

Membership in random ratio sets

*Original*

Membership in random ratio sets / Sanna, Carlo. - In: INDAGATIONES MATHEMATICAE. - ISSN 0019-3577. - 33:6(2022), pp. 1326-1333. [10.1016/j.indag.2022.08.007]

*Availability:*

This version is available at: 11583/2971803 since: 2022-09-28T06:27:16Z

*Publisher:*

Elsevier

*Published*

DOI:10.1016/j.indag.2022.08.007

*Terms of use:*

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

*Publisher copyright*

(Article begins on next page)

# MEMBERSHIP IN RANDOM RATIO SETS

CARLO SANNA<sup>†</sup>

ABSTRACT. Let  $\mathcal{A}$  be a random set constructed by picking independently each element of  $\{1, \dots, n\}$  with probability  $\alpha \in (0, 1)$ . We give a formula for the probability that a rational number  $q$  belong to the random ratio set  $\mathcal{A}/\mathcal{A} := \{a/b : a, b \in \mathcal{A}\}$ . This generalizes a previous result of Cilleruelo and Guijarro-Ordóñez. Moreover, we make some considerations about formulas for the probability of the event  $\bigvee_{i=1}^k (q_i \in \mathcal{A}/\mathcal{A})$ , where  $q_1, \dots, q_k$  are rational numbers, showing that they are related to the study of the connected components of certain graphs. In particular, we give formulas for the probability that  $q^e \in \mathcal{A}/\mathcal{A}$  for some  $e \in \mathcal{E}$ , where  $\mathcal{E}$  is a finite or cofinite set of positive integers with  $1 \in \mathcal{E}$ .

## 1. INTRODUCTION

For every positive integer  $n$  and for every  $\alpha \in (0, 1)$ , let  $\mathcal{B}(n, \alpha)$  denote the probabilistic model in which a random set  $\mathcal{A} \subseteq \{1, \dots, n\}$  is constructed by picking independently every element of  $\{1, \dots, n\}$  with probability  $\alpha$ . Several authors studied number-theoretic objects involving random sets in this probabilistic model, including: the least common multiple  $\text{lcm}(\mathcal{A})$  [1, 4] (see also [8]), the product set  $\mathcal{A}\mathcal{A} := \{ab : a, b \in \mathcal{A}\}$  [3, 6, 7], and the ratio set  $\mathcal{A}/\mathcal{A} := \{a/b : a, b \in \mathcal{A}\}$  [2, 3].

Regarding random ratio sets, Cilleruelo and Guijarro-Ordóñez [2] proved the following:

**Theorem 1.1.** *Let  $\mathcal{A}$  be a random set in  $\mathcal{B}(n, \alpha)$ . Then, for  $\alpha$  fixed and  $n \rightarrow +\infty$ , we have*

$$|\mathcal{A}/\mathcal{A}| \sim \frac{6}{\pi^2} \cdot \frac{\alpha^2 \text{Li}_2(1 - \alpha^2)}{1 - \alpha^2} \cdot n^2,$$

with probability  $1 - o(1)$ , where  $\text{Li}_2(z) := \sum_{k=1}^{\infty} z^k/k^2$  is the dilogarithm function.

A fundamental step in the proof of Theorem 1.1 is determining a formula for the probability that certain rational numbers belong to  $\mathcal{A}/\mathcal{A}$ . Precisely, Cilleruelo and Guijarro-Ordóñez [2, Eq. (2)] showed that for all positive integers  $r < s$ , with  $(r, s) = 1$  and  $s > n^{1/2}$ , we have

$$\mathbb{P}(r/s \in \mathcal{A}/\mathcal{A}) = 1 - (1 - \alpha^2)^{\lfloor n/s \rfloor}.$$

Note that the assumption  $r < s$  is not restrictive, since  $r/s \in \mathcal{A}/\mathcal{A}$  if and only if  $s/r \in \mathcal{A}/\mathcal{A}$ , while the assumption  $s > n^{1/2}$  is indeed a restriction.

