# Large families of permutations of $\mathbb{Z}_n$ whose pairwise sums are permutations

Bojan Bašić, Stefan Hačko*

*Department of Mathematics and Informatics, University of Novi Sad,*

*Trg Dositeja Obradovića 4, 21000 Novi Sad, Serbia*

bojan.basic@dmi.uns.ac.rs, stefan.hacko@dmi.uns.ac.rs

**Abstract**

We construct some large families of permutations of $\mathbb{Z}_n$ such that the sum of any two permutations from a family is again a permutation of $\mathbb{Z}_n$ (not necessarily in the same family). Our families are significantly larger than the largest such families known so far in the literature (depending on the value of $n$, the improvement can be as large as exponential). We also show that our families are maximal in the sense that no permutations can be added to them while maintaining the required property.

*Mathematics Subject Classification (2020):* 05A05, 05B30, 05D05, 11B75

*Keywords:* families of permutations, sums of permutations

## 1 Introduction

In recent years there were many interesting results concerning the maximum size of a family of permutations such that each pair among them satisfies some prescribed relation. Various techniques are employed in such works. For example, Kovács and Soltész [6] considered families of $k$-neighbor separated permutations using the natural correspondence between permutations of $n$ elements and Hamiltonian paths in the complete graph $K_n$. Ellis, Friedgut and Pilpel [3] used Fourier analysis on symmetric groups in order to obtain their well-known result on intersecting families of permutations. Cibulka [2] studied reverse-free sets of permutations and at one point in the proof of his main result appealed to a deep result concerning the size of gaps between consecutive primes. Reverse-free codes and permutations have also been the subject of the article by Füredi, Kantor, Monti and Sinaimeri [5].

The last two mentioned articles motivated Chandran, Rajendraprasad and Singh [1] to consider the following two quantities.

*corresponding author

- For a positive integer $n$, let $s(n)$ denote the maximal possible size of a family of permutations of $\mathbb{Z}_n$ such that the sum of any two permutations from a family is again a permutation of $\mathbb{Z}_n$ (not necessarily in the family).
- For a positive integer $n$, let $t(n)$ denote the maximal possible size of a family of permutations of $\mathbb{Z}_n$ such that the sum of any two permutations from a family is never again a permutation of $\mathbb{Z}_n$.

If $n$ is even, the situation is not really interesting, since it can be easily shown that in that case we have $s(n) = 1$ and $t(n) = n!$. However, if $n$ is odd, then the problem of estimating $s(n)$ and $t(n)$ is much harder. The authors of [1] showed the following bounds for that case:

$$\begin{aligned} \frac{n\varphi(n)}{2^{\omega(n)}} \leqslant s(n) &\leqslant \frac{n!}{\left(\frac{n-1}{2}\right)! \cdot 2^{\frac{n-1}{2}}}; \\ \left(\frac{n-1}{2}\right)! \cdot 2^{\frac{n-1}{2}} \leqslant t(n) &\leqslant \frac{2^{\omega(n)}(n-1)!}{\varphi(n)}, \end{aligned} \tag{1}$$

where $\omega(n)$ denotes the number of distinct prime divisors of $n$. The lower bounds were obtained by constructions of such families of the corresponding cardinalities, while the upper bounds were obtained as a consequence of the lower bounds, by showing an interesting inequality $s(n) \cdot t(n) \leqslant n!$.

Our aim in this article is to present a considerable improvement of the lower bound on $s(n)$ given above for composite (and odd) $n$; this also implies an improvement of the upper bound on $t(n)$ (because of the mentioned inequality). It is hard to quantify for how much our lower bound surpasses the one from (1) in general (it depends on the prime factorization of $n$), but in some cases (e.g., when $n$ is a prime power) Corollary 3 gives an idea: for example, if $n = 3^\alpha$, (1) gives $s(n) \geqslant 3^{2\alpha-1} = \frac{n^2}{3}$, while we obtain $s(n) \geqslant 3^{\frac{3^\alpha-1}{2}} = 3^{\frac{n-1}{2}}$; see also Table 1 for the results for some small values of $n$ (not necessarily prime powers).

At the end, we would like to add that the problem we consider here bears a resemblance to the problem of finding a family of maximal cardinality of the permutations of the set $\mathbb{Z}_n$ such that the difference of any two permutations from the family is again a permutation (better known as a family of orthogonal orthomorphisms of the group $\mathbb{Z}_n$). For the current status of this problem see [4]. Such families have been used (see, e.g., [8]) to construct codes with good cross-correlation and auto-correlation properties, which have many real world applications; for example, codes with good cross-correlation are used in PSK, 4G LTE, GPS communications, and are also useful for generating good jamming-resistant signals [7].

## 2 Lower bound

We begin by stating our main result.

