HAL
open science

On additive combinatorics of permutations of n

L. Sunil Chandran, Deepak Rajendraprasad, Nitin Singh

To cite this version:

L. Sunil Chandran, Deepak Rajendraprasad, Nitin Singh. On additive combinatorics of permutations of n. Discrete Mathematics and Theoretical Computer Science, 2014, Vol. 16 no. 2 (2), pp.35–40. 10.46298/dmtcs.2074 . hal-01185614

HAL Id: hal-01185614

https://inria.hal.science/hal-01185614v1

Submitted on 20 Aug 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Discrete Mathematics and Theoretical Computer Science DMTCS vol. **16:2**, 2014, 35–40

On Additive Combinatorics of Permutations of $\mathbb{Z}_n$

L. Sunil Chandran[1*] Deepak Rajendraprasad[2] Nitin Singh[3]

[1]*Department of Computer Science and Automation, Indian Institute of Science, Bangalore, India*
[2]*Department of Computer Science, University of Haifa, Haifa, Israel*
[3]*Department of Mathematics, Indian Institute of Science, Bangalore, India*

received 2nd Dec. 2013, revised 27th Mar. 2014, accepted 27th Apr. 2014.

Let $\mathbb{Z}_n$ denote the ring of integers modulo n. A permutation of $\mathbb{Z}_n$ is a sequence of n distinct elements of $\mathbb{Z}_n$. Addition and subtraction of two permutations is defined element-wise. In this paper we consider two extremal problems on permutations of $\mathbb{Z}_n$, namely, the maximum size of a collection of permutations such that the sum of any two distinct permutations in the collection is again a permutation, and the maximum size of a collection of permutations such that no sum of two distinct permutations in the collection is a permutation. Let the sizes be denoted by $s(n)$ and $t(n)$ respectively. The case when n is even is trivial in both the cases, with $s(n) = 1$ and $t(n) = n!$. For n odd, we prove $(n\phi(n))/2^k \leq s(n) \leq \frac{n!\cdot 2^{-(n-1)/2}}{((n-1)/2)!}$ and $2^{(n-1)/2} \cdot (\frac{n-1}{2})! \leq t(n) \leq 2^k \cdot (n-1)!/\phi(n)$, where k is the number of distinct prime divisors of n and ϕ is the Euler's totient function.

Keywords: sums of permutations, orthomorphisms, reverse free families

MSC 2010: 11A05, 11A07, 11A41, 05E99, 05D05.

1 Introduction

For $n \in \mathbb{Z}$, let $\mathbb{Z}_n$ denote the ring $\{0, \ldots, n-1\}$ with $+$ and . as addition and multiplication modulo n respectively. Let $\mathcal{S}(\mathbb{Z}_n)$ denote the set of all permutations of the set $\mathbb{Z}_n$. We are interested in obtaining bounds on the maximum size of a subset $\mathcal{P}$ of $\mathcal{S}(\mathbb{Z}_n)$ in the case when two distinct permutations in $\mathcal{P}$ sum up to a permutation, and in the case when no two distinct permutations in $\mathcal{P}$ sum up to a permutation. As far as we know the problems considered above are new, though a similar looking problem for difference of permutations is well studied, in the form of mutually orthogonal *orthomorphisms* of finite groups. For the sake of completeness, we discuss the connection between difference of permutations problem with the orthomorphisms problem in Section 4. The families of permutations we consider have similarities to *reverse free* and *reverse full* families of permutations as considered by Füredi et al. (2010) and Cibulka (2013).

*Email: `sunil@csa.iisc.ernet.in`

1365–8050 © 2014 Discrete Mathematics and Theoretical Computer Science (DMTCS), Nancy, France

2 Preliminaries

We recall some basic notions from elementary number theory that will be used in the paper. An element $s \in \mathbb{Z}_n$ is said to be *invertible* if there exists $t \in \mathbb{Z}_n$ such that $st = 1$ (recall that multiplication in $\mathbb{Z}_n$ is modulo n). The set of all invertible elements of $\mathbb{Z}_n$ is called the *unit group* of $\mathbb{Z}_n$ and is denoted by $\mathbb{Z}_n^\times$. It is easily seen that $\mathbb{Z}_n^\times$ is a group under multiplication. We know that $k \in \mathbb{Z}_n$ is invertible if and only if $\gcd(k, n) = 1$. The cardinality of the set $\{k \in \mathbb{Z} : 1 \leq k \leq n-1,\ \gcd(k, n) = 1\}$ is denoted by $\phi(n)$, also known as *Euler's totient function* in literature. The following results are well known.

