ , we can find a blue cycle in almost the same way as in Claim 24; the updated proof is given in Claim 28.

Otherwise, we may assume that  $|U_2| \leq n - b - 1$ , in which case (15) holds.

As before, to proceed, we want to use edges within  $U_1$ . Let  $k$  be such that  $|U_1 \cap V_k|$  is maximized. This intersection is still at most  $|V_k| \leq n$ , while  $|U_1| = n + a_1$ , so  $|U_1 - V_k| \geq a_1$ .

Since

$$(n + a_1) + (n + a_2) = |U_1| + |U_2| = 3n - 1 - |V_1| = 2n + a_3 - 1,$$

we have  $a_1 + a_2 = a_3 - 1$ , and therefore

$$|U_1 - V_k| \geq a_3 - a_2 - 1 = (b + a_3) + (-a_2 - b) - 1.$$

There are two possibilities:

- There are at least  $m = b + a_3$  vertices in  $U_1 - V_k$  of red degree at least  $0.1n$  to  $U_1 \cap V_k$ . In this case, we will find a red cycle of length exactly  $2n$  by Claim 29.
- There are at least  $m' = -a_2 - b$  vertices in  $U_1 - V_k$  of blue degree at least  $|U_1 \cap V_k| - 0.1n \geq 0.2n$  to  $U_1 \cap V_k$ . In this case, we find a blue cycle of length exactly  $2n$  by Claim 30.

One of these must hold, since  $|U_1 - V_k| \geq m + m' - 1$ , while by (15),  $m' \geq 1$ ; therefore there are either  $m$  vertices for Claim 29 or  $m'$  vertices for Claim 30. In either case, we obtain a monochromatic cycle of length exactly  $2n$ , completing the proof.  $\square$

**7.2.2.** *The case of large  $U_2$ :  $|U_2| \geq n - b$ .*

**Claim 28.** *If  $|U_2| = n + a_2 \geq n - b$ , then we have a blue cycle of size exactly  $2n$ .*

*Proof.* Since  $|U_2| = n + a_2 \geq n - 4\lambda n$ , we know that the largest among  $U_2 \cap V_2$ ,  $U_2 \cap V_3$ ,  $U_2 \cap V_4$  has size at least  $0.33n$ . We assume  $|U_2 \cap V_p|$  is the largest and

$$|U_2 \cap V_p| \geq 0.33n. \tag{23}$$

By (23) and  $|V_p| \leq n$ , we have

$$|U_1 \cap V_p| \leq 0.67n$$

and there is a  $q \in \{2, 3, 4\} - \{p\}$  such that

$$|U_1 \cap V_q| \geq 0.16n. \tag{24}$$

**Step 1:** We first find a path to include say  $0.8n$  vertices in  $V_1$  and  $0.8n$  vertices in  $U_2$  (all of  $(V - V_p) \cap U_2$  and  $V(C)$ ) by Theorem 17.

Details: The details are almost the same as in Step 2 of Claim 24 except every place of  $n_3$  is replaced by  $n_1$ , every place of  $V_3$  is replaced by  $V_1$ ,  $V_1$  is replaced by  $(V - V_p)$ .

- If  $a_2 \geq 0$ , then we do not need Step 2 and go to Step 3 directly.

Step 2: Use  $|a_2|$  vertices in  $B$  to obtain a blue path.

Details: Since  $b \geq |a_2|$ , let  $Z := \{z_1, \dots, z_{|a_2|}\} \subseteq B$ .

By (24) and each vertex  $v$  in  $B$  having blue degree at least  $0.9n \gg \frac{1}{2}|U_1|$  to  $U_1$ , we can find for each pair  $(z_i, z_{i+1})$  a blue common neighbor  $r_i \in U_1 - V(C)$ , where  $1 \leq i \leq |a_2| - 1$ , a blue neighbor  $r_0$  of  $z_1$  such that  $r_0 \in V_q \cap U_1 - V(C)$ , and a blue neighbor  $r_{|a_2|}$  of  $z_{|a_2|}$  such that  $r_{|a_2|} \in V_q \cap U_1 - V(C)$  and  $r_0, \dots, r_{|a_2|}$  are all distinct.

Since  $y'$  has at most one red neighbor to  $U_1 - V(C)$ , we choose  $r_{|a_2|}$  to be in  $U_1 \cap V_q - V(C)$  and such that  $r_{|a_2|}y'$  is blue.

We obtain a blue path

$$P_2 = r_0 z_1 r_1 \cdots z_i r_i \cdots z_{|a_2|} r_{|a_2|}$$

of length  $2|a_2|$ .

Step 3: Include the rest of vertices in  $U_2$  to  $U_1$  by Theorem 17.

Details: The details are almost the same as in Step 3 of Claim 24 except every place of  $V_2$  is replaced by  $V_p$ .  $\square$

### 7.2.3. Handling many vertices in $U_1 - V_k$ incident to red edges.

**Claim 29.** *If there are at least  $m = b + a_3$  vertices in  $(V - V_k) \cap U_1$  of red degree at least  $0.1n$  to  $U_1 \cap V_k$ , then we have a red cycle of length exactly  $2n$ .*

*Proof.* Let  $B'$  be the collection of vertices in  $U_1$  with blue degree at least  $0.05n$  to  $V_1$ . Since there are at most  $4\lambda n^2$  blue edges between  $U_1$  and  $V_1$ , we have

$$|B'| \leq 80\lambda n.$$

Step 1: We first find a collection of red cherries  $C_3$  with center in  $U_1 \cap (V - V_k)$  and leaves in  $U_1 \cap V_k - B'$  of size  $m$ .

Details: The details are almost the same as in Step 1 of Claim 25 except we replace everywhere  $V_2$  by  $V - V_k$ ,  $V_1$  by  $V_k$ , and  $V_3$  by  $V_1$ .

Step 2: By Hall's theorem we find a matching  $M$  for  $V(C_3) \cap V_k$  to  $R$  and then find a common neighbor back to connect those vertices.

Details: The details are almost the same as in Step 2 of Claim 25 except we replace everywhere  $V_3$  by  $V_1$  and  $n_3$  by  $n_1$ .

Step 3: Use Theorem 17 to get a path saturating all vertices left in  $V_1 - B - V(M)$ .

Details: Let  $X = V_1 - B - \{w_2, \dots, w_{2m-1}\}$  and we know  $|X| = n - a_3 - b - (2m - 2) = n - 3m + 2$ . We have  $a_1 = a_3 - a_2 - 1 = m - a_2 - b - 1 \geq m$ , and therefore

$$n + a_1 - m - (2m - 1) - (m - 1) = n + a_1 - 4m + 2 \geq n - 3m + 2.$$

We can take  $Y \subseteq U_1 - \{u_1, \dots, u_m\} - \{v_2, \dots, v_{2m}\} - \{g_1, \dots, g_{m-1}\}$  such that  $v_1 \in Y$  and  $|Y| = n - 3m + 2$ .

The rest of details are almost the same as in Step 3 of Claim 25 except we replace everywhere  $V_3$  by  $V_1$  and  $n_3$  by  $n_1$ .  $\square$

**7.2.4. Handling many vertices in  $U_1 - V_k$  incident to blue edges.** In the case when many vertices in  $U_1 - V_k$  are incident to blue edges, there are many disjoint blue cherries inside  $U_1$ , and we find a blue cycle.

**Claim 30.** *If there are at least  $m' = -a_2 - b$  vertices in  $U_1 - V_k$  of blue degree at least  $|U_1 \cap V_k| - 0.1n$  to  $U_1 \cap V_k$ , then we have a blue cycle of length exactly  $2n$ .*

*Proof.* Since  $U_1 \cap V_k$  is the largest among  $U_1 \cap V_2$ ,  $V_3 \cap U_1$ , and  $V_4 \cap U_1$ , we know

$$|U_1 \cap V_k| \geq 0.33n, \quad |U_2 \cap V_k| \leq 0.67n, \quad \text{and} \quad |U_2 - V_k| \geq 0.32n. \quad (25)$$

Step 1: We find  $m'$  blue cherries from  $U_1 \cap (V - V_k)$  to  $U_1 \cap V_k$ , possibly avoiding bad vertices. Then we find common neighbors in  $U_2$  to connect those cherries.

Details: The details are almost the same as in Step 1 of Claim 26 until the following sentence except that we replace everywhere  $V_2$  by  $V - V_k$  and  $V_1$  by  $V_k$ .

For all pairs  $(v_{2i}, v_{2i+1})$  we can find distinct common blue neighbors,  $w_i$ , in  $(V - V_k) \cap U_2 - V(C)$ , where  $1 \leq i \leq m' - 1$ .