**Theorem 1.** *Let $n$ be an odd composite positive integer. Then:*

$$s(n) \geqslant \max_{d|n,\, d\neq 1,n} s(d)s\left(\frac{n}{d}\right)^d. \tag{2}$$

The theorem will be proved by constructing a set of $\max_{d|n,\, d\neq 1,n} s(d)s\left(\frac{n}{d}\right)^d$ distinct permutations with the required property.

Before we proceed to the construction, let us introduce the necessary notation. For a positive integer $n$, let $S_n$ denote a set of permutations of $\mathbb{Z}_n$ such that, for any two permutations $\pi', \pi'' \in S_n$, their sum $\pi' + \pi''$ is again a permutation, and that $S_n$ has the maximal cardinality among all such sets (that is, $|S_n| = s(n)$). Let $\mathrm{id}_n$ denote the permutation $(0, 1, \ldots, n-1)$. Finally, we add that, in order to make the notation less cumbersome, the sign "+" will denote the addition in all the groups $\mathbb{Z}_n$, $\mathbb{Z}_d$, $\mathbb{Z}_{\frac{n}{d}}$ etc. (instead of differentiating them by $+_n$, $+_d$, $+_{\frac{n}{d}}$ etc.), and it should always be clear from the context in which group we are performing the operation.

The following lemma will be needed.

**Lemma 2.** *If $\pi \in S_n$, then $\pi + i \in S_n$ for any $i$, $i \in \{0, \ldots, n-1\}$.*

*Proof.* Let $\pi' \in S_n$. It is enough to show that $(\pi + i) + \pi'$ is a permutation (then the result follows by the maximality of $|S_n|$, since if $\pi + i \notin S_n$, we could add it to $S_n$ and thus obtain a larger set). We have $(\pi + i) + \pi' = (\pi + \pi') + i$, and since $\pi + \pi'$ is a permutation (by the definition of $S_n$, because $\pi, \pi' \in S_n$), it follows that $(\pi + \pi') + i$ is also a permutation. This completes the proof. □

We are now ready for the proof of the main theorem.

*Proof of Theorem 1.* Fix $d \mid n$, $d \neq 1, n$, for which the value $s(d)s\left(\frac{n}{d}\right)^d$ is maximal. Also, fix one set $S_{\frac{n}{d}}$ such that (w.l.o.g.) $\mathrm{id}_{\frac{n}{d}} \in S_{\frac{n}{d}}$, and fix one set $S_d$ such that $\mathrm{id}_d \in S_d$. Let

$$\begin{aligned} S = \{(d\pi_0 + \sigma(0))^\frown (d\pi_1 + \sigma(1))^\frown \cdots^\frown (d\pi_{d-1} + \sigma(d-1)) \\ : \pi_0, \pi_1, \ldots, \pi_{d-1} \in S_{\frac{n}{d}},\, \sigma \in S_d\}, \end{aligned} \tag{3}$$

where $^\frown$ denotes the concatenation of two permutations (more formally, but less clear, each permutation $\pi$ from $S$ is given by $\pi(i) = d\pi_{\lfloor \frac{i}{\frac{n}{d}} \rfloor}(i \bmod \frac{n}{d}) + \sigma\left(\lfloor \frac{i}{\frac{n}{d}} \rfloor\right)$); note that $\pi_0, \ldots, \pi_{d-1}$ are not necessarily different. We easily see that each member of $S$ is a permutation of $\mathbb{Z}_n$: indeed, the first $\frac{n}{d}$ elements are all the elements that leave the remainder $\sigma(0)$ when divided by $d$, the next $\frac{n}{d}$ elements are all the elements that leave the remainder $\sigma(1)$ when divided by $d$ etc.

We are now going to show that the sum of any two permutations obtained by the construction above is again a permutation. Let $\pi', \pi'' \in S$, where $\pi'$ is obtained from the parameters $\pi'_0, \ldots, \sigma'$, and $\pi''$ from the parameters $\pi''_0, \ldots, \sigma''$. Let $\sigma' + \sigma'' = \tau$ ($\tau$ is also a permutation of $\mathbb{Z}_d$, since $\sigma', \sigma'' \in S_d$).

We shall consider the summation $\pi' + \pi''$ "blockwise," where blocks are as presented in (3): the $k^{\text{th}}$ block of the sum, for $k = 0, 1, \ldots, d-1$, will be the tuple $(d\pi'_k + \sigma'(k)) + (d\pi''_k + \sigma''(k))$.