Lemma 2.1 *Let $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, where $p_1, \ldots, p_k$ are distinct prime divisors of n. Then, we have*

$$\phi(n) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1).$$

Lemma 2.2 (Chinese Remainder Theorem) *Let $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, where $p_1, \ldots, p_k$ are distinct prime divisors of n. Then, we have the following isomorphism*

$$\begin{aligned} \mathbb{Z}_n &\longrightarrow \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}} \\ s &\longmapsto (s \bmod p_1^{\alpha_1}, \ldots, s \bmod p_k^{\alpha_k}). \end{aligned} \tag{1}$$

From the above lemma we see that $s = (s_1, \ldots, s_k)$ is invertible in $\mathbb{Z}_n$ if and only if s_i is invertible in $\mathbb{Z}_{p_i^{\alpha_i}}$ for all $i = 1, \ldots, k$.

Notation 2.3 We will denote permutations of $\mathbb{Z}_n$ as n-tuples $(\sigma_1, \ldots, \sigma_n)$ where $\sigma_i \in \mathbb{Z}_n$, and all σ_i are distinct. This is not to be confused with the cycle representation of a permutation, which is customary in algebra. Since we do not use cycle representation of permutations in this paper, we hope there is no confusion. Let $\sigma = (\sigma_1, \ldots, \sigma_n)$ and $\tau = (\tau_1, \ldots, \tau_n)$, be n-tuples over $\mathbb{Z}_n$. Then $\sigma \pm \tau$ denotes the tuple $(\sigma_1 \pm \tau_1, \ldots, \sigma_n \pm \tau_n)$. For $c \in \mathbb{Z}_n$, $c.\sigma$ will denote the tuple $(c\sigma_1, \ldots, c\sigma_n)$, and $c + \sigma$ will denote the tuple $(c + \sigma_1, \ldots, c + \sigma_n)$.

Lemma 2.4 *Let n be even and $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ be two permutations of $\mathbb{Z}_n$. Then $a + b$ is not a permutation of $\mathbb{Z}_n$.*

Proof: Let $c = a + b = (c_1, \ldots, c_n)$. For contradiction, assume that c is a permutation. Treating a, b, c as n-tuples over $\mathbb{Z}$ we have, $c_i \equiv a_i + b_i \pmod{n}$. Summing up over all i, we have,

$$\begin{aligned} \sum_{i=1}^{n} c_i &\equiv \sum_{i=1}^{n} (a_i + b_i) \pmod{n} \\ \text{or, } \sum_{i=1}^{n} (i-1) &\equiv \sum_{i=1}^{n} 2(i-1) \pmod{n} \\ \text{or, } \frac{n(n-1)}{2} &\equiv n(n-1) \equiv 0 \pmod{n} \end{aligned}$$

which is a contradiction as $(n-1)/2$ is not an integer when n is even. This proves the lemma. □

Lemma 2.5 *Let $a = (a_0, \ldots, a_{n-1})$ and $b = (b_0, \ldots, b_{n-1})$ be distinct permutations of the set $\{0, \ldots, n-1\}$ such that the component-wise sums $c_i = a_i + b_i$ are all distinct. Then there exist $0 \leq j, k \leq n-1$ such that $c_j = c_k + 1$.*

Proof: Without loss of generality assume $c_i = a_i + b_i$ satisfy the ordering $c_0 < c_1 < \cdots < c_{n-1}$. Now suppose the claim is not true. Then we have, $c_i - c_{i-1} \geq 2$ for $1 \leq i \leq n-1$. Summing up we get $2n-2 \leq \sum_{i=1}^{n-1}(c_i - c_{i-1}) = c_{n-1} - c_0 \leq 2n-2$. Thus $c_i - c_{i-1} = 2$ for all $1 \leq i \leq n-1$, which implies $c_i = 2i$ for all $0 \leq i \leq n-1$. Now $a_0 + b_0 = c_0 = 0$ implies $a_0 = b_0 = 0$. Now $c_1 = a_1 + b_1 = 2$, therefore we must have $a_1 = b_1 = 1$. Continuing this way, we conclude that $a_i = b_i = i$ for all $0 \leq i \leq n-1$, contradicting the fact that the permutations were distinct. □

3 Results and Proofs

In this section, we consider the maximum sizes of collections of permutations of $\mathbb{Z}_n$ under two different constraints, namely,

(i) Sum of any two distinct permutations in the collection is again a permutation (not necessarily in the collection). We will say that such a collection satisfies property $(\mathbf{P1})$.