By (25), there is an  $\ell \in \{2, 3, 4\} - \{k\}$  such that

$$|V_\ell \cap U_2| \geq 0.16n. \quad (26)$$

We also find for  $v_1$  a blue neighbor  $w_0 \in V_\ell \cap U_2$  and  $v_{2m'}$  a blue neighbor  $w_{m'} \in V_\ell \cap U_2$  distinct from  $\{w_1, \dots, w_{m'-1}\}$  and  $V(C)$ .

We obtain a blue path

$$P_1 = w_0 v_1 u_1 v_2 w_1 \cdots v_{2m'-1} u_{m'} v_{2m'} w_{m'}$$

of length  $4m'$ .

Step 2: We find for vertices in  $B$  common neighbors in  $U_1 \cap V_k$ , avoiding vertices already used.

Details: By (25) and each vertex  $v$  in  $B$  having red degree at most  $0.1n + a_1$  to  $U_1$ ,  $v$  has at least

$$|U_1 \cap V_k| - 2m' - 0.1n - a_1 > 0.6|U_1 \cap V_k - V(C)| \quad (27)$$

edges to  $U_1 \cap V_k - V(C)$ . We can find for each pair  $(z_i, z_{i+1})$  a common neighbor  $r_i$ , where  $1 \leq i \leq b - 1$ , a blue neighbor  $r_0$  of  $z_1$ , and a blue neighbor  $r_b$  of  $z_b$  such that  $\{r_0, \dots, r_b\} \subseteq U_1 \cap V_k - V(C)$  are all distinct and  $w_0 r_b$  is blue.

We obtain a blue path

$$P_2 = r_0 z_1 r_1 \cdots z_i r_i \cdots z_b r_b$$

of length  $2b$ .

Step 3: Take  $0.9n$  vertices in  $V_1$  and  $0.9n$  vertices in  $U_2$  including  $(V - V_\ell) \cap U_2$  and  $V(C)$ . Use Theorem 17 to find a path.

Details: The details are almost the same as in Step 3 of Claim 26 except we replace everywhere  $V_1$  by  $V - V_\ell$ ,  $V_3$  by  $V_1$ , and  $n_3$  by  $n_1$ .

Step 4: Finally, the rest of vertices in  $U_2 \cap V_\ell$  have large blue degree to  $(V - V_\ell) \cap U_1$ , and we find common neighbors to include them.

Details: The details are almost the same as in Step 4 of Claim 26 except we replace everywhere  $V_1$  by  $V - V_\ell$ ,  $V_2$  by  $V_\ell$ ,  $V_3$  by  $V_1$ , and  $n_3$  by  $n_1$ .  $\square$

**7.2.5. Changes in the proof when  $s \neq 4$ .** When  $s \neq 4$ , essentially the proof for  $s = 4$  works, with minor modifications.

Case 1:  $s = 3$ . Then  $n_2 + n_3 \geq 2n - 1$  implies  $n_1 \geq n_2 \geq n$  and therefore

$$n_1 = n_2 = n \quad \text{and} \quad n_3 = n - 1.$$

This case is addressed in Lemma 22.

Case 2:  $s = 5$ . If  $j = 2$ , then since  $n_4 + n_5 > n$ ,  $n_1 \geq n_2 \geq (1 - \lambda)n$ , and  $n_3 > \frac{1}{2}n$ , we have

$$N = n_1 + n_2 + n_3 + n_4 + n_5 \geq 2(1 - \lambda)n + \frac{3}{2}n > 3n,$$

which is not the case. By a similar argument,  $j \notin \{3, 4, 5\}$ . Thus, we may assume  $j = 1$ .

The argument is almost the same as for  $s = 4$ . We only mention differences.

In our case,  $n_4 + n_5 > n$  implies

$$n_1 \geq n_2 \geq n_3 \geq n_4 > \frac{1}{2}n; \tag{28}$$

thus

$$n_2 + n_3 = 3n - 1 - n_1 - n_4 - n_5 < n + \lambda n - 1. \tag{29}$$

By (28) and (29), we have

$$\frac{1}{2}n - \lambda n \leq n_5 \leq n_4 \leq n_3 \leq n_2 \leq \frac{1}{2}n + \lambda n. \tag{30}$$

In Section 7.2.2, in (23) we now can only guarantee  $|U_2 \cap V_p| \geq 0.24n$  instead of  $0.33n$ . By (30), we can find a  $q \in \{2, 3, 4, 5\} - \{p\}$  such that  $|U_1 \cap V_q| \geq 0.16n$ .

In Section 7.2.4, in (25) we can now only guarantee the largest  $|U_1 \cap V_k| \geq 0.24n$ . Equation (26) still holds with  $\ell \in \{2, 3, 4, 5\} - \{k\}$ . Everything else is the same.

## 8. Completion of the proof of Theorem 5

In the previous three sections, we proved Theorem 5 in the cases when  $N - n_1 - n_2 \geq 3$ . By (10), in the case  $N - n_1 - n_2 \leq 2$ , it is sufficient to show that for every 2-edge-coloring of  $K_{2n, 2n-1}$ , there is a monochromatic cycle of length exactly  $2n$ . Thus, the next lemma completes the proof of Theorem 5.

**Lemma 31.** *If  $n$  is sufficiently large, then for every 2-edge-coloring of  $K_{2n, 2n-1}$ , there is a monochromatic cycle of length exactly  $2n$ .*

*Proof.* Let  $G = K_{2n, 2n-1}$ . From Section 5, we know that if the reduced graph  $G^r$  has a connected matching of size at least  $(1 + \gamma)n$ , then we can find a monochromatic cycle of length exactly  $2n$ . Suppose  $G^r$  has no connected matching of size  $(1 + \gamma)n$  and thus, by Section 5 again,  $G$  has a  $(\lambda, i, j)$ -bad partition for some  $i \in [2]$  and  $j \in [2]$ .

Without loss of generality, we assume  $i = 1$  and discuss separately cases  $j = 1$  and  $j = 2$ .

Case 1:  $G$  has a  $(\lambda, 1, 1)$ -bad partition. By the setup in Section 6, we have a partition  $W_1 \cup W_2$  of  $V(G)$  such that

- (i)  $(1 - \lambda)n \leq |W_2| \leq (1 + \lambda)n_1 = (1 + \lambda) \cdot 2n$ ,
- (ii)  $|E(G_1[W_1, W_2])| \leq \lambda n^2$ ,
- (iii)  $|E(G_2[W_1])| \leq \lambda n^2$ .

We know  $|W_1| = N - |W_2| = 4n - 1 - |W_2|$ , so by condition (i),

$$(2 - 3\lambda)n \leq |W_1| \leq (3 + \lambda)n. \quad (31)$$

For simplicity, let  $A := W_1 \cap V_1$ ,  $B := W_2 \cap V_1$ ,  $C := W_1 \cap V_2$ , and  $D := W_2 \cap V_2$ . Let  $A^*$  be the collection of vertices in  $A$  with less than  $0.6|C|$  red edges to  $C$ ,  $B^*$  be the collection of vertices in  $B$  with at least  $0.6|C|$  red edges to  $C$ ,  $C^*$  be the collection of vertices in  $C$  with less than  $0.6|A|$  red edges to  $A$ , and  $D^*$  be the collection of vertices in  $D$  with at least  $0.6|A|$  red edges to  $A$ . Let  $A = (A - A^*) \cup B^*$ ,  $B = (B - B^*) \cup A^*$ ,  $C = (C - C^*) \cup D^*$ , and  $D = (D - D^*) \cup C^*$ . By conditions (ii) and (iii),

$$|A^*| \leq \frac{5}{2|C|}\lambda n^2, \quad |B^*| \leq \frac{5}{3|C|}\lambda n^2, \quad |C^*| \leq \frac{5}{2|A|}\lambda n^2, \quad \text{and} \quad |D^*| \leq \frac{5}{3|A|}\lambda n^2.$$

Let  $\lambda' = 10\lambda$ ,  $W_1 = A \cup C$ , and  $W_2 = B \cup D$ .

**Remark 32.** Conditions (i)–(iii) still hold with  $\lambda'$  replacing  $\lambda$  and every vertex in  $A$  has red degree at least  $0.59|C|$  to  $C$ , every vertex in  $B$  has blue degree at least  $0.39|C|$  to  $C$ , every vertex in  $C$  has red degree at least  $0.59|A|$  to  $A$ , and every vertex in  $D$  has red degree at least  $0.39|A|$  to  $A$ .