The $k^{\text{th}}$ block is $d(\pi'_k + \pi''_k) + (\sigma'(k) + \sigma''(k))$, that is, $d(\pi'_k + \pi''_k) + \tau(k)$. Since $\pi'_k + \pi''_k$ is a permutation of $\mathbb{Z}_{\frac{n}{d}}$ (because $\pi'_k, \pi''_k \in S_{\frac{n}{d}}$), we conclude that the $k^{\text{th}}$ block consists precisely of all the elements of $\mathbb{Z}_n$ that leave the remainder $\tau(k)$ when divided by $d$. But since $\tau$ is a permutation of $\mathbb{Z}_d$, we conclude that $\pi' + \pi''$ is a permutation of $\mathbb{Z}_n$, as needed.

We now easily calculate:

$$s(n) \geqslant |S| = |S_{\frac{n}{d}}|^d \cdot |S_d| = s\left(\frac{n}{d}\right)^d s(d),$$

which was to be proved. □

In the following corollary we give a nonrecursive lower bound on $s(n)$ that can be deduced from Theorem 1.

**Corollary 3.** *a) Let $p$ be an odd prime number and $\alpha$ a positive integer. Then*

$$s(p^\alpha) \geqslant s(p)^{\frac{p^\alpha - 1}{p-1}} \geqslant \binom{p}{2}^{\frac{p^\alpha - 1}{p-1}}. \tag{4}$$

*b) Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, where $p_1, p_2, \ldots, p_k$ are different primes enumerated in the following order: $5, 3, 7, 11, 13, 17, 19, 23 \ldots$ Then:*

$$s(n) \geqslant \prod_{t=1}^{k} s(p_t^{\alpha_t})^{\prod_{j=t+1}^{k} p_j^{\alpha_j}} \geqslant \prod_{t=1}^{k} \binom{p_t}{2}^{\frac{p_t^{\alpha_t} - 1}{p_t - 1} \prod_{j=t+1}^{k} p_j^{\alpha_j}}.$$

*Proof.* a) Let us first show the first inequality. We proceed by induction on $\alpha$. The conclusion is trivial for $\alpha = 1$. Assume now that the inequality holds for all the numbers less than a given $\alpha$, and let us prove it for $\alpha$. Fix any $i$, $1 \leqslant i < \alpha$. With respect to Theorem 1, together with the inductive assumption, we have:

$$s(p^\alpha) \geqslant s(p^i) s(p^{\alpha - i})^{p^i} \geqslant s(p)^{\frac{p^i - 1}{p-1}} (s(p)^{\frac{p^{\alpha-i} - 1}{p-1}})^{p^i} = s(p)^{\frac{p^i - 1}{p-1} + \frac{p^\alpha - p^i}{p-1}} = s(p)^{\frac{p^\alpha - 1}{p-1}},$$

which was to be proved.

The second inequality follows from the first inequality and the lower bound from (1) (which, for a prime number $p$, reduces to $s(p) \geqslant \binom{p}{2}$).

b) We show only the first inequality (the second one directly follows by (4)). We proceed by induction on $k$. The base (for $k = 1$) is trivial (the inequality becomes $s(n) \geqslant s(n)$). Assume now that the inequality holds for $k-1$ and let us prove it for $k$. Since $p_k^{\alpha_k} \mid n$, by choosing $d = p_k^{\alpha_k}$ in (2) and then using the

inductive assumption, we get:

$$s(n) \geqslant s(p_k^{\alpha_k}) s\left(\prod_{i=1}^{k-1} p_i^{\alpha_i}\right)^{p_k^{\alpha_k}}$$
$$\geqslant s(p_k^{\alpha_k}) \left(\prod_{t=1}^{k-1} s(p_t^{\alpha_t})^{\prod_{j=t+1}^{k-1} p_j^{\alpha_j}}\right)^{p_k^{\alpha_k}} = s(p_k^{\alpha_k}) \prod_{t=1}^{k-1} s(p_t^{\alpha_t})^{\prod_{j=t+1}^{k} p_j^{\alpha_j}},$$

which was to be proved. □

**Remark 4.** Later in Section 3, for $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, it will be more convenient to write $n = p'_1 p'_2 \cdots p'_{k'}$ with $k' = \alpha_1 + \alpha_2 + \cdots + \alpha_k$ and $p'_1 = p'_2 = \cdots = p'_{\alpha_1} = p_1$ etc. Let us show that allowing this way of representing $n$ does not affect the rightmost bound from Corollary 3b). Indeed, starting from the considered bound that corresponds to the representation $n = p'_1 p'_2 \cdots p'_{k'}$, we have:

$$\begin{aligned}
\prod_{t=1}^{k'} \binom{p'_t}{2}^{\prod_{j=t+1}^{k'} p'_j} &= \left(\prod_{t=1}^{\alpha_1} \binom{p'_t}{2}^{\prod_{j=t+1}^{k'} p'_j}\right) \left(\prod_{t=\alpha_1+1}^{k'} \binom{p'_t}{2}^{\prod_{j=t+1}^{k'} p'_j}\right) \\
&= \binom{p_1}{2}^{(\sum_{t=1}^{\alpha_1} p_1^{\alpha_1 - t}) \prod_{j=\alpha_1+1}^{k'} p'_j} \left(\prod_{t=\alpha_1+1}^{k'} \binom{p'_t}{2}^{\prod_{j=t+1}^{k'} p'_j}\right) \\
&= \binom{p_1}{2}^{\frac{p_1^{\alpha_1}-1}{p_1-1} \prod_{j=2}^{k} p_j^{\alpha_j}} \left(\prod_{t=\alpha_1+1}^{k'} \binom{p'_t}{2}^{\prod_{j=t+1}^{k'} p'_j}\right) \\
&= \cdots = \prod_{t=1}^{k} \binom{p_t}{2}^{\frac{p_t^{\alpha_t}-1}{p_t-1} \prod_{j=t+1}^{k} p_j^{\alpha_j}},
\end{aligned}$$

which was to be shown.

Note that the ordering of the primes mentioned in the statement of Corollary 3b) was never used in the proof (that is, the assertion holds for any ordering), but the corollary was stated in the presented way because in that case we get the strongest inequality that is possible to obtain from (2) if for the prime values of $n$ (needed during the recursion) we use the bound $s(n) \geqslant \binom{n}{2}$. More formally, we have the following claim.

**Claim 5.** *Let $s'(n)$ be defined on odd integers $n$ greater than 1 in the following way:*

$$s'(n) = \begin{cases} \binom{n}{2}, & \text{if } n \text{ is a prime number;} \\ \max\limits_{d|n,\, d\neq 1,n} s'(d) s'\left(\frac{n}{d}\right)^d, & \text{otherwise.} \end{cases}$$

*Then $s'(n)$ equals the rightmost bound from Corollary 3b).*

Since the proof of this claim is quite technical, we give it in a separate section.

**Note.** In Table 1 we give a comparison of the old and the new lower bound on $s(n)$ for composite odd values of $n$ less than 40, where for the prime values of $n$ we have used the bound $s(n) \geqslant \binom{n}{2}$.

| $n$ | 9 | 15 | 21 | 25 | 27 | 33 | 35 | 39 |
|---|---|---|---|---|---|---|---|---|
| old bound | 27 | 30 | 63 | 250 | 243 | 165 | 210 | 234 |
| new bound | 81 | 3000 | 45 927 | 1 000 000 | 1 594 323 | 9 743 085 | 210 000 000 | 124 357 194 |

Table 1: Comparison of the lower bounds for composite odd $n$ less than 40.

With the help of a computer, we calculated that the lower bounds for $s(3)$, $s(5)$, $s(7)$, $s(9)$ and $s(11)$ are sharp (in other words, these five numbers are known exactly: they equal 3, 10, 21, 81 and 55, respectively). However, we have also been able to calculate the number $s(13)$, and we were quite surprised by the discovery that $s(13) = 91$, instead of the "expected" value 78 (this is actually the smallest possible improvement, since it is not hard to show that, in general, $n \mid s(n)$; however, it was still unexpected). One of the families achieving this value is given by:

$$\{(0,1,2,3,4,5,6,7,8,9,10,11,12), (0,1,2,3,6,7,8,4,12,9,11,5,19),$$
$$(0,3,5,9,4,1,10,7,2,6,8,11,12), (0,3,9,2,6,1,8,5,7,11,12,10,4),$$
$$(0,7,9,6,1,10,11,12,2,3,4,5,8), (0,9,6,1,5,7,10,12,3,11,8,4,2),$$
$$(0,11,12,3,5,2,9,4,8,1,7,10,6)\}$$

plus all the translations of these seven permutations (that is, their sum with a constant). This is not the only possible 91-member family: we have enumerated that there are exactly 273 such families (with an additional constraint that $\mathrm{id}_{13}$ belongs to all the families; this is not a loss of generalization, because we can always permute the order of elements in any considered family and thus obtain a family that contains $\mathrm{id}_{13}$), but been unable to find any noticeable pattern in any of them.

We would like to add: note that the equality $s(13) = 91$ leads to a further improvement of the lower bound on $s(39)$ from Table 1; namely, we now have $s(39) \geqslant 145\,083\,393$.

# 3 Proof of Claim 5

We first need the following two lemmas.