(ii) No sum of two distinct permutations in the collection is a permutation. We will say that such a collection satisfies property $(\mathbf{P2})$.

Let $s(n)$ and $t(n)$ denote the maximum sizes of the collections of permutations of $\mathbb{Z}_n$ satisfying $(\mathbf{P1})$ and $(\mathbf{P2})$ respectively. We prove the following:

Theorem 3.1 *Let $n \geq 3$ be an odd integer and $s(n), t(n)$ be as defined. Then, we have*

(a) $\dfrac{n\phi(n)}{2^k} \leq s(n) \leq \dfrac{n! \cdot 2^{-(n-1)/2}}{((n-1)/2)!}$,

(b) $((n-1)/2)! \cdot 2^{(n-1)/2} \leq t(n) \leq 2^k (n-1)!/\phi(n)$,

where k denotes the number of distinct prime divisors of n.

The sizes of collections of permutations of $\mathbb{Z}_n$ satisfying $(\mathbf{P1})$ and $(\mathbf{P2})$ satisfy a similar inequality as the sizes of the families of *reverse free* and *reverse full* permutations considered by Füredi et al. (2010) and Cibulka (2013).

Lemma 3.2 *For an integer $n \geq 1$, let $s(n), t(n)$ be as defined. Then, we have $s(n) \cdot t(n) \leq n!$.*

Proof: Let $\mathcal{S} = \{\sigma_1, \ldots, \sigma_s\}$ and $\mathcal{T} = \{\tau_1, \ldots, \tau_t\}$ be collections of permutations satisfying $(\mathbf{P1})$ and $(\mathbf{P2})$ respectively. We show that $\sigma_i \circ \tau_j$ are distinct for all $1 \leq i \leq s$ and $1 \leq j \leq t$, which would imply $st \leq n!$. For sake of contradiction, without loss of generality assume $\sigma_1 \circ \tau_1 = \sigma_2 \circ \tau_2$. Now consider the collections of permutations $\mathcal{S}' = \{\sigma_1^{-1} \circ \sigma_i : 1 \leq i \leq s\}$ and $\mathcal{T}' = \{\tau_j \circ \tau_1^{-1} : 1 \leq j \leq t\}$. It can be seen that $\mathcal{S}'$ and $\mathcal{T}'$ also satisfy $(\mathbf{P1})$ and $(\mathbf{P2})$ respectively. We note that $\mathrm{id} \in \mathcal{S}' \cap \mathcal{T}'$, where id denotes the identity permutation. Since $\sigma_1^{-1} \circ \sigma_2 \in \mathcal{S}'$, $\mathrm{id} + \sigma_1^{-1} \circ \sigma_2$ is a permutation. Composing with the permutation $\sigma_2^{-1} \circ \sigma_1$, we conclude that $\mathrm{id} + \sigma_2^{-1} \circ \sigma_1$ is a permutation. However $\sigma_2^{-1} \circ \sigma_1 = \tau_2 \circ \tau_1^{-1}$ by assumption, and thus $\mathrm{id} + \tau_2 \circ \tau_1^{-1}$ is a permutation. But this is a contradiction as both id and $\tau_2 \circ \tau_1^{-1}$ are in the collection $\mathcal{T}'$, which satisfies $(\mathbf{P2})$. The lemma now follows. □

From Lemma 2.4, we note that $s(n) = 1$ when n is even. Now we present a construction for the lower bound on $s(n)$ when n is odd.

Lemma 3.3 *Let n be an odd number ≥ 3. Then $s(n) \geq (n\phi(n))/2^k$ where $\phi(n)$ is the Euler's totient function and k is the number of distinct prime divisors of n.*

Proof: Our construction is based on the following observations.

(a) For a permutation τ of $\mathbb{Z}_n$, $k.\tau$ is a permutation of $\mathbb{Z}_n$ if and only if k is invertible in $\mathbb{Z}_n$.

(b) For a permutation τ of $\mathbb{Z}_n$, $k + \tau$ is a permutation for all $k \in \mathbb{Z}_n$.