Case 1.1:  $|A| \geq n$  and  $|C| \geq n$ . Let  $X \subseteq A$  and  $Y \subseteq C$  such that  $|X| = |Y| = n$ . For each  $x \in X$  and  $y \in Y$ , by  $|A|, |C| \leq 2n$  and Remark 32,

$$d_1(x, Y) \geq |Y| - 0.41|C| \geq n - 0.82n = 0.18n \quad \text{and similarly} \quad d_1(y, X) \geq |X| - 0.41|A| \geq 0.18n.$$

By condition (iii), we know that the number of vertices in  $X$  with at least  $0.95n$  edges to  $Y$  in  $G_1$  is at least  $n - 20\lambda'n$  and the number of vertices in  $Y$  with at least  $0.95n$  edges to  $X$  in  $G_1$  is at least  $n - 20\lambda'n$ . Therefore, if we order vertices in  $X$  by their degrees in nondecreasing order, say the ordering follows from  $d(x_1) \leq \dots \leq d(x_n)$ , then the smallest index  $i$  such that  $d(x_i) \leq i + 1$  has the property that  $d(x_i) \geq 0.95n$ . Similarly, if we order vertices in  $Y$  by their degree in nondecreasing order, say the ordering follows from  $d(y_1) \leq \dots \leq d(y_n)$ , then the smallest index  $j$  such that  $d(y_j) \leq j + 1$  has the property that  $d(y_j) \geq 0.95n$ . Since  $d(x_i) + d(y_j) \gg n + 2$ , by Theorem 17, we know  $G_1[X, Y]$  is Hamiltonian biconnected and we can find a cycle in  $G_1$  of length exactly  $2n$ .

**Remark 33.** The same proof shows that there is a red cycle of length exactly  $\min\{|A|, |C|\}$ .

Case 1.2:  $|A| \leq (1 - 30\lambda')n$ . By (31) and  $|V_1| = 2n$ ,

$$|C| \geq (1 + 27\lambda')n \quad \text{and} \quad |B| \geq (1 + 30\lambda')n. \quad (32)$$

By condition (ii), there are at most  $20\lambda'n$  vertices in  $C$  with red degree at least  $0.05n$  to  $B$ . Let  $C'$  be the  $20\lambda'n$  vertices in  $C$  of largest red degree to  $B$ . Let  $Y$  be a subset of  $C - C'$  with size  $n$ . Similarly, let  $B'$  be the  $20\lambda'n$  vertices in  $B$  of largest red degree to  $C$  and we define  $X \subseteq B - B'$  of size  $n$ . We show there is a blue cycle of length exactly  $2n$  in  $G_2[X, Y]$ .

By the definitions of  $X$  and  $Y$ , we know that  $d_2(x, Y) \geq 0.95n$  for  $x \in X$  and  $d_2(y, X) \geq 0.95n$  for  $y \in Y$ . By an argument similar to the last paragraph of Case 1.1, we can find a blue cycle of length exactly  $2n$  in  $G_2[X, Y]$ .

Case 1.3:  $|C| \leq (1 - 30\lambda')n$ . We find a blue cycle by an argument similar to Case 1.2.

Case 1.4:  $|A| \geq (1 + 30\lambda')n$  and  $|D| \geq n$ . By condition (iii), there are at most  $20\lambda'n$  vertices in  $A$  of red degree at least  $0.05n$  to  $D$ . Let  $X'$  be the  $20\lambda'n$  vertices in  $A$  of largest red degree to  $D$ .

By condition (ii), there are at most  $20\lambda'n$  vertices in  $D$  of red degree at least  $0.05n$  to  $A$ . Let  $R$  be the  $20\lambda'n$  vertices in  $D$  of largest red degree to  $A$ . Since  $d_2(v, A) \geq 0.39|A| > 0.39n$  for each  $v \in R$  and  $|R| = 20\lambda'n =: m$ , we can order vertices in  $R$  so that  $R = \{r_1, \dots, r_m\}$  and find for  $R$  a distinct collection of blue cherries to  $A - X'$ . We may assume the other ends of the cherries are  $S = \{s_1, \dots, s_{2m}\}$  so that each  $s_{2i-1}r_i s_{2i}$  is a cherry. Since  $S \subseteq A - X'$ , each  $s_i$  has blue degree at least  $|D| - 0.05n$  to  $D$  and we can find for each  $(s_{2i}, s_{2i+1})$  a distinct common blue neighbor  $f_i$  in  $D - R$ , where  $1 \leq i \leq m - 1$ , and thus form a blue path

$$P_1 = s_1 r_1 s_2 f_1 s_3 \cdots s_{2m}$$

from  $s_1$  to  $s_{2m}$ . We then extend the path  $P_1$  by finding a blue neighbor  $r_0$  of  $s_1$  in  $D - R$  distinct from each vertex chosen in  $P_1$ . Note now  $P_1$  has length  $4m - 1$  from  $r_0$  to  $s_{2m}$ .

Let  $X \subseteq (A - X' - V(P_1)) \cup \{s_{2m}\}$  such that  $s_{2m} \in X$  and  $|X| = n - 2m + 1$ . Let  $Y \subseteq (D - R - V(P_1)) \cup \{r_0\}$  such that  $|Y| = n - 2m + 1$ . Since  $d_2(y, X) \geq 0.9n$  for  $y \in Y$  and  $d_2(x, Y) \geq 0.9n$  for  $x \in X$ , we claim that  $G_2[X, Y]$  is Hamiltonian biconnected by an argument similar to the last paragraph of Case 1.2. Therefore, we can find a blue path  $P_2$  of length  $2n - 4m + 1$  from  $r_0$  to  $s_{2m}$ .

Finally, we glue  $P_1$  and  $P_2$  at  $r_0$  and  $s_{2m}$  to complete a blue cycle of length exactly  $2n$ .

Case 1.5:  $|C| \geq (1 + 30\lambda')n$  and  $|B| \geq n$ . It is similar to Case 1.4.

Case 1.6:  $|B| \geq n$  and  $|D| \geq n$ .

- If there is no blue edge in  $G[B, D]$ , then  $G_1[B, D]$  is a complete bipartite graph and thus we can find a red cycle of length exactly  $2n$ .
- If there is a blue matching of size 2 in  $G_2[B, D]$ , say the two matching edges are  $v_1 v_2$  and  $u_1 u_2$ , where  $v_1, u_1 \in V_1$  and  $v_2, u_2 \in V_2$ , then by Cases 1.2 and 1.3, we know  $|A| \geq (1 - 30\lambda')n$  and  $|C| \geq (1 - 30\lambda')n$ . By condition (ii), there are at most  $20\lambda'n$  vertices in  $A$  such that the red degree to  $D$  is at least  $0.05n$  and there are at most  $20\lambda'n$  vertices in  $D$  such that the red degree to  $A$  is at least  $0.05n$ . Similarly, there are at most  $20\lambda'n$  vertices in  $C$  such that the red degree to  $B$  is at least  $0.05n$  and there are at most  $20\lambda'n$  vertices in  $B$  such that the red degree to  $C$  is at least  $0.05n$ .

Let  $A' \subseteq A$  be the  $|A| - 20\lambda'n$  vertices with the largest blue degree to  $D$ ,  $D' \subseteq D$  be the  $|D| - 20\lambda'n$  vertices with the largest blue degree to  $A$ ,  $C' \subseteq C$  be the  $|C| - 20\lambda'n$  vertices with the largest blue degree to  $B$ , and  $B' \subseteq B$  be the  $|B| - 20\lambda'n$  vertices with largest blue degree to  $C$ .

By condition (i) and  $|W_2| = |B| + |D| \geq 2n$ , we know  $|A| \geq n - 2\lambda'n$ . Thus, by Remark 32,

$$d_2(u_2, A) \geq 0.39|A| \geq 0.38n.$$

We find a blue neighbor  $w_1 \in A'$  of  $u_2$ . Let  $A'' \subseteq A$  such that  $w_1 \in A''$  and  $|A''| = \lfloor \frac{1}{2}n \rfloor$ . Let  $D'' \subseteq D'$  such that  $v_2 \in D''$  and  $|D''| = \lfloor \frac{1}{2}n \rfloor$ . By  $A'' \subset A'$  and  $D'' \subseteq D'$ ,  $d_2(v, A'') \geq 0.4n$  for every  $v \in D''$  and  $d_2(v, D'') \geq 0.4n$  for every  $v \in A''$ . Since  $0.4n + 0.4n > 0.5n + 1$ , we can use Theorem 17 to find a blue

path  $P_1$  of length  $2(\lfloor \frac{1}{2}n \rfloor - 1)$  from  $v_2$  to  $w_1$  and then extend  $P_1$  by adding  $w_1u_2$ . Similarly, we can find a blue path  $P_2$  with vertices in  $B \cup C$  from  $v_1$  to  $u_1$  of length exactly  $2(\lceil \frac{1}{2}n \rceil - 1)$ .

Finally, we connect  $P_1$  and  $P_2$  by adding the edge  $v_1v_2$  and  $u_1u_2$  to form a blue cycle of length exactly  $2n$ .

**Remark 34.** The argument also works whenever all of  $A, B, C, D$  are of size in  $[n - 100\lambda', n + 100\lambda'n]$ .