**Lemma 6.** *For any positive integers $n$ and $m$ greater than 2, we have*

$$\binom{n}{2}^{m-1} > \binom{m}{2}^{n-1}$$

*whenever $n$ precedes $m$ in the following order:* $4, 5, 3, 6, 7, 8, 9, 10, 11 \ldots$

*Proof.* It is easy to see that the function $x \mapsto (\frac{x(x-1)}{2})^{\frac{1}{x-1}}$ is decreasing for $x \geqslant 4$ (its first derivative equals $\frac{1}{(x-1)^2}(\frac{x(x-1)}{2})^{\frac{1}{x-1}}(2 - \frac{1}{x} - \ln\frac{x(x-1)}{2})$, which is negative for $x \geqslant 4$). We also directly check $\binom{5}{2}^{\frac{1}{4}} > \binom{3}{2}^{\frac{1}{2}} > \binom{6}{2}^{\frac{1}{5}}$, which completes the proof. □

For the rest of this section, whenever a sequence of integers follows the order from the previous lemma, we shall say that those integers are *in the happy order* (we do not require that those integers are different, unless stated otherwise; for example, $4, 5, 5, 3, 9, 9, 10 \ldots$ are in the happy order). Note that this is precisely the order in which the primes from the statement of Corollary 3b) are assumed to be.

**Lemma 7.** *Let a positive integer $l$, $l \geqslant 2$, be given. Assume that different primes $p_1, p_2, \ldots, p_l$ are given in the happy order, and let $\beta_1, \beta_2, \ldots, \beta_{l-1}$ be any positive integers. Then:*

$$\binom{p_l}{2}^{\prod_{j=1}^{l-1} p_j^{\beta_j} - 1} < \prod_{t=1}^{l-1} \binom{p_t}{2}^{\frac{p_t^{\beta_t}-1}{p_t-1}(\prod_{j=t+1}^{l-1} p_j^{\beta_j})(p_l-1)}. \tag{5}$$

*Proof.* We proceed by induction on $l$. For $l = 2$, the asserted inequality reduces to

$$\binom{p_2}{2}^{p_1^{\beta_1}-1} < \binom{p_1}{2}^{\frac{p_1^{\beta_1}-1}{p_1-1}(p_2-1)},$$

which is equivalent to

$$\binom{p_2}{2}^{p_1-1} < \binom{p_1}{2}^{p_2-1},$$

and this is true by the previous lemma.

Assume now that the assertion holds for $l-1$ and let us prove it for $l$. We have:

$$\begin{aligned}\binom{p_l}{2}^{\prod_{j=1}^{l-1} p_j^{\beta_j} - 1} &= \binom{p_l}{2}^{\prod_{j=1}^{l-1} p_j^{\beta_j} - p_{l-1}^{\beta_{l-1}} + p_{l-1}^{\beta_{l-1}} - 1} \\ &= \left(\binom{p_l}{2}^{\prod_{j=1}^{l-2} p_j^{\beta_j} - 1}\right)^{p_{l-1}^{\beta_{l-1}}} \binom{p_l}{2}^{p_{l-1}^{\beta_{l-1}} - 1}.\end{aligned}$$

By the inductive assumption, as well as the base case, we have:

$$\binom{p_l}{2}^{\prod_{j=1}^{l-2} p_j^{\beta_j}-1} < \prod_{t=1}^{l-2} \binom{p_t}{2}^{\frac{p_t^{\beta_t}-1}{p_t-1}(\prod_{j=t+1}^{l-2} p_j^{\beta_j})(p_l-1)}$$

and

$$\binom{p_l}{2}^{p_{l-1}^{\beta_{l-1}}-1} < \binom{p_{l-1}}{2}^{\frac{p_{l-1}^{\beta_{l-1}}-1}{p_{l-1}-1}(p_l-1)}.$$

The asserted inequality now clearly follows. □

We are now ready for the main part of this section.

*Proof of Claim 5.* During the course of the proof, we let $n = p_1 p_2 p_3 \cdots p_k$, where $p_1, p_2, \ldots, p_k$ are (not necessarily different) primes in the happy order. We proceed by total induction on $k$. For $k = 1$, that is, a prime $n$, the assertion reduces to $s'(n) = \binom{n}{2}$, which is true by the definition. Assume now that the assertion holds for all numbers less than a given $k$, and let us prove it for $k$. The proof will be divided into two parts.

**Part 1.** In this part we prove that, if $d$ is a proper divisor of $n$ of the form $d = p_l p_{l+1} p_{l+2} \cdots p_k$ for some $l$, $1 < l \leqslant k$, then, for each such divisor $d$, we have:

$$s'(d) s'\left(\frac{n}{d}\right)^d = \prod_{t=1}^{k} \binom{p_t}{2}^{\prod_{j=t+1}^{k} p_j}$$

