

Distinct partial products in prime dihedral groups

Abstract

Let D_{2p} be the dihedral group of order $2p$, where p is prime. For every fixed $0 < \alpha < 1$, we prove that every subset $A \subseteq D_{2p} \setminus \{e\}$ with $C_\alpha \leq |A| \leq p^\alpha$ admits an ordering whose nonempty partial products are pairwise distinct. Combined with the known small- and large-set theorems, this covers every subset size for all sufficiently large primes. Pairing reflections reduces the products to partial sums with fixed parity-labelled offsets. Two passes of block rotations remove distant collisions; bounded displacement allows the local condition to exclude the remaining collisions. The existence of suitable rotations follows from Pham–Sauermaann’s subset-sum anticoncentration theorem, an affine-rank estimate, and a count of clustered collision witnesses.

1 Introduction

An ordering $a_1, \dots, a_n$ of a finite subset A of a group is *valid* if its nonempty partial products

$$P_1 = a_1, \quad P_2 = a_1 a_2, \quad \dots, \quad P_n = a_1 \cdots a_n$$

are pairwise distinct. The empty product $P_0 = e$ is excluded from this condition. Graham [7, Problem 10, p. 36] asked whether every subset of $\mathbb{Z}_p \setminus \{0\}$ has a valid ordering, for every prime p ; the question was repeated by Erdős and Graham [6, p. 95]. The corresponding nonabelian problem asks for distinct partial products. We consider the dihedral group D_{2p} of order $2p$.

Theorem 1.1. *For every $0 < \alpha < 1$ there is an integer C_α such that, for every prime p , every subset $A \subseteq D_{2p} \setminus \{e\}$ satisfying*

$$C_\alpha \leq |A| \leq p^\alpha$$

has a valid ordering.

Corollary 1.2. *For all sufficiently large primes p , every subset of $D_{2p} \setminus \{e\}$ has a valid ordering.*

The proof of Corollary 1.2 uses the eventual overlap of three size ranges and leaves a finite set of primes untreated. The assertion for every prime is unresolved. The constants in Theorem 1.1 are not optimised.

The size range in Theorem 1.1 lies between two existing results. The small-set theorem [4, Theorem 1.3] gives a stronger sequencing property for dihedral subsets of size at most $\exp(c_s(\log p)^{1/4})$, with an absolute $c_s > 0$. It extends the small-set method of Bedert and Kravitz [2] to suitable semidirect products. The general large-set theorem [3, Theorem 1.4] guarantees that, for an absolute $c > 0$, every subset $S \subseteq G \setminus \{e\}$ of any finite group G with

$|S| \geq |G|^{1-c}$ has a valid ordering. These ranges overlap the range of Theorem 1.1 for a suitable fixed $\alpha < 1$, giving Corollary 1.2.

Ollis [12] studied distinct partial products in dihedral groups. For prime cyclic groups, Pham and Sauermann [13, Theorem 1.2] proved the intermediate range $C_\alpha \leq |A| \leq p^\alpha$, and hence Graham's conjecture for sufficiently large primes. Their exponent is written $1 - \alpha$; we have reparametrised it. Their proof combines subset-sum anticoncentration with local changes to a random ordering. The dihedral intermediate range is explicitly identified as a further problem after extensions to cyclic groups [5, Section 7]. Theorem 1.1 supplies that range by an additive reduction which retains the signs caused by reflections.

There is also a graph formulation. In the directed Cayley graph, give the edge $g \rightarrow ga$ colour a . For nonempty A , a valid ordering exists if and only if some $a \in A$ can be omitted so that the remaining colours form a simple directed rainbow path. Indeed, left multiplication of $P_1, \dots, P_n$ by a_1^{-1} gives the distinct prefixes, including the empty prefix, of $a_2, \dots, a_n$. Conversely, prepending the omitted element to such an ordering translates its entire prefix list. This equivalence explains the endpoint convention: a simple path using all colours would impose the additional requirement that P_0 be distinct from every P_j .

1.1 The proof

Write $D_{2p} = \mathbb{F}_p \rtimes \mathbb{Z}_2$, with

$$(x, \epsilon)(y, \delta) = (x + (-1)^\epsilon y, \epsilon + \delta).$$

A reflection reverses every subsequent sign until the next reflection. Pairing reflections into cells of length at most four produces $m \geq |A|/4$ variable positions, all with coefficient $+1$. After the other entries have been fixed, the variables $x_1, \dots, x_m$ form a uniform permutation of a fixed subset of $\mathbb{F}_p$. Every partial product in cell j then belongs to

$$s_j + \mathcal{D}_j, \quad s_j = \sum_{h \leq j} x_h, \quad \mathcal{D}_j \subseteq \mathbb{F}_p \times \mathbb{Z}_2, \quad |\mathcal{D}_j| \leq 4,$$

where the sets $\mathcal{D}_j$ remain attached to their positions when variables are permuted. Parity-preserving permutations in semidirect products already appear in [4, Section 2].

For each fixed K , the permutation local lemma gives a probability $c_K > 0$ that every short identity subword is absent, even after arbitrary variable permutations in any window of at most K cells. The lower bound is uniform in the ratio of the rotation and reflection counts. For a small reflection pool, a pattern count proportional to its size cancels the corresponding probability denominator; see Appendix A. Separately, with probability tending to one on every fixed-decoration fibre, each member of a predetermined linear-size family of blocks has a cyclic rotation avoiding all distant target sets. Two staggered passes of these rotations preserve selected cut sums and move every variable by a bounded distance. Any remaining collision can therefore be reproduced by a permutation inside an original bounded window, contradicting the local condition.

The distant-avoidance estimate uses the sharp subset-sum theorem [13, Theorem 1.3]. If all ℓ cyclic rotations of one block fail, one collision per rotation gives an affine system $Hx = z$. Suppose its target anchors form q clusters separated from the source cluster. The

affine dimension of the columns of H is at least $(\ell + q)/2$; long gaps also supply q independent differences of repeated columns. Conditioning on disjoint position pools then yields

$$\Pr(Hx = z) = O(m^{-(\ell+q)/2-\eta q}), \quad \eta = \min\{\beta, 1/6\}, \quad p \geq m^{1+\beta}.$$

With gap scale $m^{1/3}$, there are $O(m^q m^{(\ell-q)/3})$ anchor tuples, giving a total of $O(m^{-\eta \ell})$. Clustered targets have fewer possible locations; separated targets give stronger anticoncentration. This balance permits a union bound over the entire repair family.