- If the size of a maximum matching in  $G_2[B, D]$  is exactly 1, then let  $v_1v_2$  be a blue edge, and let  $\{v_2\} \subseteq D$  be a smallest vertex cover in  $G_2[B, D]$  (the case  $\{v_1\}$  is a smallest vertex cover has a similar proof and is simpler). If we delete  $v_2$ , then the remaining graph is a complete bipartite graph in  $G_1$ . If  $|D| \geq n + 1$  then we can find a red cycle of length  $2n$  in  $G_1[B, D - \{v_2\}]$ . Thus, we may assume  $|D| = n$  and  $|C| = n - 1$ .

Let  $B'' \subseteq B$  such that  $|B''| = n$ . We find a blue cycle in  $G_2[B'', C \cup \{v_2\}]$ . By condition (i) and  $|W_2| = |B| + |D| \geq 2n$ , we know  $|C| \geq n - 2\lambda'n$ . Thus, by Remark 32, for each  $v \in B''$  we have

$$d_2(v, C) \geq 0.39|C| \geq 0.38n.$$

We also know that each vertex  $v_c$  in  $C \cup \{v_2\}$  can have red degree at most 1 to  $B$  (so it has blue degree at least  $n - 1$  to  $B''$ ) since otherwise with vertices in  $D - \{v_2\}$  we can find a red cycle of length  $2n$ . Since  $n - 1 + 0.19n > n + 1$ , we can use Theorem 17 to find a blue cycle of length exactly  $2n$ .

Case 1.7:  $n + 1 \leq |A| \leq (n + 30\lambda'n)$  and  $n \leq |D| \leq n + 30\lambda'n$ . By Remark 34, the size of a maximum matching in  $G_2[B, D]$  is at most 1. Let  $v_1v_2 \in G_2$  such that  $v_1 \in B$  and  $v_2 \in D$ . We may also assume that  $\{v_2\}$  is a minimum vertex cover of  $G_2[B, D]$  (the case  $\{v_1\}$  is a smallest vertex cover has a similar proof and is simpler). Let  $R \subseteq A$  be the set of vertices with red degree at least  $0.8n$  to  $D$ . By condition (ii), we know  $|R| \leq 2\lambda'n$ .

We first show that  $|D| = n$ . Assume not, i.e.,  $|D| \geq n + 1$ . Then  $|D - \{v_2\}| \geq n$ .

If  $|A - R| \geq n$ , then we find a blue cycle of length  $2n$  in  $G_2[A - R, D]$ . To do so, take a subset  $A' \subseteq A - R$  of size  $n$  and  $D' \subseteq D - \{v_2\}$  of size  $n$ . By Remark 32, for every  $v \in D$  we have

$$d_2(v, C) \geq 0.39|C| = 0.39(2n - |D|) \geq 0.38n.$$

Thus,  $d_2(v, A') \geq$  for  $v \in D'$ . By the definition of  $A'$ , we know  $d_2(v, D') \geq 0.2n$  for  $v \in A'$ . By condition (ii), we also know there are at most  $20\lambda'n$  vertices in  $A'$  of red degree at least  $0.05n$  to  $D$  and thus if we order vertices in  $A'$  and  $D'$  in nondecreasing order respectively, say  $A' = \{u_1, \dots, u_n\}$  and  $D' = \{w_1, \dots, w_n\}$ , then the smallest index such that  $d_2(u_i) \leq i + 1$  has  $d_2(u_i) \geq 0.95n$  and the smallest index such that  $d_2(w_j) \leq j + 1$  has  $d_2(w_j) \geq 0.19n$ . Since  $0.95n + 0.19n > n + 1$ , we can use Theorem 17 to find a blue cycle of length exactly  $2n$  in  $G_2[A', D']$ .

If  $|A - R| \leq n - 1$ , then we find a red cycle of length exactly  $2n$  in  $G_1[B \cup R, D - \{v_2\}]$ . To do so, note that (1)  $|B \cup R| = 2n - |A - R| \geq n + 1$ , (2)  $G_1[B, D - \{v_2\}]$  is a red complete bipartite graph, and (3) each vertex in  $R$  has degree at least  $0.8n$  to  $D - \{v_2\}$ . We can use Theorem 17 to find a red cycle of length exactly  $2n$ , since this red graph is very dense and has both parts large enough.

**Remark 35.** The proof also shows we can find a monochromatic cycle when  $|A| \in [n - 100\lambda'n, n + 100\lambda'n]$  and  $n + 1 \leq |D| \leq (1 + 100\lambda')n$ .

We assume  $|D| = n$  from now on. Since each vertex in  $R$  has red degree at least  $0.8n$  to  $D$ , if there are at least two vertices in  $R$ , say  $r_1$  and  $r_2$ , then we find a red common neighbor  $w \in D$  for  $r_1$  and  $r_2$ . Note that by Remark 33,  $G_1[A, C]$  is Hamiltonian-biconnected. Therefore, we can find a red cycle of length exactly  $2n$  from a path  $P_1$  from  $r_1$  to  $r_2$  of length  $2n - 2$  glued with the path  $P_2 = r_1wr_2$ . The only case remaining is  $|R| \leq 1$ . Then we have  $|A - R| \geq n$  and we find a blue cycle of length  $2n$  by the same argument as in two paragraphs ahead of this paragraph.

**Remark 36.** Note that the last sentence of the previous paragraph shows why we need  $|A| \geq n + 1$ .

The only uncovered case is:

Case 1.8:  $n \leq |C| \leq (1 + 30\lambda')n$  and  $(1 - 30\lambda')n \leq |A| \leq n - 1$ . We define  $R$  to be vertices in  $C$  with red degree at least  $0.8n$  to  $B$ . By Remark 34, we may assume that the size of a maximum matching in  $G_2[B, D]$  is at most 1.

If  $|C - R| \geq n$ , then we find a blue cycle of length exactly  $2n$  in  $G_2[B, C - R]$ . Thus, we may assume

$$|C - R| \leq n - 1. \quad (33)$$

- If there is no edge in  $G_2[B, D]$ , then  $G_1[B, D]$  is a complete bipartite graph and we are done if  $|D \cup R| \geq n$ . Thus, we may assume that  $|D \cup R| \leq n - 1$ . Since  $|C - R| + |R| + |D| = 2n - 1$ ,  $|C - R| \geq n$  and we have a contradiction.
- If the size of a maximum matching in  $G_2[B, D]$  is exactly 1, say  $v_1v_2$  is such a matching with  $v_1 \in B$  and  $v_2 \in D$ , then one of  $\{v_1\}$  or  $\{v_2\}$  is a minimum vertex cover of  $G_2[B, D]$ . We may assume that  $\{v_2\}$  is a minimum vertex cover of  $G_2[B, D]$ , and the case when  $\{v_1\}$  is a minimum vertex cover has a similar proof and is simpler.

Since  $G_1[B, D - \{v_2\}]$  is a complete bipartite graph, we are done if  $|D| \geq n + 1$ . Thus, we may assume  $|D| \leq n$ . Moreover, if  $|D \cup R - \{v_2\}| \geq n$  then we can find a red cycle of length  $2n$  in  $G_1[D \cup R - \{v_2\}, B]$ ; hence we may assume

$$|D| + |R| - 1 \leq n - 1.$$

But we also know that  $|D| + |R| + |C - R| = 2n - 1$ . Thus,

$$|C - R| \geq n - 1,$$

and by (33) we know

$$|C - R| = n - 1 \quad \text{and} \quad |D \cup R| = n.$$

If  $v_2$  has at least two red edges to  $B$  then we can find a red cycle in  $G_1[B, D \cup R]$  by first considering the two edges incident with  $v_2$ . Thus,  $v_2$  has at most one red edge to  $B$  and thus has at least  $|B| - 1$  blue edges to  $B$ . We can find a blue cycle in  $G_2[(C - R) \cup \{v_2\}, B]$ .

Case 2:  $G$  has a  $(\lambda, 1, 2)$ -bad partition. This case is covered in Case 1 in Section 7.1.5 (with the same proof).  $\square$

### 9. Proof of Theorem 6 on monochromatic $C_{\geq 2n}$

For large  $n$ , we need to prove the theorem for every  $N$ -vertex complete  $s$ -partite graph  $G$  with parts  $(V_1^*, V_2^*, \dots, V_s^*)$  such that the numbers  $n_i = |V_i^*|$  satisfy  $n_1 \geq n_2 \geq \dots \geq n_s$  and conditions (1), (2), (4) and (5).