(c) Let $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, where p_i's are distinct prime divisors of n. Then there exists a subset S of invertible elements of $\mathbb{Z}_n$ with $|S| = \prod_{i=1}^{k} p^{\alpha_i - 1}(p_i - 1)/2$ such that for any $x, y \in S$, $x + y$ is invertible in $\mathbb{Z}_n$. To describe the set S, we use the isomorphism in Lemma 2.2. Let $S = \{s \in \mathbb{Z}_n : s = (s_1, \ldots, s_k)$ where $s_i \equiv c_i \bmod p_i$ for some $1 \leq c_i \leq (p_i - 1)/2\}$. Note that in the description of S, each s_i has $p_i^{\alpha_i - 1}(p_i - 1)/2$ choices, and hence the set S has the desired cardinality. Further each element of S is invertible in $\mathbb{Z}_n$. Now for $s, t \in S$, we have $s + t = (s_1 + t_1, \ldots, s_k + t_k)$ where $s = (s_1, \ldots, s_k)$ and $t = (t_1, \ldots, t_k)$. By definition of S, observe that $s_i + t_i \not\equiv 0 \pmod{p_i}$ for all $1 \leq i \leq k$. Thus $s + t$ is invertible in $\mathbb{Z}_n$.

Now consider the set $\mathcal{P} = \{s.(x+0, x+1, \ldots, x+n-1) : s \in S, x \in \mathbb{Z}_n\}$. By observations (a),(b) and (c), we see that $\mathcal{P}$ consists of permutations of $\mathbb{Z}_n$. Let σ, τ be two distinct permutations in $\mathcal{P}$ with $\sigma = s.(x+0, \ldots, x+n-1)$ and $\tau = t.(y+0, \ldots, y+n-1)$. Then $\sigma+\tau = (sx+ty)+(s+t).(0, 1, \ldots, n-1)$. Since $s + t$ is invertible, by observations (a) and (b), we conclude that $\sigma + \tau$ is a permutation. Thus $\mathcal{P}$ satisfies $(\mathbf{P1})$. Finally we observe that $|\mathcal{P}| = n \cdot |S| = n \cdot \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1)/2 = (n \cdot \phi(n))/2^k$. This proves the lemma. □

Remark 3.4 We note that when n is a prime number, the bound in Lemma 3.3 reduces to $n(n-1)/2$.

From Lemma 2.4, we see that $t(n) = n!$ when n is an even integer. We note that when n is even, we have equality in Lemma 3.2. Now we consider the lower bound for $t(n)$ when n is an odd integer.

Lemma 3.5 *Let n be an odd number. Then, we have $t(n) \geq 2^{(n-1)/2} \cdot (\frac{n-1}{2})!$, where k is the number of distinct prime divisors of n.*

Proof: We say the pair of permutations $(a_0, \ldots, a_{n-1})$ and $(b_0, \ldots, b_{n-1})$ of the set $\{0, \ldots, n-1\}$ are *admissible* if the sums $a_i + b_i$, $0 \leq i \leq n-1$, are not all distinct (the addition being in $\mathbb{Z}$). We construct a collection $\mathcal{P}$ of mutually admissible permutations of $\{0, \ldots, n-1\}$. Note that $\mathcal{P}$ when viewed as a set of permutations of $\mathbb{Z}_n$, satisfies $(\mathbf{P2})$. Let $m = (n-1)/2$. For $0 \leq i \leq m-1$, let $B_i = (2i, 2i+1)$ and $\overline{B}_i = (2i+1, 2i)$. Let $c = c_0 c_1 \ldots c_{m-1}$ be a binary string of length m, and σ be a permutation of $\{0, \ldots, m-1\}$. Define $P_{\sigma,c} = (x_0, x_1, \ldots, x_{n-2}, x_{n-1})$ where,

$$(x_{2i}, x_{2i+1}) = \begin{cases} B_{\sigma(i)} & \text{if } c_i = 0, \\ \overline{B}_{\sigma(i)} & \text{if } c_i = 1 \end{cases}$$

for $0 \leq i \leq m-1$ and $x_{n-1} = n-1$. It is easily observed that $P_{\sigma,c}$ is a permutation of the set $\{0, \ldots, n-1\}$ and $P_{\sigma,c} \neq P_{\sigma',c'}$ for $(\sigma, c) \neq (\sigma', c')$. Let $\mathcal{P}$ denote the collection of permutations

$\{P_{\sigma,c}\}$. We now show that any two permutations in the collection $\mathcal{P}$ are admissible. Let $P_{\sigma,c}$ and $P_{\sigma',c'}$ be two distinct permutations in $\mathcal{P}$. We consider two cases:

Case: $c \neq c'$. Let i be such that $c_i \neq c'_i$. Without loss of generality assume $c_i = 0, c'_i = 1$. Let $P_{\sigma,c} = (x_0, \ldots, x_{n-1})$ and $P_{\sigma',c'} = (x'_0, \ldots, x'_{n-1})$. Then we have, $(x_{2i}, x_{2i+1}) = B_{\sigma(i)} = (a, a+1)$ and $(x'_{2i}, x'_{2i+1}) = \overline{B}_{\sigma'(i)} = (b+1, b)$ for some a, b. Thus $x_{2i} + x'_{2i} = x_{2i+1} + x'_{2i+1} = a + b + 1$, and hence the permutations are admissible.

Case: $c = c'$. In this case we must have $\sigma \neq \sigma'$. In the block $B_i = (2i, 2i+1)$, let us call $2i$ as the *little* end and $2i+1$ as the *big* end. Then $c = c'$ implies that in the component-wise addition of $P_{\sigma,c}$ and $P_{\sigma',c'}$ the little ends are summed with little ends, and big ends are summed with big ends. Let L be the set of sums of little ends, i.e, $L = \{2\sigma(i) + 2\sigma'(i) : 0 \leq i \leq m-1\}$ and B be the sums of big ends, i.e., $B = \{2\sigma(i) + 2\sigma'(i) + 2 : 0 \leq i \leq m-1\}$. Clearly the permutations $P_{\sigma,c}$ and $P_{\sigma',c'}$ are admissible if $\sigma(j) + \sigma'(j) = \sigma(k) + \sigma'(k)$ for some $0 \leq j, k \leq m-1$. Assume that it is not the case. Then we show that $L \cap B$ is non-empty which will prove that $P_{\sigma,c}$ and $P_{\sigma',c'}$ are admissible. By Lemma 2.5, there exist $0 \leq j, k \leq m-1$ such that $\sigma(j) + \sigma'(j) = \sigma(k) + \sigma'(k) + 1$, or $2\sigma(j) + 2\sigma'(j) = 2\sigma(k) + 2\sigma'(k) + 2$. We see that the left side of the identity is in L and the right side is in B. Thus $L \cap B$ is non-empty.

Hence the collection of permutations $P_{\sigma,c}$, when viewed as permutations of $\mathbb{Z}_n$ satisfy $(\mathbf{P2})$. Finally we note that the number of permutations is $2^m \cdot m! = 2^{(n-1)/2} \cdot (\frac{n-1}{2})!$. This completes the proof. □

We can now complete the proof of Theorem 3.1.

Proof of Theorem 3.1**:** From Lemmata 3.2, 3.3 and 3.5, we have $s(n) \leq 2^{-(n-1)/2} \cdot \frac{n!}{((n-1)/2)!}$, and $t(n) \leq \frac{2^k (n-1)!}{\phi(n)}$. The result then follows from the lower bounds for $s(n)$ and $t(n)$. □

Remark 3.6 We note that for a prime number n, the upper bound for $t(n)$ is roughly $(n/e)^n \sqrt{n}$ whereas the lower bound is roughly $(n/e)^{n/2}\sqrt{n}$. Thus there is a quadratic gap between the upper and lower bounds. We also mention that one way to obtain permutations summing up to a non permutation is to consider a family of permutations with mutual reverses. Two permutations σ, τ of $\{0, \ldots, n-1\}$ are said to have a *mutual reverse* if there exist $i \neq j$ such that $\sigma(i) = \tau(j)$ and $\sigma(j) = \tau(i)$. A family of permutations, every two of which have a mutual reverse is called *reverse full*, Füredi et al. (2010). Note that a reverse full family of permutations satisfies $(\mathbf{P2})$. From a result of Cibulka (2013) on size of reverse-free families of permutations, the maximum size of a reverse full family of permutations on n symbols is at most $n^{n/2+O(\log n)}$, though we are unaware of any non-trivial lower bound for the same. Our construction achieves $\sim (n/e)^{n/2}\sqrt{n}$, but under a much more flexible constraint.