The reservoir exposure is related to the chain estimate [13, Corollary 4.2] and to the standard rank-exposure argument [11]; see also [9, Lemma 3.7]. The boundary constraints [2, Section 6] and transposition repairs [13, Section 5] are antecedents of the random-ordering and local-repair approach. The fixed-offset calculation, the repeated-column estimate and the two-pass rotation argument are proved below.

2 Cells and fixed offsets

For an odd prime p , use coordinates

$$D_{2p} = \mathbb{F}_p \rtimes \mathbb{Z}_2, \quad (x, \epsilon)(y, \delta) = (x + (-1)^\epsilon y, \epsilon + \delta).$$

Let $A \subseteq D_{2p} \setminus \{e\}$ be nonempty. Write $R \subseteq \mathbb{F}_p^\times$ and $F \subseteq \mathbb{F}_p$ for its rotation and reflection coordinate sets, and put $r = |R|$, $f = |F|$ and $n = r + f$. Coordinates within either pool are distinct; the two pools may intersect. For $s \in \mathbb{F}_p$ and $(c, \epsilon) \in \mathbb{F}_p \times \mathbb{Z}_2$, write $s + (c, \epsilon) = (s + c, \epsilon)$.

Lemma 2.1. *There is a random arrangement of A into m consecutive cells, each beginning with a variable, such that $n/4 \leq m \leq n$ and every cell has length at most four. All variables have the same type and distinct coordinates. Conditional on the nonvariable entries and the variable coordinate set X , their coordinates $x_1, \dots, x_m$ form a uniform permutation of X . There are fixed sets $\mathcal{D}_j \subseteq \mathbb{F}_p \times \mathbb{Z}_2$, $|\mathcal{D}_j| \leq 4$, such that, for every assignment of X to the variables, the nonempty prefixes ending in cell j are exactly*

$$s_j + \mathcal{D}_j, \quad s_j = \sum_{h=1}^j x_h. \tag{2.1}$$

The prefixes within each cell are pairwise distinct for every assignment.

Proof. In the *rotation-majority* case $r \geq f$, take $m = r$ cells, each starting with a variable rotation. For $f = 2t$, append two reflection slots to each of t distinct cells. For $f = 2t + 1$, reserve the last cell for one reflection and append two reflections to each of t earlier cells. Any such choice of cells is allowed and is fixed before sampling. The reservation is feasible since $2t + 1 \leq m$ implies $t \leq m - 1$. The types are

$$(\underline{R}), \quad (\underline{R}, F, F), \quad \text{possibly a final } (\underline{R}, F).$$

Choose independent uniform assignments of R and F to their slots, with an empty permutation space interpreted as a singleton. Conditioning on the reflections leaves a uniform permutation of $X = R$. Here $m \geq n/2$, and each cell has length at most three.

In the *reflection-majority* case $f > r$, start with f successive reflection slots. Choose arbitrary distinct reflection slots after which to place the rotations, and fix an arbitrary bijection from these rotation slots to R before sampling. Only the reflection assignment is random in this case. Assign F uniformly to its slots, pair successive reflections into cells and retain each following rotation in its reflection's cell. The types are

$$(\underline{E}, [R], F, [R]), \quad \text{possibly a final } (\underline{E}, [R]),$$

where brackets indicate optional entries and odd reflection slots are variable. Then $m = \lceil f/2 \rceil > n/4$, and cells have length at most four. Conditioning on the even reflection slots leaves a uniform bijection from the odd slots to the remaining set X .

Every nonfinal cell has even reflection parity, so the prefix preceding each variable has parity zero and its coordinate has coefficient $+1$. Permutations within fixed parity classes that preserve the total product in a semidirect product also occur in [4, Section 2]. Let $\epsilon_* \in \mathbb{Z}_2$ be the common variable type. If cell j has d_j fixed entries following its variable, let $(u_{j,h}, v_{j,h})$ be the product of their first h entries, including $(u_{j,0}, v_{j,0}) = (0, 0)$. Set

$$C_0 = 0, \quad C_j = C_{j-1} + (-1)^{\epsilon_*} u_{j,d_j},$$

$$\mathcal{D}_j = \{(C_{j-1} + (-1)^{\epsilon_*} u_{j,h}, \epsilon_* + v_{j,h}) : 0 \leq h \leq d_j\}.$$

The product before cell j is $(s_{j-1} + C_{j-1}, 0)$, proving (2.1). The possible odd parity of the final cell occurs after its variable and causes no exception.

Subtracting $s_j + C_{j-1}$, a paired rotation cell with reflections y, z has prefixes

$$(0, 0), \quad (y, 1), \quad (y - z, 0).$$

Its equal-parity pair differs by $y - z \neq 0$. A paired reflection cell with second reflection y and optional rotations a, b has prefixes

$$(0, 1), \quad (-a, 1), \quad (-a - y, 0), \quad (-a - y + b, 0).$$

If a is absent, set $a = 0$ and omit the second point; if b is absent, omit the fourth. Every remaining equal-parity pair differs by a present nonzero rotation coordinate. The shorter cells satisfy the same checks. $\square$

3 Robust local separation

Fix an integer $K \geq 1$ and consider the full probability space of Lemma 2.1. In the rotation-majority case this includes both independent permutation factors; in the reflection-majority case only the reflection assignment is random. Let $\mathcal{L}_K$ be the event that, in every interval of at most K cells, every permutation of its variables leaves every nonempty contiguous subword in that interval with nonidentity product. For each realisation, these permutations move only variable coordinates among variable slots in the chosen window. All nonvariable entries, including sampled nonvariable reflections, remain fixed during these permutations.

Lemma 3.1. *There are $m_0(K)$ and $c_K > 0$, depending only on K , such that $m \geq m_0(K)$ implies*

$$\Pr(\mathcal{L}_K) \geq c_K$$

in either cell construction, uniformly over p, A , the permitted placements and the ratio of the two pool sizes.

The proof, given in Appendix A, applies the quantitative permutation local lemma to canonical assignments. Its probability is unconditional in the cell construction. In particular, no lower bound on each fixed-decoration fibre is asserted. The condition excludes short identity subwords beginning at the first entry as well as those between two nonempty prefixes; the final conclusion still concerns nonempty prefixes only.