Consider a possible counterexample  $G$  with 2-edge-coloring  $f$  and minimum  $N + s$ . If  $N - n_1 - n_2 \geq 3$ , then restriction (7) does not apply, so by Theorem 5,  $G$  has a monochromatic  $C_{2n}$ , a contradiction. If  $N - n_1 - n_2 \leq 2$  and (7) holds, then again by Theorem 5,  $G$  has a monochromatic  $C_{2n}$ . Hence we need to consider only the case that  $N - n_1 - n_2 \leq 2$ , all (1), (2), (4) and (5) hold, but (7) does not hold. In particular,  $n_1 \geq 2n - 1$ , but  $N \leq 4n - 2$ . This means  $N - n_1 \leq (4n - 2) - (2n - 1) = 2n - 1$ , so by (2),  $N = 4n - 2$  and  $n_1 = 2n - 1$ . If  $N - n_1 - n_2 \leq 1$ , this does not satisfy (5). Thus  $N - n_1 - n_2 = 2$ , and hence  $G \supseteq K_{2n-1, 2n-3, 2}$ . Therefore, the following lemma implies Theorem 6.

**Lemma 37.** *If  $n$  is sufficiently large, then for every 2-edge-coloring of  $K_{2n-1, 2n-3, 2}$ , there is a monochromatic cycle of length at least  $2n$ .*

*Proof.* The set-up of the proof is similar to the proof of Lemma 31. We only show the differences.

Let  $V_3 = \{u_1, u_2\}$ . Define  $V'_1 = V_1$  and  $V'_2 = V_2 \cup V_3$ . We first consider  $G[V'_1, V'_2]$  and then use the fact that  $V'_2 = V_2 \cup V_3$ . Note that we have  $|V'_1| = |V'_2| = 2n - 1$ .

By the proof in Lemma 31, we narrow the uncovered cases to (1)  $|A| = n - 1$  and  $n \leq |C| \leq (1 + 30\lambda')n$  and (2)  $n \leq |A| \leq (1 + 30\lambda')n$  and  $|C| = n - 1$ .

Case 1:  $|A| = n - 1$  and  $n \leq |C| \leq (1 + 30\lambda')n$ .

Then we know  $|B| = n$  and  $(1 - 30\lambda')n - 1 \leq |D| \leq n - 1$ . By Remark 34, we know the size of a maximum matching,  $\alpha'$ , in  $G_2[B, D]$  is at most 1. Let  $R$  be the set of vertices in  $C$  with at least  $0.8n$  red neighbors in  $B$ . By condition (ii),  $|R| \leq 2\lambda'n$ .

**Claim 38.** *If  $|C - R| \geq n$  then we find a blue cycle of length  $2n$  in  $G_2[B, C - R]$ .*

*Proof.* We pick  $C' \subseteq C - R$  of size  $n$ . We know:

- (1) By Remark 32 and the definition of  $R$ , each vertex in  $B$  has blue degree at least  $0.38n$  to  $C'$  and each vertex in  $C'$  has blue degree at least  $0.2n$  to  $B$ .
- (2) By condition (ii), all but at most  $20\lambda'n$  vertices in  $B$  have red degree at most  $0.05n$  to  $C'$  and all but at most  $20\lambda'n$  vertices in  $C$  have red degree at most  $0.05n$  to  $B$ .
- (3) If we order vertices in  $C'$  and  $B$  in nondecreasing order by their degree in  $G_2[C', B]$  respectively, then the smallest index with  $d(x_i) \leq i + 1$  and the smallest index with  $d(y_j) \leq j + 1$  satisfy  $d(x_i) \geq 0.95n$  and  $d(y_j) \geq 0.95n$ .

Since  $0.95n + 0.95n > n + 1$ , we can use Theorem 17 to show  $G_2[C', B]$  is Hamiltonian biconnected and thus we can find a cycle by fixing an edge  $e$  first and then find a Hamiltonian path in  $G_2[C', B]$  without  $e$ , which is still Hamiltonian biconnected.  $\square$

**Remark 39.** Similarly to Claim 38, we can show:

- (1) For any two vertices  $c_1 \in C$ ,  $a_1 \in A$ , graph  $G_1[A, C]$  has a red path of length  $2n - 3$  from  $c_1$  to  $a_1$ .
- (2) For any two vertices  $c_1, c_2 \in C$ , graph  $G_1[A, C]$  has a red path of length  $2n - 2$  from  $c_1$  to  $c_2$ .
- (3) For any two vertices  $b_1, b_2 \in B$ , graph  $G_2[B, C - R]$  has a blue path of length  $2n - 2$  from  $b_1$  to  $b_2$ .

- (4) For any two vertices  $c_1 \in C - R$ ,  $b_1 \in B$ , graph  $G_2[B, C - R]$  has a blue path of length  $2n - 3$  from  $c_1$  to  $b_1$ .

Therefore, we may assume

$$|C - R| \leq n - 1 \quad \text{and thus} \quad |D \cup R| \geq n. \quad (34)$$

If  $|R| \geq 2$ , say  $r_1, r_2 \in R$ , then we find a common neighbor  $r_b \in B$  for them. By Remark 39, we can find a red path  $P_1$  of length  $2n - 2$  in  $G_1[C, A]$  and then extend  $P_1$  to a red cycle of length  $2n$  by adding  $r_1 r_b r_2$ . Thus, we may assume

$$|C - R| = n - 1, \quad |R| = 1 \quad \text{and} \quad |D| = n - 1. \quad (35)$$

Let  $R = \{r\}$ . If  $\alpha' = 0$ , then  $G_1[B, D]$  is a complete bipartite graph. We can find a red cycle of length  $2n$  in  $G_1[B, D \cup R]$  by first fixing two neighbors in  $B$  for  $r$ .

If  $\alpha' = 1$ , say  $v_1 v_2$  is a maximum matching in  $G_2[B, D]$ , where  $v_1 \in B$  and  $v_2 \in D$ . If  $\{v_2\}$  is a minimum vertex cover, then  $v_2$  has at most one red edge to  $B$  since otherwise we find a red cycle by (35) in  $G_1[D \cup R, B]$  by first fixing two neighbors in  $B$  for  $v_2$ . Thus, we may assume  $v_2$  has at least  $|B| - 1$  blue edges to  $B$  and thus we can find a blue cycle in  $G_2[(C - R) \cup \{v_2\}, B]$  by Remark 39.

We may assume  $\{v_1\}$  is a minimum vertex cover. Note that  $v_1$  has at most one red edge to  $D$  since otherwise we find a red cycle in  $G_1[B, D \cup R]$  by first fixing two red neighbors for  $v_1$ . For the same reason, each vertex in  $A$  has at most one red edge to  $D$ . We use vertices in  $V_3$  to find a monochromatic cycle.

If there is a red edge from  $D$  to  $C - R$ , say  $u_1 y_1$  with  $u_1 \in D$  and  $y_1 \in C$ , then we find a red cycle of length at least  $2n$ . To do so, by Remark 39, we first find a red path  $P_1$  from  $y_1$  to  $r$  of length  $2n - 2$  in  $G_1[A, C]$ . Since  $r$  has at least  $0.8n$  red neighbors in  $B$  and  $G_1[B - \{v_1\}, D]$  is complete bipartite, we find for  $r$  and  $u_1$  a red common neighbor in  $B - \{v_1\}$ , say  $r_b$ . Finally, we extend  $P_1$  to a red cycle of length  $2n + 1$  by adding the red path  $rr_b u_1 y_1$ . Since at least one of  $u_1$  and  $u_2$  are not in  $R$ , say  $u_1 \notin R$ , we may assume there is a blue edge  $u_1 y_1$  from  $C - R$  to  $D$  with  $u_1 \in C - R$  and  $y_1 \in D$ .

We find a blue cycle of length at least  $2n$  by using  $u_1$ . To do so, by Remark 32, each vertex in  $D$  has blue degree at least  $0.38n$  to  $A \cup \{v_1\}$  and each vertex in  $C - R$  has blue degree at least  $0.2n - 1$  to  $B$ . We first fix a blue neighbor  $z_1$  of  $y_1$  with  $z_1 \in A$  and then find a common blue neighbor, say  $y_2 \in D - \{y_1\}$ , for  $v_1$  and  $z_1$ . We can find a blue path  $P_1$  of length  $2n - 3$  from  $u_1$  to  $v_1$  in  $G_2[C - R, B]$  by Remark 39 and then extend  $P_1$  by adding the path  $v_1 y_2 z_1 y_1 u_1$  to obtain a blue cycle of length  $2n + 1$ .