Our first result is a general formula for the probability that a rational number belongs to the ratio set  $\mathcal{A}/\mathcal{A}$ .

**Theorem 1.2.** *Let  $\mathcal{A}$  be a random set in  $\mathcal{B}(n, \alpha)$ . Then we have*

$$(1) \quad \mathbb{P}(r/s \in \mathcal{A}/\mathcal{A}) = 1 - \prod_{i=1}^{\lfloor \frac{\log n}{\log s} \rfloor} \gamma_i^{\lfloor n/s^i \rfloor},$$

for all positive integers  $r < s$  with  $(r, s) = 1$ , where  $\gamma_i := \beta_{i-1}\beta_{i+1}/\beta_i^2$  with  $\beta_0 := 1$ ,  $\beta_1 := 1$ , and  $\beta_{i+1} := (1 - \alpha)\beta_i + \alpha(1 - \alpha)\beta_{i-1}$ , for all integers  $i \geq 1$ .

*Remark 1.1.* If  $\alpha = 1/2$  then for all integers  $i \geq 0$  we have  $\beta_i = F_{i+2}/2^i$ , where  $\{F_i\}_{i=0}^{\infty}$  is the sequence of Fibonacci numbers, defined recursively by  $F_0 := 0$ ,  $F_1 := 1$ , and  $F_{i+2} := F_{i+1} + F_i$ .

2010 *Mathematics Subject Classification.* Primary: 11N25, Secondary: 11K99.

*Key words and phrases.* probability, random set, ratio set.

<sup>†</sup>C. Sanna is a member of GNSAGA of INdAM and of CryptTO, the group of Cryptography and Number Theory of Politecnico di Torino.

As a consequence of Theorem 1.2, we obtain the following corollary:

**Corollary 1.1.** *Let  $\mathcal{A}$  be a random set in  $\mathcal{B}(n, \alpha)$ . Then we have*

$$(2) \quad \mathbb{P}(r/s \in \mathcal{A}/\mathcal{A}) = 1 - \exp(-\delta(s)n + O_\alpha(1)),$$

for all positive integers  $r < s \leq n$  with  $(r, s) = 1$ , where

$$(3) \quad \delta(s) := \sum_{i=1}^{\infty} \frac{\log(1/\gamma_i)}{s^i}$$

is an absolutely convergent series.

It is natural to ask if Theorem 1.2 can be generalized to a formula for the probability of the event  $\bigvee_{i=1}^k (r_i/s_i \in \mathcal{A}/\mathcal{A})$ , where  $r_1/s_1, \dots, r_k/s_k$  are rational numbers. The answer should be “yes”, but the task seems very complex (see Section 6 for more details).

However, we proved the following result concerning powers of the same rational number.

**Theorem 1.3.** *Let  $\mathcal{A}$  be a random set in  $\mathcal{B}(n, \alpha)$ , and let  $\mathcal{E}$  be a finite or cofinite set of positive integers with  $1 \in \mathcal{E}$ . Then we have*

$$(4) \quad \mathbb{P}\left(\bigvee_{e \in \mathcal{E}} ((r/s)^e \in \mathcal{A}/\mathcal{A})\right) = 1 - \prod_{i=1}^{\lfloor \frac{\log n}{\log s} \rfloor} \left(\gamma_i^{(\mathcal{E})}\right)^{\lfloor n/s^i \rfloor},$$

for all positive integers  $r < s$  with  $(r, s) = 1$ , where  $\gamma_i^{(\mathcal{E})} := \beta_{i-1}^{(\mathcal{E})}\beta_{i+1}^{(\mathcal{E})}/(\beta_i^{(\mathcal{E})})^2$ , for all integers  $i \geq 1$ , and  $\{\beta_j^{(\mathcal{E})}\}_{j=0}^{\infty}$  is a linear recurrence depending only on  $\mathcal{E}$  and  $\alpha$ . In particular, if  $\mathcal{E}$  is cofinite then  $\gamma_i^{(\mathcal{E})}$  is a rational function of  $i$ , for all sufficiently large  $i$ .