4 Two-pass repair

Fix $k \geq 2$, put $M = 4k$ and suppose $m \geq k$. Let $x_1, \dots, x_m \in \mathbb{F}_p$, set $s_t = \sum_{j \leq t} x_j$, $s_0 = 0$, and fix $\mathcal{D}_j \subseteq \mathbb{F}_p \times \mathbb{Z}_2$ with $|\mathcal{D}_j| \leq B$. All indices refer to the original ordering, and decorations remain attached to positions. For $0 \leq t \leq m$, define

$$\mathcal{V}_t = \left\{ s_t + \sum_{j \in J} x_j + d : \begin{array}{l} J \subseteq \{t+1, \dots, \min(m, t+M)\}, \\ d \in \mathcal{D}_h, \quad h \in [1, m] \cap [t, t+M] \end{array} \right\}. \quad (4.1)$$

Then $|\mathcal{V}_t| \leq B(M+1)2^M$ and $\mathcal{V}_m = s_m + \mathcal{D}_m$.

A source consists of a window $W = \{b+1, \dots, b+w\} \subseteq [m]$ of length $w \leq M$, disjoint sets $U, Q \subseteq W$ with $k \leq |Q| \leq 2k$, and a cyclic order of Q . A rotation is safe if

$$s_b + \sum_{j \in U} x_j + \sum_{j \in I} x_j + d \notin \mathcal{V}_t \quad (4.2)$$

for every nonempty proper prefix I of the rotation, every $d \in \bigcup_{h \in [1, m] \cap [b, b+M]} \mathcal{D}_h$ and every $t \in \{0, \dots, m\}$ with $|t - b| > 2M$. A prefix denotes its set of original labels when used in a sum. The window W bounds original labels; the rotating list may occupy different positions. Since the safety test includes every decoration in the source interval, it protects the list's proper prefixes whenever they end at positions in $[1, m] \cap [b, b+M]$ and the list has starting sum $s_b + \sum_{j \in U} x_j$.

Partition $[m]$ into consecutive intervals $Q_i = \{b_i + 1, \dots, b_i + n_i\}$, $k \leq n_i \leq 2k$, $1 \leq i \leq a$. Such a partition exists by using lengths $k+u, k, \dots, k$ when $m = ak + u$, $0 \leq u < k$. For $c \in Q_i$, let $T_i(c)$ be the original cyclic order of Q_i starting after c and omitting c . Before sampling coordinates, list the following sources:

1. For each i , use $b = b_i$, $W = Q_i$, $U = \emptyset$, $Q = Q_i$ and its original cyclic order.
2. For each $i < a$ and $(c, d) \in Q_i \times Q_{i+1}$, use $b = b_i$, $W = Q_i \cup Q_{i+1}$, $U = \{c\}$, $Q = (Q_i \setminus \{c\}) \cup \{d\}$ and cyclic order $(T_i(c), d)$.

Let $\mathcal{R}_{\text{menu}}$ assert that every listed source has a safe rotation. The list has at most

$$a + \sum_{i < a} n_i n_{i+1} \leq (1 + 4k^2)m/k \quad (4.3)$$

items, all satisfying the source restrictions.

Proposition 4.1. *If $\mathcal{R}_{\text{menu}}$ holds, there is a permutation σ of $[m]$ with $|\sigma(j) - j| \leq 4k - 2 < M$ such that, on setting $u_j = \sum_{h \leq j} x_{\sigma(h)}$, equality between a point of $u_i + \mathcal{D}_i$ and a point of $u_j + \mathcal{D}_j$, $i < j$, implies $j - i \leq 4M$.*

Proof. For each source of the first family, choose a safe rotation, let c_i be its first label, and write the block as $(c_i, T_i(c_i))$. After this first pass, completed blocks retain their sums, so every proper nonempty prefix inside block i is $s_{b_i} + \sum_{h \in I} x_h$. With its position's decoration, this lies in $\mathcal{V}_{b_i}$ and avoids $\mathcal{V}_t$ for $|t - b_i| > 2M$. Put a cut at $h_i = b_i + 1$. Since $n_i \geq 2$, its prefix is proper and has sum

$$s_{b_i} + x_{c_i}. \quad (4.4)$$

The list between cuts h_i and h_{i+1} is $P_i = (T_i(c_i), c_{i+1})$, of length n_i . Rotate it safely using the second-family source indexed by (i, c_i, c_{i+1}) . These position intervals are disjoint. Their preserved sums, together with the fixed first label c_1 , preserve every cut sum (4.4), even if its label moves. Thus $s_{b_i} + x_{c_i}$ remains the starting sum for P_i , even though the sum through the original boundary b_i may change. For $h_i < j < h_{i+1}$, the final prefix is

$$u_j = s_{b_i} + x_{c_i} + \sum_{h \in I} x_h,$$

where I is a proper nonempty prefix of the chosen rotation of P_i . The labels in $\{c_i\} \cup I$ lie within M original positions after b_i , and $j \in [b_i, b_i + M]$. Thus (4.1) and (4.2) give membership and protection at the original anchor b_i .

Leave the final tail $T_a(c_a)$ unchanged. Its preceding cut sum is preserved, so its prefixes retain their first-pass values. The cuts, interiors between cuts and final tail cover every position $j < m$. For each such j , the corresponding original boundary $a_j = b_i$ satisfies

$$\begin{aligned} |j - a_j| &\leq M, & u_j + \mathcal{D}_j &\subseteq \mathcal{V}_{a_j}, \\ (u_j + \mathcal{D}_j) \cap \mathcal{V}_t &= \emptyset & \text{if } |t - a_j| > 2M. \end{aligned} \quad (4.5)$$

When there is one block, the first pass alone gives these conclusions. At the final position, $u_m = s_m$ and $u_m + \mathcal{D}_m = \mathcal{V}_m$; set $a_m = m$.

Each pass moves labels within intervals of length at most $2k$, so their composition has displacement at most $4k - 2$. If decorated points at $i < j$ coincide, protection at $i < m$ and membership at j force $|a_i - a_j| \leq 2M$. Hence $j - i \leq |i - a_i| + |a_i - a_j| + |a_j - j| \leq 4M$. $\square$

Lemma 4.2. *Suppose a cell realisation satisfies $\mathcal{L}_K$ for $K \geq 6M + 1$. After any variable permutation σ with $|\sigma(h) - h| \leq M$, no equal nonempty prefixes can end in distinct cells $i < j$ with $j - i \leq 4M$.*

Proof. Equal prefixes give an identity subword by left cancellation. It begins after the selected prefix in cell i , which already contains that cell's variable, and ends in cell j . The subword therefore starts strictly after the variable of cell i and uses exactly the variable slots $i + 1, \dots, j$; its other entries remain fixed. The interval

$$W = [\max(1, i - M), \min(m, j + M)] \cap \mathbb{Z}$$

contains the subword's cells and every original variable label $\sigma(h)$ it uses, and $|W| \leq j - i + 2M + 1 \leq 6M + 1$. The prescriptions $h \mapsto \sigma(h)$ for $i + 1 \leq h \leq j$ form a partial injection of W into itself. Extend it to a permutation of W by matching unused domain and range points. That local permutation reproduces the identity subword in the original realisation, contradicting $\mathcal{L}_K$. $\square$

5 Subset-sum anticoncentration

The analytic input is the following theorem of Pham and Saueremann.