(note that the right-hand side does not depend on $d$; further note, the right-hand side is exactly the bound we want to prove, because of Remark 4). We show this by direct calculation, relying on the inductive assumption:

$$\begin{aligned}
s'(d) s'\left(\frac{n}{d}\right)^d &= s'\left(\prod_{j=l}^{k} p_j\right) s'\left(\prod_{j=1}^{l-1} p_j\right)^{\prod_{j=l}^{k} p_j} \\
&= \left(\prod_{t=l}^{k} \binom{p_t}{2}^{\prod_{j=t+1}^{k} p_j}\right) \left(\prod_{t=1}^{l-1} \binom{p_t}{2}^{\prod_{j=t+1}^{l-1} p_j}\right)^{\prod_{j=l}^{k} p_j} \\
&= \left(\prod_{t=l}^{k} \binom{p_t}{2}^{\prod_{j=t+1}^{k} p_j}\right) \left(\prod_{t=1}^{l-1} \binom{p_t}{2}^{\prod_{j=t+1}^{k} p_j}\right) \\
&= \prod_{t=1}^{k} \binom{p_t}{2}^{\prod_{j=t+1}^{k} p_j},
\end{aligned}$$

which was to be proved.

**Part 2.** Let $d$ be a divisor of $n$, $d \neq 1, n$, for which $s'(d) s'(\frac{n}{d})^d$ reaches its maximal value. It is enough to prove that $d$ can be represented in the form considered in Part 1. The divisor $d$ can be written in the form $p_{u_1} p_{u_2} \cdots p_{u_a}$

where $1 \leqslant u_1 < u_2 < \cdots < u_a \leqslant k$; we may also assume, without loss of generality, that whenever $p_i = p_j$ for $i < j$, then it is not possible that $i$ is among $u_1, u_2, \ldots, u_a$ while $j$ is not (in other words, within each cluster of same primes, all the "selected ones" have larger indices than all those that are not "selected"). Let $v_1, v_2, \ldots, v_b$ be such that $1 \leqslant v_1 < v_2 < \cdots < v_b \leqslant k$ and $\{v_1, v_2, \ldots, v_b\} = \{1, 2, \ldots, k\} \setminus \{u_1, u_2, \ldots, u_a\}$ (note that then $p_{v_1} p_{v_2} \cdots p_{v_b} = \frac{n}{d}$). We need to prove that $(v_1, v_2, \ldots, v_b) = (1, 2, \ldots, b)$ and, consequently, $(u_1, u_2, \ldots, u_a) = (b+1, b+2, \ldots, k)$.

Let $d' = p_{v_b} d$. Note that $d' \mid n$. Also, $d'$ is a proper divisor, unless $b = 1$; this exceptional case will be treated at the end of the proof, for now we assume $d' \neq n$. By the choice of $d$, we have

$$s'(d) s'\left(\frac{n}{d}\right)^d \geqslant s'(d') s'\left(\frac{n}{d'}\right)^{d'}.$$

By the inductive assumption, this reduces to:

$$\begin{aligned}
&\left(\prod_{t=1}^{a} \binom{p_{u_t}}{2}^{\prod_{j=t+1}^{a} p_{u_j}}\right) \left(\prod_{t=1}^{b} \binom{p_{v_t}}{2}^{\prod_{j=t+1}^{b} p_{v_j}}\right)^{\prod_{j=1}^{a} p_{u_j}} \\
&\quad \geqslant \left(\prod_{\substack{t=1 \\ u_t < v_b}}^{a} \binom{p_{u_t}}{2}^{(\prod_{j=t+1}^{a} p_{u_j}) p_{v_b}}\right) \binom{p_{v_b}}{2}^{\prod_{j=v_b+1}^{k} p_j} \left(\prod_{t=v_b+1}^{k} \binom{p_t}{2}^{\prod_{j=t+1}^{k} p_j}\right) \\
&\qquad \cdot \left(\prod_{t=1}^{b-1} \binom{p_{v_t}}{2}^{\prod_{j=t+1}^{b-1} p_{v_j}}\right)^{(\prod_{j=1}^{a} p_{u_j}) p_{v_b}}.
\end{aligned} \tag{6}$$

The third and the fourth factor on the right-hand side also appear on the left-hand side (the fourth factor is obviously a part of the second parenthesis, while we can see that the third factor is a part of the first parenthesis, since $v_b + 1, v_b + 2, \ldots, k$ are exactly those $u_t$'s that are larger than $v_b$). Canceling them leaves:

$$\begin{aligned}
&\left(\prod_{\substack{t=1 \\ u_t < v_b}}^{a} \binom{p_{u_t}}{2}^{\prod_{j=t+1}^{a} p_{u_j}}\right) \binom{p_{v_b}}{2}^{\prod_{j=1}^{a} p_{u_j}} \\
&\qquad \geqslant \left(\prod_{\substack{t=1 \\ u_t < v_b}}^{a} \binom{p_{u_t}}{2}^{(\prod_{j=t+1}^{a} p_{u_j}) p_{v_b}}\right) \binom{p_{v_b}}{2}^{\prod_{j=v_b+1}^{k} p_j}.
\end{aligned}$$