4 Differences of Permutations being Permutation

In this section, we wish to obtain upper and lower bounds on the maximum size of set $\mathcal{P} \subseteq \mathcal{S}(\mathbb{Z}_n)$ such that for any two distinct permutations $\sigma, \tau \in \mathcal{P}$, $\sigma - \tau$ is also a permutation of $\mathbb{Z}_n$. We say that $\mathcal{P} \subseteq \mathcal{S}(\mathbb{Z}_n)$ satisfies property $(\mathbf{P3})$ if for any two $\sigma, \tau \in \mathcal{P}$, $\sigma \neq \tau$, $\sigma - \tau$ is a permutation of $\mathbb{Z}_n$. Let $f(n) = \max\{|\mathcal{P}| : \mathcal{P} \subseteq \mathcal{S}(\mathbb{Z}_n) \text{ satisfies } (\mathbf{P3})\}$.

The above problem is only superficially different from the well studied problem of finding mutually orthogonal orthomorphisms of finite groups (See Evans (2002)). For a finite group G, a bijection $\theta : G \to G$ is called an *orthomorphism* of G if the map $x \mapsto \theta(x) - x$ is a bijection. Two orthomorphisms θ, ϕ are called *orthogonal* if $\theta - \phi$ is a bijection. It is not hard to see that a set of k permutations of $\mathbb{Z}_n$ satisfying **(P3)** gives a set of $k-1$ mutually orthogonal orthomorphisms of $\mathbb{Z}_n$ and vice versa.

4.1 Latin Squares

Orthogonal orthomorphisms have been used in construction of mutually orthogonal Latin squares (MOLS). Although the construction appears in any standard text on combinatorics (cf. Lint and Wilson (2001)), we describe it in our setting. We will say a map $L : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ to be an $n \times n$ Latin square, if (i) $L(i,j) \neq L(i',j)$ for $i \neq i'$ and (ii) $L(i,j) \neq L(i,j')$ for $j \neq j'$. One can think of L as $n \times n$ square array with entries from $\{0, \ldots, n-1\}$ where each row and column contains distinct entries. Two $n \times n$ Latin squares L, L' are called *orthogonal* if $L(i,j) = x$ and $L'(i,j) = y$ has a *unique* solution for all $(x,y) \in \mathbb{Z}_n \times \mathbb{Z}_n$. The following is easy to verify:

Lemma 4.1 *Let $\sigma_1, \ldots, \sigma_k$ be a collection of permutations of $\mathbb{Z}_n$ satisfying* $(\mathbf{P3})$. *Then, there are k mutually orthogonal Latin squares $L_1, \ldots, L_k$ where the Latin square L_r is defined by $L_r(i,j) = i + \sigma_r(j)$.*

If we write the permutations of $\mathcal{P}$ as rows of a matrix, we get a $|\mathcal{P}| \times n$ matrix over $\mathbb{Z}_n$ with the property that the difference of any two distinct rows is a permutation of $\mathbb{Z}_n$. Such matrices have been used in connection with constructions of Latin squares and orthogonal arrays (cf. (Lint and Wilson, 2001, Chapter 22)). Well known bounds for mutually orthogonal orthomorphisms yield the following lemma.

Lemma 4.2 *For $n \geq 2$, we have*

(a) $f(n) \leq n - 1$,

(b) $f(n) = 1$, *when n is an even number;*

(c) $f(n) = n - 1$, *when n is a prime number.*

Question 4.3 What are the values of $f(n)$ for odd composite numbers n?

From the results of Evans (2002) it follows that for odd numbers $n > 3$ and n not divisible by 9, we have $f(n) \geq 3$.

Acknowledgements

The authors would like to thank the anonymous referees for their useful comments. The Lemma 3.2 in particular is due to a referee, which has greatly simplified the paper and also enhanced the symmetry of the results. The earlier version of the paper contained separate upper bound proofs for $s(n)$ and $t(n)$, however using Lemma 3.2, those are implied by respective lower bounds on $s(n)$ and $t(n)$. The second author is supported by VATAT Post-doctoral Fellowship, Council of Higher Education, Israel. The third author thanks National Mathematics Initiative, India for support.

References

J. Cibulka. Maximum size of reverse-free sets of permutations. *SIAM J. Discrete Math.*, 27(1):232–239, 2013.

A. B. Evans. On orthogonal orthomorphisms of cyclic and non-abelian groups. *Discrete Mathematics*, 243:229–233, 2002.

Z. Füredi, I. Kantor, A. Monti, and B. Sinaimeri. On reverse-free codes and permutations. *SIAM J. Discrete Math.*, 24(3):964–978, 2010.

J. H. V. Lint and R. M. Wilson. *A Course in Combinatorics*. Cambridge University Press, 2001.