Case 2:  $n \leq |A| \leq (1 + 30\lambda')n$  and  $|C| = n - 1$ . It is symmetric to Case 1 until we use vertices in  $V_3$ . Thus, we may assume the maximum size of a matching in  $G_2[B, D]$  is 1,  $v_1 v_2$  is one maximum matching and  $\{v_2\}$  is a minimum vertex cover and every vertex in  $C \cup \{v_2\}$  has blue degree at least  $|B| - 1$  to  $B$ . Moreover, we may define  $R \subseteq A$  similarly to Case 1; i.e.,  $R$  is the collection of vertices in  $A$  with at least  $0.8n$  red degrees to  $D$ , and assume

$$|A - R| = n - 1, \quad |R| = 1 \quad \text{and} \quad |B| = n - 1. \quad (36)$$

Let  $R = \{r\}$ . If there is a red edge from  $C$  to  $D - \{v_2\}$ , say  $u_1 y_1$  with  $u_1 \in C$  and  $y_1 \in D$ , then we can find a red cycle of length at least  $2n$ . To do so, we first find a red path  $P_1$  of length  $2n - 3$  from  $u_1$  to  $r$

by Remark 39. Then we find a red neighbor  $r_d$  of  $r$  in  $D - \{v_2, y_1\}$  and a common red neighbor  $r_b$  of  $r_d$  and  $y_1$  in  $B$ . We extend the path  $P_1$  to a red cycle of length  $2n + 1$  by adding the red path  $rr_d r_b y_1 u_1$  to  $P_1$ .

Then we may assume there is a blue edge from  $C$  to  $D - \{v_2\}$ , say  $u_1 y_1$  with  $u_1 \in C$  and  $y_1 \in D - \{v_2\}$ . We first find a blue path of length  $2n - 2$  from  $y_1$  to  $v_2$  in  $G_2[A - R, D]$  by Remark 39 and then find a common blue neighbor  $y \in B$  for  $v_2$  and  $u_1$ . Finally, we add the path  $y_1 u_1 y v_2$  to  $P_1$  to obtain a blue cycle of length  $2n + 1$ .  $\square$

## 10. Proof of Theorem 7 on monochromatic $P_{2n}$

**10.1. A useful lemma.** If  $G$  contains a monochromatic  $C_{2n}$ , then it certainly contains a monochromatic  $P_{2n}$ . So suppose  $G = K_{n_1, \dots, n_s}$  does not have a monochromatic  $C_{2n}$ . The lemma below is very helpful here and in the next section.

**Lemma 40.** *Let  $s \geq 3$  and  $n$  be sufficiently large. Let  $n_1 \geq \dots \geq n_s$  and  $N = n_1 + \dots + n_s$  satisfy (1) and (2). Suppose that for some 2-edge-coloring  $f$  of the complete  $s$ -partite graph  $G = K_{n_1, \dots, n_s}$ , there are no monochromatic cycles  $C_{2n}$ . Then  $G$  contains a monochromatic  $P_{2n+1}$ .*

*Proof.* By Theorem 5, if (1) and (2) hold but  $G$  does not have a monochromatic  $C_{2n}$ , then (7) fails. In particular,  $N - n_1 - n_2 \leq 2$ . Since  $s \geq 3$ ,  $N - n_1 - n_2 \geq 1$ . We may assume  $s = 3$ : if  $s > 3$ , then  $N - n_1 - n_2 \leq 2$  yields  $s = 4$  and  $n_3 = n_4 = 1$ . In this case, deleting the edges between  $V_3$  and  $V_4$  and combining them into one part (of size 2) only makes the case harder.

We use condition (7) to find a monochromatic  $C_{2n}$  only in the nearly-bipartite subcase of Section 6: in Section 6.2. Therefore, if there is no monochromatic  $C_{2n}$ , but (1) and (2) hold, we have a graph  $G$  that falls under this subcase.

In this case, we have found disjoint subsets  $X_{11}, X_{12} \subseteq V_1$  and  $X_{21}, X_{22} \subseteq V_2$  with  $|X_{11}| = |X_{21}| = |X_{12}| = |X_{22}| = \frac{1}{2}n + 10$  satisfying the following property: if  $H$  is any of the graphs  $G_1[X_{11}, X_{21}]$ ,  $G_1[X_{12}, X_{22}]$ ,  $G_2[X_{12}, X_{21}]$ , or  $G_2[X_{11}, X_{22}]$ , then given any vertices  $v, w$  in  $H$ , we can find a  $(v, w)$ -path in  $H$  on  $m$  vertices, provided that  $n - 10 \leq m \leq n + 10$  and that the parity of  $m$  is correct.

Now let  $x \in V_3$  be an arbitrary vertex (since we know that  $1 \leq n_3 \leq 2$ ). Without loss of generality, we may assume that  $x$  has an edge in  $G_1$  to  $X_{11}$ . If  $x$  also has an edge in  $G_1$  to  $X_{12} \cup X_{22}$ , then we obtain a long path in  $G_1$  as follows:

- Let  $P_1$  be a path in  $G_1[X_{11}, X_{21}]$  of length at least  $n$  starting from a neighbor of  $x$  in  $X_{11}$ .
- Let  $P_2$  be a path in  $G_1[X_{12}, X_{22}]$  of length at least  $n$  starting from a neighbor of  $x$ .
- Use  $x$  to join  $P_1$  and  $P_2$  into a path.

Otherwise, all edges of  $x$  to  $X_{12} \cup X_{22}$  are in  $G_2$ ; in particular,  $x$  has a neighbor in  $G_2$  in both  $X_{12}$  and  $X_{22}$ . We obtain a long path in  $G_2$  in a similar way:

- Let  $P_1$  be a path in  $G_2[X_{12}, X_{21}]$  of length at least  $n$  starting from a neighbor of  $x$  in  $X_{12}$ .
- Let  $P_2$  be a path in  $G_2[X_{11}, X_{22}]$  of length at least  $n$  starting from a neighbor of  $x$  in  $X_{22}$ .
- Use  $x$  to join  $P_1$  and  $P_2$  into a path.

In either case,  $G$  contains a monochromatic  $P_{2n+1}$ .  $\square$

**10.2. Completion of the proof of Theorem 7.** As observed above, if  $G$  has a monochromatic  $C_{2n}$ , then we are done. Otherwise, by Theorem 5 and Lemma 40,  $G$  is bipartite. In this case, (2) yields  $n_2 \geq 2n - 1$ . Hence  $n_1 \geq 2n - 1$ , and  $G \supseteq K_{2n-1, 2n-1}$ . In this case, Theorem 2 yields the result.  $\square$

### 11. Proof of Theorem 8 on monochromatic $P_{2n+1}$

**11.1. Setup of the proof.** For large  $n$ , we need to prove the theorem for each complete  $s$ -partite graph  $G = K_{n_1, \dots, n_s}$  such that the numbers  $n_i$  satisfy  $n_1 \geq n_2 \geq \dots \geq n_s$  and the three conditions

$$N = n_1 + \dots + n_s \geq 3n, \quad (\text{T1}')$$

$$N - n_1 = n_2 + \dots + n_s \geq 2n - 1, \quad (\text{T2}')$$

$$\text{if } s = 2, \text{ then } n_1 \geq 2n + 1. \quad (\text{T3}')$$

For a given large  $n$ , we consider a possible counterexample with the minimum  $N + s$ . In view of this, it is enough to consider the lists  $(n_1, \dots, n_s)$  satisfying (T1'), (T2') and (T3') such that:

- (a) For each  $1 \leq j \leq s$ , if  $n_j > n_{j+1}$ , then the list  $(n_1, \dots, n_{j-1}, n_j - 1, n_{j+1}, \dots, n_s)$  does not satisfy some of (T1'), (T2') and (T3').
- (b) If  $s \geq 4$ , then the list  $(n_1, \dots, n_{s-2}, n_{s-1} + n_s)$  (possibly with the entries rearranged into a nonincreasing order) does not satisfy some of (T1'), (T2') and (T3').

Case 1:  $s \geq 3$  and  $N > 3n$ . Then (T3') holds by default. If  $n_1 > n_2$ , then the list  $(n_1 - 1, n_2, n_3, \dots, n_s)$  still satisfies the conditions (T1'), (T2') and (T3'), a contradiction to (a). Hence  $n_1 = n_2$ . Choose the maximum  $i$  such that  $n_1 = n_i$ . If  $N - n_1 > 2n - 1$ , consider the list  $(n_1, \dots, n_{i-1}, n_i - 1, n_{i+1}, \dots, n_s)$ . In this case (T1') and (T2') still are satisfied; so by (a), (T3') fails. But this means  $s = 3$  and  $n_1 = n_i = 1$ , so  $N \leq 3$ , a contradiction. Thus in this case  $N - n_1 = 2n - 1$ . Therefore,  $n_1 = N - (N - n_1) \geq 3n + 1 - (2n - 1) = n + 2$  and hence  $n_2 \geq n + 2$ , so  $N - n_1 - n_2 \leq (2n - 1) - (n + 2) = n - 3$ . Then the list  $(n_1, n_1, N - 2n_1)$  satisfies (T1')–(T3'). Summarizing, we get

$$\text{if } s \geq 3 \text{ and } N > 3n, \text{ then } s = 3, n_2 + n_3 = 2n - 1 \text{ and } n_1 = n_2 \geq n + 2. \quad (37)$$