As a matter of example, we provide the following:

*Example 1.1.*  $\beta_0^{\{1,2\}} = 1$ ,  $\beta_1^{\{1,2\}} = 1$ ,  $\beta_2^{\{1,2\}} = 1 - \alpha^2$ , and

$$\beta_i^{\{1,2\}} = (1 - \alpha)\beta_{i-1}^{\{1,2\}} + \alpha(1 - \alpha)^2\beta_{i-3}^{\{1,2\}}$$

for all integers  $i \geq 3$ .

*Example 1.2.*  $\beta_0^{\{1,3\}} = 1$ ,  $\beta_1^{\{1,3\}} = 1$ ,  $\beta_2^{\{1,3\}} = 1 - \alpha^2$ ,  $\beta_3^{\{1,3\}} = 1 - 2\alpha^2 + \alpha^3$ , and

$$\beta_i^{\{1,3\}} = (1 - \alpha)\beta_{i-1}^{\{1,3\}} + \alpha(1 - \alpha)\beta_{i-2}^{\{1,3\}} - \alpha(1 - \alpha)^2\beta_{i-3}^{\{1,3\}} + \alpha(1 - \alpha)^3\beta_{i-4}^{\{1,3\}}$$

for all integers  $i \geq 4$ .

*Example 1.3.*  $\beta_i^{(\mathbb{N})} = (1 - \alpha)^{i-1}((1 - \alpha) + i\alpha)$  and

$$\gamma_i^{(\mathbb{N})} = 1 - \frac{1}{(i + \alpha^{-1} - 1)^2}$$

for all integers  $i \geq 1$ .

*Example 1.4.*  $\beta_i^{\mathbb{N} \setminus \{2\}} = (1 - \alpha)^{i-2}((1 - \alpha)^2 + i\alpha(1 - \alpha) + (i - 2)\alpha^2)$  and

$$\gamma_i^{\mathbb{N} \setminus \{2\}} = 1 - \frac{1}{(i + \alpha^{-1} - \alpha - 2)^2}$$

for all integers  $i \geq 3$ .

## 2. NOTATION

We employ the Landau–Bachmann “Big Oh” notation  $O$  with its usual meaning. Any dependence of implied constants is explicitly stated or indicated with subscripts. Greek letters are reserved for quantities that depends on  $\alpha$ .



Therefore, also using (6), we have

$$\begin{aligned}
(7) \quad \mathbb{P}(r/s \notin \mathcal{A}/\mathcal{A}) &= \prod_{i=1}^k \prod_{\substack{m_1 \rightarrow \dots \rightarrow m_i \\ \text{con. com. of } \mathcal{G}(n; r, s)}} \mathbb{P}(E(m_1, m_2) \wedge \dots \wedge E(m_{i-1}, m_i)) \\
&= \prod_{i=1}^k \beta_i^{c_i} = \prod_{i=1}^k \beta_i^{d_i - 2d_{i+1} + d_{i+2}} = \prod_{i=1}^{k-1} \left( \frac{\beta_{i-1} \beta_{i+1}}{\beta_i^2} \right)^{d_{i+1}} = \prod_{i=1}^{\lfloor \frac{\log n}{\log s} \rfloor} \gamma_i^{\lfloor n/s^i \rfloor},
\end{aligned}$$

and (1) follows. The proof is complete.