Theorem 5.1 ([13, Theorem 1.3]). *There is an absolute constant $C \geq 1$ such that the following holds. Let p be prime, let $Y \subseteq \mathbb{F}_p$ have size $N \geq 2$, and let Z be a uniformly random v -element subset of Y , where*

$$C \log N \leq v \leq 10^{-3} N / \log N.$$

Then

$$\sup_{z \in \mathbb{F}_p} \Pr \left(\sum_{y \in Z} y = z \right) \leq \frac{1}{p} + \frac{C}{N \sqrt{v}}.$$

Zero is allowed in Y . Fix $\beta > 0$ and put

$$L = \lfloor m^{1/3} \rfloor, \quad \eta = \min\{\beta, 1/6\}. \quad (5.1)$$

The cube-root scale balances the scalar estimate with the count of clustered collision witnesses.

Lemma 5.2. *For each fixed $0 < a \leq 1$, there is a threshold m_a , depending only on a and C , with the following property. Suppose $m \geq m_a$, $p \geq m^{1+\beta}$, and $am \leq N \leq m$. If Z is a uniform L -subset of an arbitrary N -element set $Y \subseteq \mathbb{F}_p$, then*

$$\sup_z \Pr \left(\sum_{y \in Z} y = z \right) \leq K_a m^{-1-\eta}, \quad K_a = 1 + \frac{\sqrt{2}C}{a}. \quad (5.2)$$

Proof. Choose m_a so that, for every $m \geq m_a$,

$$m \geq \max\{8, 2/a\}, \quad 2C \log m \leq m^{1/3}, \quad 1000 \log m \leq am^{2/3}.$$

Such a threshold exists and is independent of β . Then $N \geq 2$, $L \geq m^{1/3}/2$, and

$$\begin{aligned} C \log N &\leq C \log m \leq L \\ &\leq m^{1/3} \leq 10^{-3} am / \log m \\ &\leq 10^{-3} N / \log N. \end{aligned}$$

The last inequality uses $N \geq am$ and $0 < \log N \leq \log m$. Theorem 5.1 therefore bounds the largest atom by

$$m^{-1-\beta} + \frac{\sqrt{2}C}{a} m^{-1-1/6} \leq K_a m^{-1-\eta}. \quad \square$$

6 Affine systems in a random permutation

For an $h \times m$ matrix H with columns $H_1, \dots, H_m$, set

$$S(H) = \text{span}\{H_j - H_{j'} : j, j' \in [m]\}, \quad d = \dim S(H). \quad (6.1)$$

An actual column value is a vector c that occurs as some H_j ; its multiplicity is $|\{j \in [m] : H_j = c\}|$. When x is a permutation of X , replacing every column H_j by $H_j + c$ translates Hx

by the fixed vector $c \sum_{u \in X} u$. The affine column dimension is therefore the relevant quantity. The rank-exposure argument is standard; see [11, proof of Proposition 2.2] and [9, Lemma 3.7]. Related exposures retaining a large reservoir occur in the chain estimate [13, Corollary 4.2]. Disjoint position pools recover independent scalar sums inside a permutation.

Lemma 6.1. *Fix an integer $h \geq 1$ and $0 < \gamma \leq 1$. Suppose H is an $h \times m$ matrix over $\mathbb{F}_p$ with an actual column value c_0 of multiplicity at least γm . Suppose actual column values $c_1, \dots, c_q$ each have multiplicity at least L and the differences $c_1 - c_0, \dots, c_q - c_0$ are independent. If $x : [m] \rightarrow X$ is a uniform bijection onto an arbitrary m -element set $X \subseteq \mathbb{F}_p$, then, for every fixed $z \in \mathbb{F}_p^h$,*

$$\Pr(Hx = z) \leq P_{h,\gamma} m^{-d-\eta q} \quad (6.2)$$

provided $p \geq m^{1+\beta}$ and m exceeds a threshold depending only on h, γ, C . The constant $P_{h,\gamma}$ has the same parameter dependence. The independence assumption implies $q \leq d \leq h$. The cases $q = 0$ and $d = 0$ are allowed.

Proof. If $d = 0$, every column is c_0 , necessarily $q = 0$, and $Hx = c_0 \sum_{u \in X} u$ is deterministic. Assume $d \geq 1$. Extend the specified differences to a basis

$$v_i = c_i - c_0, \quad 1 \leq i \leq d,$$

by choosing further actual column values. For $i \leq q$, select L positions of column value c_i ; for $q < i \leq d$, select one. Denote these disjoint position sets by E_i and their sizes by r_i . None is a baseline position.

Put

$$a = \frac{\gamma}{4h}, \quad t = \left\lfloor \frac{\gamma m}{2h} \right\rfloor.$$

For $m \geq 4h/\gamma$, one has $t \geq am$. Choose disjoint sets F_i of t baseline positions, also disjoint from every E_i . There are enough baseline positions because $dt \leq ht \leq \gamma m/2$. The disjoint pools $E_i \cup F_i$ have sizes $N_i = t + r_i \in [am, m]$.

Condition on the assignments outside these pools and on the unordered value set Y_i assigned to each pool. Every nonempty fibre has exactly $\prod_i N_i!$ assignments, one for each tuple of bijections from the pools to their value sets. The restrictions to the pools are therefore independent uniform bijections. Pool i contributes

$$c_0 \sum_{y \in Y_i} y + v_i Z_i, \quad Z_i = \sum_{j \in E_i} x_j$$

to Hx . The baseline terms and the contribution outside the pools are fixed. Since $v_1, \dots, v_d$ are independent, $Hx = z$ permits at most one tuple $(Z_1, \dots, Z_d)$.

For $i \leq q$, Lemma 5.2 bounds the largest atom of Z_i by $K_a m^{-1-\eta}$. For $i > q$, the singleton value is uniform on Y_i and has largest atom $N_i^{-1} \leq a^{-1} m^{-1}$. Multiplying the bounds on each fibre and averaging proves (6.2), with

$$P_{h,\gamma} = \max\{1, K_a, a^{-1}\}^h.$$

Increase the threshold to include m_a and $4h/\gamma$. This constant also covers $d = 0$. $\square$

The residual right-hand side may vary between fibres, since the bound is uniform in z . It is fixed on each fibre before the independent pool assignments are exposed.