We now note that there are further cancellations possible, which reduces the

considered inequality to:

$$\binom{p_{v_b}}{2}^{(\prod_{1\leqslant j\leqslant a,\, u_j<v_b} p_{u_j}-1)\prod_{j=v_b+1}^{k} p_j} \geqslant \prod_{\substack{t=1\\ u_t<v_b}}^{a} \binom{p_{u_t}}{2}^{(\prod_{j=t+1}^{a} p_{u_j})(p_{v_b}-1)}.$$

Raising both sides to the power $\frac{1}{\prod_{j=v_b+1}^{k} p_j}$ leaves:

$$\binom{p_{v_b}}{2}^{\prod_{1\leqslant j\leqslant a,\, u_j<v_b} p_{u_j}-1} \geqslant \prod_{\substack{t=1\\ u_t<v_b}}^{a} \binom{p_{u_t}}{2}^{(\prod_{t+1\leqslant j\leqslant a,\, u_j<v_b} p_{u_j})(p_{v_b}-1)}. \tag{7}$$

We are now left only to note that, if there existed a number $u_j$ less than $v_b$, the last inequality would contradict Lemma 7. Indeed, in that case, for $p_1, p_2, \ldots, p_l$ in the lemma we can take all the different primes from $\{p_{u_j} : 1 \leqslant j \leqslant a,\, u_j < v_b\} \cup \{p_{v_b}\}$ (enumerated in the happy order), and for $\beta_1, \beta_2, \ldots, \beta_{l-1}$ we take their multiplicities (of all but $p_{v_b}$); then the left-hand side of (5) is exactly the left-hand side of (7), while the right-hand side of (5) can also be seen to be equal to the right-hand side of (7), because of Remark 4. This completes the proof, unless (recall) the exceptional case $b = 1$ and $d = \frac{n}{p_{v_1}}$.

Finally, assume that $s'(d)s'(\frac{n}{d})^d$ achieves its maximal value in the described exceptional case. We need to show that in this case the only possibility is $v_1 = 1$. We have:

$$s'\left(\frac{n}{p_{v_1}}\right) s'(p_{v_1})^{\frac{n}{p_{v_1}}} \geqslant \prod_{t=1}^{k} \binom{p_t}{2}^{\prod_{j=t+1}^{k} p_j}$$

(since the value on the right-hand side has been reached in Part 1, and the expression on the left-hand side is assumed to be the maximum). However, we can see (by direct comparison) that this inequality is again (6), and thus we again conclude that there does not exist a number $u_j$ less than $v_1$, which gives $v_1 = 1$. The proof is thus finished. □

# 4 A kind of optimality

It turns out that the collection constructed in the proof of Theorem 1 is maximal in the sense that it is not possible to add any more permutations to it while maintaining the required property (note that, of course, this does not imply that the obtained lower bound is the best possible).

**Claim 8.** *Let $S$ be the set (3) from the proof of Theorem 1. Then for any permutation $\pi$ of $\mathbb{Z}_n$ such that $\pi \notin S$ there exists $\pi' \in S$ such that $\pi + \pi'$ is not a permutation of $\mathbb{Z}_n$.*

*Proof.* Let $S$ be as in (3) (the necessary notation is transferred from the proof

of Theorem 1). Let $\pi$ be a permutation of $\mathbb{Z}_n$ such that $\pi + \pi'$ is also a permutation whenever $\pi' \in S$. We need to prove that $\pi \in S$.

Let

$$\pi' = (0, d, \ldots, n-d)^\frown(1, d+1, \ldots, n-d+1)^\frown \cdots^\frown (d-1, 2d-1, \ldots, n-1);$$

in other words, $\pi'$ is obtained as in (3) for $\pi_0 = \pi_1 = \cdots = \pi_{d-1} = \mathrm{id}_{\frac{n}{d}}$ and $\sigma = \mathrm{id}_d$.

First we are going to show that for a fixed $i \in \mathbb{Z}_d$ there exists $q \in \mathbb{Z}_d$ such that, for all $x \in \mathbb{Z}_{\frac{n}{d}}$, we have $\pi(\frac{n}{d}i + x) \equiv q \pmod d$. Suppose that this were not the case. We claim that there exist $x, y \in \mathbb{Z}_d$ and $i, j \in \mathbb{Z}_{\frac{n}{d}}$, where $i \neq j$, such that:

$$(\pi + \pi')\left(\frac{n}{d}i + x\right) \equiv (\pi + \pi')\left(\frac{n}{d}j + y\right) \pmod d. \tag{8}$$

Indeed, since $\pi + \pi'$ is a permutation of $\mathbb{Z}_n$, it is enough to show that there exists $i \in \mathbb{Z}_{\frac{n}{d}}$ such that $(\pi+\pi')(\frac{n}{d}i+x)$ is not constant modulo $d$ for $x \in \mathbb{Z}_d$. But such $i$ must exist, since otherwise, having in mind that $\pi'(\frac{n}{d}i + x)$ is constant modulo $d$ for $x \in \mathbb{Z}_d$, it would follow that $\pi(\frac{n}{d}i + x)$ is also constant modulo $d$ for $x \in \mathbb{Z}_d$, which was supposed not to be the case (for at least one $i$).