#### 4. PROOF OF COROLLARY 1.1

Throughout this section, implied constants may depend on  $\alpha$ . Let  $\rho_1, \rho_2$  be the roots of the characteristic polynomial  $X^2 - (1 - \alpha)X - \alpha(1 - \alpha)$  of the linear recurrence  $\{\beta_i\}_{i=0}^\infty$ . Recalling that  $\alpha \in (0, 1)$ , an easy computation shows that  $|\rho_1| \neq |\rho_2|$ . Without loss of generality, assume  $|\rho_1| > |\rho_2|$  and put  $\varrho := |\rho_2/\rho_1|$ , so that  $\varrho \in (0, 1)$ . Hence, there exist complex numbers  $\zeta_1, \zeta_2$  such that

$$\beta_i = \zeta_1 \rho_1^i + \zeta_2 \rho_2^i = \zeta_1 \rho_1^i (1 + O(\varrho^i)),$$

for every integer  $i \geq 0$ . Consequently, we have

$$\gamma_i = \frac{\beta_{i-1} \beta_{i+1}}{\beta_i^2} = \frac{\zeta_1 \rho_1^{i-1} (1 + O(\varrho^{i-1})) \zeta_1 \rho_1^{i+1} (1 + O(\varrho^{i+1}))}{(\zeta_1 \rho_1^i (1 + O(\varrho^i)))^2} = 1 + O(\varrho^i),$$

and  $\log \gamma_i = O(\varrho^i)$ , for every sufficiently large integer  $i$ . In particular, it follows that (3) is an absolutely convergent series.

Now put  $\ell := \lfloor \log n / \log s \rfloor$ . From Theorem 1.2, we get that

$$\mathbb{P}(r/s \in \mathcal{A}/\mathcal{A}) = 1 - e^L,$$

where

$$\begin{aligned}
L &:= \sum_{i=1}^{\ell} \left\lfloor \frac{n}{s^i} \right\rfloor \log \gamma_i = \sum_{i=1}^{\ell} \frac{\log \gamma_i}{s^i} n + O\left( \sum_{i>\ell} \frac{|\log \gamma_i|}{s^i} n \right) + O\left( \sum_{i=1}^{\ell} |\log \gamma_i| \right) \\
&= -\delta(s)n + O\left( \frac{n}{s^{\ell+1}} \right) + O\left( \sum_{i=1}^{\ell} \varrho^i \right) = -\delta(s)n + O(1),
\end{aligned}$$

as desired. The proof is complete.

*Remark 4.1.* A more detailed analysis shows that  $\{\gamma_i^{(-1)^i}\}_{i=1}^\infty$  is a strictly decreasing sequence tending to 1. In particular, (3) is an alternating series.

#### 5. PROOF OF THEOREM 1.3

Let us define the directed graph  $\mathcal{G}^{(\mathcal{E})}(n; r, s) := \bigcup_{e \in \mathcal{E}} \mathcal{G}(n; r^e, s^e)$ . For an example, see Figure 2.

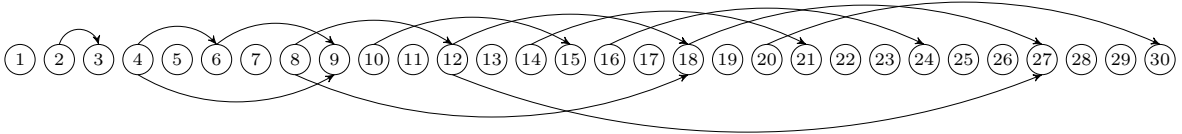


FIGURE 2. The directed graph  $\mathcal{G}^{\{1,2\}}(30; 2, 3)$ .

Since  $1 \in \mathcal{E}$ , it is easy to check that  $\mathcal{G}^{(\mathcal{E})}(n; r, s)$  is the graph obtained from  $\mathcal{G}(n; r, s)$  by adding a directed edge  $v_1 \rightarrow v_2$  between each pair  $v_1 < v_2$  of vertices of  $\mathcal{G}(n; r, s)$  that