7 Collision matrices and circular clusters

The standard incidence-rank formula gives the number of vertices minus the number of components; see [1, Theorem 2.3]. The following extension includes disjoint cluster indicators.

Lemma 7.1. *Let $g : [\ell] \rightarrow [\ell]$ have no fixed points, and let $B_0, B_1, \dots, B_q$ partition $[\ell]$, with B_0 possibly empty and $B_a \neq \emptyset$ for $a \geq 1$. Over a field of characteristic zero or characteristic $p > \ell$, put*

$$D_{ij} = \mathbf{1}_{j=i} - \mathbf{1}_{j=g(i)}, \quad w_a = \mathbf{1}_{B_a}.$$

If $C_1, \dots, C_\kappa$ are the directed cycles of g and T is the $\kappa \times q$ matrix with $T_{ua} = |C_u \cap B_a|$, $1 \leq a \leq q$, interpreted in the field, then

$$\text{rank}[D \mid w_1 \mid \dots \mid w_q] = \ell - \kappa + \text{rank } T \geq \frac{\ell + q}{2}. \quad (7.1)$$

Proof. The equations $D^\top y = 0$ read

$$y_j = \sum_{i: g(i)=j} y_i.$$

Each functional-graph component consists of a directed cycle with trees feeding into it. Deleting leaves forces y to vanish off the cycles; on each cycle it is constant. Thus $\ker D^\top$ has basis $\mathbf{1}_{C_1}, \dots, \mathbf{1}_{C_\kappa}$ and $\text{rank } D = \ell - \kappa$. The map $\pi(y)_u = \sum_{i \in C_u} y_i$ has kernel $\text{im } D$, by inclusion and dimension. The images $\pi(w_a)$ form T , proving the rank equality.

Write $t = \text{rank } T$ and select t rows spanning its row space. For every nonzero column a , choose a vertex of B_a on a selected cycle where that column is nonzero. A zero column has no cycle intersection: a positive intersection size is at most ℓ and cannot vanish in the stated characteristic. For such a column choose an off-cycle vertex of B_a . These q distinct representatives avoid all $\kappa - t$ unselected cycles. Each such cycle has at least two vertices. Hence $\ell \geq q + 2(\kappa - t)$, which proves the inequality. $\square$

Let M, L, m, ℓ be integers with

$$2 \leq \ell \leq M, \quad L \geq M, \quad m \geq 2(\ell + 1)L. \quad (7.2)$$

Fix $0 \leq b < m$, disjoint sets $U, Q \subseteq \{b + 1, \dots, \min(m, b + M)\}$ with $|Q| = \ell$, and a cyclic order $(q_1, \dots, q_\ell)$ of Q . For each i , let I_i be a nonempty proper cyclic prefix beginning at q_i , let $t_i \in \{0, \dots, m\}$ satisfy $|t_i - b| > 2M$, and choose

$$J_i \subseteq \{t_i + 1, \dots, \min(m, t_i + M)\}.$$

Define the $\ell \times m$ matrix

$$(H_j)_i = \mathbf{1}_{j \leq b} - \mathbf{1}_{j \leq t_i} + \mathbf{1}_{j \in U} + \mathbf{1}_{j \in I_i} - \mathbf{1}_{j \in J_i}. \quad (7.3)$$

Mark $b, t_1, \dots, t_\ell$ on $\mathbb{Z}/m\mathbb{Z}$. Join consecutive distinct marks when their clockwise gap is shorter than $2L$; the connected components are the clusters. Equal residues are in the same cluster. If there is only one distinct mark, its sole gap has length m . Let q count the clusters not containing b , and set $B_a = \{i : t_i \text{ lies in cluster } a\}$, with B_0 corresponding to the source cluster. The linear anchors 0 and m remain distinct in (7.3).

Lemma 7.2. *Under (7.2), in characteristic zero or characteristic $p > \ell$, the affine column dimension d of H satisfies $d \geq (\ell + q)/2$. There are actual column values $c_0, \dots, c_q$ such that c_0 occurs at least $m/[2(\ell + 1)]$ times, each other c_a occurs at least L times, and $c_1 - c_0, \dots, c_q - c_0$ are independent.*

Proof. Let $g(i) \neq i$ be the cyclic position immediately after I_i . Neither U nor J_i meets Q , and the prefix difference in (7.3) is constant on Q . Let D be the matrix of Lemma 7.1 for this map g , and write $D_{\cdot j}$ for its j -th column. Taking consecutive cyclic source-column differences gives

$$H_{q_j} - H_{q_{j-1}} = D_{\cdot j}, \quad q_0 = q_\ell. \quad (7.4)$$

Thus $\text{im } D \subseteq S(H)$.

At least one circular gap has length at least $2L$, by (7.2). Every cluster lies in an arc of length less than $2\ell L$, and there are $q + 1$ intercluster gaps. Write $H_j = A_j + E_j$, with $(A_j)_i = \mathbf{1}_{j \leq b} - \mathbf{1}_{j \leq t_i}$. For an intercluster gap of length G from a to the next mark $a + G$, the columns A_j are constant on the half-open circular arc $(a, a + G]$. Here a position of residue zero means column m . Retain the positions at distances $M + 1, \dots, G$ clockwise from a , including the next mark itself. The corrections E_j are supported at distances $1, \dots, M$ clockwise after marked anchors. Since no mark lies strictly inside the gap, these corrections vanish at every retained position. There are $G - M \geq 2L - M \geq L$ such positions, all with the same column value. The largest gap supplies an actual column value occurring at least

$$\frac{m}{\ell + 1} - M \geq \frac{m}{2(\ell + 1)}$$

times.