Case 2:  $s \geq 3$  and  $N = 3n$ . Again (T3') holds by default. By (T2'),  $n_1 \leq n + 1$ ; hence  $N - n_1 - n_2 \geq n - 2$ . If  $s \geq 4$  and  $n_{s-1} + n_s \leq n + 1$ , then let  $L$  be the list obtained from  $(n_1, \dots, n_s)$  by replacing the two entries  $n_{s-1}$  and  $n_s$  with  $n_{s-1} + n_s$  and then possibly rearrange the entries into nonincreasing order. By construction,  $L$  satisfies (T1')–(T3'), a contradiction to (b). Hence  $n_{s-1} + n_s \geq n + 2$ . If  $s \geq 6$ , then  $N \geq 3(n_{s-1} + n_s) \geq 3n + 6$ , contradicting  $N = 3n$ . Thus

$$\text{if } s \geq 3 \text{ and } N = 3n, \text{ then } s \leq 5 \quad \text{and} \quad \text{if } s \geq 4, \text{ then } n_{s-1} + n_s \geq n + 2. \quad (38)$$

Case 3:  $s = 2$ . Then by (T3'),  $n_1 \geq 2n + 1$  and by (T2'),  $n_2 \geq 2n - 1$ . Thus  $G \supseteq K_{2n+1, 2n-1}$ , and we can assume that

$$\text{if } s = 2, \text{ then } G = K_{2n+1, 2n-1}. \quad (39)$$

As we have seen, always  $s \leq 5$ .

**11.2. Completion of the proof.** Suppose  $G$  satisfies (37)–(39), and  $f$  is a 2-edge-coloring  $G$  such that there is no monochromatic  $P_{2n+1}$ .

If  $G$  has no monochromatic  $C_{2n}$ , then by Lemma 40,  $G$  is bipartite. So by (39),  $G = K_{2n+1, 2n-1}$ . But by Lemma 31,  $K_{2n, 2n-1} \mapsto (C_{2n}, C_{2n})$ . Therefore, below we assume that the 2-edge-coloring  $f$  of  $G$  is such that  $G$  contains a red cycle  $C$  with  $2n$  vertices (i.e.,  $G_1$  contains  $C$ ).

Let  $V' = V(C)$  and  $V'' = V(G) - V'$ . Similarly, for  $j = 1, \dots, s$ , let  $V'_j = V_j \cap C$  and  $V''_j = V_j - V'_j$ . If some red edge  $e$  connects  $V'$  with  $V''$ , then  $C + e$  contains a red  $P_{2n+1}$ , so below we assume that

$$\text{all the edges in } G[V', V''] \text{ are blue, i.e., } G_2[V', V''] = G[V', V'']. \quad (40)$$

Case 1:  $s = 2$ . Then  $|V'_1| = |V'_2| = n$ . By (39),  $|V''_1| = n + 1$ . By (40),  $G_2[V''_1, V'_2] = K_{n+1, n}$ , but  $K_{n+1, n}$  contains  $P_{2n+1}$ .

Case 2:  $s \geq 3$  and  $n_1 \geq n$ . If  $V_1 \supseteq V''$ , then (since  $|V''| \geq n$  by (38))

$$G_2[V'', V(G) - V_1] = G[V'', V(G) - V_1] = K_{n, N-n_1} \supseteq K_{n, 2n-1} \supseteq P_{2n+1}.$$

Because  $C$  is a cycle of length  $2n$  and  $V'_1$  is an independent set,  $|V'_1| \leq n$ . In particular, since  $s \geq 3$ ,

there are distinct  $2 \leq j_1, j_2 \leq s$  such that there are vertices  $v_1 \in V'_{j_1}$  and  $v_2 \in V''_{j_2}$ .

If  $|V''_1| \geq n$ , then  $G_2[V''_1, V' - V'_1]$  is a complete bipartite graph with parts of size at least  $n$ , so it contains a path  $P$  with  $2n$  vertices, starting from  $v_1$ . Adding to it edge  $v_1 v_2$ , we get a blue  $P_{2n+1}$ .

Suppose now  $|V''_1| \leq n - 1$ . Then the complete bipartite graph  $G_2[V''_1, V' - V'_1]$  has a path  $Q_1$  with  $2|V''_1| + 1$  vertices starting from  $v_1$  and ending in  $V' - V_1$ . Also since  $n_1 \geq n$  and  $|V''| \geq n$ , the complete bipartite graph  $G[V'_1, V'' - V_1]$  contains  $K_{n-|V''_1|, n-|V''_1|}$  and hence contains a path  $Q_2$  with  $2(n - |V''_1|)$  vertices starting from  $v_2$ . Then connecting  $Q_1$  with  $Q_2$  by the edge  $v_1 v_2$  we create a  $P_{2n+1}$ .

Case 3:  $s \geq 3$  and  $n_1 \leq n - 1$ . In this case,  $N/n_1 > 3$ , so  $s \geq 4$ . Then (37)–(39) imply that  $N = 3n$  and  $4 \leq s \leq 5$ . In particular,

$$N - n_i \geq 3n - (n - 1) = 2n + 1 \quad \text{for every } 1 \leq i \leq s. \quad (41)$$

Relabel the  $V_i$ 's so that  $|V''_1| \geq \dots \geq |V''_s|$ . Let  $s'$  be the largest  $i$  such that  $V''_i \neq \emptyset$ . We construct a path  $Q$  with  $2n + 1$  vertices greedily in two stages.

Stage 1: For  $i = 1, \dots, s' - 1$ , find a vertex  $w_i \in V' - V_i - V_{i+1}$  so that all  $s' - 1$  of them are distinct. We can do it because  $V''_i$  and  $V''_{i+1}$  are nonempty, so

$$|V'_i \cup V'_{i+1}| \leq (n_i - 1) + (n_{i+1} - 1) \leq 2n - 4 = |V'| - 4.$$

At least four choices for each of the  $s' - 1 \leq 4$  vertices  $w_i$  allow us to choose them all distinct. Then we choose  $w_0 \in V' - V_1$  and  $w_{s'} \in V' - V_{s'}$  so that all  $w_0, \dots, w_{s'}$  are distinct.

Stage 2: For  $i = 0, \dots, s' - 1$  we find a  $(w_i, w_{i+1})$ -path  $Q_i$  such that (i)  $V(Q_i) \cap V'' = V''_{i+1}$ , and (ii) all paths  $Q_0, \dots, Q_{s'-1}$  are internally disjoint.

If we succeed, then  $\bigcup_{i=0}^{s'-1} Q_i$  is a path that we are seeking.

Suppose we are constructing  $Q_i$  and  $V''_{i+1} = \{u_1, \dots, u_q\}$ . We start  $Q_i$  by the edge  $w_i u_1$ . Then on Step  $j$  for  $j = 1, \dots, q$ , do as follows.

If  $j = q$ , then add edge  $u_q w_{i+1}$  and finish  $Q_i$ . Otherwise, find a vertex  $z_j \in V' - V_{i+1}$  not yet used in any  $Q_{i'}$ , then add to  $Q_i$  edges  $u_j z_j$  and  $z_j u_{j+1}$ , and then go to Step  $j + 1$ . We can find this  $z_j$  because by (41),  $|V - V_i| \geq 2n + 1$ , at most  $n - 2$  of these vertices are in  $V''$ , and at most  $n$  vertices of all paths  $Q_{i'}$  are already chosen in  $V'$ . Since we always can choose  $z_j$ , our greedy procedure constructs  $Q_i$ , and all  $Q_i$  together form the promised path  $Q$ .  $\square$

### Acknowledgments

We thank Louis DeBiasio for helpful discussions and a referee for detailed and useful comments.