have distance  $e$ , for every  $e \in \mathcal{E}$ . In particular, this process connects only vertices that are already connected. Hence, the number of connected components of  $\mathcal{G}^{(\mathcal{E})}(n; r, s)$  that have exactly  $i$  vertices is equal to the number of connected components of  $\mathcal{G}(n; r, s)$  that have exactly  $i$  vertices, which is the number  $c_i$  that we already determined in the proof of Theorem 1.2. Moreover, the probability that a connected component of  $\mathcal{G}^{(\mathcal{E})}(n; r, s)$  having exactly  $i$  vertices has no adjacent vertices both belonging to  $\mathcal{A}$  is equal to the probability  $\beta_i^{(\mathcal{E})}$  that the random binary string  $\chi_1 \cdots \chi_i$  does not contain the substring  $10^{e-1}1$ , for all  $e \in \mathcal{E}$ , where  $\{\chi_k\}_{k=1}^\infty$  is a sequence of independent identically distributed random variables in  $\{0, 1\}$  with  $\mathbb{P}(\chi_k = 1) = \alpha$ . At this point the same reasonings of (7) yield (4). Let us prove that  $\{\beta_i^{(\mathcal{E})}\}_{i=0}^\infty$  is a linear recurrence.

Suppose that  $\mathcal{E}$  is finite and let  $m := \max(\mathcal{E}) + 1$ . Then  $\beta_i^{(\mathcal{E})}$  can be determined by considering a Markov chain. The states are the binary strings  $x_1 \cdots x_m \in \{0, 1\}^m$  not containing the substring  $10^{e-1}1$ , for every  $e \in \mathcal{E}$ , and one absorbing state. A transition from state  $x_1 \cdots x_m$  to state  $x_2 \cdots x_{m-1}1$ , respectively from state  $x_1 \cdots x_m$  to state  $x_2 \cdots x_{m-1}0$ , happens with probability  $\alpha$ , respectively  $1 - \alpha$ , and all the other transitions are to the absorbing state. Finally, the probability of  $x_1 \cdots x_m$  being the initial state is  $\alpha^{x_1 + \cdots + x_m} (1 - \alpha)^{m - (x_1 + \cdots + x_m)}$ . Therefore, letting  $u$  be the number of states, we have that  $\beta_i^{(\mathcal{E})} = \boldsymbol{\pi} \boldsymbol{\Sigma}^i (1, 1, \dots, 1, 0)^t$  for all integers  $i \geq 0$ , where  $\boldsymbol{\pi}$  is a row vector of length  $u$ ,  $\boldsymbol{\Sigma}$  is a  $u \times u$  stochastic matrix, and  $(1, 1, \dots, 1, 0)^t$  is column vector of length  $t$ , assuming the states are ordered so that the absorbing state is the last one. Consequently,  $\{\beta_i^{(\mathcal{E})}\}_{i=0}^\infty$  is a linear recurrence whose characteristic polynomial is given by the characteristic polynomial of  $\boldsymbol{\Sigma}$ .

Now suppose that  $\mathcal{E}$  is cofinite and let  $\ell$  be the minimal positive integer such that  $e \in \mathcal{E}$  for all integers  $e \geq \ell$ . If  $\chi_1 \cdots \chi_i$  does not contain  $10^{e-1}1$ , for every  $e \in \mathcal{E}$ , then the distance between each pair of 1s in  $\chi_1 \cdots \chi_i$  is less than  $\ell$  positions. In particular, the number of 1s in  $\chi_1 \cdots \chi_i$  is at most  $\ell + 1$ . Therefore, for  $i \geq \ell + 1$ , by elementary probability calculus we can write  $\beta_i^{(\mathcal{E})}$  as a linear combination, whose coefficients do not depend on  $i$ , of the power sums  $(i - k + 1)(1 - \alpha)^{i - k}$  where  $k = 0, \dots, \ell + 1$ . Consequently,  $\beta_i^{(\mathcal{E})} = (1 - \alpha)^{i - \ell - 1} B^{(\mathcal{E})}(i)$  for some  $B^{(\mathcal{E})}(X) \in \mathbb{R}[X]$ . Hence,  $\{\beta_i^{(\mathcal{E})}\}_{i=0}^\infty$  is a linear recurrence and  $\gamma_i^{(\mathcal{E})} = B(i - 1)B(i + 1)/B(i)^2$  is a rational function of  $i$ .

The proof is complete.