Extend A_j periodically. Its circular jump at residue a is

$$A_{a+1} - A_a = -\mathbf{1}_{a \equiv b} \mathbf{1}_{[\ell]} + \sum_{i: t_i \equiv a} e_i. \quad (7.5)$$

At residue zero the left side is $A_1 - A_m$. Indeed the circular derivative of $\mathbf{1}_{j \leq t}$ is $-\mathbf{1}_{a \equiv t} + \mathbf{1}_{a \equiv 0}$, including $t = 0, m$. Crossing free cluster a changes the constant gap value by w_a ; crossing the source cluster changes it by $-\sum_{a=1}^q w_a$. The w_a are independent because their supports are disjoint and nonempty. The $q + 1$ actual gap values therefore have affine dimension q and are affinely independent. Choose the largest-gap value as c_0 . Their differences span all w_a and supply the required repeated independent directions. Together with (7.4), Lemma 7.1 gives $d \geq (\ell + q)/2$. $\square$

Lemma 7.3. *For fixed b, ℓ, L, m satisfying $m \geq 2(\ell + 1)L$, the number of ordered anchor tuples $(t_1, \dots, t_\ell) \in \{0, \dots, m\}^\ell$ with q free clusters is at most*

$$A_\ell m^q L^{\ell-q}, \quad A_\ell = (\ell + 1)^{\ell+1} (8\ell + 2)^\ell. \quad (7.6)$$

Proof. Partition the labels $0, 1, \dots, \ell$ into their clusters, with label zero representing b . There are at most $(\ell + 1)^{\ell+1}$ partitions. The least label of each free cluster has at most $m + 1 \leq 2m$ anchor choices. Every other target lies at circular distance less than $2\ell L$ from its representative, which has at most $(8\ell + 2)L$ possible linear anchors, counting both representatives of residue zero. The resulting bound is (7.6), since $2^q (8\ell + 2)^{\ell-q} \leq (8\ell + 2)^\ell$. $\square$

8 The probability of a safe repair menu

We retain the potential target sets (4.1), the safety condition (4.2), and the predetermined menu from Section 4. The variable order is sampled uniformly; the decorations remain fixed.

Proposition 8.1. *Fix $\beta > 0$, an integer $k \geq 2$, and a decoration bound $B \geq 1$. Put $M = 4k$ and $\eta = \min\{\beta, 1/6\}$. There are constants $m_{\text{safe}}(k)$ and $C_{k,B}$ such that, whenever $m \geq m_{\text{safe}}(k)$, $p \geq m^{1+\beta}$, and x is a uniform ordering of an arbitrary m -element set $X \subseteq \mathbb{F}_p$,*

$$\Pr(\mathcal{R}_{\text{menu}}^c) \leq C_{k,B} m^{1-\eta k}. \quad (8.1)$$

The threshold $m_{\text{safe}}(k)$ depends only on k and the absolute constant C of Theorem 5.1, and not on β . The bound is uniform over X and all fixed decorations of size at most B . In particular the failure probability tends to zero if $\eta k > 1$.

Proof. First fix one source configuration, with cyclic order $(q_1, \dots, q_\ell)$, where $k \leq \ell \leq 2k$. If all its rotations fail, choose one collision for each rotation. For the rotation starting at q_i , this specifies a nonempty proper prefix I_i , a remote anchor t_i with $|t_i - b| > 2M$, a set

$$J_i \subseteq \{t_i + 1, \dots, \min(m, t_i + M)\},$$

and source and target decorations of equal parity. Writing z_i for target coordinate minus source coordinate, its equation is

$$s_b + \sum_{u \in U} x_u + \sum_{j \in I_i} x_j - s_{t_i} - \sum_{j \in J_i} x_j = z_i. \quad (8.2)$$

After these choices are fixed, the system is $Hx = z$ with (7.3). We sum over fixed witness tuples, rather than condition on the failure of other rotations.

Set

$$h = 2k, \quad \gamma = \frac{1}{2(2k+1)}, \quad P = P_{2k,\gamma}.$$

Choose m large enough for Lemma 6.1, for $L \geq M$, for $m \geq 2(2k+1)L$, and for $m > 2k$. These conditions depend only on k and the absolute scalar constant; they hold eventually. The prime-size condition gives $p > 2k$. If the anchors have q free clusters, Lemma 7.2 gives affine dimension at least $(\ell + q)/2$, a baseline of multiplicity at least γm , and q repeated independent directions. Pad H with zero rows to height $2k$. Neither its affine dimension nor its column multiplicities change. Lemma 6.1 therefore gives

$$\Pr(Hx = z) \leq P m^{-(\ell+q)/2-\eta q}. \quad (8.3)$$

For fixed b, ℓ, q , Lemma 7.3 bounds the anchor tuples by $A_\ell m^q L^{\ell-q}$. The remoteness restrictions only reduce this count. For each rotation, the prefix has at most $2k$ choices, each decoration has at most $B(M+1)$ choices, and J_i has at most 2^M choices. Thus, for fixed anchors, the remaining witness choices number at most $E_{k,B}^\ell$, where

$$E_{k,B} = 2k[B(M+1)]^2 2^M.$$

Counting pairs of incompatible parities only enlarges this bound. Combining the counts with (8.3) gives

$$\begin{aligned} \Pr(\text{the fixed source has no safe rotation}) &\leq P A_\ell E_{k,B}^\ell \sum_{q=0}^{\ell} m^q L^{\ell-q} m^{-(\ell+q)/2-\eta q} \\ &\leq P A_\ell E_{k,B}^\ell \sum_{q=0}^{\ell} m^{-(\ell-q)/6-\eta q} \\ &\leq D_{k,B} m^{-\eta \ell}, \end{aligned}$$

where

$$D_{k,B} = P \max_{k \leq \ell \leq 2k} (\ell + 1) A_\ell E_{k,B}^\ell.$$

The second inequality uses $L \leq m^{1/3}$; the last uses $\eta \leq 1/6$. The case $q = 0$ is included.

By (4.3), the predetermined menu has at most $(1 + 4k^2)m/k$ entries. A union bound proves (8.1) with

$$C_{k,B} = \frac{1 + 4k^2}{k} D_{k,B}.$$

All configurations are listed before sampling, so the later selection of rotations introduces no additional conditioning. $\square$

The scalar saving $1/6$ and the clustered-anchor saving $1/6$ coincide at the cube-root scale. More generally, $L = m^\rho$ gives gains $\rho/2$ and $1/2 - \rho$, whose minimum is maximised at $\rho = 1/3$. The estimate is uniform on every fibre fixing the nonvariable entries and variable coordinate set of the cell construction. The local-separation event is intersected with this event only after averaging the fibre bounds.

9 Completion of the proofs

Proof of Theorem 1.1. Fix $0 < \alpha < 1$ and set

$$\beta = \alpha^{-1} - 1, \quad \eta = \min\{\beta, 1/6\}, \quad k = \lfloor \eta^{-1} \rfloor + 1, \quad M = 4k, \quad K = 6M + 1. \quad (9.1)$$

Thus $\eta k > 1$. Choose m_* above the thresholds in Lemma 3.1 and Proposition 8.1 for these fixed parameters and $B = 4$. Increase it, if necessary, so that $m_* \geq k$ and

$$C_{k,4} m^{1-\eta k} \leq c_K/2 \quad (m \geq m_*),$$

where c_K is the lower bound in Lemma 3.1 and $C_{k,4}$ is the constant in Proposition 8.1. All choices depend only on α and the absolute constants in the cited theorems. Take an integer $C_\alpha \geq \max\{4m_*, 4\}$.