### References

- [Balogh et al. 2019] J. Balogh, A. Kostochka, M. Lavrov, and X. Liu, “Monochromatic connected matchings in 2-edge-colored multipartite graphs”, preprint, 2019. arXiv
- [Benevides and Skokan 2009] F. S. Benevides and J. Skokan, “The 3-colored Ramsey number of even cycles”, *J. Combin. Theory Ser. B* **99**:4 (2009), 690–708. MR Zbl
- [Benevides et al. 2012] F. S. Benevides, T. Łuczak, A. Scott, J. Skokan, and M. White, “Monochromatic cycles in 2-coloured graphs”, *Combin. Probab. Comput.* **21**:1-2 (2012), 57–87. MR Zbl
- [Berge 1976] C. Berge, *Graphs and hypergraphs*, North-Holland Mathematical Library **6**, North-Holland, Amsterdam, 1976. MR Zbl
- [Bondy and Erdős 1973] J. A. Bondy and P. Erdős, “Ramsey numbers for cycles in graphs”, *J. Combinatorial Theory Ser. B* **14** (1973), 46–54. MR Zbl
- [Bucić et al. 2019a] M. Bucić, S. Letzter, and B. Sudakov, “3-color bipartite Ramsey number of cycles and paths”, *J. Graph Theory* **92**:4 (2019), 445–459. MR
- [Bucić et al. 2019b] M. Bucić, S. Letzter, and B. Sudakov, “Multicolour bipartite Ramsey number of paths”, *Electron. J. Combin.* **26**:3 (2019), art. id. P3.60. MR Zbl
- [Chvátal 1972] V. Chvátal, “On Hamilton’s ideals”, *J. Combinatorial Theory Ser. B* **12** (1972), 163–168. MR Zbl
- [DeBiasio and Krueger 2018] L. DeBiasio and R. A. Krueger, “Long monochromatic paths and cycles in 2-colored bipartite graphs”, preprint, 2018. arXiv
- [DeBiasio et al. 2020] L. DeBiasio, A. Gyárfás, R. A. Krueger, M. Ruszinkó, and G. N. Sárközy, “Monochromatic balanced components, matchings, and paths in multicolored complete bipartite graphs”, *J. Comb.* **11**:1 (2020), 35–45. MR Zbl
- [Faudree and Schelp 1974] R. J. Faudree and R. H. Schelp, “All Ramsey numbers for cycles in graphs”, *Discrete Math.* **8** (1974), 313–329. MR Zbl
- [Faudree and Schelp 1975] R. J. Faudree and R. H. Schelp, “Path-path Ramsey-type numbers for the complete bipartite graph”, *J. Combinatorial Theory Ser. B* **19**:2 (1975), 161–173. MR Zbl
- [Figaj and Łuczak 2007] A. Figaj and T. Łuczak, “The Ramsey number for a triple of long even cycles”, *J. Combin. Theory Ser. B* **97**:4 (2007), 584–596. MR Zbl
- [Figaj and Łuczak 2018] A. Figaj and T. Łuczak, “The Ramsey numbers for a triple of long cycles”, *Combinatorica* **38**:4 (2018), 827–845. MR Zbl
- [Gerencsér and Gyárfás 1967] L. Gerencsér and A. Gyárfás, “On Ramsey-type problems”, *Ann. Univ. Sci. Budapest. Eötvös Sect. Math.* **10** (1967), 167–170. MR Zbl
- [Gyárfás and Lehel 1973] A. Gyárfás and J. Lehel, “A Ramsey-type problem in directed and bipartite graphs”, *Period. Math. Hungar.* **3**:3-4 (1973), 299–304. MR Zbl
- [Gyárfás et al. 2007a] A. Gyárfás, M. Ruszinkó, G. N. Sárközy, and E. Szemerédi, “Three-color Ramsey numbers for paths”, *Combinatorica* **27**:1 (2007), 35–69. Correction in **28**:4 (2008), 499–502. MR Zbl
- [Gyárfás et al. 2007b] A. Gyárfás, M. Ruszinkó, G. N. Sárközy, and E. Szemerédi, “Tripartite Ramsey numbers for paths”, *J. Graph Theory* **55**:2 (2007), 164–174. MR Zbl

- [Knierim and Su 2019] C. Knierim and P. Su, “Improved bounds on the multicolor Ramsey numbers of paths and even cycles”, *Electron. J. Combin.* **26**:1 (2019), art. id. P1.26. MR Zbl
- [Las Vergnas 1970] M. Las Vergnas, “Sur l’existence de cycles hamiltoniens dans un graphe”, *C. R. Acad. Sci. Paris Sér. A* **270** (1970), 1361–1364. MR Zbl
- [Łuczak 1999] T. Łuczak, “ $R(C_n, C_n, C_n) \leq (4 + o(1))n$ ”, *J. Combin. Theory Ser. B* **75**:2 (1999), 174–187. MR Zbl
- [Łuczak et al. 2012] T. Łuczak, M. Simonovits, and J. Skokan, “On the multi-colored Ramsey numbers of cycles”, *J. Graph Theory* **69**:2 (2012), 169–175. MR Zbl
- [Sárközy 2016] G. N. Sárközy, “On the multi-colored Ramsey numbers of paths and even cycles”, *Electron. J. Combin.* **23**:3 (2016), art. id. P3.53. MR Zbl
- [Szemerédi 1978] E. Szemerédi, “Regular partitions of graphs”, pp. 399–401 in *Problèmes combinatoires et théorie des graphes* (Orsay, 1976), Colloq. Internat. CNRS **260**, CNRS, Paris, 1978. MR Zbl
- [Zhang et al. 2013] R. Zhang, Y. Sun, and Y. Wu, “The bipartite Ramsey numbers  $b(C_{2m}; C_{2n})$ ”, *World Acad. Sci. Eng. Tech.* **7**:1 (2013), 152–155.

Received 12 May 2019. Revised 8 Jan 2020.

JÓZSEF BALOGH:

jobal@illinois.edu

Department of Mathematics, University of Illinois, Urbana, IL, United States

and

Moscow Institute of Physics and Technology, Dolgoprudny, Russia

ALEXANDR KOSTOCHKA:

kostochk@math.uiuc.edu

Department of Mathematics, University of Illinois, Urbana, IL, United States

and

Sobolev Institute of Mathematics, Novosibirsk, Russia

MIKHAIL LAVROV:

mlavrov@illinois.edu

Department of Mathematics, University of Illinois, Urbana, IL, United States

XUJUN LIU:

xliu150@illinois.edu

Department of Mathematics, University of Illinois, Urbana, IL, United States

## Guidelines for Authors

Authors may submit manuscripts in PDF format on-line at the submission page.

**Originality.** Submission of a manuscript acknowledges that the manuscript is original and is not, in whole or in part, published or under consideration for publication elsewhere. It is understood also that the manuscript will not be submitted elsewhere while under consideration for publication in this journal.

**Language.** Articles are usually in English or French, but articles written in other languages are welcome.

**Required items.** A brief abstract of about 150 words or less must be included. It should be self-contained and not refer to bibliography keys. If the article is not in English, two versions of the abstract must be included, one in the language of the article and one in English. Also required are keywords and a Mathematics Subject Classification for the article, and, for each author, affiliation (if appropriate) and email address.

**Format.** Authors are encouraged to use  $\text{\LaTeX}$  and the standard `amsart` class, but submissions in other varieties of  $\text{\TeX}$ , and exceptionally in other formats, are acceptable. Initial uploads should normally be in PDF format; after the refereeing process we will ask you to submit all source material.

**References.** Bibliographical references should be complete, including article titles and page ranges. All references in the bibliography should be cited in the text. The use of  $\text{\BIBTeX}$  is preferred but not required. Tags will be converted to the house format, however, for submission you may use the format of your choice. Links will be provided to all literature with known web locations and authors are encouraged to provide their own links in addition to those supplied in the editorial process.

**Figures.** Figures must be of publication quality. After acceptance, you will need to submit the original source files in vector graphics format for all diagrams in your manuscript: vector EPS or vector PDF files are the most useful.

Most drawing and graphing packages — Mathematica, Adobe Illustrator, Corel Draw, MATLAB, etc. — allow the user to save files in one of these formats. Make sure that what you are saving is vector graphics and not a bitmap. If you need help, please write to [graphics@msp.org](mailto:graphics@msp.org) with as many details as you can about how your graphics were generated.

Bundle your figure files into a single archive (using zip, tar, rar or other format of your choice) and upload on the link you been provided at acceptance time. Each figure should be captioned and numbered so that it can float. Small figures occupying no more than three lines of vertical space can be kept in the text (“the curve looks like this:”). It is acceptable to submit a manuscript with all figures at the end, if their placement is specified in the text by means of comments such as “Place Figure 1 here”. The same considerations apply to tables.

**White Space.** Forced line breaks or page breaks should not be inserted in the document. There is no point in your trying to optimize line and page breaks in the original manuscript. The manuscript will be reformatted to use the journal’s preferred fonts and layout.

**Proofs.** Page proofs will be made available to authors (or to the designated corresponding author) at a Web site in PDF format. Failure to acknowledge the receipt of proofs or to return corrections within the requested deadline may cause publication to be postponed.

Complete generalized Fibonacci sequences modulo primes MOHAMMAD JAVAHERI and NIKOLAI A. KRYLOV	1
Discretized sum-product for large sets CHANGHAO CHEN	17
Positive semigroups and generalized Frobenius numbers over totally real number fields LENNY FUKSHANSKY and YINGQI SHI	29
The sum-of-digits function on arithmetic progressions LUKAS SPIEGELHOFER and THOMAS STOLL	43
A convexity criterion for unique ergodicity of interval exchange transformations RENÉ RÜHR	51
Long monochromatic paths and cycles in 2-edge-colored multipartite graphs JÓZSEF BALOGH, ALEXANDR KOSTOCHKA, MIKHAIL LAVROV and XUJUN LIU	55