Since $\pi'(\frac{n}{d}i + x) = dx + i$ (and similarly for $j, y$), (8) reduces to:

$$\pi\left(\frac{n}{d}i + x\right) + dx + i \equiv \pi\left(\frac{n}{d}j + y\right) + dy + j \pmod d.$$

Let $\pi(\frac{n}{d}i + x) + dx + i = dk + u$ and $\pi(\frac{n}{d}j + y) + dy + j = dr + u$ for some $k, r \in \mathbb{Z}_{\frac{n}{d}}$ and $u \in \mathbb{Z}_d$. Clearly, $k \neq r$, and we may assume, w.l.o.g., $k > r$. Let now $\pi''$ be a permutation obtained from the same parameters as $\pi'$, with the only change that instead of $\pi_j = \mathrm{id}_{\frac{n}{d}}$ (which was the case for $\pi'$) we now let $\pi_j = \mathrm{id}_{\frac{n}{d}} + k - r$. Since $\mathrm{id}_{\frac{n}{d}} + k - r \in S_{\frac{n}{d}}$ (by Lemma 2), we conclude $\pi'' \in S$. Now we have:

$$(\pi + \pi'')\left(\frac{n}{d}i + x\right) = (\pi + \pi')\left(\frac{n}{d}i + x\right) = dk + u$$

and

$$\begin{aligned}(\pi + \pi'')\left(\frac{n}{d}j + y\right) &= \pi\left(\frac{n}{d}j + y\right) + (d(y + k - r) + j) \\ &= \pi\left(\frac{n}{d}j + y\right) + dy + j + d(k - r) = dr + u + d(k - r) \\ &= dk + u,\end{aligned}$$

which is a contradiction.

Therefore, we conclude:

$$\pi = (d\pi_0 + \sigma(0))^\frown(d\pi_1 + \sigma(1))^\frown \cdots^\frown (d\pi_{d-1} + \sigma(d-1)),$$

where $\pi_0, \pi_1, \ldots, \pi_{d-1}$ are permutations of $\mathbb{Z}_{\frac{n}{d}}$ and $\sigma$ is a permutation of $\mathbb{Z}_d$. It remains to show that $\sigma \in S_d$ and $\pi_i \in S_{\frac{n}{d}}$ for $i \in \{0, 1, \ldots, d-1\}$.

Since $\pi + \pi'$ is a permutation for every $\pi' \in S$, it easily follows that $\sigma + \sigma'$ is a permutation for every $\sigma' \in S_d$, which implies $\sigma \in S_d$. The argument that $\pi_i \in S_{\frac{n}{d}}$ for $i \in \{0, 1, \ldots, d-1\}$ is similar. This completes the proof. □

# Acknowledgments

The authors would like to thank the anonymous reviewers for their devoted time and the careful reading of the article. A suggestion from one of the reviewers led to a better exposition of the proof of Claim 5.

The authors were supported by the Ministry of Education, Science and Technological Development of Serbia (grant no. 451-03-68/2020-14/200125).

# References

[1] Chandran, L. S., Rajendraprasad, D., and Singh, N. On additive combinatorics of permutations of $\mathbb{Z}_n$. *Discrete Math. Theor. Comput. Sci. 16* (2014), 35–40.

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

[3] Ellis, D., Friedgut, E., and Pilpel, H. Intersecting families of permutations. *J. Amer. Math. Soc. 24* (2011), 649–682.

[4] Evans, A. B. On orthogonal orthomorphisms of cyclic and non-abelian groups. II. *J. Combin. Des. 15* (2007), 195–209.

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

[6] Kovács, I., and Soltész, D. On $k$-neighbor separated permutations. *SIAM J. Discrete Math. 33* (2019), 1691–1711.

[7] Park, K.-H., Song, H.-Y., Kim, D. S., and Golomb, S. W. Optimal families of perfect polyphase sequences from the array structure of Fermat-quotient sequences. *IEEE Trans. Inform. Theory 62* (2016), 1076–1086.

[8] Zhou, Z., Zhang, D., Helleseth, T., and Wen, J. A construction of multiple optimal ZCZ sequence sets with good cross correlation. *IEEE Trans. Inform. Theory 64* (2018), 1340–1346.