Suppose that $C_\alpha \leq n = |A| \leq p^\alpha$. In particular p is odd. The construction of Lemma 2.1 gives $m \geq n/4 \geq m_*$ and

$$p \geq n^{1/\alpha} \geq m^{1/\alpha} = m^{1+\beta}.$$

In the original probability space, Lemma 3.1 gives $\Pr(\mathcal{L}_K) \geq c_K$. Condition on the nonvariable entries and the variable set X . The decorations are fixed on each such fibre, and the

variables remain a uniform permutation of X . Proposition 8.1 therefore bounds the conditional probability of $\mathcal{R}_{\text{menu}}^c$ by $C_{k,4}m^{1-\eta^k}$ on every nonempty fibre. Averaging gives

$$\begin{aligned}\Pr(\mathcal{L}_K \cap \mathcal{R}_{\text{menu}}) &\geq \Pr(\mathcal{L}_K) - \Pr(\mathcal{R}_{\text{menu}}^c) \\ &\geq c_K/2 > 0.\end{aligned}$$

No independence of these events is required. For an outcome in their intersection, apply the variable permutation σ from Proposition 4.1 to the cell arrangement and read off the resulting word. This is an ordering of A , since only its variable coordinates have been permuted. Nonempty prefixes ending in the same cell are distinct by Lemma 2.1. If two equal prefixes end in distinct cells, Proposition 4.1 places them at distance at most $4M$, whereas Lemma 4.2 excludes such a collision because $|\sigma(j) - j| < M$ and $K = 6M + 1$. Thus the ordering is valid. $\square$

Proof of Corollary 1.2. The large-set theorem [3, Theorem 1.4] gives an absolute $c > 0$ such that, for every finite group G , every $S \subseteq G \setminus \{e\}$ with $|S| \geq |G|^{1-c}$ has a valid ordering. Put $c_0 = \min\{c, 1/2\}$ and $\alpha = 1 - c_0/2$. Then

$$\frac{p^\alpha}{(2p)^{1-c_0}} = 2^{c_0-1} p^{c_0/2} \longrightarrow \infty.$$

Thus the polynomial range of Theorem 1.1 eventually overlaps the large-set range for D_{2p} .

For the small-set range, the semidirect-product theorem [4, Theorem 1.3] applies to $\mathbb{Z}_p \rtimes H$ when the fixed finite abelian group H is strongly sequenceable and acts by signs. The group $H = \mathbb{Z}_2$ is strongly sequenceable, since its only nonempty identity-free subset is a singleton. Taking its action by inversion gives an absolute $c_s > 0$ such that every identity-free dihedral subset of size at most

$$\exp(c_s(\log p)^{1/4})$$

has a sequencing. Their condition also excludes intermediate identity prefixes and hence implies the validity required here. This endpoint eventually exceeds the fixed C_α . The small-set, polynomial and large-set intervals therefore cover every integer from 1 to $2p - 1$ for sufficiently large primes. The empty set is immediate. $\square$

A Proof of robust local separation

Proof of Lemma 3.1. Put

$$\begin{aligned}\Lambda &= 4K, \quad \nu_w = 2w(4w + 1), \quad \tau_K = \sum_{w=1}^K w! \nu_w, \quad v_K = \sum_{w=1}^K w w! \nu_w, \\ \omega_K &= 2\Lambda(\tau_K + v_K), \quad m_0(K) = \max\{2\Lambda, 8, 8\Lambda\omega_K\}.\end{aligned}$$

An index pattern consists of a w -cell window, a permutation of its variables and a nonempty contiguous subword in the resulting window. It has at most $4w$ entries and ν_w subwords. There are at most $m\tau_K$ patterns, and every original random slot belongs to at most v_K patterns. In rotation majority, at most $f v_K$ patterns meet a reflection slot. Pull the random entries of each subword back to their original slots; this pullback is injective and remains within the window.

Discard deterministically nonidentity patterns. In rotation majority, a subword without rotations lies in a run of at most two distinct reflections and is nonidentity. A retained pattern uses $a \geq 1$ rotations; if $a = 1$, it uses an even number $b \geq 2$ of reflections. In reflection majority, a subword without reflections contains at most one rotation, so a retained pattern uses an even number $h \geq 2$ of reflections. Identity in a retained pattern is one affine equation in the random coordinates, each with coefficient $+1$ or -1 . The coefficients depend only on the type pattern. A canonical bad event specifies an injective assignment to the used random slots satisfying that equation. Its index includes the pattern, so identical events may occur as different vertices. Their simultaneous avoidance is exactly $\mathcal{L}_K$.

Write $(N)_a = N(N-1) \cdots (N-a+1)$, with $(N)_0 = 1$. In rotation majority, an assignment using a, b slots has probability $[(m)_a(f)_b]^{-1}$. Solving the affine equation for one rotation bounds the total event weight of one pattern by

$$\frac{1}{m-a+1} \leq \frac{2}{m}. \quad (\text{A.1})$$

For a fixed rotation value ρ and $a \geq 2$, choose its slot and solve for another rotation. There are at most $a(m-1)_{a-2}(f)_b$ assignments, of weight at most

$$\frac{a}{m(m-a+1)} \leq \frac{2\Lambda}{m^2}.$$

If $a = 1$, solve instead for a reflection after fixing ρ and the other reflections; the weight is at most

$$\frac{1}{m(f-b+1)} \leq \frac{\Lambda}{mf},$$

since $f/(f-b+1) \leq b \leq \Lambda$ for every feasible $f \geq b$. For a fixed reflection value, choose its slot and solve for a rotation, obtaining weight at most

$$\frac{b}{f(m-a+1)} \leq \frac{2\Lambda}{fm}.$$

In reflection majority, solving for one reflection gives pattern weight at most

$$\frac{1}{f-h+1} \leq \frac{2}{f} \leq \frac{2}{m}.$$

If a fixed reflection value must occur, choose its slot and solve for another reflection, giving weight at most

$$\frac{h}{f(f-h+1)} \leq \frac{2\Lambda}{f^2} \leq \frac{2\Lambda}{m^2}.$$

These inequalities use $a, h \leq \Lambda$, $m \geq 2\Lambda$ and $f \geq m$ in reflection majority. Only feasible patterns contribute denominators.