## 6. GENERAL CASE

As mentioned in the introduction, providing a general formula for the probability of the event  $\bigvee_{i=1}^k (r_i/s_i \in \mathcal{A}/\mathcal{A})$ , where  $r_1/s_1, \dots, r_k/s_k$  are rational numbers, seems very complex. In light of the previous reasonings, this task amounts to study the graph  $\mathcal{G} := \bigcup_{i=1}^k \mathcal{G}(n; r_i, s_i)$ . Precisely, one has to classify the connected components of  $\mathcal{G}$ , and to determine the probability that each of them does not have two adjacent vertices both belonging to  $\mathcal{A}$ .

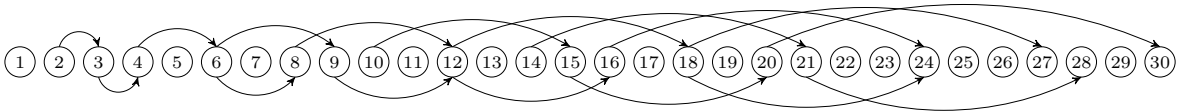


FIGURE 3. The directed graph  $\mathcal{G}(30; 2, 3) \cup \mathcal{G}(30; 3, 4)$ .

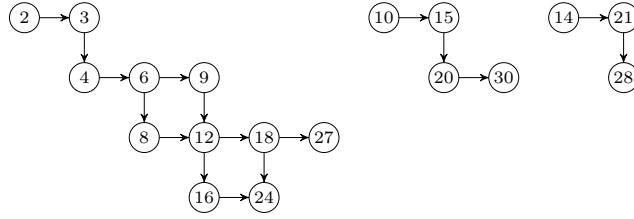


FIGURE 4. The connected components of  $\mathcal{G}(30; 2, 3) \cup \mathcal{G}(30; 3, 4)$  that have at least 2 vertices. Each horizontal, respectively vertical, edge corresponds to multiply the value of a vertex by  $3/2$ , respectively  $4/3$ .

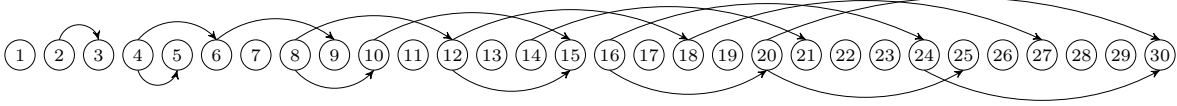


FIGURE 5. The directed graph  $\mathcal{G}(30; 2, 3) \cup \mathcal{G}(30; 4, 5)$ .

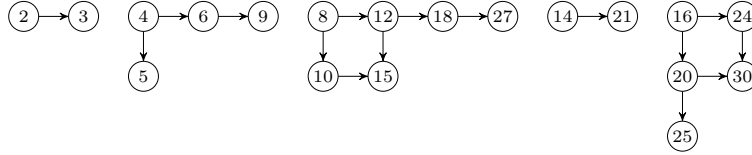


FIGURE 6. The connected components of  $\mathcal{G}(30; 2, 3) \cup \mathcal{G}(30; 4, 5)$  that have at least 2 vertices. Each horizontal, respectively vertical, edge corresponds to multiply the value of a vertex by  $3/2$ , respectively  $5/4$ .

If the multiplicative group generated by  $\{r_i/s_i\}_{i=1}^k$  is cyclic, then the connected components of  $\mathcal{G}$  have a somehow “linear” structure, and proving formulas similar to (1) and (4) is doable.

If the generated group has rank  $R > 1$ , then each connected component of  $\mathcal{G}$  is isomorphic to a subgraph of the  $R$ -dimensional grid graph. For examples, see Figures 3, 4, 5, and 6.