Let $p_E = \Pr(E)$. Summing pattern weights gives $\sum_E p_E \leq 2\tau_K$. Every position label has event weight at most $2v_K/m$. In rotation majority, a rotation-value label has weight at most $2\Lambda\tau_K/m + \Lambda v_K/m$: use all $m\tau_K$ patterns when $a \geq 2$ and the at most fv_K reflection-using patterns when $a = 1$. A reflection-value label has weight at most $2\Lambda v_K/m$. In reflection majority its weight is at most $2\Lambda\tau_K/m$. Thus every position or value label λ satisfies

$$\sum_{E: \lambda \text{ used by } E} p_E \leq \omega_K/m. \quad (\text{A.2})$$

A value label includes its permutation-factor tag, even when rotation and reflection coordinates coincide. For $f = 0$, reflection cases are absent; for $f = 1$, retained rotation-majority patterns have no reflections, so the case $a = 1$ is absent. For every other bounded f , the number $f\nu_K$ of reflection-using patterns cancels the small-pool denominator.

Join events sharing a position or value label in one permutation factor. This overlap graph is a negative dependency graph, as in the permutation framework of [8, Section 1.1]. For completeness, force the prescribed matches of one event E successively by swapping each desired value into its prescribed position. Injectivity of the prescribed assignment preserves all previously forced matches. With t matches already forced in a factor of size N , each permutation satisfying the next match has exactly $N - t$ preimages satisfying the preceding matches. The resulting law is the product-permutation law conditioned on E . An occurring non-neighbour survives each swap: its prescribed positions include neither the forced position nor the current position of the desired value. Hence, for avoidance C of any collection of non-neighbours, $\Pr(C \mid E) \leq \Pr(C)$. Bayes' formula gives $\Pr(E \mid C) \leq \Pr(E)$ whenever $\Pr(C) > 0$. This argument also applies to two independent factors or an empty factor.

The quantitative lopsided local lemma [10, Lemma 3] gives an avoidance probability at least $\prod_E (1 - z_E)$ if

$$p_E \leq z_E \prod_{E' \sim E} (1 - z_{E'}), \quad 0 \leq z_E < 1.$$

Each event uses at most Λ matches and 2Λ labels, so (A.2) gives

$$\sum_{E' \sim E} p_{E'} \leq 2\Lambda\omega_K/m.$$

Take $z_E = 2p_E$. The pattern bound (A.1) and its reflection-majority analogue give $z_E \leq 4/m \leq 1/2$, while $m \geq 8\Lambda\omega_K$ gives $\sum_{E' \sim E} z_{E'} \leq 1/2$. Thus $\prod_{E' \sim E} (1 - z_{E'}) \geq 1 - \sum_{E' \sim E} z_{E'} \geq 1/2$, proving the local-lemma hypothesis. Finally $\log(1 - z) \geq -2z$ for $0 \leq z \leq 1/2$ yields

$$\begin{aligned} \Pr(\mathcal{L}_K) &\geq \prod_E (1 - 2p_E) \\ &\geq \exp\left(-4 \sum_E p_E\right) \\ &\geq e^{-8\tau_K} =: c_K > 0. \end{aligned} \quad \square$$

References

- [1] R. B. Bapat. *Graphs and Matrices*. Springer London, 2010. ISBN 9781848829817. doi: 10.1007/978-1-84882-981-7.
- [2] Benjamin Bedert and Noah Kravitz. Graham's rearrangement conjecture beyond the rectification barrier. *Israel Journal of Mathematics*, 273(1):471–500, 2026. doi: 10.1007/s11856-025-2871-6. Published online 30 November 2025.
- [3] Benjamin Bedert, Matija Bucić, Noah Kravitz, Richard Montgomery, and Alp Müyesser. On Graham's rearrangement conjecture over $\mathbb{F}_2^n$, 2025. URL <https://arxiv.org/abs/2508.18254v1>. Version 1, 25 August 2025.

- [4] Simone Costa, Stefano Della Fiore, and Eva R. Engel. Graham’s rearrangement for a class of semidirect products, 2025. URL <https://arxiv.org/abs/2503.18101v2>. Version 2, 19 August 2025.
- [5] Simone Costa, Stefano Della Fiore, Tao Feng, and Hengrui Liu. Kneserized anticoncentration and reverse absorption for Graham’s rearrangement conjecture, 2026. URL <https://arxiv.org/abs/2608.10015v2>. Version 2, 18 August 2026.
- [6] P. Erdős and R. L. Graham. *Old and new problems and results in combinatorial number theory*. Number 28 in Monographies de L’Enseignement Mathématique. L’Enseignement Mathématique, Université de Genève, Genève, 1980. URL https://mathweb.ucsd.edu/~ronspubs/80_11_number_theory.pdf.
- [7] R. L. Graham. On sums of integers taken from a fixed sequence. In *Proceedings of the Washington State University Conference on Number Theory*, pages 22–40, 1971. URL https://mathweb.ucsd.edu/~ronspubs/71_08_integer_sums.pdf.
- [8] David G. Harris and Aravind Srinivasan. A constructive Lovász local lemma for permutations. *Theory of Computing*, 13(17):1–41, 2017. doi: 10.4086/toc.2017.v013a017.
- [9] Matthew Kwan and Lisa Sauermann. Resolution of the quadratic Littlewood–Offord problem. *Compositio Mathematica*, 161(12):3089–3139, 2025. doi: 10.1112/s0010437x25102789. Lemma 3.7 is cited from arXiv:2312.13826v1.
- [10] Linyuan Lu and László Székely. Using Lovász local lemma in the space of random injections. *The Electronic Journal of Combinatorics*, 14(1):R63, 2007. doi: 10.37236/981. Research Paper R63.
- [11] A. M. Odlyzko. On subspaces spanned by random selections of ± 1 vectors. *Journal of Combinatorial Theory, Series A*, 47(1):124–133, 1988. doi: 10.1016/0097-3165(88)90046-5. URL <https://www-users.cse.umn.edu/~odlyzko/doc/arch/random.vectors.pdf>. Proof of Proposition 2.2 is cited from the author’s manuscript, pp. 5–6.
- [12] M. A. Ollis. Sequences in dihedral groups with distinct partial products. *Australasian Journal of Combinatorics*, 78(1):35–60, 2020. URL https://ajc.maths.uq.edu.au/pdf/78/ajc_v78_p035.pdf.
- [13] Huy Tuan Pham and Lisa Sauermann. On Graham’s rearrangement conjecture, 2026. URL <https://arxiv.org/abs/2602.15797v1>. Version 1, 17 February 2026.