## 7. VISIBLE LATTICE POINTS

Another direction of research can be generalizing ratio sets to sets of visible lattice points. Let  $d \geq 2$  be an integer. For every  $\mathcal{A} \subseteq \mathbb{N}$ , a lattice point  $P \in \mathbb{N}^d$  is said to be visible in the lattice  $\mathcal{A}^d$  if the line segment from  $\mathbf{0} \in \mathbb{Z}^d$  to  $P$  intersects  $\mathcal{A}^d$  only in  $P$ . Let  $\text{vis}(\mathcal{A}^d)$  be the set of lattice points visible in  $\mathcal{A}^d$ . There is a natural bijection between  $\text{vis}(\mathcal{A}^2)$  and  $\mathcal{A}/\mathcal{A}$ , given by  $(x_1, x_2) \mapsto x_1/x_2$ . Hence,  $\text{vis}(\mathcal{A}^d)$  can be considered as a  $d$ -dimensional generalization of the ratio set  $\mathcal{A}/\mathcal{A}$  (see also [5] for a similar generalization of ratio sets).

Filleruelo and Guijarro-Ordóñez [2] gave an asymptotic formula for the cardinality of  $\text{vis}(\mathcal{A}^d)$  for  $\mathcal{A} \in \mathcal{B}(n, \alpha)$ . A natural question is if Theorem 1.2 can be generalized to a formula for  $\mathbb{P}((x_1, \dots, x_d) \in \text{vis}(\mathcal{A}^d))$ , where  $(x_1, \dots, x_d) \in \mathbb{N}^d$ . This amounts to study the hypergraph  $\mathcal{H}(n; x_1, \dots, x_d)$  defined as having vertices  $1, \dots, n$  and hyperedges  $(x_1 t, \dots, x_d t)$ , for every positive integer  $t \leq n/\max(x_1, \dots, x_d)$ . For an example, see Figure 7.

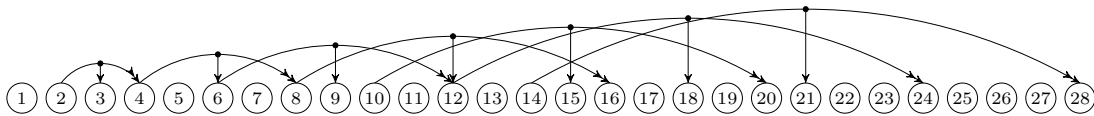


FIGURE 7. The hypergraph  $\mathcal{H}(28; 2, 3, 4)$ .

## 8. ACKNOWLEDGEMENTS

The author thanks Paolo Leonetti and Daniele Mastrostefano for suggestions that improved the quality of the article.

## REFERENCES

1. G. Alsmeyer, Z. Kabluchko, and A. Marynych, *Limit theorems for the least common multiple of a random set of integers*, Trans. Amer. Math. Soc. **372** (2019), no. 7, 4585–4603.
2. J. Cilleruelo and J. Guíjarro-Ordóñez, *Ratio sets of random sets*, Ramanujan J. **43** (2017), no. 2, 327–345.
3. J. Cilleruelo, D. S. Ramana, and O. Ramaré, *Quotient and product sets of thin subsets of the positive integers*, Proc. Steklov Inst. Math. **296** (2017), 52–64.
4. J. Cilleruelo, J. Rué, P. Šarka, and A. Zumalacárregui, *The least common multiple of random sets of positive integers*, J. Number Theory **144** (2014), 92–104.
5. P. Leonetti and C. Sanna, *Directions sets: a generalisation of ratio sets*, Bull. Aust. Math. Soc. **101** (2020), no. 3, 389–395.
6. D. Mastrostefano, *On maximal product sets of random sets*, J. Number Theory **224** (2021), 13–40.
7. C. Sanna, *A note on product sets of random sets*, Acta Math. Hungar. **162** (2020), no. 1, 76–83.
8. C. Sanna, *On the l.c.m. of random terms of binary recurrence sequences*, J. Number Theory **213** (2020), 221–231.

POLITECNICO DI TORINO, DEPARTMENT OF MATHEMATICAL SCIENCES  
CORSO DUCA DEGLI ABRUZZI 24, 10129 TORINO, ITALY  
Email address: `carlo.sanna.dev@gmail.com`